Common Tasks for Configuring Smart Licensing Using Policy

This section is a grouping of tasks that apply to SLP. It includes tasks that are 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 Configuring 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, 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.

Procedure

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

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

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

Logging into Cisco (SSM On-Prem Interface)

Based on your requirement, when working in SSM On-Prem, either be in connected or disconnected mode. To work in the connected mode, perform these steps to connect to Cisco.

Procedure

Step 1 Go to software download page.

Step 2 Click the appropriate release.

Step 3 Click **Related Links and Documentation** > **User Guide**.

Step 4 In User Guide, view the **Logging into Cisco SSM On-Prem** section.

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 the Smart and Virtual Accounts for connecting to Cisco.

Procedure

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

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

a) In the **Preferences** window, navigate to the **Smart Account** field and add the **Smart AccountName**.

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

If you are connected to CSSM (in the Preferences tab, Cisco is Available), you can select from the list of available Smart Accounts (SA) and Virtual Accounts (VA).

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

Note
SA/VA names are case-sensitive.

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

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

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

View the instructions for this section in the Cisco Smart License Utility User Guide.

Procedure

Step 1 Go to https://software.cisco.com/download/home/286285506/type/286327971/release/.
Step 2 Click the appropriate release.
Step 3 Under the **Related Links and Documentation** section, click **User Guide**.

Export CSV (CSLU Interface)

Before you begin

View the instructions for this section in the Cisco Smart License Utility (CSLU) User Guide.

Procedure

Step 1 Go to https://software.cisco.com/download/home/286285506/type/286327971/release/.
Step 2 Click the appropriate release.
Step 3 Under the **Related Links and Documentation** section, click **User Guide**.

Import CSV (CSLU Interface)

Before you begin

View the instructions for this section in the Cisco Smart License Utility (CSLU) User Guide.

Procedure

Step 1 Go to https://software.cisco.com/download/home/286285506/type/286327971/release/.
Step 2 Click the appropriate release.
Step 3 Under the **Related Links and Documentation** section, click **User Guide**.

Export to CSSM

Before you begin

View the instructions for this section in the Cisco Smart License Utility (CSLU) User Guide.

Procedure

Step 1 Go to https://software.cisco.com/download/home/286285506/type/286327971/release/.
Step 2 Click the appropriate release.
Step 3 Under the **Related Links and Documentation** section, click **User Guide**.

Import from CSSM

Before you begin

View the instructions for this section in the Cisco Smart License Utility (CSLU) User Guide.

Procedure

Step 1 Go to https://software.cisco.com/download/home/286285506/type/286327971/release/.
Step 2 Click the appropriate release.

Step 3 Under the **Related Links and Documentation** section, click **User Guide**.

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 may be required or optional, depending on the kind of product instance and network requirements. Configure the applicable commands:

Before you begin

Supported topologies: Connected to CSSM Through CSLU (product instance-initiated communication).

Procedure

Ensure that CSLU is reachable from Product instance. For more information, see SLP Configuration - Connected to CSSM Through CSLU.

Setting Up a Connection to CSSM

Ensure that product instance is reachable to CSSM. For more information about DNS configuration, see Configuring the Call Home Service for Direct Cloud Access, on page 8.

Configuring an HTTP Proxy Server

You can configure Smart Call Home to send HTTP messages through an HTTP proxy server. If you do not configure an HTTP proxy server, Smart Call Home sends HTTP messages directly to the Cisco Transport Gateway (TG).

To configure an HTTP proxy server, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **callhome**	Enters Call Home configuration submode.
Step 3	switch(config-callhome)# **transport http proxy server** *ip address*	Configures the HTTP proxy server domain name server (DNS) name, IPv4 address, or IPv6 address. Optionally configures the port number. The port range is from 1 to 65535. The default port number is 8080.

	Command or Action	Purpose
Step 4	switch(config-callhome)# **transport http proxy enable**	Enables Smart Call Home to send all HTTP messages through the HTTP proxy server. **Note** You can execute this command only after the proxy server address has been configured.
Step 5	Optional: switch(config-callhome)# **show callhome transport**	Displays the transport-related configuration for Smart Call Home. **Note** The default value for full text destination and for XML is 1 MB.

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.
- This configuration is applicable only for smart transport. If you need to change the transport mode from smart with proxy to CSLU, before switching to CSLU mode, remove the proxy configuration manually using the **no license smart proxy** *proxy-ip* command.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**license smart transport smart** **Example:** `Device(config)# license smart transport smart`	Enables Smart transport mode.
Step 3	**license smart proxy address** *address_hostname* **Example:** `Device(config)# license smart proxy address 198.51.100.10`	Perform this step only when HTTPS proxy is used in the network. 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
		sends the message on to CSSM. Provide the address information: • **address** *address_hostname:* Specifies the proxy address. Enter the IP address or hostname of the proxy server.
Step 4	**license smart proxy port** *port_num* **Example:** `Device(config)# license smart proxy port 3128`	Perform this step only when HTTPS proxy is used in the network. Configures a proxy for the Smart transport mode. When a proxy is configured, licensing messages are sent to the proxy along with the final destination URL (CSSM). The proxy sends the message on to CSSM. Provide the port information: • **port** *port_num:* Specifies the proxy port. Enter the proxy port number.
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Configuring a DNS Client

Before you begin

Make sure that the name server is reachable before you configure a DNS client.

Procedure

Step 1 switch# **configure terminal**

Enters global configuration mode.

Step 2 switch(config)# **ip domain-lookup**

Enables DNS-based address translation.

Step 3 switch(config)# **vrf context** *vrf-name*

Creates a new VRF and enters VRF configuration mode. The *name* can be any case-sensitive, alphanumeric string up to 32 characters.

Step 4 switch(config-vrf)# **ip domain-name** *domain name*

Defines the default domain name that Cisco NX-OS uses to resolve unqualified hostnames. Cisco NX-OS uses each entry in the domain list to append that domain name to any hostname that does not contain a complete domain name before starting a domain-name lookup. Cisco NX-OS continues this process for each entry in the domain list until it finds a match.

Step 5 switch(config-vrf)# **ip name-server** *address1 [address2... address6]* [**source-interface** {**loopback** | **port-channel** | **ethernet** | **mgmt.** | **vlan**}] [**use-vrf** *vrf-name*]

Defines up to six name servers. The address can be either an IPv4 or IPv6 address.

- **source-interface** - Configures the source interface for all DNS packets. Available options for source-interface are loopback, port-channel, ethernet, management, or vlan interface. Only one source-interface can be mapped to one or more ip name-servers.

Note
Multiple DNS servers are for the case of unresponsive servers.

If the first DNS server in the list replies to the DNS query with a reject, the remaining DNS servers are not queried. If the first one doesn't respond, the next DNS server in list is queried.

- **use-vrf**- Configures the VRF on which the IP name server can be reached.

Configuring the Call Home Service for Direct Cloud Access

Make sure that Smart Call Home is enabled on the switch before configuring Smart Software Licensing.

Configuring a Source Interface to Send Messages Using HTTP

Beginning with Cisco NX-OS 10.3(2)F, you can optionally specify a source interface to send Smart Call Home messages over HTTP. If a source interface is not configured, the interface used to reach the Call Home server will be chosen.

Procedure

Step 1 **configure terminal**

Example:

```
switch# configure terminal
switch(config)#
```

Enters global configuration mode.

Step 2 **callhome**

Example:

```
switch(config)# callhome
switch(config-callhome)#
```

Enters Smart Call Home configuration mode.

Step 3 **source-interface** *interface*

Example:

```
switch(config-callhome)# source-interface Ethernet1/1
switch(config-callhome)#
```

Configures Smart Call Home to use this source interface when connecting to the Call Home server.

Step 4 **enable**

Example:

```
switch(config-callhome)# enable
switch(config-callhome)#
```

Enables Call Home.

Step 5 (Optional) **show callhome**

Example:

```
switch(config-callhome)# show callhome
switch(config-callhome)#
```

(Optional) Displays information about Smart Call Home.

Step 6 (Optional) **copy running-config startup-config**

Example:

```
switch(config)# copy running-config startup-config
switch(config-callhome)#
```

(Optional) Copies the running configuration to the startup configuration.

What to do next

Optionally use VRFs to send Smart Call Home messages over HTTP.

Configuring a VRF to Send Messages Using HTTP

Procedure

Step 1 switch# **configure terminal**

Enters global configuration mode.

Step 2 switch(config)# **callhome**

Enters Call Home configuration mode.

Step 3 switch(config-callhome)# **transport http use-vrf** *vrf-name*

Configures the VRF used to send email and other Smart Call Home messages over HTTP.

Viewing a Smart Call Home Profile

Procedure

switch# **show running-config callhome**

Displays the Smart Call Home profile.

Removing the Product Instance from CSSM

To remove a product instance and return all licenses to the license pool, complete the following task:

Before you begin

Supported topologies: all

Procedure

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

Log in using the username and password that is 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. Optionally, you can enter a name or product type string in the search tab to locate the product instance.

Step 6 In the **Actions** column of the product instance you want to remove, click the **Remove** link.

Step 7 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 the same token for all the product instances that are part of one Virtual Account.

Before you begin

Supported topology: Connected Directly to CSSM

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com/software/smart-licensing/alerts and click **Smart SoftwareLicensing**.

Log in using the username and password that is 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.

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.

Installing a Trust Code

To manually install a trust code, complete the following steps:

Before you begin

Supported topology: Connected Directly to CSSM

Procedure

	Command or Action	Purpose
Step 1	Generating a New Token for a Trust Code from CSSM, on page 11	In case you have not completed this already, generate and download a trust code file from CSSM.

	Command or Action	Purpose
Step 2	**license smart trust idtoken** *id_token_value* {**local**|**all**} [**force**] **Example:** `Device# license smart trust idtoken NGMwMjk5mYtNZaxMS00NzMZmtgWm all force`	Enables you to establish a trusted connection with CSSM. For *id_token_value*, enter the token you generated in CSSM. Enter one of following options: • **local**: Submits the trust request only for the active device in a High Availability setup. This is the default option. • **all**: Submits the trust request for active and standby supervisors in HA setup. Enter the **force** keyword to submit the trust code request despite an existing trust code on the product instance. Trust codes are node-locked to the UDI of the product instance. If a UDI is already registered, CSSM does not allow a new registration for the same UDI. Entering the **force** keyword sets a force flag in the message sent to CSSM to create a new trust code even if one already exists.

Step 3	**show license status**
	Example:
	`<output truncated>`
	`Trust Code installed: Jul 16 15:15:47 2021 UTC`
	`Active: PID: N9K-C9504, SN: FOX2308PCEN`
	`Jul 16 15:15:47 2021 UTC`
	`Standby: PID: N9K-C9504, SN: FOX2308PCEN`
	`Jul 16 15:15:47 2021 UTC`
		Displays date and time if trust code is installed. Date and time are in the local time zone. See field `Trust Code Installed:`.

Downloading a Policy File from CSSM

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

Before you begin

Supported topologies:

- No Connectivity to CSSM and No CSLU
- CSLU Disconnected from CSSM
- On-Prem CSLU disconnected from CSSM

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com/software/smart-licensing/alerts and click **Smart Software Licensing**.

Log in using the username and password that is 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 Switch, on page 13.

Uploading Usage Data to CSSM and Downloading an ACK

To upload a RUM report to CSSM and download an ACK when the product instance is not connected to CSSM or CSLU, complete the following task:

Before you begin

Supported topologies: No Connectivity to CSSM and No CSLU

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com/software/smart-licensing/alerts.

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

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

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

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

You cannot delete a usage report in CSSM, after it has been uploaded.

Step 5 From the Select Virtual Accounts pop-up, select the **Virtual Account** that receives 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, the time it was Reported, which Virtual Account it was uploaded to, the Reporting Status, the Number of Product Instances reported, and the Acknowledgment status.

Step 6 In the Acknowledgment column, click **Download** to save the `.txt` ACK file for the report you uploaded.

Wait for the ACK to appear in the Acknowledgment column. If there many RUM reports to process, CSSM may take a few minutes.

You can now install the file on the product instance, or you can transfer it to CSLU or On-Prem CSLU.

Installing a File on the Switch

To install a policy or ACK on the product instance when the product instance is not connected to CSSM, CSLU, or On-Prem CSLU, complete the following task:

Before you begin

Supported topologies: No Connectivity to CSSM and No CSLU

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

- For a policy, see Downloading a Policy File from CSSM, on page 12
- For an ACK, see Uploading Usage Data to CSSM and Downloading an ACK, on page 13

SUMMARY STEPS

1. **copy source bootflash**:`file-name`
2. **license smart import bootflash**: `file-name`
3. **show license all**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**copy source bootflash**:`file-name` **Example:** `Device# copy tftp://10.8.0.6/example.txt bootflash:`	Copies the file from its source location or directory to the flash memory of the product instance. **source**: This is the location of the source file or directory to be copied. The source can be either local or remote **bootflash:**: This is the destination for boot flash memory.
Step 2	**license smart import bootflash**: `file-name` **Example:** `Device# license smart import bootflash:example.txt`	Imports and installs the file on the product instance. After installation, a system message displays the type of file you installed.
Step 3	**show license all** **Example:** `Device# show license all`	Displays license authorization, policy, and reporting information for the product instance.

Setting the Smart License Parameters

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

Before you begin

Supported topologies: all

SUMMARY STEPS

1. **configure terminal**

2. **license smart transport**{ **callhome**|**cslu**|**off**|**smart**}
3. **license smart url**{**cslu** *cslu_url*|**smart** *smart_url*}
4. [**no**] **license smart vrf** <*vrf-name*>
5. **license smart usage interval** *interval_in_days*
6. **license smart source-interface** *source-interface*
7. **exit**
8. **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**license smart transport**{ **callhome**|**cslu**|**off**|**smart**} **Example:** `Device(config)# license smart transport cslu`	Selects the type of message transport the product instance uses. Choose from the following options: • **callhome**: Enables Call Home as the transport mode. • **cslu**: Enables CSLU as the transport mode. This is the default transport mode. • **off**: Disables all communication from the product instance. • **smart**: Enables Smart transport.
Step 3	**license smart url**{**cslu** *cslu_url*|**smart** *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 (except callhome, which is in the callhome configuration). Depending on the transport mode you have chosen to configure in the previous step, configure the corresponding URL here: • **cslu** *cslu_url*: The default value for cslu_url is set to cslu_local. If you want to set a custom url, then follow below steps: If you have configured the transport mode as **cslu**, configure this option. Enter the CSLU URL as follows: **https://<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 cslu_local.

	Command or Action	Purpose
		• **smart** *smart_url*: If you have configured the transport type as **smart**, then url is automatically configured to: https://smartreceiver.cisco.com/licservice/license. The **no license smart url smart** *smart_url* command reverts to the default URL as above.
Step 4	[**no**] **license smart vrf** <*vrf-name*> **Example:** `switch (conf)# license smart vrf vrf1`	Configures non-default VRF for smart and CSLU modes of transports. The **no** form of this command reverts to management VRF. **Note** To verify this configuration, use the **show run license** command.
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 365. 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 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 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	**license smart source-interface** *source-interface* **Example:** `switch (config)# license smart source-interface Ethernet1/22`	Configures source interface only for smart and CSLU modes of transport, and not for callhome. The **no** form of this command removes the configured source interface. **Note** • If source-interface doesn't have IP address, then forwarding decision is based on configured VRF. • If source-interface IP is present but the interface is down, then forwarding fails. • If the VRF of source interface does not match with the configured VRF as part of **license smart vrf**, then forwarding fails.
Step 7	**exit** **Example:**	Exits global configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config)# exit`	
Step 8	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.