



How to Configure Smart Licensing Using Policy: Workflows by Topology

This section provides sequential configuration information to implement [supported topologies](#), in the simplest and fastest way.

- [Workflow for Topology: Connected to CSSM Through CSLU, on page 1](#)
- [Workflow for Topology: Connected Directly to CSSM, on page 4](#)
- [Workflow for Topology: Connected to CSSM Through a Controller, on page 6](#)
- [Workflow for Topology: CSLU Disconnected from CSSM, on page 9](#)
- [Workflow for Topology: No Connectivity to CSSM and No CSLU, on page 13](#)
- [Workflow for Topology: SSM On-Prem Deployment, on page 14](#)

Workflow for Topology: Connected to CSSM Through CSLU

Depending on whether you want to implement a product instance-initiated or CSLU-initiated method of communication, complete the corresponding sequence of tasks:

- [Tasks for Product Instance-Initiated Communication](#)
- [Tasks for CSLU-Initiated Communication](#)

Tasks for Product Instance-Initiated Communication

Smart Account Set-Up → **CSLU Installation** → **CSLU Preference Settings** → **Product Instance Configuration**

1. *Smart Account Set-Up*

Where task is performed: CSSM Web UI, <https://software.cisco.com/>

Ensure that you have a user role with proper access rights to a Smart Account and the required Virtual Accounts.

If you have an MSLA and are going to use the utility mode, also ensure that the licenses you use are deposited with subscription IDs in the corresponding Virtual Account in CSSM.

2. *CSLU Installation*

Where task is performed: A laptop, desktop, or a Virtual Machine (VM) running Windows 10 or Linux.

Download the file from [Smart Software Manager](#) > **Smart Licensing Utility**.

Refer to [Cisco Smart License Utility Quick Start Setup Guide](#) and [Cisco Smart Licensing Utility User Guide](#) for help with installation and set-up.

3. *CSLU Preference Settings*

Where tasks are performed: CSLU Interface

- a. [Logging into Cisco \(CSLU Interface\)](#)
- b. [Configuring a Smart Account and a Virtual Account \(CSLU Interface\)](#)
- c. [Adding a Product-Initiated Product Instance in CSLU \(CSLU Interface\)](#)

4. *Product Instance Configuration*

Where tasks are performed: Product Instance

- a. [Ensuring Network Reachability for Product Instance-Initiated Communication](#)
- b. Ensure that transport type is set to **cslu**.

CSLU is the default transport type. If you have configured a different option, enter the **license smart transport cslu** command in global configuration mode. Remember to save any changes to the configuration file

```
Device(config)# license smart transport cslu
Device(config)# exit
Device# copy running-config startup-config
```

- c. Specify how you want CSLU to be discovered (*choose one*):

- Option 1:

No action required; Zero-touch DNS discovery of `cslu-local`.

If you have configured the name server with an entry where hostname `cslu-local` is mapped to the CSLU IP address (the windows host where you installed CSLU), no configuration is required. The product instance automatically discovers hostname `cslu-local`.

- Option 2:

Configure DNS discovery of your domain.

Enter the **ip domain-name** *domain_name* command in global configuration mode. In the example below, the name-server creates entry `cslu-local.example.com`.

```
Device(config)# ip domain-name example.com
```

- Option 3:

Configure a specific URL for CSLU.

Enter the **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* command in global configuration mode. 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.

```
Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi
```

- d. Enable the utility mode only if you have an MSLA: [Enabling the Utility Mode](#)

Result:

Since the product instance initiates communication, it automatically sends out the first RUM report at the scheduled time, as per the policy. Along with this first report, if applicable, it sends a request for a UDI-tied trust code. CSLU forwards the RUM report to CSSM and retrieves the ACK, which also contains the trust code. The ACK is applied to the product instance the next time the product instance contacts CSLU.

In Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train, and from Cisco IOS XE Cupertino 17.9.1a and all later releases, in the product instance-initiated mode, the product instance does not send more than one RUM report a day. You can override this for an on-demand synchronization between the product instance and CSLU, by entering the **license smart sync** command in privileged EXEC mode.

If the utility mode is enabled on the product instance, the RUM report that the product instance sends to CSLU is flagged accordingly. The ACK from CSSM includes the subscription ID - as in Smart Account and Virtual account of the product instance. Subsequent RUM reports that are sent include the subscription ID for each license in use. In the utility mode, an ACK is required every 30 days.

To know when the product instance will be sending the next RUM report, enter the **show license all** command in privileged EXEC mode and in the output, check the date in the `Next report push` field.

Tasks for CSLU-Initiated Communication

Smart Account Set-Up → CSLU Installation → CSLU Preference Settings → Product Instance Configuration → Usage Synchronization

1. Smart Account Set-Up

Where task is performed: CSSM Web UI, <https://software.cisco.com/>

Ensure that you have a user role with proper access rights to a Smart Account and the required Virtual Accounts.

If you have an MSLA and are going to use the utility mode, also ensure that the licenses you use are deposited with subscription IDs in the corresponding Virtual Account in CSSM.

2. CSLU Installation

Where task is performed: A laptop, desktop, or a Virtual Machine (VM) running Windows 10 or Linux.

Download the file from [Smart Software Manager > Smart Licensing Utility](#).

Refer to [Cisco Smart License Utility Quick Start Setup Guide](#) and [Cisco Smart Licensing Utility User Guide](#) for help with installation and set-up.

3. CSLU Preference Settings

Where tasks are performed: CSLU interface

- a. [Logging into Cisco \(CSLU Interface\)](#)
- b. [Configuring a Smart Account and a Virtual Account \(CSLU Interface\)](#)
- c. [Adding a CSLU-Initiated Product Instance in CSLU \(CSLU Interface\)](#)

4. Product Instance Configuration

Where tasks is performed: Product Instance

- a. [Ensuring Network Reachability for CSLU-Initiated Communication](#)

- b. Enable the utility mode only if you have an MSLA: [Enabling the Utility Mode](#)

5. Usage Synchronization

Where task is performed: CSLU Interface

[Collecting Usage Reports: CSLU Initiated \(CSLU Interface\)](#)

Result:

Since CSLU is logged into CSSM, the reports are automatically sent to the associated Smart Account and Virtual Account in CSSM and CSSM will send an ACK to CSLU as well as to the product instance. It gets the ACK from CSSM and sends this back to the product instance for installation. The ACK from CSSM contains the trust code and SLAC if this was requested.

Trust code request and installation is supported starting with Cisco IOS XE Cupertino 17.9.1a.

If the utility mode is enabled on the product instance, the RUM report CSLU retrieves from the product instance is flagged accordingly. The ACK from CSSM includes the subscription ID - as in Smart Account and Virtual account of the product instance. Subsequent RUM reports that are sent, will include the subscription ID for each license in use. In the utility mode, an ACK is required every 30 days.

Workflow for Topology: Connected Directly to CSSM

Smart Account Set-Up → Product Instance Configuration → Trust Establishment with CSSM → Authorization Code Installation (Only if Applicable)

1. Smart Account Set-Up

Where task is performed: CSSM Web UI, <https://software.cisco.com/>

Ensure that you have a user role with proper access rights to a Smart Account and the required Virtual Accounts.

If you have an MSLA and are going to use the utility mode, also ensure that the licenses you use are deposited with subscription IDs in the corresponding Virtual Account in CSSM.

2. Product Instance Configuration

Where tasks are performed: Product Instance

- a. Set-Up product instance connection to CSSM: [Setting Up a Connection to CSSM](#)

- b. Configure a connection method and transport type (choose one)

- Option 1:

Smart transport: Set transport type to **smart** and configure the corresponding URL.

If the transport mode is set to **license smart transport smart**, and you configure **license smart url default**, the Smart URL (<https://smartreceiver.cisco.com/licservice/license>) is automatically configured. Remember to save any changes to the configuration file:

```
Device(config)# license smart transport smart
Device(config)# license smart url default
Device(config)# exit
Device# copy running-config startup-config
```

This option is supported in the utility mode.

- Option 2:
Smart transport through an HTTPs proxy: See the [Configuring Smart Transport Through an HTTPs Proxy](#) section.
This option is supported in the utility mode.
 - Option 3:
Configure Call Home service for direct cloud access. See the [Configuring the Call Home Service for Direct Cloud Access](#) section.
This option is *not* supported in the utility mode.
 - Option 4:
Configure Call Home service for direct cloud access through an HTTPs proxy. See the [Configuring the Call Home Service for Direct Cloud Access through an HTTPs Proxy Server](#) section.
This option is *not* supported in the utility mode.
- c. Enable the utility mode only if you have an MSLA: [Enabling the Utility Mode](#)

3. *Establishment of Trust with CSSM*

Where task is performed: CSSM Web UI and then Product Instance

- a. 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: [Generating a New Token for a Trust Code from CSSM](#).
- b. Configure the token on the product instance to establish trust with CSSM: [Establishing Trust with an ID Token](#).

4. *Authorization Code Installation (Only if Applicable)*

If you want to use a license that requires authorization before use (enforcement type: enforced or export-controlled), or configure a throughput greater than 250 Mbps (on supported product instances), you have to complete this step before this topology deployment is complete: [Manually Requesting and Auto-Installing a SLAC](#)

Result:

After establishing trust, CSSM returns a policy. The policy is automatically installed on all product instances of that Virtual Account. The policy specifies if and how often the product instance reports usage.

In Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train, and from Cisco IOS XE Cupertino 17.9.1a and all later releases, the product instance does not send more than one RUM report a day. You can override this for an on-demand synchronization between the product instance and CSSM, by entering the **license smart sync** command in privileged EXEC mode.

If the utility mode is enabled on the product instance, the RUM report that the product instance sends to CSSM is flagged accordingly. The ACK from CSSM includes the subscription ID - as in Smart Account and Virtual Account of the product instance. Subsequent RUM reports that are sent include the subscription ID for each license in use. In the utility mode, an ACK is required every 30 days.

To change the reporting interval configure the **license smart usage interval** command. For more information, see [license smart \(global config\)](#).

Workflow for Topology: Connected to CSSM Through a Controller

Depending on the controller you want to implement, complete the corresponding workflow.

Using Cisco DNA Center as a Controller

To deploy Cisco DNA Center as the controller, complete the following workflow:

Product Instance Configuration → Cisco DNA Center Configuration

1. Product Instance Configuration

Where task is performed: Product Instance

Enable NETCONF. Cisco DNA Center uses the NETCONF protocol to provision configuration and retrieve the required information from the product instance - the product instance must therefore have NETCONF enabled, to facilitate this.

For more information, see the [Programmability Configuration Guide, Cisco IOS XE Amsterdam 17.3.x](#). In the guide, go to *Model-Driven Programmability > NETCONF Protocol*.

2. Cisco DNA Center Configuration

Where tasks is performed: Cisco DNA Center GUI

An outline of the tasks you must complete and the accompanying documentation reference is provided below. The document provides detailed steps you have to complete in the Cisco DNA Center GUI:

a. Set-up the Smart Account and Virtual Account.

Enter the same log in credentials that you use to log in to the CSSM Web UI. This enables Cisco DNA Center to establish a connection with CSSM.

See the [Cisco DNA Center Administrator Guide](#) of the required release (Release 2.2.2 onwards) > *Manage Licenses > Set Up License Manager*.

b. Add the required product instances to Cisco DNA Center inventory and assign them to a site.

This enables Cisco DNA Center to push any necessary configuration, including the required certificates, for Smart Licensing Using Policy to work as expected.

See the [Cisco DNA Center User Guide](#) of the required release (Release 2.2.2 onwards) > *Display Your Network Topology > Assign Devices to a Site*.

c. Trigger the required workflows to install authorization codes if applicable.

See the [Cisco DNA Center Administrator Guide](#) of the required release (Release 2.2.2 onwards) > *Manage Licenses > Install the Authorization Code and Enable the High Security License*.

On the Cisco DNA Center GUI, you can generate the SLAC only for HSECK9 licenses, and only for these product instances:

Table 1: Product Instances that Support SLAC Generation for HSECK9 license on the Cisco DNA Center GUI

Product Instance	Minimum Required Cisco DNA Center Release	Minimum Required Cisco IOS XE Version
Cisco 1000 Series Integrated Services Routers	Cisco DNA Center Release 2.2.2	Cisco IOS XE Amsterdam 17.3.2
Cisco 4000 Series Integrated Services Routers		Cisco IOS XE Amsterdam 17.3.2
Catalyst 8300 Series Edge Platforms		Cisco IOS XE Amsterdam 17.3.2
Catalyst 8500 Series Edge Platforms		Cisco IOS XE Amsterdam 17.3.2
Catalyst 8200 Series Edge Platforms		Cisco IOS XE Bengaluru 17.4.1

Result:

After you implement the topology, you must trigger the very first ad hoc report in Cisco DNA Center, to establish a mapping between the Smart Account and Virtual Account, and product instance. See the [Cisco DNA Center Administrator Guide](#) of the required release (Release 2.2.2 onwards) > *Manage Licenses* > *Upload Resource Utilization Details to CSSM*. Once this is done, Cisco DNA Center handles subsequent reporting based on the reporting policy.

If multiple policies are available, Cisco DNA Center maintains the narrowest reporting interval. You can change this, but only to report more frequently (a narrower interval). See the [Cisco DNA Center Administrator Guide](#) of the required release (Release 2.2.2 onwards) > *Manage Licenses* > *Modify License Policy*.

If you want to change the license level after this, see the [Cisco DNA Center Administrator Guide](#) of the required release (Release 2.2.2 onwards) > *Manage Licenses* > *Change License Level*.

Using Cisco vManage as a Controller

To deploy Cisco vManage as the controller, complete the following workflow:

Smart Account Set-Up → Product Instance Configuration → Cisco vManage Configuration → Authorization Code Installation (Only if Applicable)

1. Smart Account Set-Up

Where tasks are performed: CSSM Web UI, <https://software.cisco.com/>

Ensure that you have a user role with proper access rights to a Smart Account and the required Virtual Accounts.



Note If you are migrating from an earlier release to the Connected to CSSM Through Controller topology (where Cisco vManage is deployed as the Controller), first check that all the licenses that you ordered are displayed in your Smart Account and Virtual Account in CSSM. If licenses are missing, contact [Cisco TAC](#) for help with the correction, and only then proceed with topology implementation.

2. *Product Instance Configuration*

Where tasks are performed: Product Instance

To use Cisco vManage to manage a product instance you must complete the standard bring-up process.

See the Cisco SD-WAN Getting Start Guide > [Cisco SD-WAN Overlay Network Bring-Up Process](#).

3. *Cisco vManage Configuration*

Where tasks are performed: Cisco vManage portal

See the Cisco SD-WAN Getting Start Guide > [License Management for Smart Licensing Using Policy](#) .

Cisco vManage Configuration applies only to Cisco IOS XE Bengaluru 17.5.1a and later releases.

From Cisco IOS XE Amsterdam 17.3.2 to Cisco IOS XE Bengaluru 17.4.x, Cisco vManage does not support license management. You can configure the product instance to operate in "controller mode", but usage reporting is not supported.

4. *Authorization Code Installation (Only if Applicable)*

Where tasks are performed: Product Instance and CSSM Web UI

To use an export-controlled license or throughput greater than 250 Mbps, complete SLAC installation (*choose one*):

- Option 1:

Generate a SLAC in CSSM, download it to a file, and then install it.

- a. [Generating and Downloading SLAC from CSSM to a File](#)

- b. [Installing a File on the Product Instance](#)

- Option 2:

Establish connectivity to CSSM, establish trust, and then request and install SLAC. (The example here uses Smart transport for connectivity to CSSM, you can use any of the other options to connect directly to CSSM.)



Note Even though you are configuring a connection to CSSM and establishing trust, a product instance in the SD-WAN "controller mode" does not send RUM reports.

- a. Set the transport type to **smart** and configure the corresponding URL. If the transport mode is set to **license smart transport smart**, and you configure **license smart url default**, the Smart URL (<https://smartreceiver.cisco.com/licservice/license>) is automatically configured. Remember to save any changes to the configuration file.


```
Device(config)# license smart transport smart
Device(config)# license smart url default
Device(config)# exit
Device# copy running-config startup-config
```

- b. 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: [Generating a New Token for a Trust Code from CSSM](#)

Having downloaded the token, you can now install the trust code on the product instance: [Establishing Trust with an ID Token](#).

```
Device# license smart trust idtoken NGMwMjk5mYtNZaxMS00NzMZmtgWm all force
```

- c. Request and install SLAC: [Manually Requesting and Auto-Installing a SLAC](#)

```
Device# license smart authorization request add hseck9 local
Device(config)# exit
Device# copy running-config startup-config
```

Result:

Cisco vManage records usage and automatically sends RUM reports to CSSM at the fixed reporting interval of 24 hours. You can assign licences to edge devices, view information about the licenses that are being used and the licenses that are available for assignment.

Workflow for Topology: CSLU Disconnected from CSSM

Depending on whether you want to implement a product instance-initiated or CSLU-initiated method of communication. Complete the corresponding table of tasks below.

- [Tasks for Product Instance-Initiated Communication](#)
- [Tasks for CSLU-Initiated Communication](#)

Tasks for Product Instance-Initiated Communication

Smart Account Set-Up → **CSLU Installation** → **CSLU Preference Settings** → **Product Instance Configuration** → **Usage Synchronization**

1. *Smart Account Set-Up*

Where task is performed: CSSM Web UI, <https://software.cisco.com/>

Ensure that you have a user role with proper access rights to a Smart Account and the required Virtual Accounts.

If you have an MSLA and are going to use the utility mode, also ensure that the licenses you use are deposited with subscription IDs in the corresponding Virtual Account in CSSM.

2. *CSLU Installation*

Where task is performed: A laptop, desktop, or a Virtual Machine (VM) running Windows 10 or Linux.

Download the file from [Smart Software Manager](#) > **Smart Licensing Utility**.

Refer to [Cisco Smart License Utility Quick Start Setup Guide](#) and [Cisco Smart Licensing Utility User Guide](#) for help with installation and set-up.

3. *CSLU Preference Settings*

Where tasks are performed: CSLU

- a. In the CSLU Preferences tab, click the **Cisco Connectivity** toggle switch to **off**. The field switches to “Cisco Is Not Available”.
- b. [Configuring a Smart Account and a Virtual Account \(CSLU Interface\)](#)
- c. [Adding a Product-Initiated Product Instance in CSLU \(CSLU Interface\)](#)

4. *Product Instance Configuration*

Where tasks are performed: Product Instance

- a. [Ensuring Network Reachability for Product Instance-Initiated Communication](#)
- b. Ensure that transport type is set to **cslu**.

CSLU is the default transport type. If you have configured a different option, enter the **license smart transport cslu** command in global configuration mode. Remember to save any changes to the configuration file.

```
Device(config)# license smart transport cslu
Device(config)# exit
Device# copy running-config startup-config
```

- c. Specify how you want CSLU to be discovered (*choose one*)

- Option 1:

No action required. Name server configured for Zero-touch DNS discovery of `cslu-local`

Here, if you have configured DNS (The name server IP address is configured on the product instance), and the DNS server has an entry where hostname `cslu-local` is mapped to the CSLU IP address, then no further action is required. The product instance automatically discovers hostname `cslu-local`.

- Option 2:

No action required. Name server and domain configured for Zero-touch DNS discovery of `cslu-local.<domain>`

Here if you have configured DNS, (The name server IP address and domain is configured on the product instance), and the DNS server has an entry where `cslu-local.<domain>` is mapped to the CSLU IP address, then no further action is required. The product instance automatically discovers hostname `cslu-local`.

- Option 3:

Configure a specific URL for CSLU.

Enter the **license smart url cslu** `http://<cslu_ip_or_host>:8182/cslu/v1/pi` command in global configuration mode. 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.

```
Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi
```

- d. Enable the utility mode only if you have an MSLA: [Enabling the Utility Mode](#)

5. Usage Synchronization

Where tasks are performed: CSLU and CSSM

Since the product instance initiates communication, it automatically sends out the first RUM report at the scheduled time, as per the policy. You can also enter the **license smart sync** privileged EXEC command to trigger this. Along with this first report, if applicable, it sends a request for a UDI-tied trust code.

If the utility mode is enabled on the product instance, the RUM report that the product instance sends to CSLU is flagged accordingly.

Since CSLU is disconnected from CSSM, perform the following tasks to send the RUM Reports to CSSM.

- a. [Export to CSSM \(CSLU Interface\)](#)
- b. [Uploading Data or Requests to CSSM and Downloading a File](#)
- c. [Import from CSSM \(CSLU Interface\)](#)

Result:

The ACK you have imported from CSSM contains the trust code if this was requested. The ACK is applied to the product instance the next time the product instance contacts CSLU.

In Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train, and from Cisco IOS XE Cupertino 17.9.1a and all later releases, in the product instance-initiated mode, the product instance does not send more than one RUM report a day. You can override this for an on-demand synchronization between the product instance and CSLU, by entering the **license smart sync** command in privileged EXEC mode.

If RUM report was flagged with the utility mode the ACK from CSSM includes the subscription ID - as in Smart Account and Virtual account of the product instance. Subsequent RUM reports that are sent include the subscription ID for each license in use. In the utility mode, an ACK is required every 30 days.

To know when the product instance will be sending the next RUM report, enter the **show license all** command in privileged EXEC mode and in the output, check the date for the `Next report push` field.

Tasks for CSLU-Initiated Communication

Smart Account Set-Up → **CSLU Installation** → **CSLU Preference Settings** → **Product Instance Configuration** → **Usage Synchronization**

1. Smart Account Set-Up

Where task is performed: CSSM Web UI, <https://software.cisco.com/>

Ensure that you have a user role with proper access rights to a Smart Account and the required Virtual Accounts.

If you have an MSLA and are going to use the utility mode, also ensure that the licenses you use are deposited with subscription IDs in the corresponding Virtual Account in CSSM.

2. CSLU Installation

Where task is performed: A laptop, desktop, or a Virtual Machine (VM) running Windows 10 or Linux.

Download the file from [Smart Software Manager](#) > **Smart Licensing Utility**.

Refer to [Cisco Smart License Utility Quick Start Setup Guide](#) and [Cisco Smart Licensing Utility User Guide](#) for help with installation and set-up.

3. *CSLU Preference Settings*

Where tasks is performed: Product Instance

- a. In the CSLU Preferences tab, click the **Cisco Connectivity** toggle switch to **off**. The field switches to “Cisco Is Not Available”.
- b. [Configuring a Smart Account and a Virtual Account \(CSLU Interface\)](#)
- c. [Adding a CSLU-Initiated Product Instance in CSLU \(CSLU Interface\)](#)

4. *Product Instance Configuration*

Where tasks is performed: Product Instance

- a. [Ensuring Network Reachability for CSLU-Initiated Communication](#)
- b. Enable the utility mode only if you have an MSLA: [Enabling the Utility Mode](#).

5. *Usage Synchronization*

Where tasks are performed: CSLU and CSSM

Collect usage data from the product instance. Since CSLU is disconnected from CSSM, you then save usage data which CSLU has collected from the product instance to a file. Along with this first report, if applicable, an authorization code and a UDI-tied trust code request is included in the RUM report. Then, from a workstation that is connected to Cisco, upload it to CSSM. After this, download the ACK from CSSM. In the workstation where CSLU is installed and connected to the product instance, upload the file to CSLU.

If the utility mode is enabled on the product instance, the RUM report that CSLU retrieves is flagged accordingly.

- a. [Collecting Usage Reports: CSLU Initiated \(CSLU Interface\)](#)
- b. [Export to CSSM \(CSLU Interface\)](#)
- c. [Uploading Data or Requests to CSSM and Downloading a File](#)
- d. [Import from CSSM \(CSLU Interface\)](#)

Result:

The ACK you have imported from CSSM contains the trust code and SLAC if this was requested. The uploaded ACK is applied to the product instance the next time CSLU runs an update.

Trust code request and installation is supported starting with Cisco IOS XE Cupertino 17.9.1a.

If RUM report was flagged with the utility mode the ACK from CSSM includes the subscription ID - as in Smart Account and Virtual account of the product instance. Subsequent RUM reports that are sent, will include the subscription ID for each license in use. In the utility mode, an ACK is required every 30 days.

Workflow for Topology: No Connectivity to CSSM and No CSLU

The list of tasks required to set-up this topology is a small one. See, the *Results* section at the end of the workflow to know how you can complete requisite usage reporting after you have implemented this topology.

Smart Account Set-Up Product Instance Configuration → Authorization Code Installation (Only if Applicable)

1. Smart Account Set-Up

Where task is performed: CSSM Web UI, <https://software.cisco.com/>

Ensure that you have a user role with proper access rights to a Smart Account and the required Virtual Accounts.

If you have an MSLA and are going to use the utility mode, also ensure that the licenses you use are deposited with subscription IDs in the corresponding Virtual Account in CSSM.

2. Product Instance Configuration

Where task is performed: Product Instance

a. Set transport type to **off**.

Enter the **license smart transport off** command in global configuration mode. Remember to save any changes to the configuration file.

```
Device(config)# license smart transport off
Device(config)# exit
Device# copy running-config startup-config
```

b. Enable utility mode if you have an MSLA

To enable the utility mode, enter the **license smart utility** command in global configuration mode. Save changes to the configuration file:

```
Device (config)# license smart utility
Device(config)# exit
Device# copy running-config startup-config
```

3. Authorization Code Installation (Only if Applicable)

Where tasks is performed: CSSM Web UI and Product Instance

If you want to use an export-controlled license or throughput greater than 250 Mbps, install SLAC (*choose one*):

• Option 1:

Generate and download a SLAC in the CSSM Web UI and install it on the product instance. Here you have to enter the product instance information in the CSSM Web UI to generate SLAC:

a. [Generating and Downloading SLAC from CSSM to a File](#)

b. [Installing a File on the Product Instance](#)

• Option 2:

Generate and save the SLAC request to a file, upload it to the CSSM Web UI, download the SLAC code from the CSSM Web UI, and install it on the product instance:



Note This option is supported starting with Cisco IOS XE Cupertino 17.7.1a only.

- a. [Generating and Saving a SLAC Request on the Product Instance](#)
- b. [Uploading Data or Requests to CSSM and Downloading a File](#)
- c. [Installing a File on the Product Instance](#)

Result:

Since you will have disabled all communication to and from the product instance, to report license usage you must 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):

1. Generate and save RUM reports

Enter the **license smart save usage** command in privileged EXEC mode. In the example below, all RUM reports are saved to the flash memory of the product instance, in file `all_rum.txt`.

Starting with Cisco IOS XE Cupertino 17.7.1a, configuring this command automatically includes a trust code request in the RUM report - if a trust code does not already exist on the product instance.

If the utility mode is enabled on the product instance, the RUM report is flagged accordingly.

In the example below, the file is first save to bootflash and then copied to a TFTP location:

```
Device# license smart save usage all file bootflash:all_rum.txt
Device# copy bootflash:all_rum.txt tftp://10.8.0.6/all_rum.txt
```

See the [license smart \(privileged EXEC\)](#) command for command syntax details.

2. Upload usage data to CSSM: [Uploading Data or Requests to CSSM and Downloading a File](#)
3. Install the ACK on the product instance: [Installing a File on the Product Instance](#)

If the RUM report included a flag for the utility mode, the ACK from CSSM includes the subscription ID - as in Smart Account and Virtual account of the product instance. Subsequent RUM reports that are saved will include the subscription ID for each license in use. In the utility mode, an ACK is required every 30 days.

Workflow for Topology: SSM On-Prem Deployment

Depending on whether you want to implement a product instance-initiated (push) or SSM On-Prem-initiated (pull) method of communication, complete the corresponding sequence of tasks:

Tasks for Product Instance-Initiated Communication

Smart Account Set-Up → **SSM On-Prem Installation and Configuration** → **Addition and Validation of Product Instances (Only if Applicable)** → **Product Instance Configuration** → **Initial Usage Synchronization**

1. *Smart Account Set-Up*

Where task is performed: CSSM Web UI, <https://software.cisco.com/>

Ensure that you have a user role with proper access rights to a Smart Account and the required Virtual Accounts.

If you have an MSLA and are going to use the utility mode, also ensure that the licenses you use are deposited with subscription IDs in the corresponding Virtual Account in CSSM.

2. SSM On-Prem Installation and Configuration

Where task is performed: A physical server such as a Cisco UCS C220 M3 Rack Server, or a hardware-based server that meets the necessary requirements.

Download the file from [Smart Software Manager](#) > **Smart Software Manager On-Prem**.

Refer to the [Cisco Smart Software On-Prem Installation Guide](#) and the [Cisco Smart Software On-Prem User Guide](#) for help with installation.

Installation is complete when you have deployed SSM On-Prem, configured a common name on SSM On-Prem (**Security Widget** > **Certificates**), synchronized the NTP server (**Settings** widget > **Time Settings**), and created, registered, and synchronized (**Synchronization** widget) the SSM On-Prem local account with your Smart Account and Virtual Account in CSSM.



Note Licensing functions in the **On-Prem Licensing Workspace** are greyed-out until you complete the creation, registration, and synchronization of the local account with your Smart Account in CSSM. The *local account* synchronization with CSSM is for the SSM On-Prem instance to be known to CSSM, and is different from usage synchronization which is performed in **4. Initial Usage Synchronization** below.

3. Addition and Validation of Product Instances

Where tasks are performed: SSM On-Prem UI

This step ensures that the product instances are validated and mapped to the applicable Smart Account and Virtual account in CSSM. This step is required only in the following cases:

- If you want your product instances to be added and validated in SSM On-Prem before they are reported in CSSM (for added security).
 - If you want to use a license that requires authorization before use (enforcement type: enforced or export-controlled), or to configure throughput greater than 250 Mbps. Such a product instance must be added to SSM On-Prem before you can request the necessary SLAC in Step 3 d below.
 - If you have created local virtual accounts (in addition to the default local virtual account) in SSM On-Prem. In this case you must provide SSM On-Prem with the Smart Account and Virtual Account information for the product instances in these local virtual accounts, so that SSM On-Prem can report usage to the correct license pool in CSSM.
 - If you have an MSLA and are going to use the utility mode, completing this step ensures correct subscription selection.
- a. [Assigning a Smart Account and Virtual Account \(SSM On-Prem UI\)](#)
 - b. [Validating Devices \(SSM On-Prem UI\)](#)



Note If your product instance is in a NAT set-up, also enable support for a NAT Setup when you enable device validation – both toggle switches are in the same window.

4. Product Instance Configuration

Where tasks are performed: Product Instance and the SSM On-Prem UI

Remember to save any configuration changes on the product instance, by entering the **copy running-config startup-config** command in privileged EXEC mode.

- a. [Ensuring Network Reachability for Product Instance-Initiated Communication](#)
- b. [Retrieving the Transport URL \(SSM On-Prem UI\)](#)
- c. [Setting the Transport Type, URL, and Reporting Interval](#)

The transport type configuration for CSLU and SSM On-Prem are the same (**license smart transport cslu** command in global configuration mode), but the URLs are different.

- d. Complete this sub-step only if you want to use a license that requires authorization before use (enforcement type: enforced or export-controlled), or to configure a throughput greater than 250 Mbps, on supported product instances (choose one option):
 - Option 1:
SSM On-Prem is connected to CSSM: [Submitting an Authorization Code Request \(SSM On-Prem UI, Connected Mode\)](#)
 - Option 2:
SSM On-Prem is not connected to CSSM: [Submitting an Authorization Code Request \(SSM On-Prem UI, Disconnected Mode\)](#)
- e. Enable the utility mode only if you have an MSLA: [Enabling the Utility Mode](#)

5. Initial Usage Synchronization

Where tasks are performed: Product instance, SSM On-Prem, CSSM

- a. Synchronize the product instance with SSM On-Prem.

On the product instance, enter the **license smart sync {all | local}** command, in privileged EXEC mode. This synchronizes the product instance with SSM On-Prem, to send and receive any pending data. For example:

```
Device# license smart sync local
```

If the utility mode is enabled on the product instance, the RUM report that the product instance sends to SSM On-Prem is flagged accordingly.

You can verify this in the SSM On-Prem UI. Log in and select the **Smart Licensing** workspace. Navigate to the **Inventory > SL Using Policy** tab. In the **Alerts** column of the corresponding product instance, the following message is displayed: Usage report from product instance.



Note If you have not performed Step 2 above (Addition and Validation of Product Instances), completing this sub-step will add the product instance to the SSM On-Prem database.

b. Synchronize usage information with CSSM (*choose one*)

- Option 1:

SSM On-Prem is connected to CSSM: In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports > Usage Schedules > Synchronize now with Cisco**.

- Option 2:

SSM On-Prem is not connected to CSSM: See [Exporting and Importing Usage Data \(SSM On-Prem UI\)](#).

Result:

You have completed initial usage synchronization. Product instance and license usage information is now displayed in SSM On-Prem.

If the RUM report to CSSM was flagged with the utility mode, the ACK from CSSM includes the subscription ID - as in Smart Account and Virtual account of the product instance. Subsequent RUM reports that are sent include the subscription ID for each license in use. In the utility mode, an ACK is required every 30 days.

For subsequent reporting, you have the following options:

- To synchronize data between the product instance and SSM On-Prem:

Schedule periodic synchronization between the product instance and the SSM On-Prem, by configuring the reporting interval. Enter the **license smart usage interval** *interval_in_days* command in global configuration mode.

In Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train, and from Cisco IOS XE Cupertino 17.9.1a and all later releases, in the product instance-initiated mode, the product instance does not send more than one RUM report a day. You can override this for an on-demand synchronization between the product instance and SSM On-Prem, by entering the **license smart sync** command in privileged EXEC mode.

To know when the product instance will be sending the next RUM report, enter the **show license all** command in privileged EXEC mode and in the output, check the `Next report push:` field.

- To synchronize usage information with CSSM, schedule periodic synchronization, or, upload and download the required files:
 - Schedule periodic synchronization with CSSM. In the SSM On-Prem UI, navigate to **Reports > Usage Schedules > Synchronization schedule with Cisco**. Enter the following frequency information and save:
 - **Days:** Refers to how *often* synchronization occurs. For example, if you enter 2, synchronization occurs once every two days.
 - **Time of Day:** Refers to the time at which synchronization occurs, in the 24-hour notation system. For example, if you enter 14 hours and 0 minutes, synchronization occurs at 2 p.m. (1400) in your local time zone.

- Upload and download the required files for reporting: [Exporting and Importing Usage Data \(SSM On-Prem UI\)](#).

Tasks for SSM On-Prem Instance-Initiated Communication

SSM On-Prem Installation and Configuration → Product Instance Addition → Product Instance Configuration → Initial Usage Synchronization

1. SSM On-Prem Installation and Configuration

Where task is performed: A physical server such as a Cisco UCS C220 M3 Rack Server, or a hardware-based server that meets the necessary requirements.

Download the file from [Smart Software Manager](#) > **Smart Software Manager On-Prem**.

Refer to the [Cisco Smart Software On-Prem Installation Guide](#) and the [Cisco Smart Software On-Prem User Guide](#) for help with installation.

Installation is complete when you have deployed SSM On-Prem, configured a common name on SSM On-Prem (**Security Widget** > **Certificates**), synchronized the NTP server (**Settings** widget > **Time Settings**), and created, registered, and synchronized (**Synchronization** widget) the SSM On-Prem local account with your Smart Account and Virtual Account in CSSM.



Note Licensing functions in the **On-Prem Licensing Workspace** are greyed-out until you complete the creation, registration, and synchronization of the local account with your Smart Account in CSSM. The *local account* synchronization with CSSM is for the SSM On-Prem instance to be known to CSSM, and is different from usage synchronization which is performed in **4. Initial Usage Synchronization** below.

2. Product Instance Addition

Where task is performed: SSM On-Prem UI

Depending on whether you want to add a single product instance or multiple product instances, follow the corresponding sub-steps: [Adding One or More Product Instances \(SSM On-Prem UI\)](#).

3. Product Instance Configuration

Where tasks are performed: Product Instance and the SSM On-Prem UI

Remember to save any configuration changes on the product instance, by entering the **copy running-config startup-config** command in privileged EXEC mode.

- [Ensuring Network Reachability for SSM On-Prem-Initiated Communication](#)
- Enable the utility mode only if you have an MSLA: [Enabling the Utility Mode](#)
- Complete this sub-step only if you want to use a license that requires authorization before use (enforcement type: enforced or export-controlled), or to configure throughput greater than 250 Mbps (on supported product instances): [Submitting an Authorization Code Request \(SSM On-Prem UI, Disconnected Mode\)](#).

The uploaded codes are now applied to the product instances the next time SSM On-Prem runs an update. An initial usage synchronization with the product instance is being performed in Step 4 below so this will be completed then.

4. Initial Usage Synchronization

Where tasks are performed: SSM On-Prem, and CSSM

- a. Retrieve usage information from the product instance.

In the SSM On-Prem UI, navigate to **Reports > Synchronisation pull schedule with the devices > Synchronise now with the device**.

If the utility mode is enabled on the product instance, the RUM report that SSM On-Prem retrieves, is flagged accordingly.

In the **Alerts** column, the following message is displayed: Usage report from product instance.



Tip It takes 60 seconds before synchronization is triggered. To view progress, navigate to the **On-Prem Admin Workspace**, and click the **Support Centre** widget. The system logs here display progress.

- b. Synchronize usage information with CSSM (*choose one*)

- Option 1:

SSM On-Prem is connected to CSSM: In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports > Usage Schedules > Synchronize now with Cisco**.

- Option 2:

SSM On-Prem is not connected to CSSM. See: [Exporting and Importing Usage Data \(SSM On-Prem UI\)](#).

Result:

You have completed initial usage synchronization. Product instance and license usage information is now displayed in SSM On-Prem. SSM On-Prem automatically sends the ACK back to the product instance. To verify that the product instance has received the ACK, enter the **show license status** command in privileged EXEC mode, and in the output, check the date for the `Last ACK received` field.

If the RUM report to CSSM was flagged with the utility mode, the ACK from CSSM includes the subscription ID - as in Smart Account and Virtual account of the product instance. Subsequent RUM reports that are sent include the subscription ID for each license in use. In the utility mode, an ACK is required every 30 days.

For subsequent reporting, you have the following options:

- To retrieve usage information from the product instance, you can:
 - In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports > Usage Schedules > Synchronize now with Cisco**.
 - Schedule periodic retrieval of information from the product instance by configuring a frequency. In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports > Usage Schedules > Synchronisation pull schedule with the devices**. Enter values in the following fields:
 - **Days:** Refers to how *often* synchronization occurs. For example, if you enter 2, synchronization occurs once every two days.
 - **Time of Day:** Refers to the time at which synchronization occurs, in the 24-hour notation system. For example, if you enter 14 hours and 0 minutes, synchronization occurs at 2 p.m. (1400).

- Collect usage data from the product instance without being connected to CSSM. In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Inventory > SL Using Policy** tab. Select one or more product instances by enabling the corresponding check box. Click **Actions for Selected... > Collect Usage**. On-Prem connects to the selected Product Instance(s) and collects the usage reports. These usage reports are then stored in On-Prem's local library. These reports can then be transferred to Cisco if On-Prem is connected to Cisco, or (if you are not connected to Cisco) you can manually trigger usage collection by selecting **Export/Import All.. > Export Usage to Cisco**.
- To synchronize usage information with CSSM, you can:
 - Schedule periodic synchronization with CSSM. In the SSM On-Prem UI, navigate to **Reports > Usage Schedules > Synchronization schedule with Cisco**. Enter the following frequency information and save:
 - **Days:** Refers to how *often* synchronization occurs. For example, if you enter 2, synchronization occurs once every two days.
 - **Time of Day:** Refers to the time at which synchronization occurs, in the 24-hour notation system. For example, if you enter 14 hours and 0 minutes, synchronization occurs at 2 p.m. (1400).
 - Upload and download the required files for reporting: [Exporting and Importing Usage Data \(SSM On-Prem UI\)](#).