

Implementing Smart Licensing Using Policy

This chapter provides the simplest and fastest way to implement Smart Licensing Using Policy for new deployments. If you are migrating from an existing licensing model, see Migrating to Smart Licensing Using Policy.

- 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 5
- Workflow for Topology: CSLU Disconnected from CSSM, on page 6
- Workflow for Topology: No Connectivity to CSSM and No CSLU, on page 9
- Workflow for Topology: SSM On-Prem Deployment, on page 10

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

CSLU Installation → CSLU Preference Settings → Product Instance Configuration

1. ***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.

2. ***CSLU Preference Settings***

   Where tasks are performed: CSLU

   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)

3. ***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. 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
Device(config)#exit
Device#copy running-config startup-config
```

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 the 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 all subsequent releases from Cisco IOS XE Cupertino 17.9.1 onwards:

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.

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.

To verify trust code installation, enter the **show license status** command in privileged EXEC mode. Check for the updated timestamp in the `Trust Code Installed` field.

In case of a change in license usage, see Configuring an AIR License to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1.

Tasks for CSLU-Initiated Communication

CSLU Installation → CSLU Preference Settings→ Product Instance Configuration → Usage Synchronization

1. ***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.

2. ***CSLU Preference Settings***

   Where tasks is performed: CSLU

   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)

3. ***Product Instance Configuration***

   Where tasks is performed: Product Instance

   Ensuring Network Reachability for CSLU-Initiated Communication

4. ***Usage Synchronization***

   Where tasks is performed: Product Instance

   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.

In case of a change in license usage, see Configuring an AIR License to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1.

Workflow for Topology: Connected Directly to CSSM

Smart Account Set-Up → Product Instance Configuration → Trust Establishment with CSSM

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.

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. 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
     ```

   - Option 2:

     Configure Smart transport through an HTTPs proxy. See Configuring Smart Transport Through an HTTPs Proxy

   - Option 3:

     Configure Call Home service for direct cloud access. See Configuring the Call Home Service for Direct Cloud Access.

   - Option 4:

     Configure Call Home service for direct cloud access through an HTTPs proxy. See Configuring the Call Home Service for Direct Cloud Access through an HTTPs Proxy Server.

3. ***Trust Establishment with CSSM***

   Where task is performed: CSSM Web UI and then the product instance

   a. 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

   b. Having downloaded the token, you can now install the trust code on the product instance: Installing a Trust Code

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 the 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 all subsequent releases from Cisco IOS XE Cupertino 17.9.1 onwards: 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.

To change the reporting interval, configure the **license smart usage interval** command in global configuration mode. For syntax details see the *license smart (privileged EXEC)* command in the Command Reference for the corresponding release.

In case of a change in license usage, see Configuring an AIR License to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1.

Workflow for Topology: Connected to CSSM Through a Controller

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

Product Instance Configuration → Cisco Catalyst Center **Configuration**

1. ***Product Instance Configuration***

   Where task is performed: Product Instance

   Enable NETCONF. Cisco Catalyst 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 Catalyst Center Configuration***

   Where tasks is performed: Cisco Catalyst 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 Catalyst 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 Catalyst Center to establish a connection with CSSM.

      See the *Cisco Catalyst 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 Catalyst Center inventory and assign them to a site.

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

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

Result:

After you implement the topology, *you* must trigger the very first ad hoc report in Cisco Catalyst Center, to establish a mapping between the Smart Account and Virtual Account, and product instance. See the *Cisco Catalyst 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 Catalyst Center handles subsequent reporting based on the reporting policy.

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

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller.

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

CSLU Installation → CSLU Preference Settings → Product Instance Configuration→ Usage Synchronization

1. ***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.

2. ***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)

3. ***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. 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
        Device(config)#exit
        Device#copy running-config startup-config
        ```

4. ***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. 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 the 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 all subsequent releases from Cisco IOS XE Cupertino 17.9.1 onwards: 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.

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.

To verify trust code installation, enter the `show license status` command in privileged EXEC mode. Check for the updated timestamp in the `Trust Code Installed` field.

In case of a change in license usage, see Configuring an AIR License to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1.

Tasks for CSLU-Initiated Communication

CSLU Installation → CSLU Preference Settings → Product Instance Configuration → Usage Synchronization

1. ***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.

2. ***CSLU Preference Settings***

   Where tasks is 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 CSLU-Initiated Product Instance in CSLU (CSLU Interface)

   d. Collecting Usage Reports: CSLU Initiated (CSLU Interface)

3. ***Product Instance Configuration***

   Where task is performed: Product Instance

   Ensuring Network Reachability for CSLU-Initiated Communication

4. ***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.

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 and SLAC if this was requested. The uploaded ACK is applied to the product instance the next time CSLU runs an update.

In case of a change in license usage, see Configuring an AIR License to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1.

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

Workflow for Topology: No Connectivity to CSSM and No CSLU

Since you do not have to configure connectivity to any other component, the list of tasks required to set-up the 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.

Product Instance Configuration

Where task is performed: Product Instance

Set transport type to **off**.

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

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

Result:

All communication to and from the product instance is disabled. To report license usage you must save RUM reports to a file on the product instance. From a workstation that has connectivity to the Internet and Cisco, upload the file to CSSM:

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 17.7.1, if a trust code does not already exist on the product instance, configuring this command automatically includes a trust code request in the RUM report. This is supported in a standalone, as well as a High Availability set-up.

In the example below, the file is first saved 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
```

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 you want to change license usage, see Configuring an AIR License.

If you want to return an SLR authorization code, see Removing and Returning an Authorization Code.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1.

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

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

1. ***SSM On-Prem Installation***

   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. ***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 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.

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.

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.

   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.

4. ***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
   ```

   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.

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 the 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: 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.

  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)).

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller.

Tasks for SSM On-Prem Instance-Initiated Communication

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

1. ***SSM On-Prem Installation***

   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.

4. ***Initial Usage Synchronization***

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

   a. Retrieve usage information from the product instance.

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

      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.

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** > **Synchronization 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 coresponding 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)).

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller.