How Smart Licensing Using Policy Works

This section lists the components that are involved in an implementation of Smart Licensing Using Policy, followed by the sequential stages of managing licenses for Cisco Enterptise Routing Platforms.

Components Involved

All possible components involved in an implementation of Smart Licensing Using Policy are listed here, along with a brief description of the component's role in the implementation.

Out of all these components, two are necessarily part of any implementation:

- Product Instance: This component consumes the license.
- Cisco SSM: This component is the central portal for information about Cisco software licenses.

Product Instance

A product instance is a single instance of a Cisco product, identified by a Unique Device Identifier (UDI).

A product instance records and reports license usage (RUM reports) and provides alerts and system messages about overdue reports, communication failures, etc. RUM reports and usage data are securely stored in the product instance.

Throughout this document, the term *product instance* refers to all supported physical and virtual product instances, unless noted otherwise. For information about the product instances that are within the scope of this document, see Supported Products.

Cisco Smart Software Manager (Cisco SSM)

Cisco SSM is a portal that enables you to manage all your Cisco software licenses from a centralized location. CSSM helps you manage current requirements and review usage trends to plan for future license requirements.

Access the Cisco SSM Web UI from https://software.cisco.com. To manage your licenses, under **Smart Software Manager**, click **Manage Licenses**.

The Connecting to SSM section in this document explains the different ways in which you can connect to CSSM.

Cisco Smart License Utility (CSLU)

CSLU is a Windows-based reporting utility that provides aggregate licensing workflows. This utility performs these key functions:

- Provides options relating to how workflows are triggered. The workflows can be triggered by CSLU or by the product instance.
- Collects usage reports from the product instance and uploads these usage reports to the corresponding Smart Account or Virtual Account – online, or offline, using files. Similarly, the RUM report ACK is collected online, or offline, and sent back to the product instance.
- Sends authorization code requests to Cisco SSM and receives authorization codes[1] from CSSM.

CSLU can be integrated into the Smart Licensing Using Policy implementation in several ways. As a Windows application that is a standalone tool connected to or disconnected from Cisco SSM. Alternatively, it can be deployed on a machine (laptop or desktop) running Linux. It can also be embedded by Cisco in a controller such as Cisco Catalyst Center.

CSLU supports Windows 10 and Linux operating systems. We recommend that you always use the latest version of CSLU that is available. For the release notes and to download the latest version, click **Smart Licensing Utility** on the Software Download page.

CSLU can be part of your implementation in the following ways:

Note CSLU is not supported in Cisco SD-WAN (Cisco vManage) and CSLU cannot be used to report license usage for routing product instances that are managed by Cisco vManage.

Controller

A management application or service that manages multiple product instances.

Information about supported controllers, product instances that support the controller, and minimum required software versions on the controller and on the product instance is provided in the tables below:

- Support Information for Controller: Cisco DNA Center

[1] You can use CSLU to forward authorization code requests for Cisco routers that operate in controller mode (for Cisco SD-WAN features).

- Support Information for Controller: Cisco vManage

Table 1: Support Information for Controller: Cisco DNA Center

Minimum Required Cisco DNA Center Version for Smart Licensing Using Policy [2]	Minimum Required Cisco IOS XE Version [3]	Supported Product Instances
Cisco DNA Center Release 2.2.2	Cisco IOS XE Amsterdam 17.3.2	Cisco Aggregation, Integrated, and Cloud Service Routers: • Cisco ASR 1000 Series Aggregation Services Routers • Cisco 1000 Series Integrated Services Routers • Cisco 4000 Series Integrated Services Routers Cisco Catalyst 8000 Edge Platforms Family: • Catalyst 8300 Series Edge Platforms • Catalyst 8500 Series Edge Platforms
	Cisco IOS XE Bengaluru 17.4.1	Cisco Catalyst 8000 Edge Platforms Family: • Catalyst 8200 Series Edge Platforms Cisco Terminal Services Gateways: • Cisco 1100 Terminal Services Gateway

[2] The minimum required version for this controller. This means support continues on all subsequent releases - unless noted otherwise.

[3] The minimum required Cisco IOS-XE version on the product instance. This means support continues on all subsequent releases - unless noted otherwise

For more information about Cisco DNA Center, see the support page at:
https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/series.html

Table 2: Support Information for Controller: Cisco vManage

Minimum Required Cisco vManage Version for Smart Licensing Using Policy [4]	Minimum Required Cisco IOS XE Version [5]	Supported Product Instances
Cisco vManage Release 20.5.1	Cisco IOS XE Bengaluru 17.5.1a	For the up-to-date list of supported product instances, see Cisco SD-WAN Getting Started Guide→ *License Management for Smart Licensing Using Policy* → *Supported Devices*.

[4] The minimum required version for this controller. This means support continues on all subsequent releases - unless noted otherwise.

[5] The minimum required Cisco IOS-XE version on the product instance. This means support continues on all subsequent releases - unless noted otherwise

For more information about Cisco vManage, see the support page at: https://www.cisco.com/c/en/us/support/routers/sd-wan/series.html.

For information about how to implement a topology with a supported controller, see Connected to CSSM Through a Controller, on page 10.

Cisco Smart Software Manager On-Prem (SSM On-Prem)

SSM On-Prem is a license server that enables license administration from a server inside an organization's premises, instead of having to connect directly to Cisco SSM.

SSM On-Prem is locally connected and acts as a local license authority. It involves setting up an SSM on-prem license server, which synchronizes its license database with Cisco SSM periodically and functions similarly to Cisco SSM.

This table provides information about the minimum required version of SSM On-Prem and the minimum required software version on the supported product instances.

Minimum Required SSM On-Prem Version for Smart Licensing Using Policy[6]	Minimum Required Cisco IOS XE Version [7]	Supported Product Instances
Version 8, Release 202102	Cisco IOS XE Amsterdam 17.3.3	All Supported Products

[6] The minimum required SSM On-Prem version. This means support continues on all subsequent releases - unless noted otherwise

[7] The minimum required software version on the product instance. This means support continues on all subsequent releases - unless noted otherwise.

The minimum required SSM On-Prem version. This means support continues on all subsequent releases, unless noted otherwise.

The minimum required software version on the product instance. This means support continues on all subsequent releases, unless noted otherwise.

Minimum Required SSM On-Prem Version for Smart Licensing Using Policy *with MSLA*	Minimum Required Cisco IOS XE Version for Smart Licensing Using Policy *with MSLA*	Supported Product Instances
Version 8 Release 202206	Cisco IOS XE Cupertino 17.9.1	Catalyst 8000V Edge Software. For more information, see Managed Service License Agreement (MSLA), on page 5.

For more information about SSM On-Prem, see Smart Software Manager On-Prem on the Software Download page. Hover over the .iso image to display the documentation links.

Managed Service License Agreement (MSLA)

A Managed Service License Agreement (MSLA) is a buying program agreement, designed for Service Providers. This agreement enables you to report license usage to Cisco and then be billed for that usage – instead of prepaying for licenses. For more information about the terms of the agreement, see: https://www.cisco.com/c/en/us/about/legal/msla-direct-product-terms.html.

Device licenses that are under the MSLA program, are referred to as post-paid licenses. Your Smart Account and Virtual Account in Cisco Smart Software Manager (Cisco SSM) are the single source of truth to track all your post-paid licenses. All post-paid license entries have a "Subscription Id" associated with them.

You can install a post-paid license on the device in the same way as you do any Cisco router boot-level license (See Configuring a Boot Level License). To report this post-paid license usage to CSSM, you must enable the "Utility mode" on the device. To communicate with CSSM, follow one of the supported options, see: Utility Mode, on page 18.

This MSLA buying program is available in the Smart Licensing Using Policy model, in the following releases:

Minimum Required Cisco IOS XE Version for Smart Licensing Using Policy with MSLA	Supported Product Instances
Cisco IOS XE Cupertino 17.9.1a	Only on Catalyst 8000V Edge Software running *in the autonomous mode*.
Cisco IOS XE Bengaluru 17.4.1	Only on Catalyst 8000V Edge Software running *in SD-WAN controller mode*. For more information about using MSLA in the controller mode, see Licensing on Cisco Catalyst SD-WAN, Manage Licenses for Smart Licensing Using Policy.

Migrating to Smart Licensing Using Policy with MSLA

The MSLA buying program for Cisco CSR1000V and Cisco ISRv are offered under the Smart Licensing model. This is different from MSLA buying program for Cisco Catalyst 8000V Edge Software, which is offered under Smart Licensing Using Policy model. Service Providers running Cisco CSR1000V and Cisco ISRv instances cannot perform inline upgrades to a Cisco Catalyst 8000V instance. It is NOT supported.

For migration from Cisco CSR1000V or Cisco ISRv to Cisco Catalyst 8000V Edge Software, you must create new Cisco Catalyst 8000V virtual machine instance and manually copy over the older configuration files. For more information, see the *Upgrading the Cisco IOS XE Software* chapter of the Cisco Catalyst 8000V Edge Software Installation And Configuration Guide.

Supported Topologies

This section describes the various ways in which you can implement Smart Licensing Using Policy. For each topology, refer to the accompanying overview to know the how the set-up is designed to work, and refer to the considerations and recommendations, if any.

After Topology Selection

After you have selected a topology, refer to the corresponding workflow under *How to Configure Smart Licensing Using Policy: Workflows by Topology*, to know how to implement it. These workflows provide the simplest and fastest way to implement a topology. These workflows are meant for new deployments and not for upgrading or migrating from an existing licensing solution.

After initial implementation, if there are any additional configuration tasks you have to perform, for instance, if you want to manually request authorization codes in-bulk, or you want to perform a maintenance task such as synchronizing RUM reports, see the *Task Library for Smart Licensing Using Policy*.

Note Always check the "Supported topologies" where provided, before you proceed.

Connected to CSSM Through CSLU

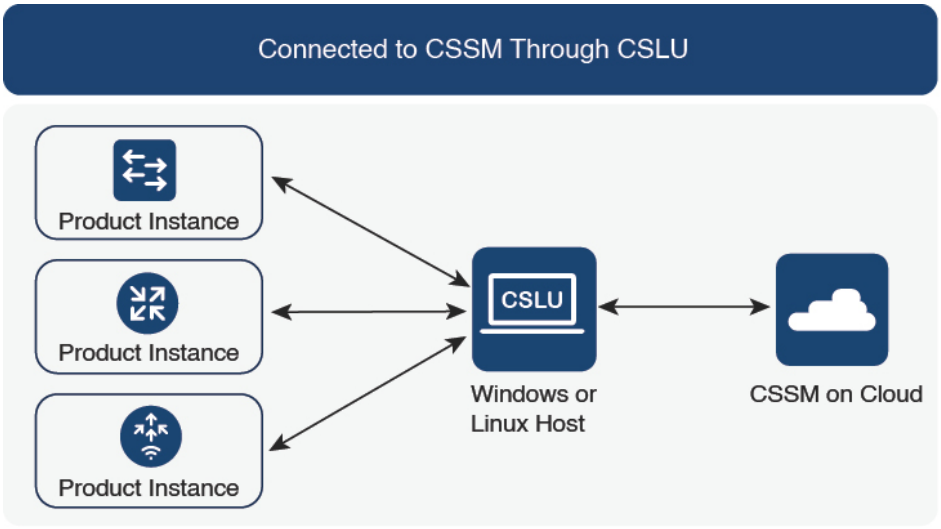
Overview:

Here, product instances in the network are connected to CSLU, and CSLU becomes the single point of interface with CSSM. A product instance can be configured to *push* the required information to CSLU. Alternatively, CSLU can be set-up to *pull* the required information from a product instance at a configurable frequency.

Product instance-initiated communication (push): A product instance initiates communication with CSLU, by connecting to a REST endpoint in CSLU. Data that is sent includes RUM reports and requests for authorization codes, UDI-tied trust codes, and policies. You can configure the product instance to automatically send RUM reports to CSLU at required intervals. This is the default method for a product instance.

CSLU-initiated communication (pull): To initiate the retrieval of information from a product instance, CSLU uses NETCONF, or RESTCONF, or gRPC with YANG models, or native REST APIs, to connect to the product instance. Supported workflows include retrieving RUM reports from the product instance and sending the same to CSSM, authorization code installation, UDI-tied trust code installation, and application of policies.

Figure 1: Topology: Connected to CSSM Through CSLU



Considerations or Recommendations:

Choose the method of communication depending on your network's security policy.

Release-Wise Changes and Enhancements:

This section outlines important release-wise software changes and enhancements that affect this topology.

From Cisco IOS XE Cupertino 17.7.1a:

- Trust code request and installation

  If a trust code is not available on the product instance, the product instance detects and automatically includes a request for one, as part of a RUM report. A corresponding ACK from CSSM includes the trust code. If there is an existing factory-installed trust code, it is automatically overwritten. A trust code obtained this way can be used for communication with CSSM.

  This is supported in a standalone, as well as a High Availability set-up. In a High Availability set-up, the active product instance requests the trust code for all connected product instances where a trust code is not available.

  In this release, this enhancement applies only to the product instance-initiated mode.

From Cisco IOS XE Cupertino 17.9.1a:

- Trust code request and installation

  From this release, trust code request and installation is supported in the CSLU-initiated mode as well.

- Virtual Routing and Forwarding (VRF) Support

  You can configure a VRF to send all licensing data. For this, the product instance must be one that supports VRF, and when implementing this topology, you must implement the product instance-initiated mode.

- RUM report throttling

  In the product instance-initiated mode, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down caused by an excessive generation of RUM reports.

  You can override the throttling restriction by entering the **license smart sync** command in privileged EXEC mode.

  RUM report throttling also applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From 17.9.1, RUM report throttling is applicable to *all* subsequent releases.

Where to Go Next:

To implement this topology, see Workflow for Topology: Connected to CSSM Through CSLU.

Connected Directly to CSSM

Overview:

This topology is available in the earlier version of Smart Licensing and continues to be supported with Smart Licensing Using Policy.

Here, you establish a *direct* and *trusted* connection from a product instance to CSSM. The direct connection, requires network reachability to CSSM. For the product instance to then exchange messages and communicate with CSSM, configure one of the transport options available with this topology (described below). Lastly, the establishment of trust requires the generation of an ID token from the corresponding Smart Account and Virtual Account in CSSM, and installation on the product instance.

Note A factory-installed trust code cannot be used for communication with CSSM. This means that for this topology, you must generate an *ID token* in the CSSM Web UI to obtain a trust code and install it on the product instance. You must overwrite the factory-installed trust code if there is one. Also see Trust Code.

You can configure a product instance to communicate with CSSM in the following ways:

- Use Smart transport to communicate with CSSM

  Smart transport is a transport method where a Smart Licensing (JSON) message is contained within an HTTPs message, and exchanged between a product instance and CSSM, to communicate. The following Smart transport configuration options are available:

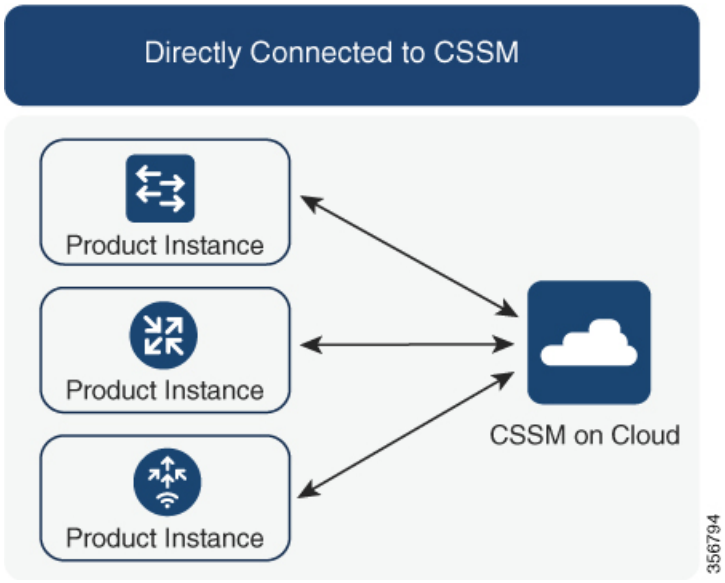
  - Smart transport: In this method, a product instance uses a specific Smart transport licensing server URL. This must be configured exactly as shown in the workflow section.
  - Smart transport through an HTTPs proxy: In this method, a product instance uses a proxy server to communicate with the licensing server, and eventually, CSSM.

- Use Call Home to communicate with CSSM.

  Call Home provides e-mail-based and web-based notification of critical system events. This method of connecting to CSSM is available in the earlier Smart Licensing environment, and continues to be available with Smart Licensing Using Policy. The following Call Home configuration options are available:

  - Direct cloud access: In this method, a product instance sends usage information directly over the internet to CSSM; no additional components are needed for the connection.
  - Direct cloud access through an HTTPs proxy: In this method, a product instance sends usage information over the internet through a proxy server - either a Call Home Transport Gateway or an off-the-shelf proxy (such as Apache) to CSSM.

Figure 2: Topology: Connected Directly to CSSM



Considerations or Recommendations:

- Smart transport is the recommended transport method when directly connecting to CSSM. This recommendation applies to:
  - New deployments
  - Earlier licensing models. Change configuration after migration to Smart Licensing Using Policy.
  - Registered licenses that currently use the Call Home transport method. Change configuration after migration to Smart Licensing Using Policy.

Note When you change from the Call Home to the Smart transport method, you do not have to disable the call-home profile "CiscoTAC-1" for Smart Licensing Using Policy to work as expected.

  - Evaluation or expired licenses in an earlier licensing model. Change configuration after migration to Smart Licensing Using Policy.

  To change configuration after migration, see Workflow for Topology: Connected Directly to CSSM > Product Instance Configuration > Configure a connection method and transport type > Option 1.

- If you implement this topology when operating in the utility mode (available from 17.9.1.a onwards), you can use only Smart transport, that is, Smart transport directly, or Smart transport through an HTTP proxy. Call Home is not supported in the utility mode.

Release-Wise Changes and Enhancements:

This section outlines important release-wise software changes and enhancements that affect this topology.

From Cisco IOS XE Cupertino 17.9.1a:

- Virtual Routing and Forwarding (VRF) Support

  You can configure a VRF to send all licensing data. For this, the product instance must be one that supports VRF, and when implementing this topology, you must use only the Smart transport option, that is, Smart transport directly, or Smart transport through an HTTP proxy.

- RUM report throttling

  The minimum reporting frequency for this topology, is throttled to one day. This means the product instance does not send more than one RUM report a day. This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down caused by an excessive generation of RUM reports.

  You can override the throttling restriction, by entering the **license smart sync** command in privileged EXEC mode.

  RUM report throttling also applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From 17.9.1, RUM report throttling is applicable to *all* subsequent releases.

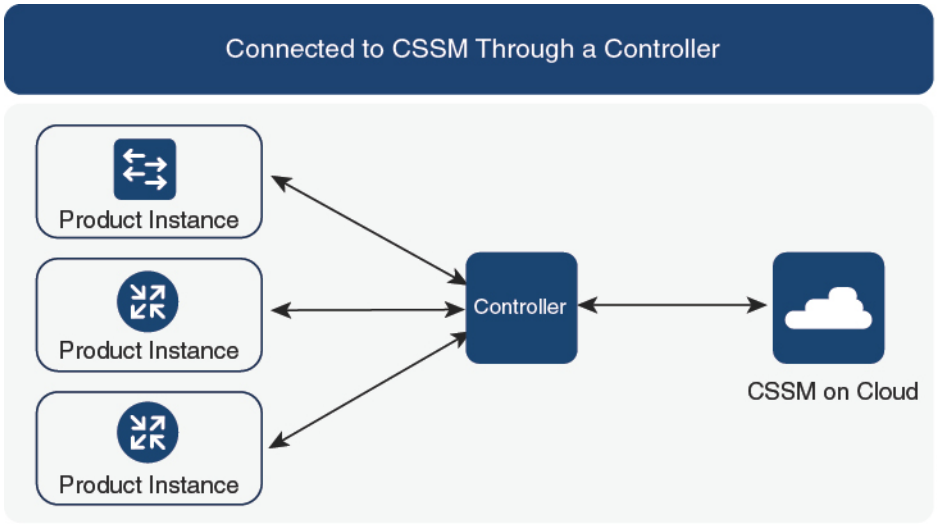
Where to Go Next:

To implement this topology, see Workflow for Topology: Connected Directly to CSSM.

Connected to CSSM Through a Controller

When you use a controller to manage a product instance, the controller connects to CSSM, and is the interface for all communication to and from CSSM.

Figure 3: Topology: Connected to CSSM Through a Controller



For Cisco Aggregation, Integrated, and Cloud Service Routers, Cisco Catalyst 8000 Edge Platforms Family, and Cisco Terminal Services Gateways, the supported controllers are Cisco DNA Center and Cisco vManage. Depending on the controller you want to implement, refer to the corresponding section below for information about how the topology is designed to work:

Cisco DNA Center as a Controller

Overview:

If a product instance is managed by Cisco DNA Center as the controller, the product instance records license usage and saves the same, but it is the Cisco DNA Center that initiates communication with the product instance to retrieve RUM Reports, report to CSSM, and return the ACK for installation on the product instance.

All product instances that must be managed by Cisco DNA Center must be part of its inventory and must be assigned to a site. 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.

In order to meet reporting requirements, Cisco DNA Center retrieves the applicable policy from CSSM and provides the following reporting options:

- Ad hoc reporting: You can trigger an ad hoc report when required.
- Scheduled reporting: Corresponds with the reporting frequency specified in the policy and is automatically handled by Cisco DNA Center.

Note Ad hoc reporting must be performed at least once before a product instance is eligible for scheduled reporting.

The first ad hoc report enables Cisco DNA Center to determine the Smart Account and Virtual Account to which subsequent RUM reports must be uploaded. You will receive notifications if ad-hoc reporting for a product instances has not been performed even once.

Cisco DNA Center enables you to install and remove SLAC. SLAC installation and removal can be performed for a single product instance or multiple product instances.

Note The Cisco DNA Center GUI provides an option to generate a SLAC only for an export-controlled license (HSECK9), and only for certain product instances. See Table 1.

A trust code is *not* required.

Considerations or Recommendations:

This is the recommended topology if you are using Cisco DNA Center.

Where to Go Next:

To implement this topology, see Workflow for Topology: Connected to CSSM Through a Controller > Using Cisco DNA Center as a Controller.

Cisco vManage as a Controller

Overview:

When you use Cisco vManage as a controller to manage a product instance, Cisco vManage connects to CSSM and is the interface for all communication to and from CSSM.

Cisco vManage records license usage, generates RUM reports, and sends RUM reports to CSSM every 24 hours - this is a fixed reporting interval determined by the policy and cannot be changed. The returning RUM ACK from CSSM is also sent to Cisco vManage.

When a product instance is managed by Cisco vManage, the product instance does not store license usage information or generate RUM reports.

In the Cisco vManage portal, you can assign licences to edge devices, view information about the licenses that are being used and the licenses that are available for assignment.

Note The Cisco vManage portal *does not* provide an option for SLAC installation. To use an export-controlled license or throughput greater than 250 Mbps, you must either request and install the SLAC by using the required CLI commands on the product instance, or download the file from CSSM and then install the same on the product instance.

If you have an HSECK9 license from an earlier licensing environment the same is supported after migration to Smart Licensing Using Policy. You do not have to install a SLAC again in this case.

For SLAC installation details, see Using Cisco vManage as a Controller.

For more information about how Cisco vManage handles license management, see the License Management for Smart Licensing Using Policy section of the *Cisco SD-WAN Getting Started Guide*.

Considerations or Recommendations:

This is the recommended topology if you are using Cisco vManage.

Cisco IOS XE Bengaluru 17.5.1a and later: Cisco SD-WAN operates together with CSSM to provide license management through Cisco vManage for devices operating with Cisco SD-WAN.

Cisco IOS XE Amsterdam 17.3.2 to Cisco IOS XE Bengaluru 17.4.x: Cisco vManage is supported as a controller, but it does not support license management. Edge devices running in the Cisco SD-WAN controller mode do not support any other features or functions of Smart Licensing Using Policy, except HSECK9 license handling.

Where to Go Next:

To implement this topology, see Workflow for Topology: Connected to CSSM Through a Controller > Using Cisco vManage as a Controller.

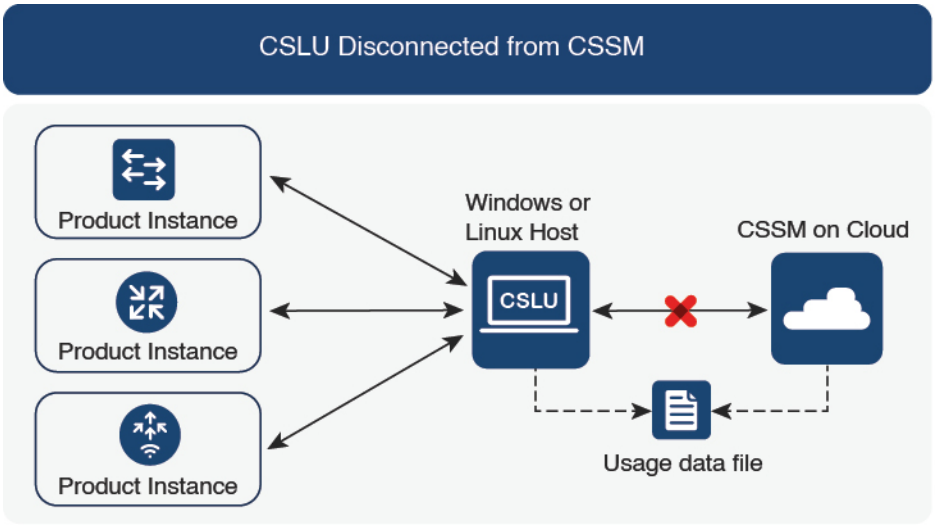
CSLU Disconnected from CSSM

Overview:

Here, a product instance communicates with CSLU, and you have the option of implementing product instance-initiated communication or CSLU-initiated communication (as in the *Connected to CSSM Through CSLU* topology). The other side of the communication, between CSLU and CSSM, is offline. CSLU provides you with the option of working in a mode that is disconnected from CSSM.

Communication between CSLU and CSSM is sent and received in the form of signed files that are saved offline and then uploaded to or downloaded from CSLU or CSSM, as the case may be.

Figure 4: Topology: CSLU Disconnected from CSSM



Considerations or Recommendations:

Choose the method of communication depending on your network's security policy.

Release-Wise Changes and Enhancements:

This section outlines important release-wise software changes and enhancements that affect this topology.

From Cisco IOS XE Cupertino 17.7.1a:

- Trust code request and installation

  If a trust code is not available on the product instance, the product instance detects and automatically includes a request for one, as part of a RUM report that is sent to CSLU, which you upload to CSSM. The ACK that you download from CSSM includes the trust code. If there is an existing factory-installed trust code, it is automatically overwritten. A trust code obtained this way can be used for communication with CSSM.

  This is supported in a standalone, as well as a High Availability set-up. In a High Availability set-up, the active product instance requests the trust code for members or standbys where a trust code is not available.

  In this release, this enhancement applies only to the product instance-initiated mode.

From Cisco IOS XE Cupertino 17.9.1a:

- Trust code request and installation

  From this release, trust code request and installation is supported in the CSLU-initiated mode as well.

- Virtual Routing and Forwarding (VRF) Support

  You can configure a VRF to send all licensing data to CSLU. For this, the product instance must be one that supports VRF, and when implementing this topology, you must implement the product instance-initiated mode.

- RUM report throttling

In the product instance-initiated mode, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down caused by an excessive generation of RUM reports.

You can override the throttling restriction by entering the **license smart sync** command in privileged EXEC mode.

RUM report throttling also applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From 17.9.1, RUM report throttling is applicable to *all* subsequent releases.

Where to Go Next:

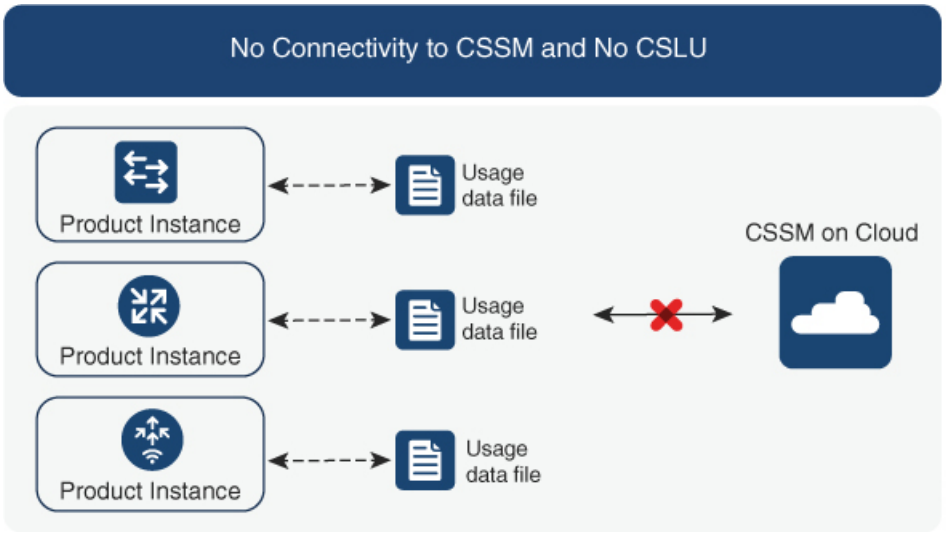
To implement this topology, see Workflow for Topology: CSLU Disconnected from CSSM.

No Connectivity to CSSM and No CSLU

Overview:

Here you have a product instance and CSSM disconnected from each other, and without any other intermediary utilities or components. All communication is in the form of uploaded and downloaded files. These files can be RUM reports, requests for UDI-tied trust codes and SLAC request files

Figure 5: Topology: No Connectivity to CSSM and No CSLU



Considerations or Recommendations:

This topology is suited to a high-security deployment where a product instance cannot communicate online, with anything outside its network.

Release-Wise Changes and Enahcements

This section outlines the release-wise software changes and enhancements that affect this topology.

From Cisco IOS XE Cupertino 17.7.1a:

- Trust code request and installation

  If a trust code is not available on the product instance, the product instance automatically includes a trust code request in the RUM report that you save, to upload to CSSM. The ACK that you then download from CSSM includes the trust code.

  If there is a factory-installed trust code, it is automatically overwritten when you install the ACK. A trust code obtained this way can be used for secure communication with CSSM.

  This is supported in a standalone, as well as a High Availability set-up. In a High Availability set-up, the active product instance requests the trust code for all connected product instances where a trust code is not available.

- SLAC request and installation

  You can generate a SLAC request and save it in a file on the product instance. The saved file includes all the required details (UDI, license information etc). With this method you do not have to gather and enter the required details on the CSSM Web UI to generate a SLAC. You have to upload the SLAC request file to CSSM and download the file containing the SLAC code and install it on the product instance - as you would a RUM report and ACK.

  Similarly, when you return a SLAC you do not have to locate the product instance in the correct Virtual Account. Simply upload the SLAC return file, as you would a RUM report.

Where to Go Next:

To implement this topology, see Workflow for Topology: No Connectivity to CSSM and No CSLU.

SSM On-Prem Deployment

Overview:

SSM On-Prem is designed to work as an extension of CSSM that is deployed on your premises.

Here, a product instance is connected to SSM On-Prem, and SSM On-Prem becomes the single point of interface with CSSM. Each instance of SSM On-Prem must be made known to CSSM through a mandatory registration and synchronization of the local account in SSM On-Prem, with a Virtual Account in CSSM.

When you deploy SSM On-Prem to manage a product instance, the product instance can be configured to *push* the required information to SSM On-Prem. Alternatively, SSM On-Prem can be set-up to *pull* the required information from a product instance at a configurable frequency.

- Product instance-initiated communication (push): The product instance initiates communication with SSM On-Prem, by connecting to a REST endpoint in SSM On-Prem. Data that is sent includes RUM reports and requests for authorization codes, trust codes, and policies.

  Options for communication between the product instance and SSM On-Prem in this mode:

  - Use a CLI command to push information to SSM On-Prem as and when required.
  - Use a CLI command and configure a reporting interval, to automatically send RUM reports to SSM On-Prem at a scheduled frequency.

- SSM On-Prem-initiated communication (pull): To initiate the retrieval of information from a product instance, SSM On-Prem NETCONF, RESTCONF, and native REST API options, to connect to the product instance. Supported workflows include receiving RUM reports from the product instance and sending the same to CSSM, authorization code installation, trust code installation, and application of policies.

  Options for communication between the product instance and SSM On-Prem in this mode:

  - Collect usage information from one or more product instances as and when required (on-demand).
  - Collect usage information from one or more product instances at a scheduled frequency.

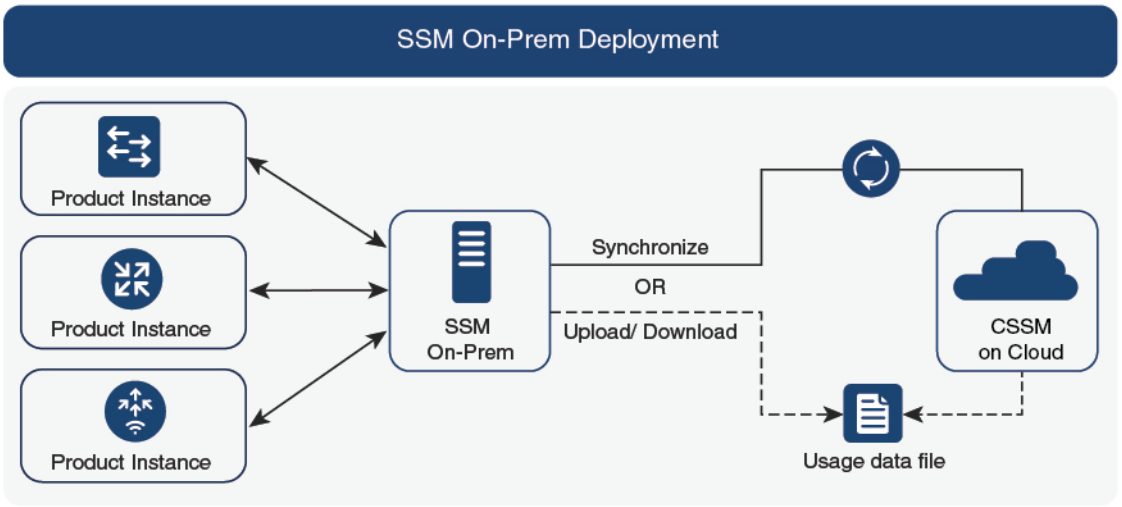
In SSM On-Prem, the reporting interval is set to the default policy on the product instance. You can change this, but only to report more frequently (a narrower interval), or you can install a custom policy if available.

After usage information is available in SSM On-Prem, you must synchronize the same with CSSM, to ensure that the product instance count, license count and license usage information is the same on both, CSSM and SSM On-Prem. Options for usage synchronization between SSM On-Prem and CSSM – for the push *and* pull mode:

- Perform ad-hoc synchronization with CSSM (Synchronize now with Cisco).
- Schedule synchronization with CSSM for specified times.
- Communicate with CSSM through signed files that are saved offline and then upload to or download from SSM On-Prem or CSSM, as the case may be.

Note This topology involves two different kinds of synchronization between SSM On-Prem and CSSM. The first is where the *local account* is synchronized with CSSM - this is for the SSM On-Prem instance to be known to CSSM and is performed by using the **Synchronization** widget in SSM On-Prem. The second is where *license usage* is synchronized with CSSM, either by being connected to CSSM or by downloading and uploading files. You must synchronize the local account before you can synchronize license usage.

Figure 6: Topology: SSM On-Prem Deployment



Considerations or Recommendations:

- This topology is suited to the following situations:
  - If you want to manage your product instances on your premises, as opposed communicating directly with CSSM for this purpose.
  - If your company's policies prevent your product instances from reporting license usage directly to Cisco (CSSM).
  - If your product instances are in an air-gapped network and cannot communicate online, with anything outside their network.
- Apart from support for Smart Licensing Using Policy, some of the key benefits of SSM On-Prem *Version 8* include:
  - Multi-tenancy: One tenant constitutes one Smart Account-Virtual Account pair. SSM On-Prem enables you to manage multiple pairs. Here you create local accounts that reside in SSM On-Prem. Multiple local accounts roll-up to a Smart Account-Virtual Account pair in CSSM. For more information, see the Cisco Smart Software Manager On-Prem User Guide > *About Accounts and Local Virtual Accounts*.

Note The relationship between CSSM and SSM On-Prem instances is still one-to-one.

  - Scale: Supports up to a total of 300,000 product instances
  - High-Availability: Enables you to run two SSM On-Prem servers in the form of an active-standby cluster. For more information, see the Cisco Smart Software On-Prem Installation Guide > Appendix 4. Managing a High Availability (HA) Cluster in Your System.

    High-Availability deployment is supported in the SSM On-Prem console and the required command details are available in the Cisco Smart Software On-Prem Console Guide.
  - Options for online and offline connectivity to CSSM.
- SSM On-Prem Limitations:
  - Proxy support for communication with CSSM, for the purpose of *license usage* synchronization is available only from Version 8 202108 onwards. The use of a proxy for *local account* synchronization, which is performed by using the **Synchronization** widget, is available from the introductory SSM On-Prem release where Smart Licensing Using Policy is supported.
  - SSM On-Prem-initiated communication is not supported on a product instance that is in a Network Address Translation (NAT) set-up. You must use product instance-initiated communication, and further, you must *enable* SSM On-Prem to support a product instance that is in a NAT setup. Details are provided in the workflow for this topology.

Release-Wise Changes and Enhancements:

This section outlines important release-wise software changes and enhancements that affect this topology.

From Cisco IOS XE Cupertino 17.9.1a:

- Virtual Routing and Forwarding (VRF) Support

You can configure a VRF to send all licensing data to CSLU. For this, the product instance must be one that supports VRF. and when implementing this topology, you must implement the product instance-initiated mode.

- RUM report throttling

  In the product instance-initiated mode, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down caused by an excessive generation of RUM reports.

  You can override the throttling restriction by entering the **license smart sync** command in privileged EXEC mode.

  RUM report throttling also applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From 17.9.1, RUM report throttling is applicable to *all* subsequent releases.

Where to Go Next:

To implement this topology, see Workflow for Topology: SSM On-Prem Deployment.

If you are migrating from an existing version of SSM On-Prem, the sequence in which you perform the various upgrade-related activities is crucial. See Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy.

Utility Mode

Overview:

The utility mode topology applies only to product instances that uses post-paid licenses.

A product instance that uses post-paid licenses may be directly connected to CSSM, or connected to CSSM via CSLU, or connected to CSSM via SSM On-Prem, or operate in a disconnected mode, to complete licensing workflows (like usage reporting). Any communication to and from the product instance is flagged, to indicate that the product instance is using post-paid licenses. This flagged communication is made possible by configuring a "utility mode" setting on the product instance. After usage information is processed by CSSM, you are billed according to usage.

Described below is an overview of how each available option to connect to CSSM works. Choose one that suits your network requirements:

- Connected Directly to CSSM:

  Here, you establish a *direct* and *trusted* connection from a product instance to CSSM. The direct connection, requires network reachability to CSSM. For the product instance to then exchange messages and communicate with CSSM, configure one of the transport options available with this topology (described below). Lastly, the establishment of trust requires the generation of an ID token from the corresponding Smart Account and Virtual Account in CSSM, and installation on the product instance.

Note You can use only Smart transport when you implement this topology with the utility mode, that is, Smart transport directly, or Smart transport through an HTTP proxy.

For more details, see: Connected Directly to CSSM, on page 8.

- Connected to CSSM Through CSLU:

  Here, product instances in the network are connected to CSLU, and CSLU becomes the single point of interface with CSSM. A product instance can be configured to *push* the required information to CSLU. Alternatively, CSLU can be set-up to *pull* the required information from a product instance at a configurable frequency.

  For more details, see: Connected to CSSM Through CSLU, on page 6, or CSLU Disconnected from CSSM, on page 12

- SSM On-Prem Deployment:

  Here, a product instance is connected to SSM On-Prem, and SSM On-Prem becomes the single point of interface with CSSM. Each instance of SSM On-Prem must be made known to CSSM through a mandatory registration and synchronization of the local account in SSM On-Prem, with a Virtual Account in CSSM.

  SSM On-Prem Deployment, on page 15

- No Connectivity to CSSM and No CSLU:

  Here you have a product instance and CSSM disconnected from each other, and without any other intermediary utilities or components. All communication is in the form of uploaded and downloaded files. These files can be RUM reports, requests for UDI-tied trust codes and SLAC request files

  No Connectivity to CSSM and No CSLU, on page 14

Note A product instance using post-paid licenses must send RUM reports and install a RUM ACK every 30 days. To ensure timely reporting, we recommend a reporting interval of 7 days or less.

Considerations or Recommendations:

- When ordering post-paid licenses on CCW, note that you cannot order a post-paid HSECK9 license. This license can only be a prepaid one.
- You cannot send usage reports to a third-party billing platform. Supported alternatives that you can use are to implement CSLU, or SSM On-Prem, which in-turn will send it to CSSM.
- If you plan to implement CSLU or SSM On-Prem, ensure that you install the minimum required, MSLA-capable versions in the Smart Licensing Using Policy environment:
  - For CSLU: Version 2.0.0
  - For SSM On-Prem: Version 8, Release 202206

Where to Go Next:

Implement one of the supported topologies:

Note All the steps in a workflow apply to a product instance using post-paid licenses - unless indicated otherwise.

High Availability

This section explains considerations that apply to a High Availability configuration, when running a software version that supports Smart Licensing Using Policy. The following High Availability set-ups are within the scope of this document:

A device stack with an active, a standby and one or more members

A dual-chassis set-up[8] (could be fixed or modular), with the active in one chassis and a standby in the other chassis.

A dual-chassis and dual-RP set-up[9], on a modular chassis. Two chassis are involved here as well, with an active RP in one chassis, a standby RP in the other chassis. The dual-RP aspect refers to an additional in-chassis standby RP in just one of the chassis, which is the minimum requirement, or an in-chassis standby RP in each chassis.

Note When you use Cisco vManage to manage a product instance, every single device requires a license - High Availability is not supported.

Authorization Code Requirements in a High Availability Set-Up

If you are using a license that requires authorization before use (whether SLAC or SLR, PLR, and so on.), and you have one of High Availability set-ups described above, the number of authorization codes that are required, corresponds to the number of UDIs.

- If the UDIs of the active and standby are the same, only one authorization code is required. This is the case when the UDI is on the chassis (and not the individual RPs).
- If two chassis are involved in your High Availability set-up, again each chassis will have its own UDI and therefore require its own authorization code.
- In case of a device stack, only the active requires an authorization code.

Use the **show license udi** command in privileged EXEC mode to display UDI information. All UDIs are displayed in case of High Availability set-ups.

[8] The Cisco StackWise Virtual feature, which is available on Cisco Catalyst switches, is an example of such a set-up.
[9] The Quad-Supervisor with Route Processor Redundancy, which is available on Cisco Catalyst switches, is an example of such a set-up.

Trust Code Requirements in a High Availability Set-Up

The number of trust codes required depends on the number of UDIs. The active product instance can submit requests for all devices in the High Availability set-up and install all the trust codes that are returned in an ACK.

Policy Requirements in a High Availability Set-Up

There are no policy requirements that apply exclusively to a High Availability set-up. As in the case of a standalone product instance, only one policy exists in a High Availability set-up as well, and this is on the active. The policy on the active applies to any standbys or members in the set-up.

Product Instance *Functions* in a High Availability Set-Up

This section explains general product instance functions in a High Availability set-up, as well as what the product instance does when a new standby or member is added to an existing High Available set-up.

For authorization and trust codes: The active product instance can request (if required) and install authorization codes and trust codes for standbys and members.

For policies: The active product instance synchronizes with the standby.

For reporting: Only the active product instance reports usage. The active reports usage information for all devices (standbys or members – as applicable) in the High Availability set-up. In addition to scheduled reporting, the following events trigger reporting:

- The addition or removal of a standby. The RUM report includes information about newly added or removed standby or member.
- A switchover.
- A reload.

When one of the above events occur, the "Next report push" date of the **show license status** privileged EXEC command is updated. But it is the implemented topology and associated reporting method that determine if the report is sent by the product instance or not. For example, if you have implemented a topology where the product instance is disconnected (Transport Type is Off), then the product instance does not send RUM reports even if the "Next report push" date is updated.

For a new member or standby addition:

- A product instance that is connected to CSLU, does not take any further action.
- A product instance that is directly connected to CSSM, performs trust synchronization. Trust synchronization involves the following:

  Installation of trust code on the standby or member if not installed already.

  If a trust code is already installed, the trust synchronization process ensures that the new standby or member is in the same Smart Account and Virtual Account as the active. If it is not, the new standby or member is *moved* to the same Smart Account and Virtual Account as the active.

  Installation of an authorization code, policy, and purchase information, if applicable

  Sending of a RUM report with current usage information.