How Smart Licensing Using Policy Works

This section lists the components that may be involved in an implementation of Smart Licensing Using Policy, followed by the sequential stages of managing licenses for Cisco Catalyst 9000 Series Switches.

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: the product instance and Cisco SSM. The product instance, because it consumes the license and Cisco SSM because it 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. Cisco SSM helps you manage current requirements and review usage trends to plan for future license requirements.

You can access the Cisco SSM Web UI at https://software.cisco.com. Under **Smart Software Manager**, click the **Manage Licenses** link.

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

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 from Cisco SSM, if applicable.

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.

Controller

A management application or service that manages multiple product instances. On Cisco Catalyst 9000 Series Switches, Cisco Catalyst Center is the supported controller.

This table provides information about the supported controller, product instances that support the controller, and minimum required software versions on the controller and on the product instance.

Table 1: Support Information for Controller: Cisco DNA Center

Component	Minimum Required Release
Cisco Catalyst Center This is the minimum required Cisco Catalyst Center version that supports Smart Licensing Using Policy. Support continues on all subsequent releases - unless noted otherwise.	Cisco DNA Center Release 2.2.2
Cisco Catalyst 9200 Series Switches Cisco Catalyst 9300 Series Switches Cisco Catalyst 9400 Series Switches Cisco Catalyst 9500 Series Switches Cisco Catalyst 9600 Series Switches	Cisco IOS XE Amsterdam 17.3.2a This is the minimum required software 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.

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.

Table 2: Support Information for SSM On-Prem

Component	Minimum Required Release
SSM On-Prem This is the minimum required SSM On-Prem version that supports Smart Licensing Using Policy. Support continues on all subsequent releases - unless noted otherwise.	Version 8, Release 202102
Cisco Catalyst 9200 Series Switches Cisco Catalyst 9300 Series Switches Cisco Catalyst 9400 Series Switches Cisco Catalyst 9500 Series Switches Cisco Catalyst 9600 Series Switches	Cisco IOS XE Amsterdam 17.3.3 This is the minimum required software version on the product instance. This means support continues on all subsequent releases - unless noted otherwise.

For more information, see Cisco Smart Software Manager On-Prem Data Sheet.

Stages of License Management with the Smart Licensing Using Policy Solution

This section describes the sequential order of license management when you deploy and use a Smart Licensing Using Policy solution.

1. Set up a Smart Account and one or more Virtual accounts to structure your Cisco assets (licenses, devices, and general terms). You can view and manage Smart Account and Virtual Accounts in the Cisco SSM portal.
2. Purchase or order licenses through existing channels. Once purchased, assets are available in your organization's Smart Account and Virtual Accounts, and can be accessed through the Cisco SSM portal. Ensuring that the licenses are in the correct Smart Account and Virtual Account is essential to consume your licenses.

   For new hardware or software orders, Cisco simplifies the implementation of Smart Licensing Using Policy by factory-installing custom policies, authorization codes (if applicable), and trust codes.

   For Cisco Catalyst 9000 Series Switches, to know more about available licenses, see Available Licenses.
3. Configure and use the required licenses.

Note Most licenses are unenforced, meaning no preliminary licensing-specific operations are needed before use. Only export-controlled and enforced licenses require Cisco authorization. License usage is recorded with timestamps, allowing required workflows to be completed later.

4. Set up a method to report license usage to Cisco SSM.

   Multiple ways of interfacing with Cisco SSM are available – each way is called a topology. An organization's network requirements and security policy are some of the factors that determine the choice of topology. For each topology, the accompanying overview describes how the set-up is designed to work, and provides considerations and recommendations, if any. To know about all the available topology options, see Connecting to Cisco SSM.

Connecting to Cisco SSM

Multiple ways of interfacing with Cisco SSM are available. An organization's network requirements and security policy are some of the factors that determine the choice of topology.

For each topology, the accompanying overview describes how the set-up is designed to work, and provides considerations and recommendations, if any.

Based on the topology that is selected, refer to the corresponding workflow under Implementing Smart Licensing Using Policy, 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.

Connected Directly to Cisco SSM

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

Note A factory-installed trust code cannot be used for communication with Cisco SSM. This means that for this topology, you must generate an *ID token* in the Cisco SSM 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 Cisco SSM in the following ways:

- Use Smart transport to communicate with Cisco SSM

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 Cisco SSM, to communicate. The following Smart transport configuration options are available:

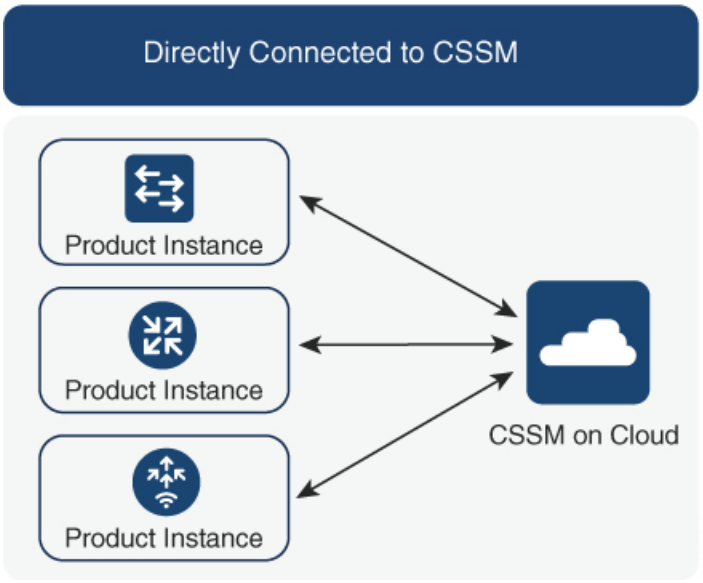
- Smart transport: In this method, a product instance uses a specific Smart transport licensing server URL. This must be configured exactly as shown in the workflow section.
- Smart transport through an HTTPs proxy: In this method, a product instance uses a proxy server to communicate with the licensing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

- Use Call Home to communicate with Cisco SSM.

  Call Home provides e-mail-based and web-based notification of critical system events. This method of connecting to Cisco SSM 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 Cisco SSM; 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 Cisco SSM.

Figure 1: Topology: Connected Directly to Cisco SSM



Considerations or Recommendations:

Smart transport is the recommended transport method when directly connecting to Cisco SSM. 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.
- Evaluation or expired licenses in an earlier licensing model. Change configuration after migration to Smart Licensing Using Policy.

To change configuration after migration, see Connected Directly to Cisco SSM, on page 4> Product Instance Configuration > Configure a connection method and transport type > Option 1.

Release-Wise Changes and Enhancements:

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

From Cisco IOS XE Cupertino 17.9.1:

- 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 Connected Directly to Cisco SSM, on page 4.

Connected to Cisco SSM Through CSLU

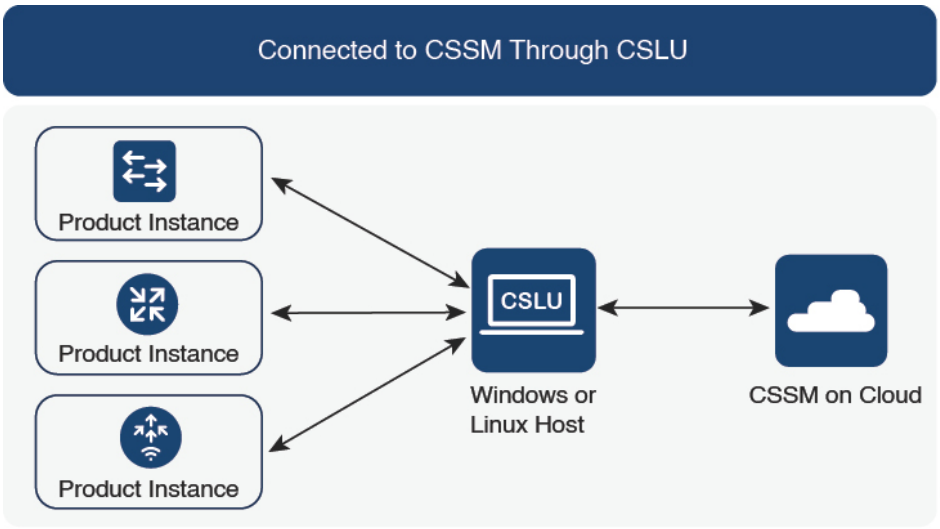
Overview:

Here, product instances in the network are connected to CSLU, and CSLU becomes the single point of interface with Cisco SSM. 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 Cisco SSM, authorization code installation, UDI-tied trust code installation, and application of policies.

Figure 2: Topology: Connected to Cisco SSM 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 17.7.1:

- 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 Cisco SSM 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 Cisco SSM.

  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 17.9.1:

- Trust code request and installation

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

- 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 Cisco SSM Through CSLU.

Connected to Cisco SSM Through a Controller

When you use a controller to manage a product instance, the controller connects to Cisco SSM, and is the interface for all communication to and from Cisco SSM. The supported controller for Cisco Catalyst Access, Core, and Aggregation Switches is Cisco DNA Center.

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 Cisco SSM, 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 Cisco SSM and provides the following reporting options:

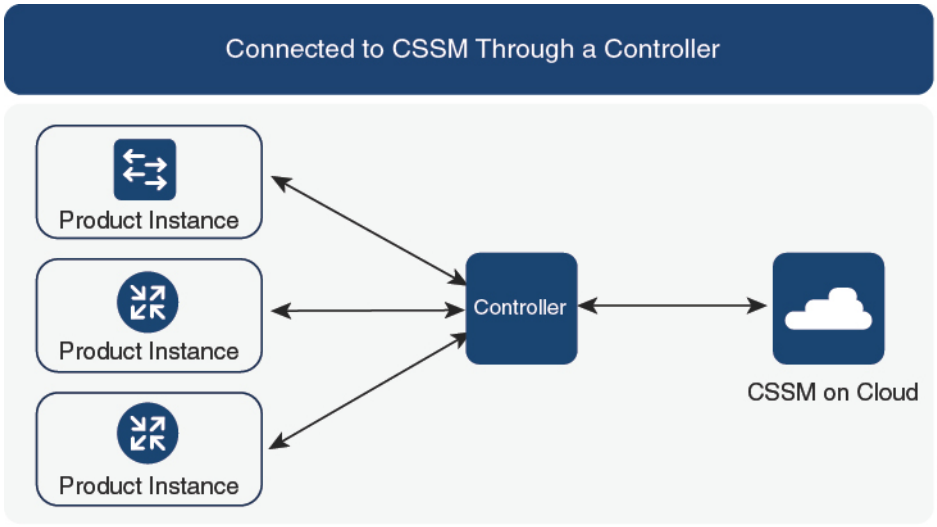
- Ad hoc reporting: You can trigger an ad hoc report when required.
- Scheduled reporting: Corresponds with the reporting frequency specified in the policy and is automatically handled by Cisco DNA Center.

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 instance has not been performed even once.

A trust code is *not* required.

Figure 3: Topology: Connected to Cisco SSM Through a Controller



Considerations or Recommendations:

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

Note The HSECK9 key, which is an export-controlled license is supported on certain models of the Cisco Catalyst Access, Core, and Aggregation Switches (See Returning an Authorization Code). If you are using a product instance where an HSECK9 key is supported, note that the Cisco DNA Center GUI does not provide an option to generate a SLAC.

Where to Go Next:

To implement this topology, see Workflow for Topology: Connected to Cisco SSM Through a Controller.

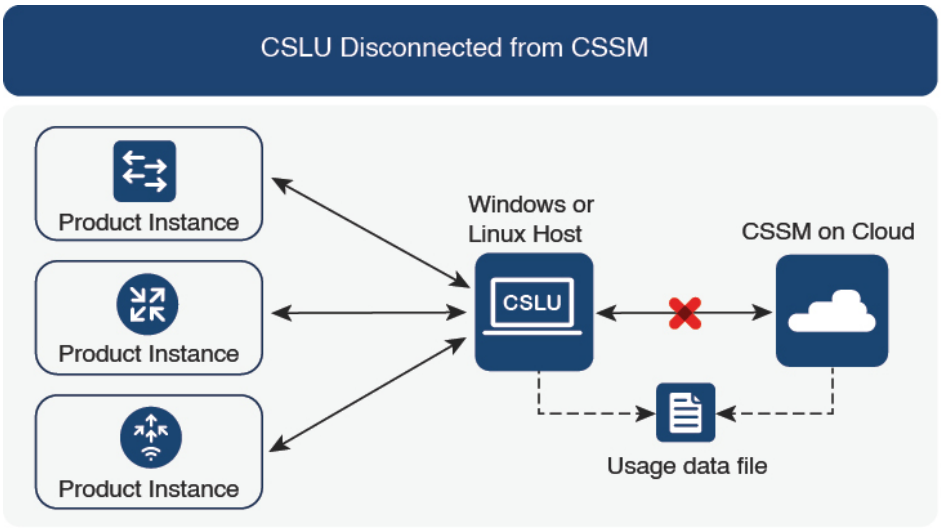
CSLU Disconnected from Cisco SSM

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 Cisco SSM Through CSLU* topology). The other side of the communication, between CSLU and Cisco SSM, is offline. CSLU provides you with the option of working in a mode that is disconnected from Cisco SSM.

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

Figure 4: Topology: CSLU Disconnected from Cisco SSM



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 17.7.1:

- 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 Cisco SSM. The ACK that you download from Cisco SSM 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 Cisco SSM.

  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 17.9.1:

- Trust code request and installation

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

- 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:

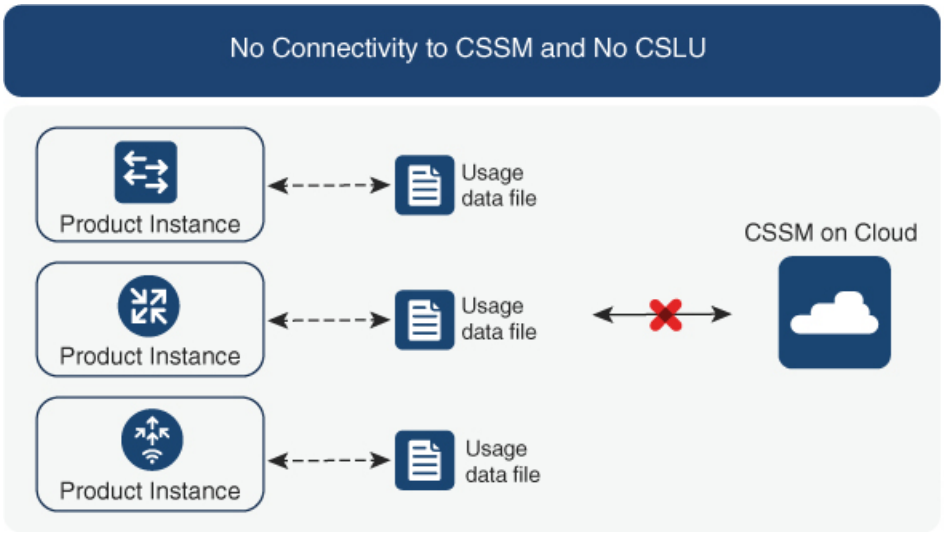
To implement this topology, see Workflow for Topology: CSLU Disconnected from Cisco SSM.

No Connectivity to Cisco SSM and No CSLU

Overview:

Here you have a product instance and Cisco SSM 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 or return files.

Figure 5: Topology: No Connectivity to Cisco SSM 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 Enhancements:

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

From Cisco IOS XE Cupertino 17.7.1:

- 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 Cisco SSM. The ACK that you then download from Cisco SSM 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 Cisco SSM.

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 Cisco SSM Web UI to generate a SLAC. You have to upload the SLAC request file to Cisco SSM 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 Cisco SSM and No CSLU.

SSM On-Prem Deployment

Overview:

SSM On-Prem is designed to work as an extension of Cisco SSM 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 Cisco SSM. Each instance of SSM On-Prem must be made known to Cisco SSM through a mandatory registration and synchronization of the local account in SSM On-Prem, with a Virtual Account in Cisco SSM.

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 Cisco SSM, 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.

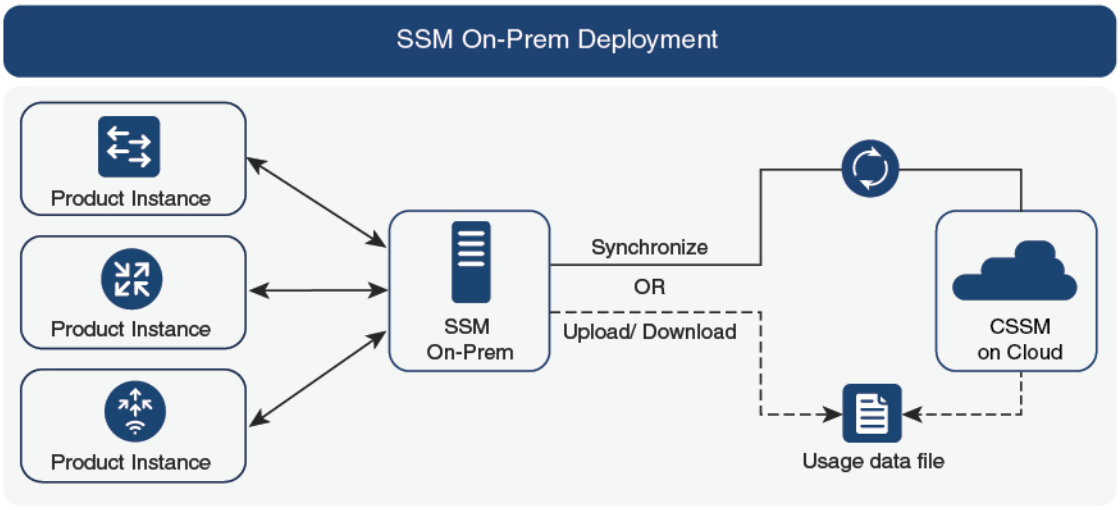
In SSM On-Prem, the reporting interval is set to the default policy on the product instance. You can change this, but only to report more frequently (a narrower interval), or you can install a custom policy if available.

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

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

Note This topology involves two different kinds of synchronization between SSM On-Prem and Cisco SSM. The first is where the *local account* is synchronized with Cisco SSM - this is for the SSM On-Prem instance to be known to Cisco SSM and is performed by using the **Synchronization** widget in SSM On-Prem. The second is where *license usage* is synchronized with Cisco SSM, either by being connected to Cisco SSM 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 Cisco SSM for this purpose.
- If your company's policies prevent your product instances from reporting license usage directly to Cisco (Cisco SSM).
- 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 Cisco SSM. For more information, see the Cisco Smart Software Manager On-Prem User Guide > *About Accounts and Local Virtual Accounts*.

Note The relationship between Cisco SSM 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 Cisco SSM.

SSM On-Prem Limitations:

- Proxy support for communication with Cisco SSM, 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 17.9.1:

- 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. For more information, see *Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy*.

High Availability Considerations

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 setups are within the scope of this document:

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

A dual-supervisor setup, where two supervisor modules are installed in a chassis, one being the active and the other, the standby.

A dual-chassis setup[1] (could be fixed or modular), with the active in one chassis and a standby in the other chassis.

A dual-chassis *and* dual-supervisor setup[2], on a modular chassis. Two chassis are involved here as well. An active supervisor module is in one chasses and a standby supervisor module in a second chassis. The "dual-supervisor" aspect refers to an additional in-chassis standby supervisor in just one of the chassis, which is the minimum requirement, or an in-chassis standby supervisor in each chassis.

Authorization Code Requirements in a High Availability Setup

The number of SLACs required in a High Availability setup, corresponds with the number of UDIs. Tabled below are the stacking and High Availability setups that are supported when using an export-controlled license (HSECK9 key), and the SLAC requirements in each setup.

Note Each HSECK9 key requires a SLAC. Therefore, the number SLACs will always correspond with the number of HSECK9 keys.

[1] The Cisco StackWise Virtual feature, which is available on certain Cisco Catalyst Access, Core, and Aggregation Switches, is an example of such a setup.
[2] The Quad-Supervisor with Route Processor Redundancy, which is available on certain Cisco Catalyst Access, Core, and Aggregation Switches, is an example of such a setup.

Product Instance Supporting HSECK9 Key	Supported High Availability Setup When Using HSECK9 Key	SLAC Requirements in the Setup
Cisco Catalyst 9300X Series Switches	A device stack with an active, a standby and one or more members.	The SLAC requirement corresponds with the number of UDIs on which you want to configure the cryptographic feature. Each such UDI in the stack requires one SLAC. At a minimum, only the active requires a SLAC. But for uninterrupted use of the cryptographic feature in the event of a switchover, we recommend that you install SLAC on the standby also.
Cisco Catalyst 9500X Series Switches.	None.	Not applicable. High Availability is not supported on Cisco Catalyst 9500X Series Switches.
C9600-LC-40YL4CD line card with supervisor module C9600X-SUP-2	A dual-supervisor setup, where two supervisor modules are installed in a chassis, one being the active and the other, the standby. No other High Availability setup is supported when using an HSECK9 key.	The SLAC requirement corresponds with the number of UDIs. The UDI is tied to the chassis and not the individual supervisor modules. (The UDIs of the active and standby supervisor modules are the same). One SLAC is required for each chassis UDI, regardless of the number of supervisors installed.
Cisco Catalyst 9400 Series Supervisor 2 and 2XL Modules (C9400X-SUP-2 and C9400X-SUP-2XL)	• A dual-supervisor setup, where two supervisor modules are installed in a chassis, one being the active and the other, the standby. • A Cisco StackWise Virtual setup, which involves two chassis. One supervisor module is installed in each chassis, one being the active and the other, the standby.	The SLAC requirement corresponds with the number of UDIs. The UDI is tied to the chassis and not the individual supervisor modules. • In a dual-supervisor setup, one SLAC is required for each chassis UDI, regardless of the number of supervisors installed. • In a Cisco StackWise Virtual setup, at a minimum, you must obtain a SLAC for the chassis with the active supervisor module. But for uninterrupted use of the cryptographic feature in the event of a switchover, we recommend that you obtain an SLAC for the chassis with the standby supervisor module also.

Trust Code Requirements in a High Availability setup

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 setup and install all the trust codes that are returned in an ACK.

Policy Requirements in a High Availability setup

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

Product Instance *Functions* in a High Availability setup

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

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 setup.

In addition to scheduled reporting, the following events trigger reporting:

- The addition or removal of a standby. The RUM report includes information about the standby that was added or removed.
- The addition or removal of a member, including stack merge and stack split events. The RUM report includes information about member that was added or removed.
- 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.