Information About Smart Licensing Using Policy

Overview

Smart Licensing Using Policy is a software license management solution that provides a seamless experience with the various aspects of licensing.

- Purchase or order licenses: Purchase licenses through the existing channels and use the Cisco Smart Software Manager (CSSM) portal to view product instances and licenses.

  You can also order postpaid licenses. You can also view these licenses in CSSM. They are listed with a subscription ID.

Note For new hardware or software orders, Cisco simplifies the implementation of Smart Licensing Using Policy, by factory-installing the following (terms are explained in the Concepts, on page 7 section further below):

- A custom policy, if available.
- An authorization code, if applicable. For this, you must provide your Smart Account and Virtual Account information when placing the order.
- A trust code, which ensures authenticity of data sent to CSSM. This is installed starting with Cisco IOS XE Cupertino 17.7.1a. This trust code cannot be used to *communicate* with CSSM.

- Use: Most licenses are unenforced. This means that you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. Only export-controlled and enforced licenses require Cisco authorization *before* use.

License usage is recorded on your device with timestamps and the required workflows can be completed at a later date.

- Report license usage to CSSM: Multiple options are available for license usage reporting. You can use the Cisco Smart Licensing Utility (CSLU), report usage information directly to CSSM, use a Controller (like Cisco DNA Center or Cisco vManage), deploy Smart Software Manager On-Prem (SSM On-Prem) to administer products and licenses on your premises. A provision for offline reporting for closed networks, where you download usage information and upload to CSSM, is also available.

  The usage report is in plain text XML format. See: Sample Resource Utilization Measurement Report.

- Reconcile: For situations where delta billing applies (purchased versus consumed). This applies when you use postpaid licenses - you are billed according to usage.

Supported Products

This section provides information about the Cisco IOS-XE product instances that support Smart Licensing Using Policy. All models (Product IDs or PIDs) in a product series are supported – unless indicated otherwise.

Table 1: Smart Licensing Using Policy: Supported Products

Product Category	Product Series	Introductory Release When Support was Introduced
Cisco Aggregation, Integrated, and Cloud Service Routers		
	Cisco 1000 Series Integrated Services Routers	Cisco IOS XE Amsterdam 17.3.2
	Cisco 4000 Series Integrated Services Routers	Cisco IOS XE Amsterdam 17.3.2
	Cisco ASR 1000 Series Aggregation Services Routers	Cisco IOS XE Amsterdam 17.3.2
	Cisco Cloud Services Router 1000v (Requires upgrade from a CSRv .bin image to a Catalyst 8000V software image.)	Cisco IOS XE Bengaluru 17.4.1
	Cisco Integrated Services Virtual Router (Requires upgrade from an ISRv .bin image to a Catalyst 8000V software image.)	Cisco IOS XE Bengaluru 17.4.1
Cisco Catalyst 8000 Edge Platforms Family		

Product Category	Product Series	Introductory Release When Support was Introduced
	Catalyst 8200 Series Edge Platforms	Cisco IOS XE Bengaluru 17.4.1
	Catalyst 8300 Series Edge Platforms	Cisco IOS XE Amsterdam 17.3.2
	Catalyst 8500 Series Edge Platforms	Cisco IOS XE Amsterdam 17.3.2
	Catalyst 8000V Edge Software	Cisco IOS XE Bengaluru 17.4.1
Cisco Terminal Services Gateways		
	Cisco 1100 Terminal Services Gateway	Cisco IOS XE Bengaluru 17.4.1

Architecture

This section explains the various components that can be part of your implementation of Smart Licensing Using Policy.

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, on page 2.

CSSM

Cisco Smart Software Manager (CSSM) 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.

You can access the CSSM Web UI at https://software.cisco.com. Under the **License** tab, click the **Smart Software Licensing** link.

In CSSM you can:

- Create, manage, or view virtual accounts.
- Transfer licenses between virtual accounts or view licenses.

- Transfer, remove, or view product instances.
- Run reports against your virtual accounts.
- Modify your email notification settings.
- View overall account information.

CSLU

Cisco Smart License Utility (CSLU) is a Windows-based reporting utility that provides aggregate licensing workflows while being connected to CSSM or in a disconnected mode. This utility performs the following 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 CSSM and receives authorization codes[1] from CSSM.

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

- Install the windows application, to use CSLU as a standalone tool that is connected to CSSM.
- Install the windows application, to use CSLU as a standalone tool that is disconnected from CSSM. With this option, the required usage information is downloaded to a file and then uploaded to CSSM. This is suited to air-gapped networks.
- Embedded (by Cisco) in a controller such as Cisco DNA Center.
- Deploy CSLU on a machine (laptop or desktop) running Linux.

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.

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 2: 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 3: 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 17.

SSM On-Prem

Smart Software Manager On-Prem (SSM On-Prem) is an asset manager, which works in conjunction with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM.

Information about the required software versions to implement Smart Licensing Using Policy with SSM On-Prem, is provided below:

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, on page 2

[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.

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 MSLA, on page 6.

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.

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 CSSM 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 26.

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 CSR 1000V and ISRv are offered under the Smart Licensing model. This is different from MSLA buying program for Catalyst 8000V Edge Software, which is offered under Smart Licensing Using Policy model. Service Providers running CSR 1000V and ISRv instances cannot perform inline upgrades to a Catalyst 8000V instance. It is NOT supported.

For migration from CSR 1000V or ISRv to Catalyst 8000V Edge Software, you must create new 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.

Concepts

This section explains the key concepts of Smart Licensing Using Policy.

License Enforcement Types

A given license belongs to one of three enforcement types. The enforcement type indicates if the license requires authorization before use, or not.

- Unenforced or Not Enforced

  The vast majority of licenses belong to this enforcement type. Unenforced licenses *do not* require authorization before use in air-gapped networks, or registration, in connected networks. The terms of use for such licenses are as per the end user license agreement (EULA).

- Enforced

Licenses that belong to this enforcement type require authorization before use. The required authorization is in the form of an authorization code, which must be installed in the corresponding product instance.

An example of an enforced license is the Media Redundancy Protocol (MRP) Client license, which is available on Cisco's Industrial Ethernet Switches.

- Export-Controlled

  Licences that belong to this enforcement type are export-restricted by U.S. trade-control laws and these licenses require authorization before use. The required authorization code must be installed in the corresponding product instance for these licenses as well. Cisco may pre-install export-controlled licenses when ordered with hardware purchase.

  An example of an export-controlled license is the High Security (HSECK9) license, which is available on certain Cisco Routers.

The list of enforced and export-controlled licenses is a limited one. Cisco may pre-install the necessary authorizations for export-controlled and enforced licenses when ordered with hardware purchase. See Table 4: License That Requires SLAC, on page 8 in the *Authorization Code* section for the complete and up-to-date list.

License Duration

This refers to the duration or term for which a purchased license is valid. A given license may belong to any one of the enforcement types mentioned above and be valid for the following durations:

- Perpetual: There is no expiration date for such a license.
- Subscription: The license is valid only until a certain date.

Authorization Code

The Smart Licensing Authorization Code (SLAC) allows activation and continued use of a license that is export-controlled or enforced. The authorization code is installed on the product instance. If an authorization code is required for the license you are using, you can request one from CSSM.

You can remove and return a SLAC to your CSSM license pool. But in order to do this, you must first disable the feature that uses the license. You cannot return a SLAC if it is in-use.

Table 4: License That Requires SLAC

Enforcement Type	License
Export-controlled	HSECK9
Enforced	MRP Client MRP Manager

In addition to the above licenses throughput greater than 250 Mbps (Tier 2 or a higher tier) requires SLAC.

Table 5: Throughput Level That Requires SLAC

Product Instance	Throughput Level that Requires SLAC	Additional Considerations
Cisco 4000 Series Integrated Services Routers Cisco 1100 Terminal Services Gateway	Encrypted throughput *greater* than 250 Mbps	If the product instance already has one of the following, then you do not have to install SLAC again: • SLAC for an HSECK9 license • HSECK9 PAK license • SLR authorization code including an HSECK9 license
Cisco 1000 Series Integrated Services Routers Catalyst 8200 Series Edge Platforms Catalyst 8300 Series Edge Platforms Catalyst 8500 Series Edge Platforms Catalyst 8000V Edge Software	Encrypted throughput *greater* than 250 Mbps	
Catalyst 8000V Edge Software (Also applicable to Cisco Cloud Services Router 1000v and Cisco Integrated Services Virtual Routers, which require a Catalyst 8000V software image from Cisco IOS XE Bengaluru 17.4.1)	Encrypted and unencrypted throughput (combined) *greater* than 250 Mbps	

Note If you are upgrading from an earlier licensing model to Smart Licensing Using Policy, you may have one of these licenses, each having its own authorization code: Specific License Reservation (SLR), or Product Activation Key (PAK), Permanent License Reservation (PLR).

The SLR authorization code is supported after upgrade to Smart Licensing Using Policy.

If you have a PAK-fulfilled license, see Snapshots for PAK Licenses , on page 40, complete the necessary tasks to continue using a PAK-fulfilled license.

If you have a Permanent License Reservation (PLR) authorization code, and you want to continue using it, see: Permanent License Reservation in the Smart Licensing Using Policy Environment, on page 42.

Policy

A policy provides the product instance with these reporting instructions:

- License usage report acknowledgement requirement (Reporting ACK required): The license usage report is known as a RUM Report and the acknowledgement is referred to as an ACK (See RUM Report and Report Acknowledgement). This is a yes or no value which specifies if the report for this product instance requires CSSM acknowledgement or not. The default policy is always set to “yes”.

- First report requirement (days): The first report must be sent within the duration specified here.

  If the value here is zero, no first report is required.

- Reporting frequency (days): The next RUM report must be sent within the duration specified here.

  If the value here is zero, it means no further reporting is required *unless* there is a usage change.

- Report on change (days): In case of a change in license usage, a report must be sent within the duration specified here.

  If the value here is zero, no report is required on usage change.

  If the value here is not zero, reporting *is* required after the change is made. All the scenarios listed below count as changes in license usage on the product instance:

  - Changing licenses consumed (includes changing to a different license, and, adding or removing a license).
  - Going from consuming zero licenses to consuming one or more licenses.
  - Going from consuming one or more licenses to consuming zero licenses.

Note If a product instance has *never* consumed a license, reporting is not required even if the policy has a non-zero value for any of the reporting requirements (First report requirement, Reporting frequency, Report on change).

Understanding Policy Selection

CSSM determines the policy that is applied to a product instance. Only one policy is in use at a given point in time. The policy and its values are based on a number of factors, including the licenses being used.

`Cisco default` is the default policy that is always available in the product instance. If no other policy is applied, the product instance applies this default policy. The table below (Table 6: Policy: Cisco default, on page 11) shows the `Cisco default` policy values.

While you cannot configure a policy, you can request for a customized one, by contacting the Cisco Global Licensing Operations team. Go to Support Case Manager. Click **OPEN NEW CASE** > Select **Software Licensing**. The licensing team will contact you to start the process or for any additional information. Customized policies are also made available through your Smart account in CSSM.

Note To know which policy is applied (the policy in-use) and its reporting requirements, enter the **show license all** command in privileged EXEC mode.

Table 6: Policy: Cisco default

Policy: `Cisco default`	**Default Policy Values**
Export (Perpetual/Subscription) **Note** Applied only to licenses with enforcement type "Export-Controlled".	Reporting ACK required: Yes First report requirement (days): 0 Reporting frequency (days): 0 Report on change (days): 0
Enforced (Perpetual/Subscription) **Note** Applied only to licenses with enforcement type "Enforced".	Reporting ACK required: Yes First report requirement (days): 0 Reporting frequency (days): 0 Report on change (days): 0
Unenforced/Non-Export Perpetual[8]	Reporting ACK required: Yes First report requirement (days): 365 Reporting frequency (days): 0 Report on change (days): 90
Unenforced/Non-Export Subscription	Reporting ACK required: Yes First report requirement (days): 90 Reporting frequency (days): 90 Report on change (days): 90

[8] For Unenforced/Non-Export Perpetual: the default policy’s first report requirement (within 365 days) applies only if you have purchased hardware or software from a distributor or partner.

RUM Report and Report Acknowledgement

A Resource Utilization Measurement report (RUM report) is a license usage report, which fulfils reporting requirements as specified by the policy. RUM reports are generated by the product instance and consumed by CSSM. The product instance records license usage information and all license usage changes in an open RUM report. At system-determined intervals, open RUM reports are closed and new RUM reports are opened to continue recording license usage. A closed RUM report is ready to be sent to CSSM.

A RUM acknowledgement (RUM ACK or ACK) is a response from CSSM and provides information about the status of a RUM report. Once the ACK for a report is available on the product instance, it indicates that the corresponding RUM report is no longer required and can be deleted.

The reporting method, that is, how a RUM report is sent to CSSM, depends on the topology you implement.

CSSM displays license usage information as per the last received RUM report.

A RUM report may be accompanied by other requests, such as a trust code request, or a SLAC request. So in addition to the RUM report IDs that have been received, an ACK from CSSM may include authorization codes, trust codes, and policy files.

The policy that is applied to a product instance determines the following aspects of the reporting requirement:

- Whether a RUM report is sent to CSSM and the maximum number of days provided to meet this requirement.
- Whether the RUM report requires an acknowledgement (ACK) from CSSM.
- The maximum number of days provided to report a change in license consumption.

RUM report generation, storage, and management

Starting with Cisco IOS XE Cupertino 17.7.1, RUM report generation and related processes have been optimized and enhanced as follows:

- You can display the list of all available RUM reports on a product instance (how many there are, the processing state each one is in, if there are errors in any of them, and so on). This information is available in the show license rum, show license all, show license tech privileged EXEC commands.
- RUM reports are stored in a new format that reduces processing time, and reduces memory usage. In order to ensure that there are no usage reporting inconsistencies resulting from the difference in the old and new formats, we recommend that you send a RUM report in the method that will apply to your topology, in these situations:

  When you upgrade from an earlier release supporting Smart Licensing Using Policy, to Cisco IOS XE Cupertino 17.7.1 or a later release.

  When you downgrade from Cisco IOS XE Cupertino 17.7.1 or a later release to an earlier release supporting Smart Licensing Using Policy.
- To ensure continued disk space and memory availability, the product instance detects and triggers deletion of RUM reports that are deemed eligible.

Trust Code

A *UDI-tied public key*, which the product instance uses to

- Sign a RUM report. This prevents tampering and ensures data authenticity.
- Enable secure communication with CSSM.

There are multiple ways to obtain a trust code.

- From Cisco IOS XE Cupertino 17.7.1a, a trust code is factory-installed for all new orders.

Note A factory-installed trust code cannot be used for *communication* with CSSM.

- A trust code can obtained from CSSM, using an ID token.

  Here you 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. If a product instance is directly connected to CSSM, use this method to enable the product instance to communicate with CSSM in a secure manner. This method of obtaining a trust code is applicable to all the options of directly connecting to CSSM. For more information, see Connected Directly to CSSM, on page 15.

- From Cisco IOS XE Cupertino 17.7.1, a trust code is automatically obtained in topologies where the product instance initiates the sending of data to CSLU and in topologies where the product instance is in an air-gapped network.

  From Cisco IOS XE Cupertino 17.9.1a, a trust code is automatically obtained in topologies where CSLU initiates the retrieval of data from the product instance.

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

  Refer to the corresponding topology description and workflow to know how the trust code is requested and installed in each scenario: Supported Topologies, on page 13.

If a trust code is installed on the product instance, the "Trust Code Installed" field in the output of the **show license status** command displays an updated timestamp. For example: `Trust Code Installed: Oct 09 17:56:19 2020 UTC`.

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

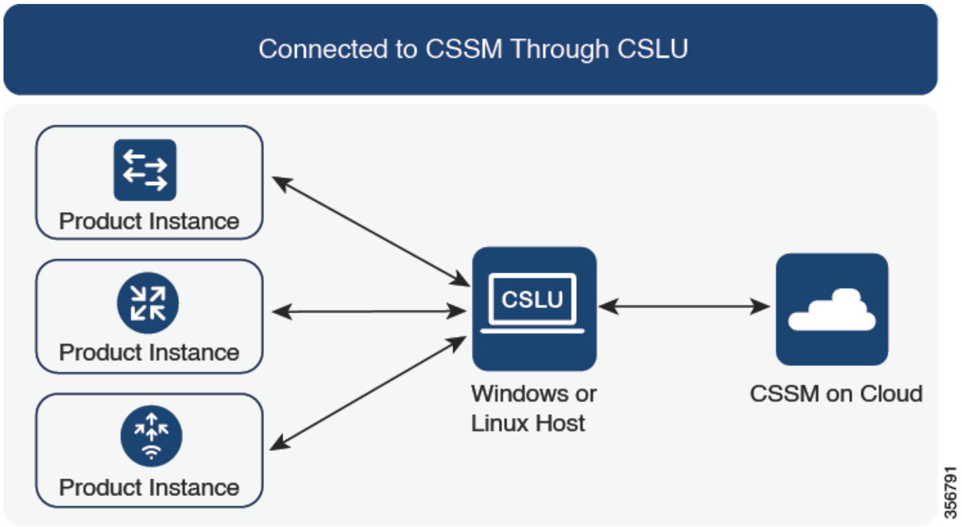
Overview:

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, on page 12.

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.

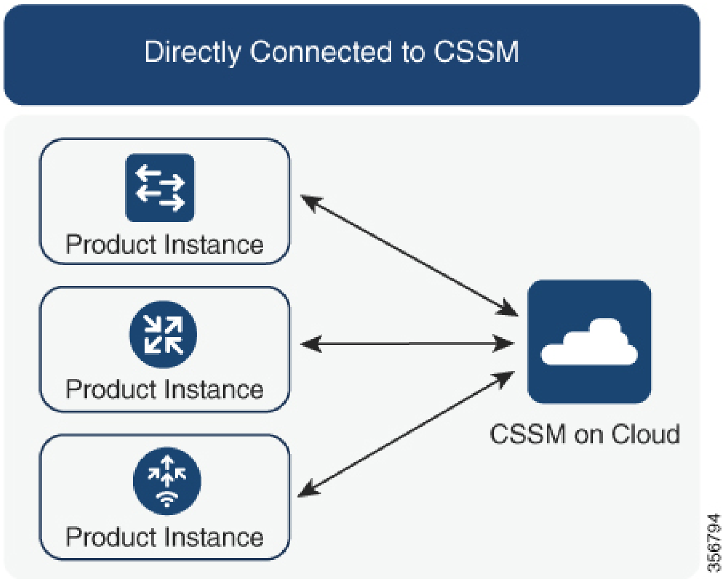
  - Smart transport through an HTTPs proxy: In this method, a product instance uses a proxy server to communicate with the licensing server, and eventually, CSSM.

- 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.

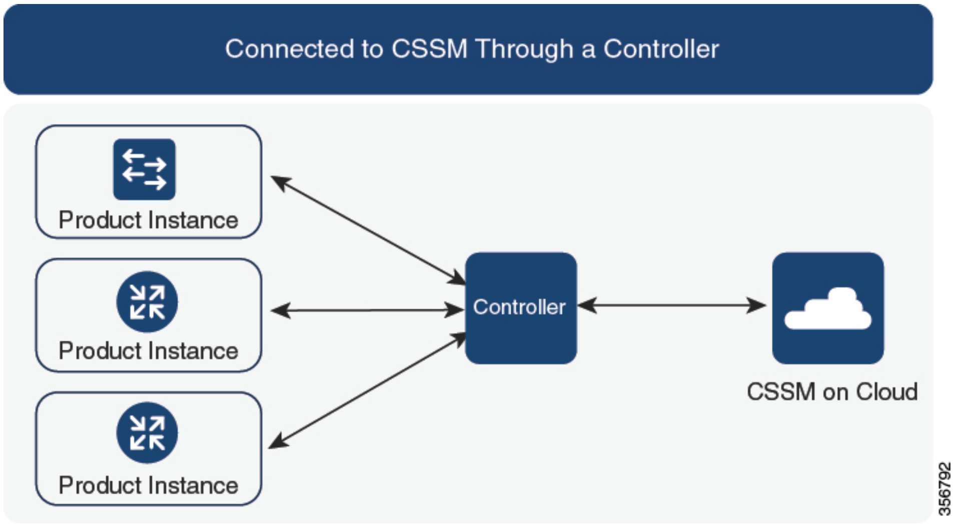
Where to Go Next:

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.

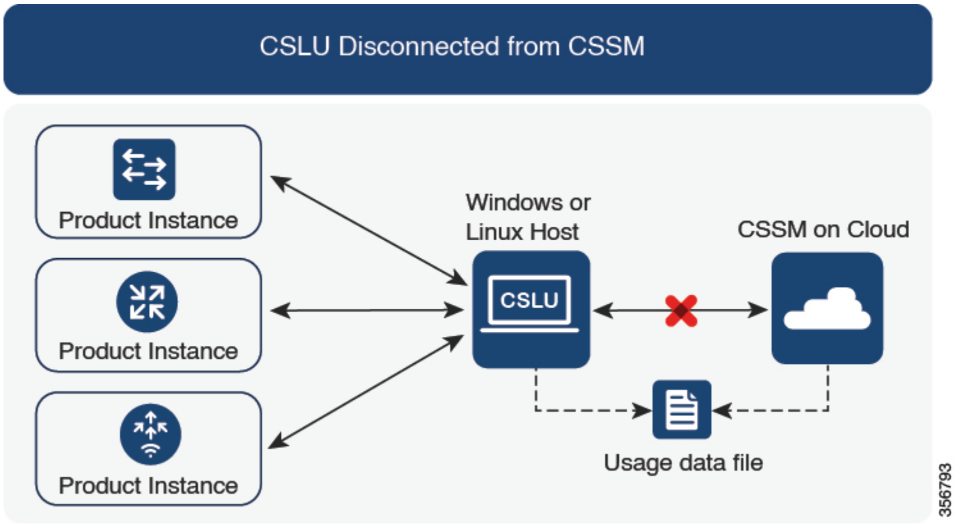
CSLU Disconnected from CSSM

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:

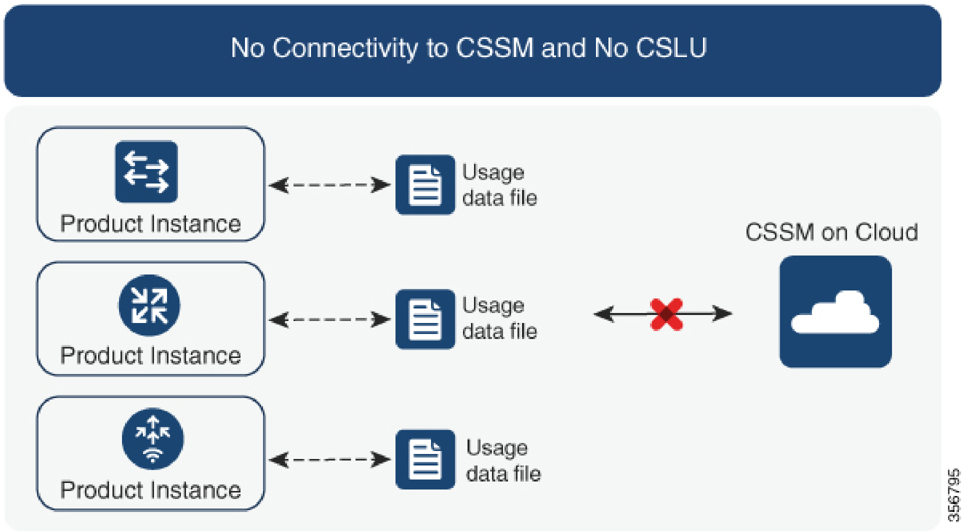
To implement this topology, see Workflow for Topology: CSLU Disconnected from CSSM.

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.

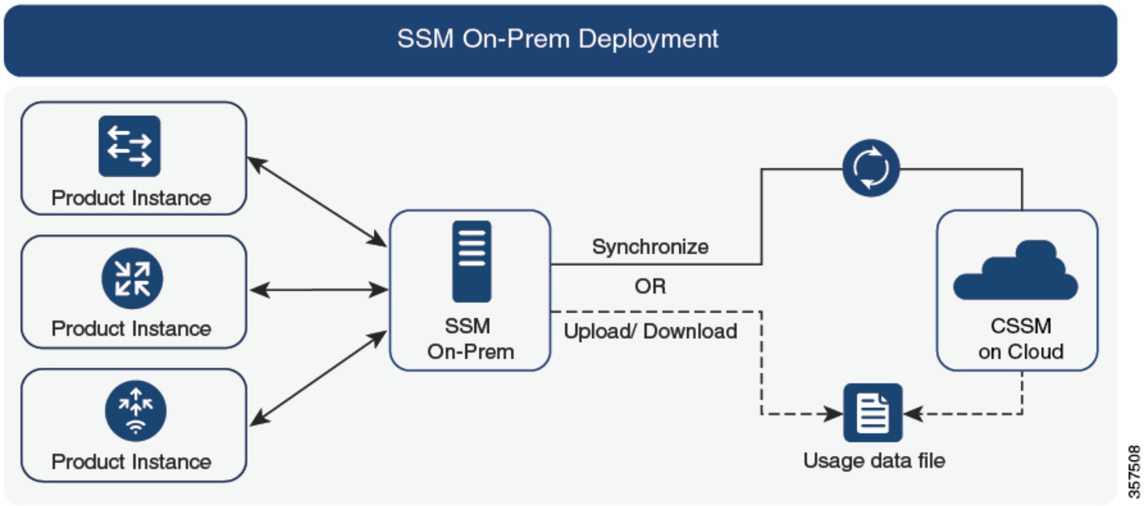
In SSM On-Prem, the reporting interval is set to the default policy on the product instance. You can change this, but only to report more frequently (a narrower interval), or you can install a custom policy if available.

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 15.

- 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 13, or CSLU Disconnected from CSSM, on page 20

- 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 23

- 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 21

Note A product instance using post-paid licenses must send RUM reports and install a RUM Report and Report Acknowledgement 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.

Workflow for Topology: Connected Directly to CSSM

Workflow for Topology: Connected to CSSM Through CSLU

Workflow for Topology: CSLU Disconnected from CSSM

Workflow for Topology: No Connectivity to CSSM and No CSLU

Workflow for Topology: SSM On-Prem Deployment

Interactions with Other Features

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[9] (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[10], 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.

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.

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

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.

Upgrades

This section explains the following aspects:

- Migrating from earlier licensing models to Smart Licensing Using Policy.

  After you upgrade from any earlier licensing model, to a software image that supports Smart Licensing Using Policy, Smart Licensing Using Policy is the only supported licensing model and the product instance continues to operate without any licensing changes. However, there may be other settings that you have to configure, to ensure all aspects of the licensing workflow continue to work as expected. This section provides an overview of such changes. The Migrating to Smart Licensing Using Policy section provides examples of migration scenarios.

- Upgrading in the Smart Licensing Using Policy environment - where the software version you are upgrading from and the software version you are upgrading to, both support Smart Licensing Using Policy.

Identifying the Current Licensing Model Before Upgrade

Before you upgrade to Smart Licensing Using Policy, if you want to know the current licensing model that is effective on the product instance, enter the **show license all** command in privileged EXEC mode. This command displays information about the current licensing model for all except the RTU licensing model. The

show license right-to-use privileged EXEC command displays license information only if the licensing model is RTU.

How Upgrade Affects Enforcement Types for Existing Licenses

When you upgrade to a software version which supports Smart Licensing Using Policy, the way existing PLR, SLR, CSL, PAK, and RTU licenses are handled, depends on the enforcement type:

- An **unenforced** license that was being used before upgrade, continues to be available after the upgrade.

  If you are using a PAK license, ensure that you are familiar with the changes in the way the system handles a PAK license and the options available to you. For detailed information, see: Snapshots for PAK Licenses , on page 40.

- An **enforced** license that was being before upgrade, continues to be available after upgrade if the required authorization exists. This is authenticated by the system on upgrade. If the requisite authorization does not exist, you must install a SLAC before use. See Manually Requesting and Auto-Installing a SLAC.

- An **export-controlled** license that was being used before upgrade, does, in general, continue to be available after upgrade if the required authorization exists.

  However, there is an exception: Prior to upgrade, if a product instance was registered to a Smart Account and had only the export-control flag in CSSM enabled to allow throughput greater than 250 Mbps - and not an export-controlled license (HSECK9) license, you may have to perform a few more steps as part of the migration to Smart Licensing Using Policy. This is because *U.S. export control regulations no longer allow the use of only the export control flag as a way of authorizing throughput greater than 250 Mbps.*

  - For a virtual product instance (A Cisco Cloud Services Router 1000v [CSR 1000v] or a Cisco Integrated Services Virtual Router [ISRv]), with throughput greater than 250 Mbps and with only the export-control flag enabled in CSSM, proceed as per the requirements for your set-up:

    - CSR 1000v or ISRv with throughput greater than 250 Mbps, in an SLR set-up: First update the SLR authorization code to include an applicable HSECK9 license and only then upgrade the product instance. This ensures uninterrupted throughput after upgrade.

Note In this scenario, if you upgrade the software image without updating the SLR authorization code to include an HSEK9 license first, the system sets the throughput to 250 Mbps after upgrade to Smart Licensing Using Policy - until SLAC is installed. Immediately after SLAC is installed, the system restores the value that you last configured.

      For the product-specific HSECK9 license name information, see HSECK9 License Mapping Table for Routing Product Instances. For a sample migration scenario, see Example: Smart Licensing (SLR With Throughput >250 Mbps, Without Export-Controlled License) to Smart Licensing Using Policy

    - CSR 1000v or ISRv with throughput greater than 250 Mbps, connected to CSSM and in autonomous mode: Ensure that the throughput of greater than 250 Mbps is part of start-up configuration. Also ensure that you have a positive balance of the applicable HSECK9 license in the corresponding Smart Account and Virtual Account in CSSM. No further pre-upgrade action is required. As long as the product instance is connected to CSSM, on upgrade, the product instance will automatically trigger the HSECK9 request and install SLAC.

- For a physical product instance (a Cisco 1000 Series Integrated Services Router (ISR 1000) or Cisco 4000 Series Integrated Services Router (ISR 4000) or Cisco 1000 Series Aggregation Services Router (ASR 1000)) with throughput greater than 250 Mbps, with only the export-control flag in CSSM, connected to CSSM and in autonomous mode: Ensure that the **license feature hseck9** command is configured in the start-up configuration, and you have a positive balance of the applicable HSECK9 license in the corresponding Smart Account and Virtual Account in CSSM. No further pre-upgrade action is required. As long as the product instance is connected to CSSM on upgrade, the product instance will automatically trigger the HSECK9 request and install SLAC.
- For physical or virtual product instances, with throughput greater than 250 Mbps with only the export-control flag in CSSM, operating in the SD-WAN controller mode: you must request and install SLAC after upgrade. After upgrade complete Generating and Downloading SLAC from CSSM to a File and then Installing a File on the Product Instance.

By contrast, note the following scenarios where an export-controlled license in the earlier licensing environment does not require you install a SLAC again after upgrade:

- If a product instance (such as a Cisco 1000 Series Integrated Services Router or a Cisco 4000 Series Integrated Services Router) had an HSECK9 license registered to a Smart Account, and had the export-control flag enabled in CSSM, the authorization code is honoured after upgrade to Smart Licensing Using Policy. You only have to synchronize license usage information with CSSM after upgrade. You do not have to install a SLAC again. See Example: Smart Licensing (Registered and Authorized Licenses) to Smart Licensing Using Policy.
- If a product instance had an HSECK9 PAK license before upgrade, you do not have to install a SLAC again after upgrade. See Example: Cisco Software Licensing (PAK Licenses) to Smart Licensing Using Policy.

  If you are using a PAK license, ensure that you are familiar with the changes in the way the system handles a PAK license and the options available to you. For detailed information, see: Snapshots for PAK Licenses , on page 40.
- If a product instance had an SLR authorization code that included an HSECK9 license, in such cases the license will be honoured after upgrade to Smart Licensing Using Policy, you do not have to install a SLAC again. See Example: Smart Licensing (SLR with Export-Controlled License) to Smart Licensing Using Policy.

How Upgrade Affects Reporting for Existing Licenses

Existing License	Reporting Requirements After Migration to Smart Licensing Using Policy
Right-to-Use (RTU)	Depends on the license being used. After migration and deployment of a supported topology, in output of the **show license usage** command, refer to the `Next ACK deadline` field to know if and when reporting is required.
Smart Licensing (Registered and Authorized license)	Depends on the policy.
Specific License Reservation (SLR)	Required only if there is a change in license consumption. An existing SLR authorization code authorizes existing license consumption after upgrade to Smart Licensing Using Policy.

Existing License	Reporting Requirements After Migration to Smart Licensing Using Policy
Product Authorization Keys (PAK)	Required only if there is a change in license consumption. PAK licenses have perpetual validity, but reporting is required if there is a change in license consumption. Also ensure that you are familiar with the changes in the way the system handles a PAK license and the options available to you. For detailed information, see: Snapshots for PAK Licenses , on page 40.
Permanent License Reservation (PLR)	Not required. PLR licenses have perpetual validity, and reporting is not required even if there is a change in license consumption.
Cisco Software Licensing (CSL)	Not required. CSL licenses have perpetual validity, and reporting is not required even if there is a change in license consumption.
Evaluation or expired licenses	Based on the reporting requirements of the Cisco default policy.

How Upgrade Affects Transport Type for Existing Licenses

The transport type, if configured in your existing set-up, is retained after upgrade to Smart Licensing Using Policy.

When compared to the earlier version of Smart Licensing, additional transport types are available with Smart Licensing Using Policy. There is also a change in the default transport mode. The following table clarifies how this may affect upgrades:

Transport type Before Upgrade	License or License State Before Upgrade	Transport Type After Upgrade
Default (callhome)	evaluation	cslu (default in Smart Licensing Using Policy)
	SLR PLR	off
	registered	callhome
smart	evaluation	off
	SLR PLR	off
	registered	smart
Not applicable For example, if the existing licensing model is RTU or PAK.	Not applicable For example, if the existing licensing model is RTU or PAK.	cslu

How Upgrade Affects the Token Registration Process

In the earlier version of Smart Licensing, a token was used to register and connect to CSSM. ID token *registration* is not required in Smart Licensing Using Policy. The token generation feature is still available in CSSM, and is used to *establish trust*, in certain topologies in the Smart Licensing Using Policy environment.

In-Service Software Upgrade

When you upgrade from one release to another, by using the ISSU method, enforcement, reporting, and transport aspects follow the same rules as with a regular upgrade (described above).

No additional considerations relating to Smart Licensing Using Policy, apply.

Upgrades Within the Smart Licensing Using Policy Environment

This section covers any release-specific considerations or actions that apply when you upgrade the product instance from one release where Smart Licensing Using Policy is supported to another release where Smart Licensing Using Policy is supported.

Starting with Cisco IOS XE Cupertino 17.7.1a, RUM reports are stored in a format that reduces processing time. In order to ensure that there are no usage reporting inconsistencies resulting from the differences in the old and new formats, we recommend completing one round of usage reporting as a standard practice when upgrading from an earlier release that supports Smart Licensing Using Policy, to Cisco IOS XE Cupertino 17.7.1a or a later release.

Downgrades

This section provides information about downgrades to an earlier licensing model. It also covers information relevant to downgrades within the Smart Licensing Using Policy environment.

New Deployment Downgrade

This section describes considerations and actions that apply if a newly purchased product instance with a software version where Smart Licensing Using Policy is enabled by default, is downgraded to a software version where Smart Licensing Using Policy is not supported.

The outcome of the downgrade depends on whether a trust code (Trust Code, on page 12) was installed while still operating in the Smart Licensing Using Policy environment, and further action may be required depending on the release you downgrade to.

If the topology you implemented while in the Smart Licensing Using Policy environment was "Connected Directly to CSSM", then a trust code installation can be expected or assumed, because it is required as part of topology implementation. For any of the other topologies, trust establishment is not mandatory. Downgrading product instances with one of these other topologies will therefore mean that you have to restore licenses to a registered and authorized state by following the procedures that are applicable in the Smart Licensing environment. See the table below.

- If trust was established while in the Smart Licensing Using Policy environment, the product instance attempts to renew trust with CSSM after downgrade.

  After a successful renewal, licenses are in a registered state and the earlier version of Smart Licensing is effective on the product instance.

- If trust was *not* established while in the Smart Licensing Using Policy environment, licenses on the product instance are in evaluation mode after downgrade, and the earlier version of Smart Licensing is effective on the product instance.

Downgrades Within the Smart Licensing Using Policy Environment

This section covers any release-specific considerations or actions that apply when you downgrade the product instance from one release where Smart Licensing Using Policy is supported to another release where Smart Licensing Using Policy is supported.

Starting with Cisco IOS XE Cupertino 17.7.1a, RUM reports are stored in a format that reduces processing time. In order to ensure that there are no usage reporting inconsistencies resulting from the differences in the old and new formats, we recommend completing one round of usage reporting as a standard practice when downgrading from Cisco IOS XE Cupertino 17.7.1a or a later release to an earlier release supporting Smart Licensing Using Policy.

Changes in Traditional Licenses

This section explains the changes that certain traditional licenses are undergoing, to continue to be supported in the Smart Licensing Using Policy environment. These changes may involve actions that the system performs automatically, actions that you must perform, or both, and have been called out accordingly.

Phasing Out of Device-Specific HSECK9 Licenses

HSECK9 licenses are supported on various Cisco Aggregation, Integrated Services, and Cloud Services Routers. On Cisco 1000 Series Integrated Services Routers and Cisco 4000 Series Integrated Services Routers, the license name is tagged according to the router model (For example, a Cisco 4461 Integrated Services Router that is using an HSECK9 license, uses “ISR_4400_Hsec”).

This section explains what is changing for these device-specific HSECK9 licenses, how it affects you, actions (if any) that you may have to take, and the options available to you as device-specific HSECK9 license holder.

For the list of device-specific HSECK9 licenses, see HSECK9 License Mapping Table for Routing Product Instances.

What is Changing for Device-Specific HSECK9 Licenses

Device-specific HSECK9 licenses that are available on Cisco 1000 Series Integrated Services Routers and Cisco 4000 Series Integrated Services Routers, are being phased-out to simplify HSECK9 license management.

Starting with Cisco IOS XE Bengaluru 17.6.1a, instead of tagging HSECK9 licenses according to router model (for example, ISR_4331_Hsec), HSECK9 licenses are tagged as *Router US Export Lic for DNA (DNA_HSEC)*. If you want to purchase new HSECK9 licenses for these products, you should buy DNA_HSEC.

If the software version running on the product instance is Cisco IOS XE Bengaluru 17.6.1a or later, it has the following implications:

- A device-specific HSECK9 license that is already IN-USE, continues to be supported and no further action is required.

- An *unused* device-specific HSECK9 license in the Smart Account and Virtual Account in CSSM can still be used on the product instance. Mutiple options are available and you can proceed with the suitable one. For more information, see the Available Options for an HSECK9 License section below.

For more information about ordering an HSECK9 license, see: Ordering Information for HSECK9 Licenses.

Product Instances Affected by this Change

Cisco 1000 Series Integrated Services Routers and Cisco 4000 Series Integrated Services Routers

Available Options for an HSECK9 License

The following table provides information about the options available to you as the holder of an unused device-specific HSECK9 license. It also covers additional scenarios where no action is required but have been provided for the purpose of clarification or confirmation.

Clarifications and definitions for important terms and abbreviations used in the tables below:

- Device-specific HSECK9 license: refers to HSECK9 license name that is tagged to the device model
- DNA_HSEC: Router US Export Lic for DNA
- Honor (HSECK9 license): Means if the HSECK9 format exists on the product instance, then HSECK9 or export-controlled functionality is allowed. But you cannot install a new HSECK9 license in that form.
- SLP: Smart Licensing Using Policy
- SL: Smart License.
- PAK: Product Activation Key

Table 7: Available Options for an HSECK9 License

Current State	HSECK9 Entitlement-Type in CSSM	Current Software Version on the Product Instance	Result and Required Action If Applicable
Product instance is not using an HSECK9 license	Device-specific HSECK9 license	Cisco IOS XE Bengaluru 17.6.1a or later	If you want to use an HSECK9 license, choose one of the following options: • **Option 1**: Install SLAC for device-specific HSECK9 license in offline mode. Complete: Generating and Downloading SLAC from CSSM to a File and Installing a File on the Product Instance. • **Option 2**: Purchase DNA-HSEC-UPGD= at 0 USD from CCW, convert device-specific HSECK9 license to DNA_HSEC, and install SLAC to use DNA_HSEC. Complete: Converting a Device-Specific HSECK9 License, and then request and install SLAC for DNA_HSEC according to the topology you have implemented. • **Option 3**: **1.** Downgrade to any release between 17.3.x and 17.5.x. **2.** Install SLAC for the device-specific HSECK9 license according to the topology you have implemented. **3.** Revert to Cisco IOS XE Bengaluru 17.6.1a or later release.
Product instance is not using an HSECK9 license	DNA_HSEC	Cisco IOS XE Bengaluru 17.6.1a or later	If you want to use an HSECK9 license, install SLAC for DNA_HSEC according to the topology you have implemented.
Product instance is not using an HSECK9 license	Device-specific HSECK9 license	Any release between Cisco IOS XE Amsterdam 17.3.2 and Cisco IOS XE Bengaluru 17.5.x	If you want to use an HSECK9 license, install SLAC for the device-specific HSECK9 license according to the topology you have implemented.

Current State	HSECK9 Entitlement-Type in CSSM	Current Software Version on the Product Instance	Result and Required Action If Applicable
Product instance is using an HSECK9 PAK license or an SLR authorization code including an HSECK9 license.	Device-specific HSECK9 license or DNA_HSEC	Cisco IOS XE Amsterdam 17.3.1 or any earlier release	If you want to upgrade to Cisco IOS XE Amsterdam 17.3.2 or a later release: No further action required. Device-led conversion (DLC) is automatically triggered on upgrade and the HSECK9 PAK license or the SLR authorization code including an HSECK9 license is honored.
Product instance is using an HSECK9 license.	Device-specific HSECK9 license or DNA_HSEC	Cisco IOS XE Amsterdam 17.3.4 or later release in the 17.3.x train (>=17.3.4). or Cisco IOS XE Bengaluru 17.4.2 or later release of the 17.4.x train (>=17.4.2). or Cisco IOS XE Bengaluru 17.5.x (17.5.x)	No further action required. The HSECK9 license that is being used is honored.

Current State	HSECK9 Entitlement-Type in CSSM	Current Software Version on the Product Instance	Result and Required Action If Applicable
Product instance is *not* using an HSECK9 license	DNA_HSEC	>=17.3.4, or >=17.4.2, or 17.5.x	If DNA_HSEC is the entitement type in the CSSM, this means the device was ordered with software version 17.6.1a or later in CCW. Further, if DNA_HSEC is purchased with hardware, SLAC is factory-installed. But if it is not, ensure that you install SLAC in one of the following ways (choose one option): • **Option 1**: Install SLAC for the DNA_HSEC license in offline mode. Complete: Generating and Downloading SLAC from CSSM to a File and Installing a File on the Product Instance • **Option 2**: **1.** Upgrade to Cisco IOS XE Bengaluru 17.6.1a or a later release. **2.** Install SLAC for DNA_HSEC according to the topology you have implemented **3.** Revert (downgrade) to the required release.

Current State	HSECK9 Entitlement-Type in CSSM	Current Software Version on the Product Instance	Result and Required Action If Applicable
SLAC may or may not be installed	DNA_HSEC	Cisco IOS XE Everest 16.10.1a to Cisco IOS XE Amsterdam 17.3.1	**Note** Although available as an option, we do NOT recommend this conversion since the releases involved are end of software maintenance. If you want to convert DNA_HSEC licenses to device-specific HSECK9 license, complete this process: **1.** Go to Support Case Manager. Click **OPEN NEW CASE** > Select **Software Licensing**. Provide a reason for downgrade and a proof of purchase of the existing HSEC license. **2.** The support team will contact you and request you to raise a purchase order for device-specific HSECK9 spares (For example, FL-4330-HSEC-K9= for ISR4330), with 100 percent discount. **3.** The support team revokes the same number of DNA_HSEC licenses as in purchase order. The support team also processes the request including seeking internal approvals for the discount. Once approved, the order goes through. **4.** The applicable number of device-specific HSECK9 licenses are deposited in your Smart Account and Virtual Account in CSSM.

Current State	HSECK9 Entitlement-Type in CSSM	Current Software Version on the Product Instance	Result and Required Action If Applicable
SLAC may or may not be installed	Device-specific HSECK9 license	Cisco IOS XE Fuji 16.9.x	**Note** Although available as an option, we do NOT recommend this conversion since the releases involved are end of software maintenance. If you want to convert the device-specific HSECK9 licenses to PAK HSECK9 licenses, open a case. Go to Support Case Manager. Click **OPEN NEW CASE** > Select **Software Licensing**. The support team will contact you to start the process or for any additional information.

Table 8: Licensing Model Where HSECK9 License is Used and Release Matrix

Release	Licensing Model Available with the Release	PAK HSECK9 Supported?	SLR inclu Supported
<=16.9	PAK	Yes	Not applic
16.10.1a – 17.3.1	SL	Honor	Yes
17.3.2-17.3.3, 17.4.1	SLP	Honor	Honor
>=17.3.4, >=17.4.2,17.5.x,	SLP	Honor	Honor
>=17.6.1a	SLP	Honor	Honor

Snapshots for PAK Licenses

There is a significant change in the way Product Activation Key (PAK) licenses are handled by the system. This section explains the change, how it affects you, actions (if any) that you may have to take, and the options available to you as a PAK license holder.

What is a PAK License

A license issued by using PAK fulfilment is called a PAK license. For example, an “adventerprise” license available on Cisco ASR 1000 can be PAK-fulfilled, a “securityk9” license, which is available on a Cisco 4000 Series ISR can also be PAK fulfilled. Similarly, an HSECK9 license which is available on various Cisco routers, can be PAK-fulfilled.

What is Changing for PAK Licenses - Snapshots for PAK Licenses

Starting with Cisco IOS XE Dublin 17.11.1a, the library that manages PAK licenses is deprecated from the software image.

In order to support and honor any existing PAK licenses, the system automatically performs the following actions in *select* release trains:

- The system takes a snapshot of the PAK license. This snapshot serves as a permanent record of the PAK license - as it is, at the time of the snapshot.
- The system automatically triggers a Device-Led Conversion (DLC) process. After DLC, the PAK-fulfilled license is available in your Smart Account.

  For information about the DLC process, see: After Upgrading the Software Version. DLC is triggered for all topologies in the Smart Licensing Using Policy environment.

The system takes snapshots for a PAK license and automatically triggers DLC only in and until the following releases and trains:

- Cisco IOS XE Amsterdam 17.3.5 and later releases of the 17.3.x train.
- Cisco IOS XE Bengaluru 17.6.2 and later releases of the 17.6.x train.
- All releases of subsequent trains: Cisco IOS XE Cupertino 17.7.x, Cisco IOS XE Cupertino 17.8.x, Cisco IOS XE Cupertino 17.9.x, and until Cisco IOS XE Dublin 17.10.x.

⚠

Caution Starting with Cisco IOS XE Dublin 17.11.1a, the PAK-managing library is discontinued and the provision to ***take*** a snapshot is no longer available. DLC is not available either. Software images from Cisco IOS XE Dublin 17.11.1a onwards rely only on the snapshotted information about PAK licenses.

If you have a PAK license without a snapshot, and you want to upgrade to Cisco IOS XE Dublin 17.11.1a or a later release, you will have to upgrade twice. First upgrade to one of the above-mentioned releases where the system can take a snapshot of the PAK license and complete DLC, and then again upgrade to the required, later release.

Only permanent PAK licenses are honored; any evaluation PAK licenses are not.

Once a snapshot is taken, any changes to the PAK license are not supported. Even if you downgrade the software version (after the snapshot is taken) to an earlier release, make a change in the PAK license (including trying to return it), and then revert to the later release, the PAK license change is not supported.

To know if the PAK license on a product instance has been snapshotted, enter the **show platform software sl-infra pak-info** command in privileged EXEC mode. If a snapshot has been taken, the following information is displayed in the command's output:

```
Device# show platform software sl-infra pak-info
<output truncated>

Pak License Snapshot Information
=================================
Platform Supports PAK License snapshot
PAK License Snapshot integrity check pass
PAK License Snapshot available

<output truncated>
```

Product Instances that Support PAK Licenses

The following product instances support PAK licenses. If you are using one of these product instances and a PAK license is being used on the product instance, refer to the *Available Options for a PAK License* section, to know more about what you can do.

- Cisco 1000 Series Integrated Services Routers
- Cisco 4000 Series Integrated Services Routers
- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco Cloud Services Router 1000v
- Catalyst 8000V Edge Software (Only if it is a Cloud Services Router 1000v on which a .bin upgrade to Cisco IOS XE Bengaluru 17.4.1 or a later release has been performed)

Available Options for a PAK License

If you have a PAK license, you can proceed in the following ways:

Note If there are multiple PAK licenses on the product instance, either continue using *all* of them or remove and return *all* of them. If you forsee the need for changes in the PAK licenses you have, remove all the PAKs license and start afresh by configuring Smart licenses on the product instance.

- If you have a PAK license and you want to continue using it on the product instance, *without making any changes*, see: Continue Using a PAK License.
- If you have a PAK license on a product instance and you want to remove it, see: Removing a PAK License.
- If you have a PAK license on a failed product instance, and you want to return or remove the license, see: Removing a PAK License on a Failed Product Instance.

Permanent License Reservation in the Smart Licensing Using Policy Environment

What is a Permanent License Reservation

A Permanent License Reservation (PLR) enables you to use an unlimited count of any license on the product instance. The PLR code is an authorization code generated by CSSM that must installed on the product instance in order to authorise any license request.

A PLR is suited to a high-security deployment or entirely air-gapped networks where a product instance cannot communicate online, with anything outside its network.

PLR Requirements in the Smart Licensing Using Policy Environment

The use of PLR in the Smart Licensing Using Policy environment requires:

- Software version Cisco IOS XE Dublin 17.10.1a or later.

- Version 3 of the PLR code.

Product Instances that Support PLR in the Smart Licensing Using Policy Environment

- Catalyst 8000V Edge Software
- Cisco Cloud Services Router 1000v (Has been .bin upgraded from a CSRv image to a Catalyst 8000V software image)

How an Existing PLR is Handled - Upgrade and Downgrade

Current Setup	**Condition** **(If This Action is Performed)**	**Result and Implication**
Product Instance: Cisco Cloud Services Router 1000v PLR status: PLR is activated. An older version of the PLR code installed (Version 1 or Version 2). Software version: Cisco IOS XE Everest 16.5.x to Cisco IOS XE Amsterdam 17.3.x.	You perform a .bin upgrade to software version *Cisco IOS XE Dublin 17.10.1a or later* release.	All existing features that have been enabled are honored and continue to work - except for throughput greater than 250 Mbps, and any export-controlled features that require an HSECK9 license. The older version of the PLR code is not removed from the product instance, but it is not supported. To restore throughput and to use an HSECK9 license, upgrade the PLR code to Version 3. See: Upgrading a PLR.
Product Instance: Cisco Cloud Services Router 1000v PLR status: PLR is activated. An older version of the PLR code installed (Version 1 or Version 2). Software version: Cisco IOS XE Everest 16.5.x to Cisco IOS XE Amsterdam 17.3.x.	You perform a .bin upgrade to a release *between Cisco IOS XE Bengaluru 17.4.x and Cisco IOS XE Cupertino 17.9.x.*	All existing features that have been enabled are honored and continue to work - except for throughput greater than 250 Mbps, and any export-controlled features that require an HSECK9 license. The older version of the PLR code is not removed from the product instance, but it is not supported. To use PLR, you must upgrade the software version to Cisco IOS XE Dublin 17.10.1a and then upgrade the PLR code to Version 3. See: Upgrading a PLR.

Current Setup	Condition (If This Action is Performed)	Result and Implication
Product Instance: Cisco Cloud Services Router 1000v Router (.bin upgraded to a Catalyst 8000V software image) PLR status: PLR is activated. Version 3 of the PLR code is installed. Software version: Cisco IOS XE Dublin 17.10.1a or later.	You downgrade to Cisco IOS XE Amsterdam 17.3.x or earlier release.	After downgrade, the older version of the software image cannot validate the PLR code Version 3 and does not honor or support it. The product instance behaves as if no licenses are installed. The PLR code is not removed from product instance.
Product Instance: Cisco Cloud Services Router 1000v Router (.bin upgraded to a Catalyst 8000V software image) PLR status: PLR upgrade is not complete. An older version (Version 1 or Version 2) of the PLR code installed. Software version: Cisco IOS XE Dublin 17.10.1a or later.	You downgrade to Cisco IOS XE Amsterdam 17.3.x or earlier release.	After downgrade the older version of the software image can validate the PLR code and use it to fulfill license requests.

Activating, Upgrading to, Deactivating a PLR in the Smart Licensing Using Policy Environment

- If you are implementing PLR on a Catalyst 8000V Edge Software, see: Activating a PLR.
- If you performing a .bin upgrade on a Cisco Cloud Services Router 1000v Router and want to continue using PLR, see: Upgrading a PLR.
- If you want to deactive a PLR, see: Deactivating a PLR.