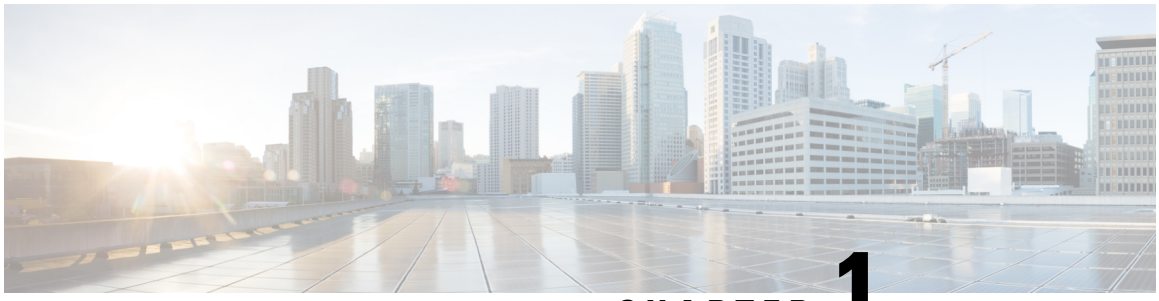


Smart Licensing Using Policy for Cisco Enterprise Routing Platforms

First Published: 2020-09-25

Last Modified: 2023-08-01

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Information About Smart Licensing Using Policy

Smart Licensing Using Policy is an enhanced version of Smart Licensing with the objective of providing a licensing solution that does not interrupt the operations of your network. Rather, this solution enables a compliance relationship to account for the hardware and software licenses you purchase and use.

This document focuses on guidance for implementing Smart Licensing Using Policy on new deployments.

- Benefits of Smart Licensing Using Policy, on page 1
- Benefits of Smart Licensing Using Policy, on page 1
- Supported Products, on page 2
- Key Concepts of Smart Licensing Using Policy, on page 3

Benefits of Smart Licensing Using Policy

With the Smart Licensing Using Policy solution, preliminary steps such as registration or generation of keys are not required, unless you use an export-controlled or an enforced license. This means that you can configure licenses and move on to configure the product features right-away.

Consistency is provided through a uniform licensing experience across campus, industrial ethernet switching, routing, and wireless devices - all of which run Cisco IOS XE software.

Visibility and manageability are ensured through tools, telemetry, and product tagging, to know what is in-use.

Flexible, time series reporting is another key benefit where you have multiple options when it comes to ensuring compliance. Depending on an organization's network requirements and security policy, the connection to Cisco Smart Software Manager (Cisco SSM) may be a direct connection over the internet, or through mediated access, or through offline communication for air-gapped networks.

Benefits of Smart Licensing Using Policy

With this solution, preliminary steps such as registration or generation of keys are not required, unless you use an export-controlled or an enforced license. This means you can configure licenses and then move on to configuring the product features right-away.

Consistency is provided through a uniform licensing experience across campus, industrial ethernet switching, routing, and wireless devices - all of which run Cisco IOS XE software.

Visibility and manageability are ensured through tools, telemetry, and product tagging, to know what is in-use.

Flexible, time series reporting is another key benefit where you have multiple options when it comes to ensuring compliance. Depending on an organization's network requirements and security policy, the connection to Cisco Smart Software Manager (Cisco SSM) may be a direct connection over the internet, or through mediated access, or through offline communication for air-gapped networks.

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		
	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		

Product Category	Product Series	Introductory Release When Support was Introduced
	Cisco 1100 Terminal Services Gateway	Cisco IOS XE Bengaluru 17.4.1

Key Concepts of Smart Licensing Using Policy

This section explains the important concepts that helps you understand how the Smart Licensing Using Policy solution is designed to work.

License Enforcement Types

All licenses have an enforcement type. The enforcement type indicates if a license requires authorization before use or not. These are the enforcement types.

Unenforced or Not Enforced

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 general terms.

Cisco DNA licenses available on all Cisco Enterprise Routing Platforms are examples of unenforced licenses.

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.

Export-Controlled

Licenses that belong to this enforcement type are restricted by U.S. trade-control laws and require authorization before use. The required authorization is in the form of an authorization code, which must be installed on the device. Cisco may pre-install export-controlled licenses when ordered with hardware purchase.

An example of an export-controlled license is the High Security (HSECK9) key, which is available on Cisco Catalyst 8000 Enterprise Routing platforms.

For information about all the licenses that are available on Cisco Catalyst 8000 Series Enterprise Platforms, see *Configuring Available Licenses*.

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. Installing SLAC on a device enables the use of the license.

If an authorization code is required for the license you are using, you can request one from Cisco SSM. For detailed information about the HSECK9 key on supported products, see Available Options for an HSECK9 License, on page 154.

Table 2: License That Requires SLAC

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

You can also remove and return a SLAC to return the license to the license pool in Cisco SSM. But in order to do this, the feature that uses the license must be disabled first. You cannot remove or return a SLAC if it is in-use.

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

Table 3: 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 159, 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 161.

SLR Authorization Codes

SLR authorization codes are from the older Smart Licensing model. You cannot request a new SLR in the Smart Licensing Using Policy environment because the notion of *reservation* does not apply. If you are in an air-gapped network, the Workflow for Topology: No Connectivity to CSSM and No CSLU, on page 45 topology applies instead.

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. 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**. For more information, see RUM Report and Report Acknowledgement.
- 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 here 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 4: Policy: Cisco default, on page 7) 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 4: 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[1]	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

[1] 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, on page 291, show license all, on page 272, show license tech, on page 309 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 18.

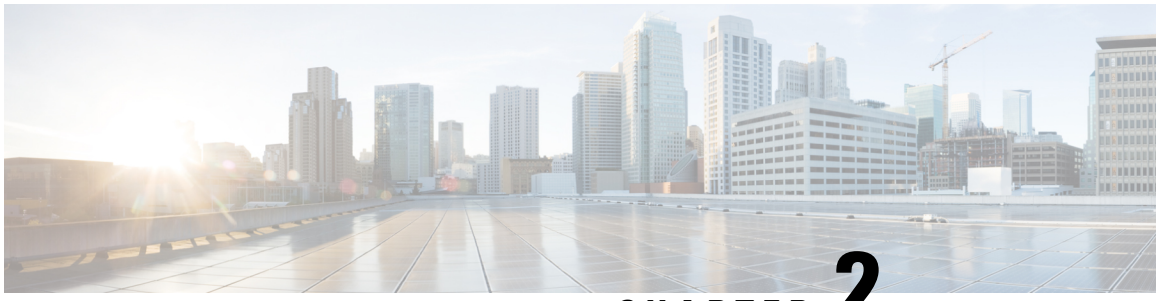
- From Cisco IOS XE Cupertino 17.7.1, a trust code is automatically obtained in topologies where the product instance initiates the sending of data to CSLU and in topologies where the product instance is in an air-gapped network.

  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 15.

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`.



CHAPTER 2

How Smart Licensing Using Policy Works

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

Components Involved

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

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

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

- Product Instance, on page 11
- Cisco Smart Software Manager (Cisco SSM), on page 12
- Cisco Smart License Utility (CSLU), on page 12
- Controller, on page 12
- Cisco Smart Software Manager On-Prem (SSM On-Prem), on page 14
- Managed Service License Agreement (MSLA), on page 15
- Supported Topologies, on page 15
- High Availability, on page 30

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.

Cisco Smart Software Manager (Cisco SSM)

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

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

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

Cisco Smart License Utility (CSLU)

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

- Provides options relating to how workflows are triggered. The workflows can be triggered by CSLU or by the product instance.
- Collects usage reports from the product instance and uploads these usage reports to the corresponding Smart Account or Virtual Account – online, or offline, using files. Similarly, the RUM report ACK is collected online, or offline, and sent back to the product instance.
- Sends authorization code requests to Cisco SSM and receives authorization codes[2] from CSSM.

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

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

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



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

Controller

A management application or service that manages multiple product instances.

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

- Support Information for Controller: Cisco DNA Center

[2] 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 5: Support Information for Controller: Cisco DNA Center

Minimum Required Cisco DNA Center Version for Smart Licensing Using Policy [3]	Minimum Required Cisco IOS XE Version [4]	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

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

[4] 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 6: Support Information for Controller: Cisco vManage

Minimum Required Cisco vManage Version for Smart Licensing Using Policy [5]	Minimum Required Cisco IOS XE Version [6]	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*.

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

[6] 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 20.

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

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

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

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

Minimum Required SSM On-Prem Version for Smart Licensing Using Policy[7]	Minimum Required Cisco IOS XE Version [8]	Supported Product Instances
Version 8, Release 202102	Cisco IOS XE Amsterdam 17.3.3	All Supported Products, on page 2

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

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

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

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

Minimum Required SSM On-Prem Version for Smart Licensing Using Policy *with MSLA*	Minimum Required Cisco IOS XE Version for Smart Licensing Using Policy *with MSLA*	Supported Product Instances
Version 8 Release 202206	Cisco IOS XE Cupertino 17.9.1	Catalyst 8000V Edge Software. For more information, see Managed Service License Agreement (MSLA), on page 15.

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

Managed Service License Agreement (MSLA)

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

Device licenses that are under the MSLA program, are referred to as post-paid licenses. Your Smart Account and Virtual Account in 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 29.

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

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

Migrating to Smart Licensing Using Policy with MSLA

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

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

Supported Topologies

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

After Topology Selection

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

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

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

Connected to CSSM Through CSLU

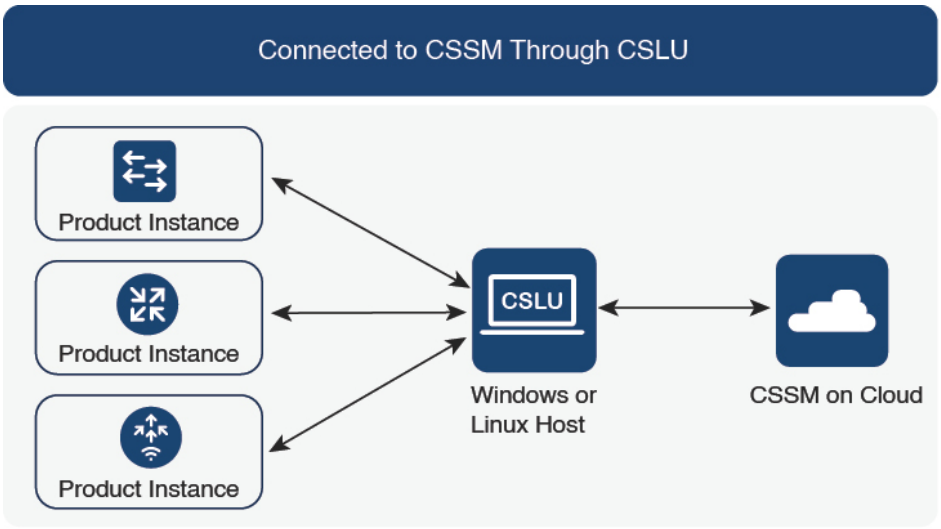
Overview:

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

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

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

Figure 1: Topology: Connected to CSSM Through CSLU



Considerations or Recommendations:

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

Release-Wise Changes and Enhancements:

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

From Cisco IOS XE Cupertino 17.7.1a:

- Trust code request and installation

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

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

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

From Cisco IOS XE Cupertino 17.9.1a:

- Trust code request and installation

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

- Virtual Routing and Forwarding (VRF) Support

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

- RUM report throttling

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

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

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

Where to Go Next:

To implement this topology, see Workflow for Topology: Connected to CSSM Through CSLU, on page 33.

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 8.

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:

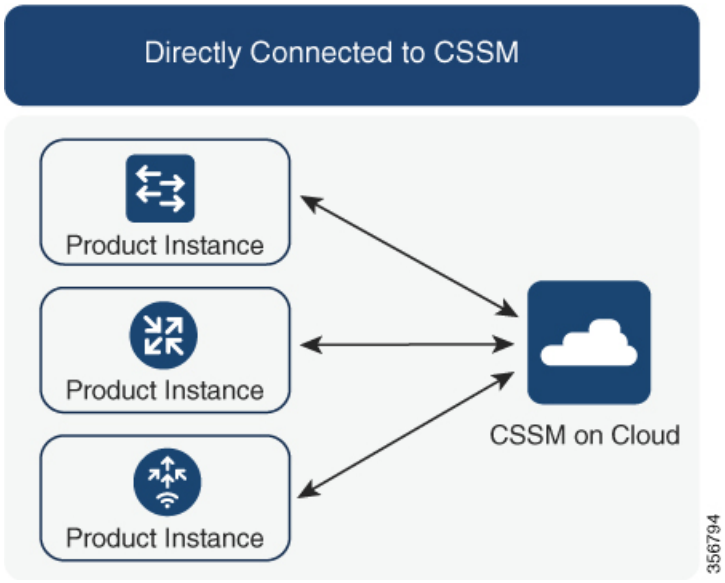
  - Smart transport: In this method, a product instance uses a specific Smart transport licensing server URL. This must be configured exactly as shown in the workflow section.
  - Smart transport through an HTTPs proxy: In this method, a product instance uses a proxy server to communicate with the licensing 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, on page 36 > 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.

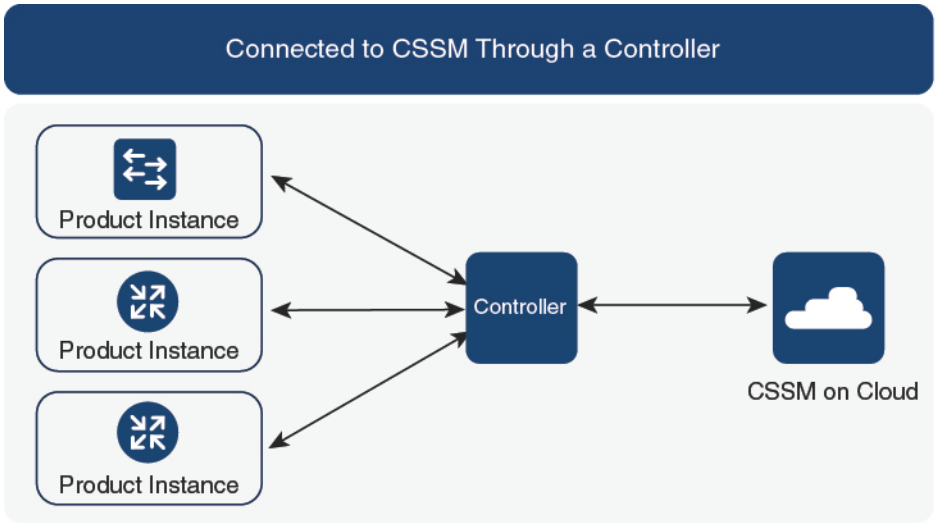
Where to Go Next:

To implement this topology, see Workflow for Topology: Connected Directly to CSSM, on page 36.

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 7: Product Instances that Support SLAC Generation for HSECK9 license on the Cisco DNA Center GUI, on page 39.

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, on page 38 > Using Cisco DNA Center as a Controller, on page 38.

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, on page 38 > Using Cisco vManage as a Controller.

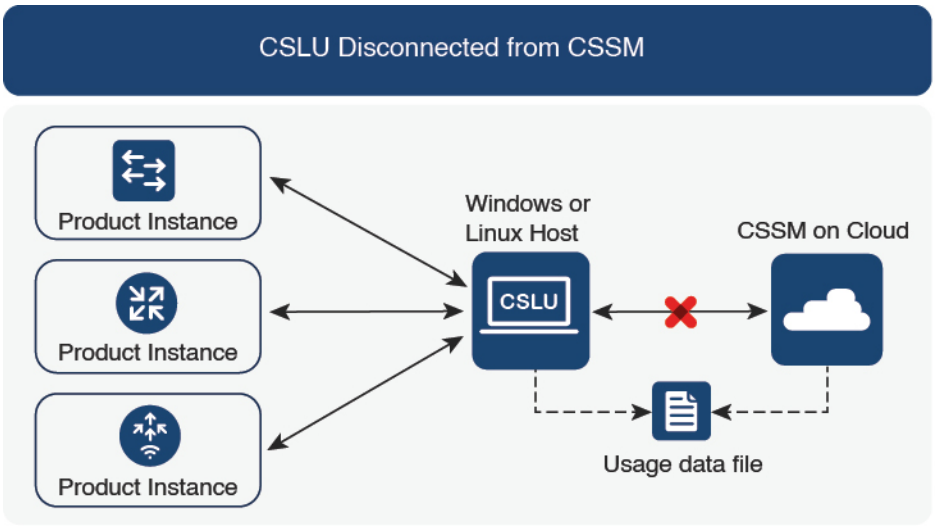
CSLU Disconnected from CSSM

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:

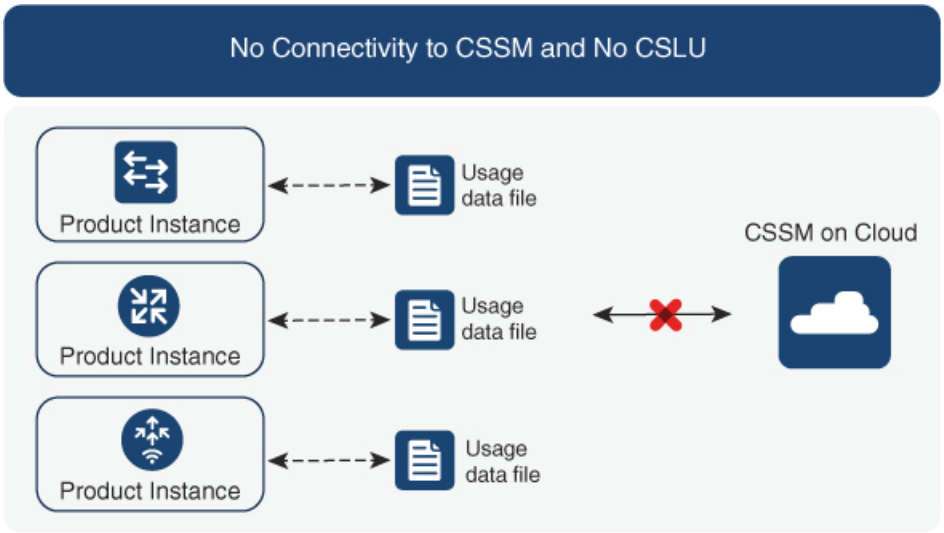
To implement this topology, see Workflow for Topology: CSLU Disconnected from CSSM, on page 41.

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, on page 45.

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.

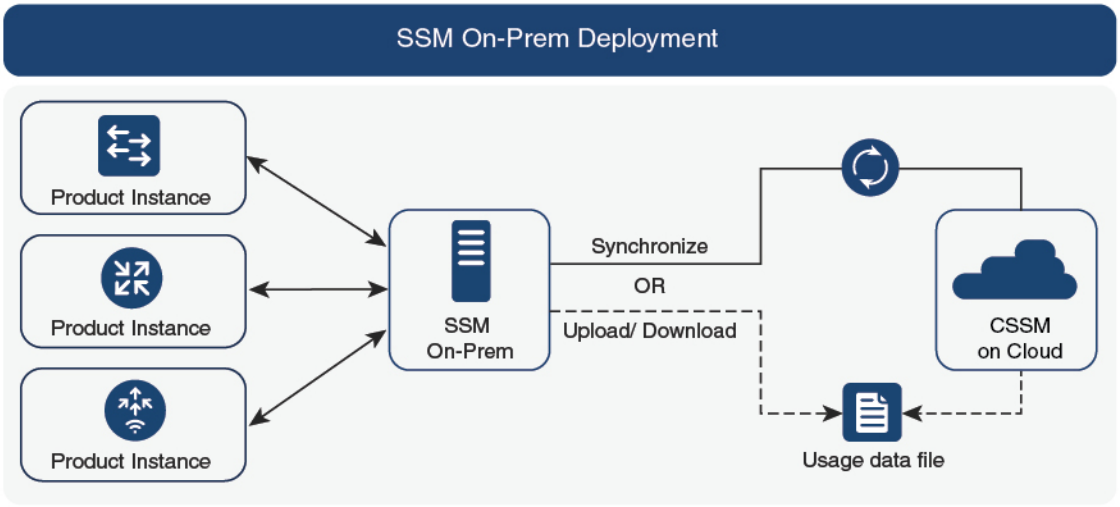
In SSM On-Prem, the reporting interval is set to the default policy on the product instance. You can change this, but only to report more frequently (a narrower interval), or you can install a custom policy if available.

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, on page 46.

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, on page 147.

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 18.

- 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 16, or CSLU Disconnected from CSSM, on page 23

- 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 26

- 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 24

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

Considerations or Recommendations:

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

Where to Go Next:

Implement one of the supported topologies:

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

Workflow for Topology: Connected Directly to CSSM, on page 36
Workflow for Topology: Connected to CSSM Through CSLU, on page 33
Workflow for Topology: CSLU Disconnected from CSSM, on page 41
Workflow for Topology: No Connectivity to CSSM and No CSLU, on page 45
Workflow for Topology: SSM On-Prem Deployment, on page 46

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

[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.

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.

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:

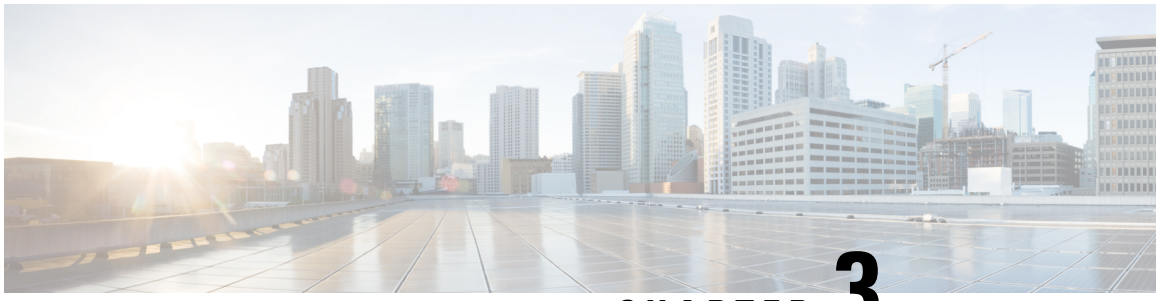
- A product instance that is connected to CSLU, does not take any further action.
- A product instance that is directly connected to CSSM, performs trust synchronization. Trust synchronization involves the following:

  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.



CHAPTER 3

Implementing Smart Licensing Using Policy

This chapter provides the simplest and fastest way to implement Smart Licensing Using Policy for new deployments.

If you are migrating from an existing licensing model, see Migrating to Smart Licensing Using Policy, on page 53.

- Workflow for Topology: Connected to CSSM Through CSLU, on page 33
- Workflow for Topology: Connected Directly to CSSM, on page 36
- Workflow for Topology: Connected to CSSM Through a Controller, on page 38
- Workflow for Topology: CSLU Disconnected from CSSM, on page 41
- Workflow for Topology: No Connectivity to CSSM and No CSLU, on page 45
- Workflow for Topology: SSM On-Prem Deployment, on page 46

Workflow for Topology: Connected to CSSM Through CSLU

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

- Tasks for Product Instance-Initiated Communication
- Tasks for CSLU-Initiated Communication

Tasks for Product Instance-Initiated Communication

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

1. ***Smart Account Set-Up***

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

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

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

2. ***CSLU Installation***

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

Download the file from Smart Software Manager > **Smart Licensing Utility**.

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

3. ***CSLU Preference Settings***

   Where tasks are performed: CSLU Interface

   a. Logging into Cisco (CSLU Interface), on page 166

   b. Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 166

   c. Adding a Product-Initiated Product Instance in CSLU (CSLU Interface), on page 167

4. ***Product Instance Configuration***

   Where tasks are performed: Product Instance

   a. Ensuring Network Reachability for Product Instance-Initiated Communication, on page 167

   b. Ensure that transport type is set to **cslu**.

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

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

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

      - Option 1:

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

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

      - Option 2:

        Configure DNS discovery of your domain.

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

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

      - Option 3:

        Configure a specific URL for CSLU.

        Enter the **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* command in global configuration mode. For `<cslu_ip_or_host>`, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

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

   d. Enable the utility mode only if you have an MSLA: Enabling the Utility Mode, on page 219

Result:

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

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

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

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

Tasks for CSLU-Initiated Communication

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

1. ***Smart Account Set-Up***

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

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

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

2. ***CSLU Installation***

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

   Download the file from Smart Software Manager > **Smart Licensing Utility**.

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

3. ***CSLU Preference Settings***

   Where tasks are performed: CSLU interface

   a. Logging into Cisco (CSLU Interface), on page 166

   b. Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 166

   c. Adding a CSLU-Initiated Product Instance in CSLU (CSLU Interface), on page 169

4. ***Product Instance Configuration***

   Where tasks is performed: Product Instance

   a. Ensuring Network Reachability for CSLU-Initiated Communication, on page 171

b. Enable the utility mode only if you have an MSLA: Enabling the Utility Mode, on page 219

5. ***Usage Synchronization***

   Where task is performed: CSLU Interface

   Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 170

Result:

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

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

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

Workflow for Topology: Connected Directly to CSSM

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

1. ***Smart Account Set-Up***

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

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

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

2. ***Product Instance Configuration***

   Where tasks are performed: Product Instance

   a. Set-Up product instance connection to CSSM: Setting Up a Connection to CSSM , on page 177

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

   - Option 1:

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

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

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

     This option is supported in the utility mode.

- Option 2:

  Smart transport through an HTTPs proxy: See the Configuring Smart Transport Through an HTTPs Proxy, on page 180 section.

  This option is supported in the utility mode.

- Option 3:

  Configure Call Home service for direct cloud access. See the Configuring the Call Home Service for Direct Cloud Access, on page 181 section.

  This option is *not* supported in the utility mode.

- Option 4:

  Configure Call Home service for direct cloud access through an HTTPs proxy. See the Configuring the Call Home Service for Direct Cloud Access through an HTTPs Proxy Server, on page 184 section.

  This option is *not* supported in the utility mode.

c. Enable the utility mode only if you have an MSLA: Enabling the Utility Mode, on page 219

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

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

   a. Generate one token for each *Virtual Account* you have. You can use the same token for all the product instances that are part of one Virtual Account: Generating a New Token for a Trust Code from CSSM, on page 211.

   b. Configure the token on the product instance to establish trust with CSSM: Establishing Trust with an ID Token, on page 212.

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

   If you want to use a license that requires authorization before use (enforcement type: enforced or export-controlled), or configure a throughput greater than 250 Mbps (on supported product instances), you have to complete this step before this topology deployment is complete: Manually Requesting and Auto-Installing a SLAC , on page 201

Result:

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

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

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

To change the reporting interval configure the **license smart usage interval** command. For more information, see license smart (global config), on page 249.

Workflow for Topology: Connected to CSSM Through a Controller

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

Using Cisco DNA Center as a Controller

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

Product Instance Configuration → Cisco DNA Center Configuration

1. ***Product Instance Configuration***

   Where task is performed: Product Instance

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

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

2. ***Cisco DNA Center Configuration***

   Where tasks is performed: Cisco DNA Center GUI

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

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

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

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

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

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

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

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

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

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

Table 7: Product Instances that Support SLAC Generation for HSECK9 license on the Cisco DNA Center GUI

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

Result:

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

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

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

Using Cisco vManage as a Controller

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

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

1. ***Smart Account Set-Up***

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

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

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

2. ***Product Instance Configuration***

   Where tasks are performed: Product Instance

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

   See the Cisco SD-WAN Getting Start Guide > Cisco SD-WAN Overlay Network Bring-Up Process.

3. ***Cisco vManage Configuration***

   Where tasks are performed: Cisco vManage portal

   See the Cisco SD-WAN Getting Start Guide > License Management for Smart Licensing Using Policy .

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

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

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

   Where tasks are performed: Product Instance and CSSM Web UI

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

   - Option 1:

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

     a. Generating and Downloading SLAC from CSSM to a File, on page 199

     b. Installing a File on the Product Instance, on page 215

   - Option 2:

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

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

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

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

b. Generate one token for each *Virtual Account* you have. You can use same token for all the product instances that are part of one Virtual Account: Generating a New Token for a Trust Code from CSSM, on page 211

Having downloaded the token, you can now install the trust code on the product instance: Establishing Trust with an ID Token, on page 212.

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

c. Request and install SLAC: Manually Requesting and Auto-Installing a SLAC , on page 201

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

Result:

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

Workflow for Topology: CSLU Disconnected from CSSM

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

- Tasks for Product Instance-Initiated Communication
- Tasks for CSLU-Initiated Communication

Tasks for Product Instance-Initiated Communication

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

1. ***Smart Account Set-Up***

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

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

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

2. ***CSLU Installation***

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

   Download the file from Smart Software Manager > **Smart Licensing Utility**.

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

3. ***CSLU Preference Settings***

   Where tasks are performed: CSLU

   a. In the CSLU Preferences tab, click the **Cisco Connectivity** toggle switch to **off**. The field switches to "Cisco Is Not Available".

   b. Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 166

   c. Adding a Product-Initiated Product Instance in CSLU (CSLU Interface), on page 167

4. ***Product Instance Configuration***

   Where tasks are performed: Product Instance

   a. Ensuring Network Reachability for Product Instance-Initiated Communication, on page 167

   b. Ensure that transport type is set to **cslu**.

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

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

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

      - Option 1:

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

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

      - Option 2:

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

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

      - Option 3:

        Configure a specific URL for CSLU.

        Enter the **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* command in global configuration mode. For `<cslu_ip_or_host>`, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

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

d. Enable the utility mode only if you have an MSLA: Enabling the Utility Mode, on page 219

5. ***Usage Synchronization***

   Where tasks are performed: CSLU and CSSM

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

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

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

   a. Export to CSSM (CSLU Interface), on page 175

   b. Uploading Data or Requests to CSSM and Downloading a File, on page 214

   c. Import from CSSM (CSLU Interface), on page 176

Result:

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

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

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

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

Tasks for CSLU-Initiated Communication

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

1. ***Smart Account Set-Up***

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

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

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

2. ***CSLU Installation***

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

Download the file from Smart Software Manager > **Smart Licensing Utility**.

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

3. ***CSLU Preference Settings***

   Where tasks is performed: Product Instance

   a. In the CSLU Preferences tab, click the **Cisco Connectivity** toggle switch to **off**. The field switches to "Cisco Is Not Available".

   b. Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 166

   c. Adding a CSLU-Initiated Product Instance in CSLU (CSLU Interface), on page 169

4. ***Product Instance Configuration***

   Where tasks is performed: Product Instance

   a. Ensuring Network Reachability for CSLU-Initiated Communication, on page 171

   b. Enable the utility mode only if you have an MSLA: Enabling the Utility Mode, on page 219.

5. ***Usage Synchronization***

   Where tasks are performed: CSLU and CSSM

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

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

   a. Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 170

   b. Export to CSSM (CSLU Interface), on page 175

   c. Uploading Data or Requests to CSSM and Downloading a File, on page 214

   d. Import from CSSM (CSLU Interface), on page 176

Result:

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

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

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

Workflow for Topology: No Connectivity to CSSM and No CSLU

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

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

1. ***Smart Account Set-Up***

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

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

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

2. ***Product Instance Configuration***

   Where task is performed: Product Instance

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

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

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

   b. Enable utility mode if you have an MSLA

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

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

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

   Where tasks is performed: CSSM Web UI and Product Instance

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

   - Option 1:

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

     a. Generating and Downloading SLAC from CSSM to a File

     b. Installing a File on the Product Instance, on page 215

   - Option 2:

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

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

a. Generating and Saving a SLAC Request on the Product Instance, on page 203

b. Uploading Data or Requests to CSSM and Downloading a File, on page 214

c. Installing a File on the Product Instance, on page 215

Result:

Since you will have disabled all communication to and from the product instance, to report license usage you must save RUM reports to a file (on your product instance) and upload it to CSSM (from a workstation that has connectivity to the internet, and Cisco):

1. Generate and save RUM reports

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

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

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

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

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

   See the license smart (privileged EXEC), on page 264 command for command syntax details.

2. Upload usage data to CSSM: Uploading Data or Requests to CSSM and Downloading a File, on page 214

3. Install the ACK on the product instance: Installing a File on the Product Instance, on page 215

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

Workflow for Topology: SSM On-Prem Deployment

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

Tasks for Product Instance-Initiated Communication

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

1. ***Smart Account Set-Up***

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

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

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

2. ***SSM On-Prem Installation and Configuration***

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

   Download the file from Smart Software Manager > **Smart Software Manager On-Prem**.

   Refer to the *Cisco Smart Software On-Prem Installation Guide* and the *Cisco Smart Software On-Prem User Guide* for help with installation.

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

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

3. ***Addition and Validation of Product Instances***

   Where tasks are performed: SSM On-Prem UI

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

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

   a. Assigning a Smart Account and Virtual Account (SSM On-Prem UI), on page 185

   b. Validating Devices (SSM On-Prem UI), on page 186

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

4. ***Product Instance Configuration***

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

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

   a. Ensuring Network Reachability for Product Instance-Initiated Communication, on page 186

   b. Retrieving the Transport URL (SSM On-Prem UI), on page 189

   c. Setting the Transport Type, URL, and Reporting Interval, on page 216

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

   d. Complete this sub-step only if you want to use a license that requires authorization before use (enforcement type: enforced or export-controlled), or to configure a throughput greater than 250 Mbps, on supported product instances (choose one option):

      - Option 1:

        SSM On-Prem is connected to CSSM: Submitting an Authorization Code Request (SSM On-Prem UI, Connected Mode), on page 190

      - Option 2:

        SSM On-Prem is not connected to CSSM: Submitting an Authorization Code Request (SSM On-Prem UI, Disconnected Mode), on page 191 .

   e. Enable the utility mode only if you have an MSLA: Enabling the Utility Mode, on page 219

5. ***Initial Usage Synchronization***

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

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

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

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

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

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

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

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

- Option 1:

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

- Option 2:

  SSM On-Prem is not connected to CSSM: See Exporting and Importing Usage Data (SSM On-Prem UI), on page 192.

Result:

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

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

For subsequent reporting, you have the following options:

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

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

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

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

- To synchronize usage information with CSSM, schedule periodic synchronization, or, upload and download the required files:

  - Schedule periodic synchronization with CSSM. In the SSM On-Prem UI, navigate to **Reports** > **Usage Schedules** > **Synchronization schedule with Cisco**. Enter the following frequency information and save:

    - **Days**: Refers to how *often* synchronization occurs. For example, if you enter 2, synchronization occurs once every two days.

    - **Time of Day:**: Refers to the time at which synchronization occurs, in the 24-hour notation system. For example, if you enter 14 hours and 0 minutes, synchronization occurs at 2 p.m. (1400) in your local time zone.

- Upload and download the required files for reporting: Exporting and Importing Usage Data (SSM On-Prem UI), on page 192).

Tasks for SSM On-Prem Instance-Initiated Communication

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

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

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

   Download the file from Smart Software Manager > **Smart Software Manager On-Prem**.

   Refer to the *Cisco Smart Software On-Prem Installation Guide* and the *Cisco Smart Software On-Prem User Guide* for help with installation.

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

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

2. ***Product Instance Addition***

   Where task is performed: SSM On-Prem UI

   Depending on whether you want to add a single product instance or multiple product instances, follow the corresponding sub-steps: Adding One or More Product Instances (SSM On-Prem UI), on page 193.

3. ***Product Instance Configuration***

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

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

   a. Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 194

   b. Enable the utility mode only if you have an MSLA: Enabling the Utility Mode, on page 219

   c. Complete this sub-step only if you want to use a license that requires authorization before use (enforcement type: enforced or export-controlled), or to configure throughput greater than 250 Mbps (on supported product instances): Submitting an Authorization Code Request (SSM On-Prem UI, Disconnected Mode), on page 191.

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

4. ***Initial Usage Synchronization***

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

   a. Retrieve usage information from the product instance.

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

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

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



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

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

   - Option 1:

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

   - Option 2:

     SSM On-Prem is not connected to CSSM. See: Exporting and Importing Usage Data (SSM On-Prem UI), on page 192.

Result:

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

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

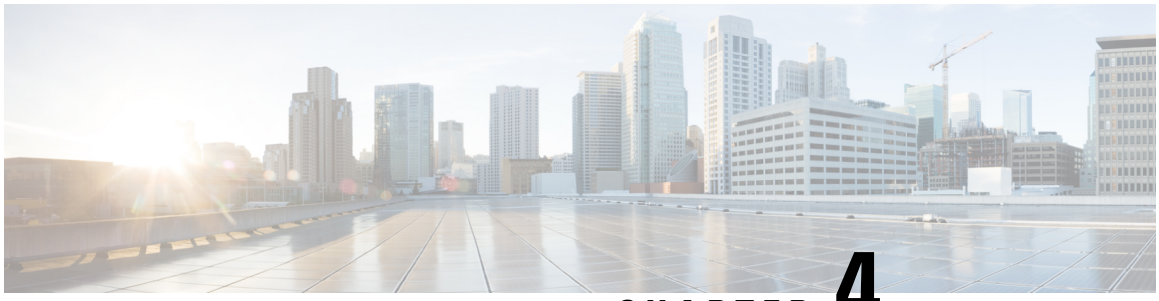
For subsequent reporting, you have the following options:

- To retrieve usage information from the product instance, you can:
  - In the SSM On-Prem UI, Smart Licensing workspace, nagivate to **Reports** > **Usage Schedules** > **Synchronize now with Cisco**.
  - Schedule periodic retrieval of information from the product instance by configuring a frequency. In the SSM On-Prem UI, Smart Licensing workspace, nagivate to **Reports** > **Usage Schedules** > **Synchronisation pull schedule with the devices**. Enter values in the following fields:
    - **Days**: Refers to how *often* synchronization occurs. For example, if you enter 2, synchronization occurs once every two days.

- **Time of Day:**: Refers to the time at which synchronization occurs, in the 24-hour notation system. For example, if you enter 14 hours and 0 minutes, synchronization occurs at 2 p.m. (1400).

- Collect usage data from the product instance without being connected to CSSM. In the SSM On-Prem UI, Smart Licensing workspace, nagivate to **Inventory** > **SL Using Policy** tab. Select one or more product instances by enabling the coresponding check box. Click **Actions for Selected...** > **Collect Usage**. On-Prem connects to the selected Product Instance(s) and collects the usage reports. These usage reports are then stored in On-Prem's local library. These reports can then be transferred to Cisco if On-Prem is connected to Cisco, or (if you are not connected to Cisco) you can manually trigger usage collection by selecting **Export/Import All..** > **Export Usage to Cisco**.

- To synchronize usage information with CSSM, you can:
  - Schedule periodic synchronization with CSSM. In the SSM On-Prem UI, navigate to **Reports** > **Usage Schedules** > **Synchronization schedule with Cisco**. Enter the following frequency information and save:
    - **Days**: Refers to how *often* synchronization occurs. For example, if you enter 2, synchronization occurs once every two days.
    - **Time of Day:**: Refers to the time at which synchronization occurs, in the 24-hour notation system. For example, if you enter 14 hours and 0 minutes, synchronization occurs at 2 p.m. (1400).
  - Upload and download the required files for reporting: Exporting and Importing Usage Data (SSM On-Prem UI), on page 192).



CHAPTER 4

Migrating to Smart Licensing Using Policy

To migrate to Smart Licensing Using Policy, you must upgrade the software version (image) on the product instance and any other components that are part of your pre-ugrade set up, to a supported version.

Before you Begin

Ensure that you have read the Upgrades section, to understand how Smart Licensing Using Policy handles all earlier licensing models.

The release in which Smart Licensing Using Policy was introduced is the *minimum* required software version for that product instance. Information about the introductory release for supported routing products is provided here: Supported Products, on page 2.

Note that all the licenses that you are using prior to migration will be available after upgrade. This means that not only registered and authorized licenses (including reserved licenses), but also evaluation licenses, will all be migrated. Default licenses like ipbasek9 and internal_service, will be migrated but not displayed in **show** command outputs. (They do not have entitlement tags and are always available, by default).

The advantage with migrating registered and authorized licenses is that you will have fewer configuration steps to complete after migration, because your configuration is retained after upgrade (transport type configuration and configuration for connection to CSSM, all authorization codes). This ensures a smoother transition to the Smart Licensing Using Policy environment.

- Upgrades, on page 53
- Downgrades, on page 60
- Sample Migration Scenarios, on page 61

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, on page 53 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 159.

- 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 , on page 201.

- 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, on page 231. For a sample migration scenario, see Example: Smart Licensing (SLR With Throughput >250 Mbps, Without Export-Controlled License) to Smart Licensing Using Policy, on page 92

- 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, on page 199 and then Installing a File on the Product Instance, on page 215.

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, on page 61.

- 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, on page 121.

  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 159.

- 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, on page 76.

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.
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 159.
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.

Upgrading the Software Version

Information about the upgrade procedures for supported product instances is provided in the table below:

Product Series	Link to Upgrade Information
Cisco 1000 Series Integrated Services Routers	How to Install and Upgrade the Software
Cisco 4000 Series Integrated Services Routers	How to Install and Upgrade the Software
Cisco ASR 1000 Series Aggregation Services Routers	Software Upgrade Processes Supported by Cisco ASR 1000 Series Routers
Cisco Cloud Services Router 1000v	Upgrading the Cisco IOS XE Software
Cisco Integrated Services Virtual Router	Upgrading the Cisco IOS XE Software
Catalyst 8200 Series Edge Platforms	How to Install and Upgrade the Software
Catalyst 8300 Series Edge Platforms	How to Install and Upgrade the Software
Catalyst 8500 Series Edge Platforms	Cisco Catalyst 8500 Software Upgrade
Catalyst 8000V Edge Software	Upgrading the Cisco IOS XE Software
Cisco 1100 Terminal Services Gateway	How to Install and Upgrade the Software

Upgrading Other Components

If your pre-upgrade set-up includes Cisco DNA Centre, or Cisco vManage, or SSM On-Prem, ensure that you have checked the following before you migrate to Smart Licensing Using Policy:

- If the component is running a compatible version or if it requires an upgrade.

  For each component, information about the version that is compatible with Smart Licensing Using Policy (if applicable) is provided here: How Smart Licensing Using Policy Works, on page 11.

- If upgrade must follow a prescribed sequence. This is to ensure that you upgrade the component and the product instance in the correct order.

Cisco DNA Centre

For Cisco DNA Centre, see Cisco DNA Center Upgrade Guide.

Cisco vManage

For Cisco vManage, see Cisco SD-WAN Getting Started Guide.

SSM On-Prem

For SSM On-Prem, see SSM On-Prem 8 Installation Guide.

After Upgrading the Software Version

- Complete topology implementation.

  If a transport mode is available in your pre-upgrade set-up, this is retained after you upgrade. Only in some cases, like with evaluation licenses or with licensing models where the notion of a transport type does not exist, the default (**cslu**) is applied - in these cases you may have a few more steps to complete before you are set to operate in the Smart Licensing Using Policy environment.

  No matter which licensing model you upgrade from, you can change the topology after upgrade. If you do, then complete implmentation for the corresponding toplogy as described here: Implementing Smart Licensing Using Policy, on page 33.

- Check if any of the product instances require SLAC after upgrade.

  For export-controlled or enforced licenses, SLAC installation *after* upgrade is required *only in certain cases*. See: How Upgrade Affects Enforcement Types for Existing Licenses, on page 54.

- Check if device-led conversion (DLC) applies and is completed.

  DLC is the process of converting traditional licenses to Smart Licenses, without manual intervention. So a DLC is applicable only when migrating licenses that are *not Smart* licenses, that is, Right-To-Use (RTU) licenses and Product Authorization Keys (PAK) licenses. Once DLC is complete, the consumption of these converted licenses is reflected in CSSM.

  The DLC process is triggered automatically on the product instance only when you upgrade to a release that supports Smart Licensing Using Policy. DLC is supported for all topologies.

  DLC data is collected one hour after the product instance is upgraded to a software version that supports Smart Licensing Using Policy. This DLC data is also automatically included in the RUM report. So if DLC applies to your upgrade scenario, you can wait for the product instance to finish collecting DLC data (**show platform software license dlc** privileged EXEC command) before you send the initial usage report to CSSM. If you send the initial usage report before the DLC data collection is completed, simply follow the reporting method that applies to the topology you implement, and complete another round of reporting to send DLC data. CSSM generates an ACK after processing DLC data. The DLC process is complete after the ACK is installed on the product instance. The amount of time the DLC process takes, depends on the number of licenses.

  DLC itself requires no action from you.



Note Cisco 1000 Series Integrated Services Routers, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Aggregation Services Routers support DLC.

Cisco Cloud Services Routers 1000v and Cisco Integrated Services Virtual Routers do not support DLC.

- Synchronize license usage with CSSM.

  No matter which licensing model you are upgrading from and no matter which topology you implement, synchronize your usage information with CSSM. For this you have to follow the reporting method that applies to the topology you implement. This initial synchronization ensures that up-to-date usage information is reflected in CSSM and a custom policy (if available), is applied. The policy that is applicable after this synchronization also indicates subsequent reporting requirements. These rules are also tabled here: How Upgrade Affects Reporting for Existing Licenses, on page 56.

Note After initial usage synchronization is completed, reporting is required only if the policy, or, system messages indicate that it is.

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 8) 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.

Sample Migration Scenarios

Sample migration scenarios have been provided considering the various existing licensing models and licenses. All scenarios provide sample outputs before and after migration, any CSSM Web UI changes to look out for (as an indicator of a successful migration or further action), and how to identify and complete any necessary post-migration steps.

Note For SSM On-Prem, the sequence in which you perform the various upgrade-related activities is crucial. So only for this scenario, the migration sequence has been provided.

Example: Smart Licensing (Registered and Authorized Licenses) to Smart Licensing Using Policy

The following is an example of a **Cisco 4461 Integrated Services Router** with authorized and registered licenses, migrating from Smart Licensing to Smart Licensing Using Policy. The software version on the product instance is upgraded from Cisco IOS XE Gibraltar 16.12.4 to Cisco IOS XE Amsterdam 17.3.2. The following is a summary of what to expect after upgrade for this example:

- Enforcement type after migration: All the licenses in this scenario are registered and authorised (implying that any license that requires authorization before use has this already). Accordingly, the export-controlled license (ISR_4400_Hsec) will be available and have enforcement type: EXPORT RESTRICTED, after migration. Further, SLAC installation after upgrade is not required. See the point about an HSECK9 license registered to a Smart Account, and with the export-control flag enabled in CSSM here: How Upgrade Affects Enforcement Types for Existing Licenses, on page 54.

  All remaining registered and authorized licenses will have enforcement type: NOT ENFORCED after migration.

- Transport type after migration: Call Home is the configured transport type before migration. Since the licenses are registered, the transport type (**callhome**) and the configuration to connect to CSSM is retained after migration.

- Device-Led Conversion (DLC): DLC does not apply to the licenses in this scenario, because they are licenses from the earlier Smart Licensing environment (they are already Smart licenses).

- Reporting after migration: For this example, refer to the sample output under ***show version*** *Before and After Migration*. The system messages that are displayed after software version upgrade show that the product instance has retained the connection to CSSM after migration and has already successfully synchronized with CSSM (reporting, authorization code, and policy). But a separate synchronization will be performed for this example, for the sake of clarity and completion.

  Subsequent reporting depends on the policy. After initial synchronization is completed, refer to the output of **show license status** command to know if and by when reporting is required. In the output check fields `Next report push` and `Next ACK deadline`. You will also receive system messages when reporting is required.

Show Commands Before and After Migration

show version Before and After Migration

```
------------------------------------------------------------------------------------------------------------
show version Before Migration
------------------------------------------------------------------------------------------------------------
```

The output here shows the software version before upgrade, followed by an excerpt of licensing-related system messages that were displayed when this earlier software version was loaded:

```
Device# show version
Cisco IOS XE Software, Version 16.12.04
Cisco IOS Software [Gibraltar], ISR Software
(X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.12.4, RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 09-Jul-20 21:44 by mcpre
<output truncated>



*Jul 23 13:36:25.062: %SMART_LIC-5-IN_COMPLIANCE: All entitlements and licenses in use on
this device are authorized
*Jul 23 13:36:25.064: %SMART_LIC-5-END_POINT_RESET: End Point list reset
*Jul 23 13:36:25.065: %SMART_LIC-6-AUTH_RENEW_SUCCESS: Authorization renewal successful.
State=authorized for udi PID:ISR4461/K9,SN:FDO222815Y4
```

```
------------------------------------------------------------------------------------------------------------
show version After Migration
------------------------------------------------------------------------------------------------------------
```

The output here shows the software version after migration, followed by an excerpt of the licensing-related system messages after system restart with the new image.

```
Device# show version
Cisco IOS Software [Amsterdam], ISR Software
(X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.2, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Sat 31-Oct-20 13:21 by mcpre
<output truncated>


<output truncated>
Press RETURN to get started!

*Jan 15 03:21:10.823: %CALL_HOME-6-CALL_HOME_ENABLED: Call-home is enabled by Smart Agent
for Licensing.
*Jan 15 03:21:15.341: %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement will
 be required
in 365 days.
*Jan 15 03:21:29.510: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was
successfully
installed on PID:ISR4461/K9,S:FDO222815Y4.
*Jan 15 03:21:31.981: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing
authorization code was
successfully installed on PID:ISR4461/K9,SN:FDO222815Y4
*Jan 15 03:26:07.805: %SIP-1-LICENSING: SIP service is Up. License report acknowledged.
*Jan 15 03:26:07.812: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
is allowed
for feature hseck9
*Jan 15 03:26:08.282: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was
successfully installed
<output truncated>
```

show license summary Before and After Migration

```
------------------------------------------------------------------------------------------------------
show license summary Before Migration
------------------------------------------------------------------------------------------------------
```

The output before migration shows that all licenses are REGISTERED and AUTHORIZED. Therefore, they will all be migrated and displayed as IN USE after migration.

```
Device# show license summary
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Eg-SA-01
  Virtual Account: Eg-VA-01
  Export-Controlled Functionality: ALLOWED
  Last Renewal Attempt: None
  Next Renewal Attempt: Jul 14 02:15:39 2021 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Feb 14 02:37:24 2021 UTC

License Usage:
  License                 Entitlement tag            Count Status
  -----------------------------------------------------------------------
  ISR_4400_Application    (ISR_4400_Application)         1 AUTHORIZED
  ISR_4400_UnifiedComm... (ISR_4400_UnifiedCommun...)    1 AUTHORIZED
  ISR_4400_Security       (ISR_4400_Security)            1 AUTHORIZED
  Booster Performance ... (ISR_4460_BOOST)               1 AUTHORIZED
  ISR_4400_Hsec           (ISR_4400_Hsec)                1 AUTHORIZED
```

```
------------------------------------------------------------------------------------------------------
show license summary After Migration
------------------------------------------------------------------------------------------------------
```

The output after migration shows that all five licenses have been migrated and are displayed with status IN USE.

```
Device# show license summary
License Usage:
  License                 Entitlement Tag            Count Status
  -----------------------------------------------------------------
  hseck9                  (ISR_4400_Hsec)                1 IN USE
  Booster Performance ... (ISR_4460_BOOST)               1 IN USE
  ISR_4400_Application    (ISR_4400_Application)         1 IN USE
  ISR_4400_UnifiedComm... (ISR_4400_UnifiedCommun...)    1 IN USE
  ISR_4400_Security       (ISR_4400_Security)            1 IN USE
```

show license status Before and After Migration

```
------------------------------------------------------------------------------------------------------
show license status Before Migration
------------------------------------------------------------------------------------------------------
```

The output before migration shows that Call Home is the configured transport type. Since all the licenses here have status REGISTERED, the transport type configuration will be retained as is after migration.

```
Device# show license status
Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: REGISTERED
  Smart Account: Eg-SA-01
  Virtual Account: Eg-VA-01
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Jan 15 02:15:40 2021 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Jul 14 02:15:39 2021 UTC
  Registration Expires: Jan 15 01:12:26 2022 UTC

License Authorization:
  Status: AUTHORIZED on Jan 15 02:37:24 2021 UTC
  Last Communication Attempt: SUCCEEDED on Jan 15 02:37:24 2021 UTC
  Next Communication Attempt: Feb 14 02:37:23 2021 UTC
  Communication Deadline: Apr 15 01:34:11 2021 UTC

License Conversion:
  Automatic Conversion Enabled: False
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>
```

---

show license status After Migration

The output after migration shows that the product instance is now in the Smart Licensing Using Policy environment (`Smart Licensing Using Policy: Status: ENABLED`).

The transport type is retained (`Type: Callhome`). Since the product instance has been able to communicate with CSSM at system restart (after software image upgrade), the following events have already occurred:

- A RUM report has been sent, and an ACK received (`Last report push: Jan 15 03:22:05 2021 UTC`, `Last ACK received: Jan 15 03:26:07 2021 UTC`).
- A policy that was returned with the ACK has been installed (`Policy in use: Installed On Jan 15 03:26:08 2021 UTC`) .
- A trust code that was returned with the ACK has also been installed (`Trust Code Installed: Jan 15 03:21:29 2021 UTC`).

```
Device# show license status

Utility:
  Status: DISABLED
```

```
Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Policy:
  Policy in use: Installed On Jan 15 03:26:08 2021 UTC
  Policy name: SLP Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 150 (Customer Policy)
    Report on change (days): 120 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: Jan 15 03:26:07 2021 UTC
  Next ACK deadline: Mar 16 03:26:07 2021 UTC
  Reporting push interval: 30  days
  Next ACK push check: <none>
  Next report push: Feb 14 03:22:05 2021 UTC
  Last report push: Jan 15 03:22:05 2021 UTC
  Last report file write: <none>

Trust Code Installed: Jan 15 03:21:29 2021 UTC
```

show license usage Before and After Migration

```
-----------------------------------------------------------------------------------------------------
show license usage Before Migration
-----------------------------------------------------------------------------------------------------
```

The output before migration shows all the licenses that are being used.

All licenses that have export status NOT RESTRICTED will have enforcement type NOT ENFORCED after migration.

Licenses that have export status RESTRICTED - ALLOWED, will continue to display the same after migration, and also have enforcement type EXPORT RESTRICTED.

```
Device# show license usage

License Authorization:
  Status: AUTHORIZED on Jan 15 02:37:24 2021 UTC

ISR_4400_Application (ISR_4400_Application):
  Description: AppX License for Cisco ISR 4400 Series
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED

ISR_4400_UnifiedCommunication (ISR_4400_UnifiedCommunication):
  Description: Unified Communications License for Cisco ISR 4400 Series
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED

ISR_4400_Security (ISR_4400_Security):
  Description: Security License for Cisco ISR 4400 Series
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED

Booster Performance License for 4460 Series (ISR_4460_BOOST):
  Description: Booster Performance License for 4460 Series
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED

ISR_4400_Hsec (ISR_4400_Hsec):
  Description: U.S. Export Restriction Compliance license for 4400 series
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: Export Controlled Feature hseck9
```

---

show license usage After Migration

The output after migration shows the licenses being used (`Status: IN USE`) and their enforcement type.

Licenses that do not require authorization are displayed with `Enforcement type: NOT ENFORCED`.

The export-controlled license which requires authorization before use is also correctly displayed with `Enforcement type: EXPORT RESTRICTED` and `Export status: RESTRICTED - ALLOWED`, which means that the required authorization is in place.

```
Device# show license usage

License Authorization:
  Status: Not Applicable

hseck9 (ISR_4400_Hsec):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
```

```
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Perpetual

Booster Performance License for 4460 Series (ISR_4460_BOOST):
  Description: Booster Performance License for 4460 Series
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: booster_performance
  Feature Description: booster_performance
  Enforcement type: NOT ENFORCED
  License type: Perpetual

ISR_4400_Application (ISR_4400_Application):
  Description: AppX License for Cisco ISR 4400 Series
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: appxk9
  Feature Description: appxk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

ISR_4400_UnifiedCommunication (ISR_4400_UnifiedCommunication):
  Description: Unified Communications License for Cisco ISR 4400 Series
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: uck9
  Feature Description: uck9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

ISR_4400_Security (ISR_4400_Security):
  Description: Security License for Cisco ISR 4400 Series
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: securityk9
  Feature Description: securityk9
  Enforcement type: NOT ENFORCED
```

show platform hardware throughput level Before and After Migration

```
------------------------------------------------------------------------------------------------------------
show platform hardware throughput level Before Migration
------------------------------------------------------------------------------------------------------------
```

The output before migration shows that the throughput level is unthrottled. On a Cisco ISR 4000 Series router, the Booster Performance license enables unthrottled Cisco Express Forwarding (CEF) throughput. There will therefore be no change in this configuration after migration.

```
Device# show platform hardware throughput level
The current throughput level is unthrottled
```

```
------------------------------------------------------------------------------------------------------------
show platform hardware throughput level After Migration
------------------------------------------------------------------------------------------------------------
```

The output after migration shows that the same throughput level configuration is the retained after migration.

```
Device# show platform hardware throughput level
The current throughput level is unthrottled
```

show platform software cerm-information Before and After Migration

```
------------------------------------------------------------------------------------------------------------
show platform software cerm-information Before Migration
------------------------------------------------------------------------------------------------------------
```

The output before migration shows that CERM functionality is disabled. There will be no change in this configuration after migration.

```
Device# show platform software cerm-information
Crypto Export Restrictions Manager(CERM) Information:
 CERM functionality: DISABLED
```

```
------------------------------------------------------------------------------------------------------------
show platform software cerm-information After Migration
------------------------------------------------------------------------------------------------------------
```

The output after migration shows that the same CERM configuration is retained after migration.

```
Device# show platform software cerm-information
Crypto Export Restrictions Manager(CERM) Information:
 CERM functionality: DISABLED
```

show license authorization Before and After Migration

```
------------------------------------------------------------------------------------------------------------
show license authorization Before Migration
------------------------------------------------------------------------------------------------------------
```

The **show license authorization** command is not available in the Smart Licensing environment. But for the purpose of verification before migration, the **show license usage** output above shows that the required authorization is in place. You could also use the **show license reservation** command to note the authorization code before migration, and check that the same is displayed after migration.

-

```
------------------------------------------------------------------------------------------------------------
show license authorization After Migration
------------------------------------------------------------------------------------------------------------
```

The output after migration shows that the authorization code has been migrated and honored (`Status: SMART AUTHORIZATION INSTALLED on Jan 15 03:21:31 2021 UTC`). If you have noted the authorization code before migration you can check that against the `Last Confirmation code:` field here - it will be the same.

```
Device# show license authorization
Overall status:
  Active: PID:ISR4461/K9,SN:FDO222815Y4
      Status: SMART AUTHORIZATION INSTALLED on Jan 15 03:21:31 2021 UTC
      Last Confirmation code: 30bdf595

Authorizations:
  ISR_4400_Hsec (ISR_4400_Hsec):
```

```
    Description: U.S. Export Restriction Compliance license for 4400 series
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:ISR4461/K9,SN:FDO222815Y4
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available

Derived Licenses:
  Entitlement Tag: regid.2017-12.com.cisco.ISR_4460_BOOST,
1.0_79633860-0c9a-472c-9306-bb2dfd1b030d
  Entitlement Tag: regid.2015-01.com.cisco.ISR_4400_Application,
1.0_da87444e-68bb-4821-8aab-63f8531a0430
  Entitlement Tag: regid.2014-12.com.cisco.ISR_4400_UnifiedCommunication,
1.0_ee2d8156-7e01-4f48-8cad-4859385e6524
  Entitlement Tag: regid.2014-12.com.cisco.ISR_4400_Security,
1.0_02ea4d4a-2469-46c1-afaf-d6cdfa1980aa
```

Required Tasks After Migration

As stated in the introduction above, the product instance has already synchronized with CSSM immediately after upgrade and no further action is actually required after migration here, until the next reporting and ACK deadline (Next ACK deadline: Mar 16 03:26:07 2021 UTC). For the sake of clarity and completion the applicable steps are displayed here:

1. Complete topology implementation.

   In this example, we're retaining the pre-migration configuration (The Connected Directly to CSSM, on page 18 topology with the transport type **callhome**. The corresponding workflow to refer to is: Workflow for Topology: Connected Directly to CSSM, on page 36.

   Smart Account set-up, product instance connection to CSSM, a connection method and transport type, and trust establishment with CSSM are all already complete. This completes topology implementation.

2. Synchronize license usage with CSSM, verify synchronization, and check subsequent reporting requirements.

   For this topology you can synchronize usage by entering the **license smart sync** command in privileged EXEC mode. This manually synchronizes (sends and receives) any pending data with CSSM.

   The sample configuration below shows this, followed by system messages that show successful synchronization, and confirm that the use of export-controlled features is allowed:

   ```
   Device# license smart sync local
   Device#
   *Jan 15 03:55:42.205: %SIP-1-LICENSING: SIP service is Up. License report acknowledged.
   *Jan 15 03:55:42.211: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
    is allowed for feature hseck9
   *Jan 15 03:55:42.686: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was
   successfully installed
   ```

   Verify synchronization by entering the **show license all** command in privileged EXEC mode. In the sample output below, the following fields help verify synchronization:

   - The updated timestamp here: `Policy in use: Installed On Jan 15 03:55:42 2021 UTC`

- The updated timestamp here: `Last ACK received: Jan 15 03:55:42 2021 UTC`

Check subsequent reporting requirements also, by entering the **show license all** command in privileged EXEC mode.

In the *Connected Directly to CSSM* topology, the *product instance* sends the next RUM report to CSSM, based on the policy. In the sample output, the following fields provide this information:

- `Next ACK deadline: Mar 16 03:55:42 2021 UTC`
- `Next report push: Feb 14 03:51:41 2021 UTC`

```
Device# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

License Conversion:
  Automatic Conversion Enabled: False
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Installed On Jan 15 03:55:42 2021 UTC
  Policy name: SLP Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 150 (Customer Policy)
    Report on change (days): 120 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
```

```
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Usage Reporting:
  Last ACK received: Jan 15 03:55:42 2021 UTC
  Next ACK deadline: Mar 16 03:55:42 2021 UTC
  Reporting push interval: 30  days
  Next ACK push check: <none>
  Next report push: Feb 14 03:51:41 2021 UTC
  Last report push: Jan 15 03:51:41 2021 UTC
  Last report file write: <none>

Trust Code Installed: Jan 15 03:21:29 2021 UTC

License Usage
=============

hseck9 (ISR_4400_Hsec):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Perpetual

Booster Performance License for 4460 Series (ISR_4460_BOOST):
  Description: Booster Performance License for 4460 Series
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: booster_performance
  Feature Description: booster_performance
  Enforcement type: NOT ENFORCED
  License type: Perpetual

ISR_4400_Application (ISR_4400_Application):
  Description: AppX License for Cisco ISR 4400 Series
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: appxk9
  Feature Description: appxk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

ISR_4400_UnifiedCommunication (ISR_4400_UnifiedCommunication):
  Description: Unified Communications License for Cisco ISR 4400 Series
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: uck9
  Feature Description: uck9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

ISR_4400_Security (ISR_4400_Security):
  Description: Security License for Cisco ISR 4400 Series
  Count: 1
```

```
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: securityk9
  Feature Description: securityk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

Product Information
===================
UDI: PID:ISR4461/K9,SN:FDO222815Y4

Agent Version
=============
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
======================
Overall status:
  Active: PID:ISR4461/K9,SN:FDO222815Y4
       Status: SMART AUTHORIZATION INSTALLED on Jan 15 03:21:31 2021 UTC
       Last Confirmation code: 30bdf595

Authorizations:
  ISR_4400_Hsec (ISR_4400_Hsec):
    Description: U.S. Export Restriction Compliance license for 4400 series
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:ISR4461/K9,SN:FDO222815Y4
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available


Derived Licenses:
  Entitlement Tag:
regid.2017-12.com.cisco.ISR_4460_BOOST,1.0_79633860-0c9a-472c-9306-bb2dfd1b030d
  Entitlement Tag:
regid.2015-01.com.cisco.ISR_4400_Application,1.0_da87444e-68bb-4821-8aab-63f8531a0430
  Entitlement Tag:
regid.2014-12.com.cisco.ISR_4400_UnifiedCommunication,1.0_ee2d8156-7e01-4f48-8cad-4859385e6524

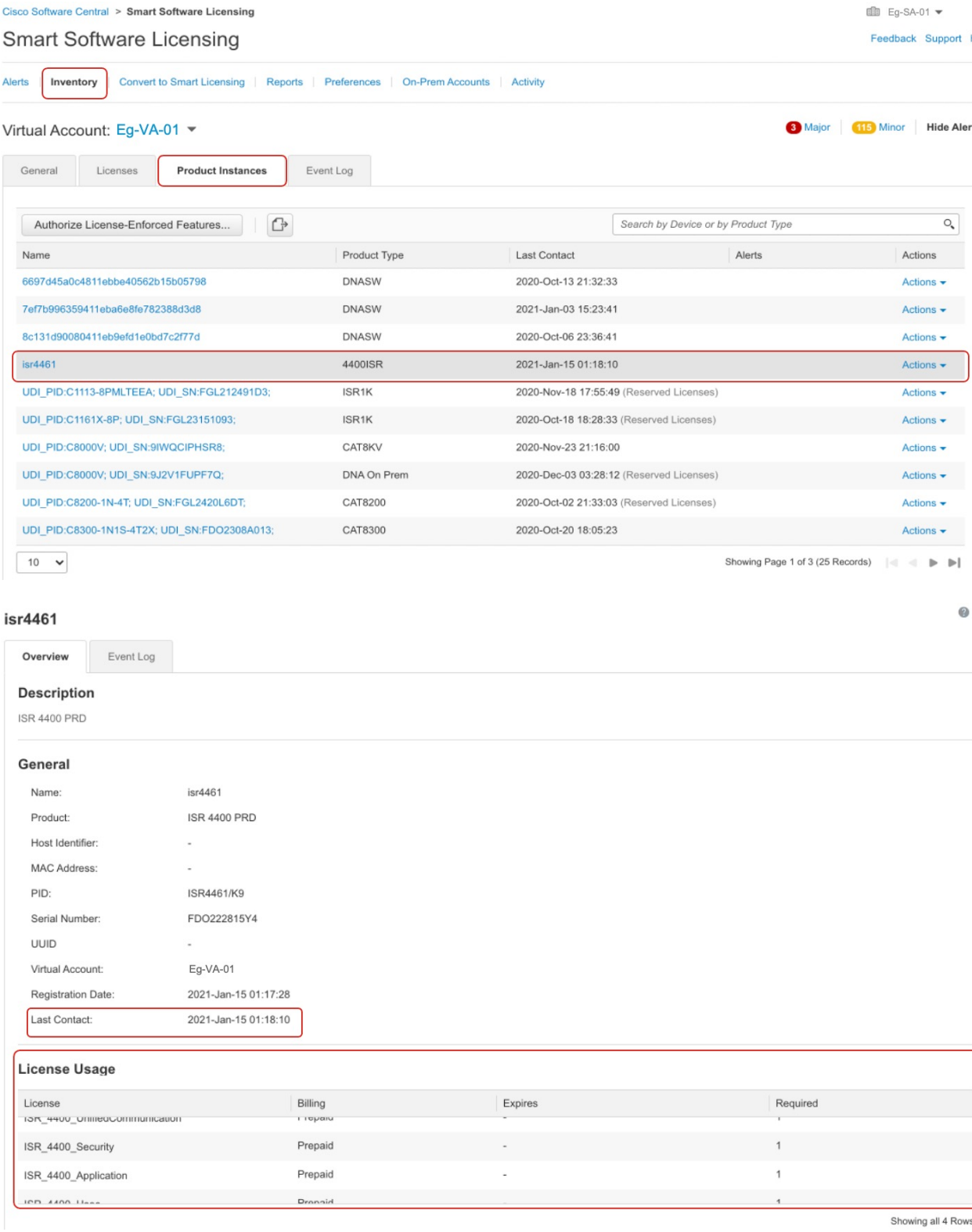
  Entitlement Tag:
regid.2014-12.com.cisco.ISR_4400_Security,1.0_02ea4d4a-2469-46c1-afaf-d6cdfa1980aa
```

CSSM Web UI Before and After Migration

Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**. In the applicable Smart Account and Virtual Account, go to **Inventory** > **Product Instances** to display all the product instances.

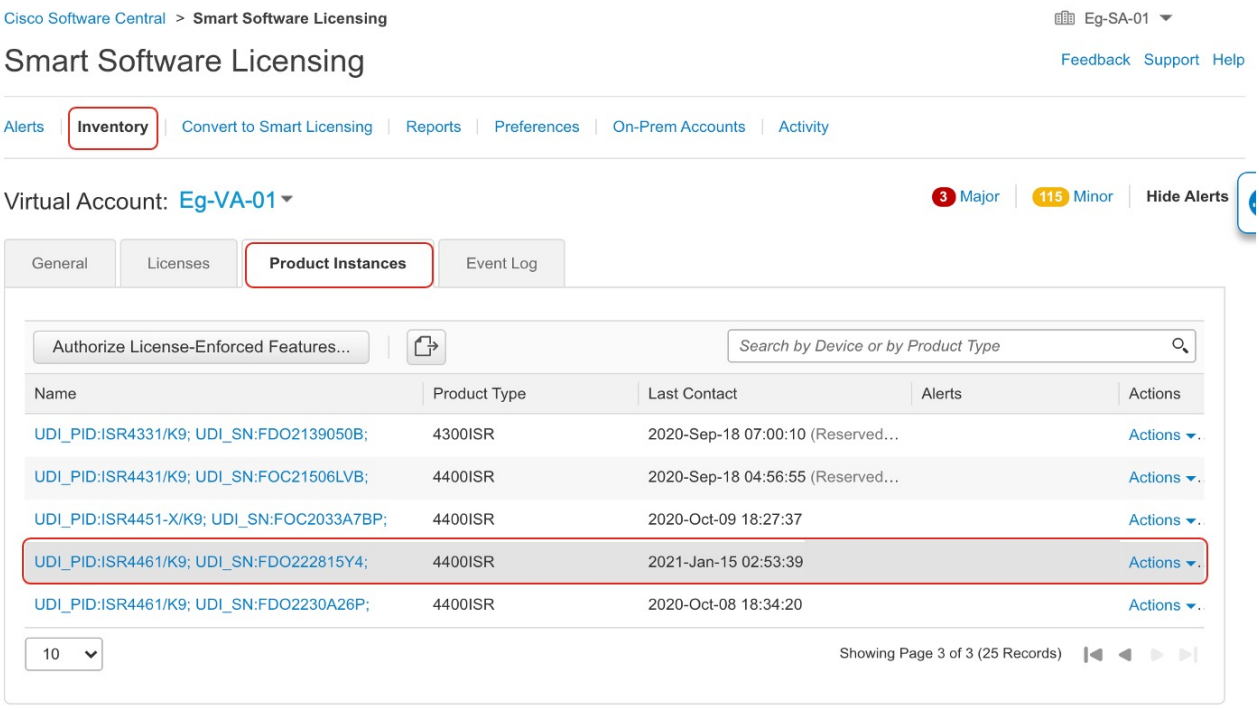
CSSM Web UI Before Migration

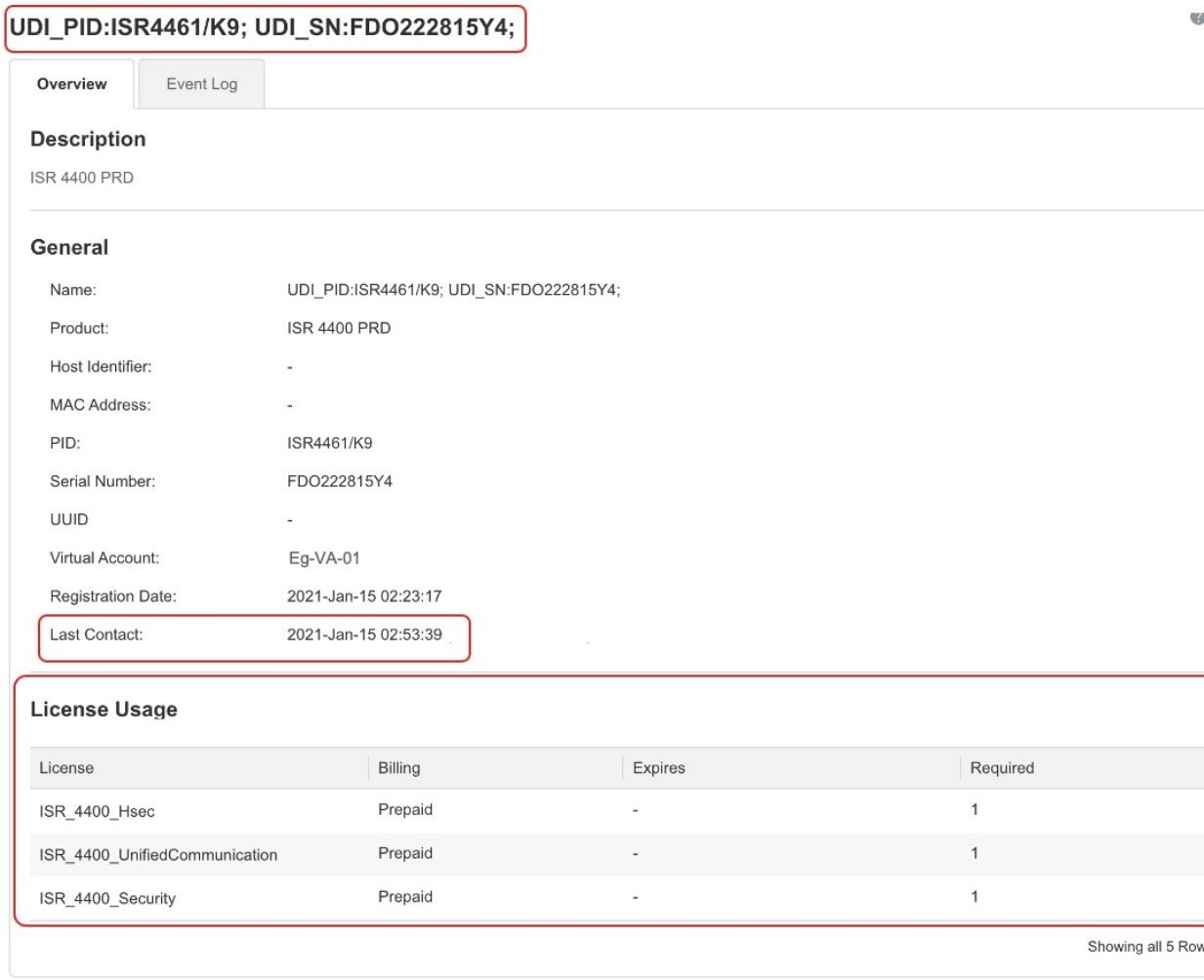
In the Smart Licensing environment, registered licenses are displayed with the hostname of the product instance in the **Name** column. Click on the product instance name to display detailed license usage information, as show in the next screenshot.



CSSM Web UI After Migration

After upgrade to Smart Licensing Using Policy, registered licenses are displayed with the UDI of the product instance in the **Name** column. In this example, the UDI is PID:ISR4461/K9,SN:FDO222815Y4. Click on the UDI to display detailed license usage information, as show in the next screenshot.





The following is a continuation of the license usage information (scrolled-down) - to display all the available licenses.



Example: Smart Licensing (SLR with Export-Controlled License) to Smart Licensing Using Policy

The following is an example of a **Cisco 1000 Series Integrated Services Router** migrating from Smart Licensing, where Specific License Reservation (SLR) is being used, to Smart Licensing Using Policy. More specifically, this is a case of an SLR with an export-controlled license, which means the SLR authorization code includes the HSECK9 authorization. The software version on the product instance is upgraded from Cisco IOS XE Gibraltar 16.12.4 to Cisco IOS XE Bengaluru 17.4.1.



Note The notion of "reservation" does not apply in the Smart Licensing Using Policy environment. The SLR equivalent here, is to implement the *No Connectivity to CSSM and No CSLU* topology. Once implemented, the product instance and CSSM are disconnected from each other, and the product instance cannot communicate online, with anything outside its network. When you upgrade from SLR, any existing SLR authorization codes are migrated - this includes authorization codes for export-controlled licenses as well. After migration, your topology itself enables you to operate in an air-gapped network and provides a way of meeting reporting requirements. No license reservation, registration, etc., applies.

- Enforcement type after migration: Two of the three licenses being used on the product instance are authorized (with an SLR authorization code). One of authorized licenses is an export-controlled license (ISR_1100_8P_Hsec). This license has the necessary authorization and will therefore be available after migration and have enforcement type: EXPORT RESTRICTED, after migration. See the point about a product instance with an SLR authorization code that includes an HSECK9 license here: How Upgrade Affects Enforcement Types for Existing Licenses, on page 54. SLAC installation after upgrade is not required.

  The third and remaining license, which does not have an SLR authorization code (**show license usage**: ISR_1100_8P_UnifiedCommunication, Reservation status: NOT INSTALLED) is not an export-controlled license (**show license usage**: Export status: NOT RESTRICTED). This will also be migrated and will have enforcement type NOT ENFORCED after migration.

- Transport type after migration: Since this an upgrade from SLR, when the software version is upgraded, the transport type will be set **off**.

- Device-Led Conversion (DLC): DLC does not apply to the licenses in this scenario, because they are authorized and reserved licenses from the earlier Smart Licensing environment (they are already Smart licenses).

- Reporting after migration: For initial synchronization, the RUM report will be manually uploaded to CSSM and the corresponding ACK will be installed on the product instance. This initial synchronization will also address usage reporting requirement for the ISR_1100_8P_UnifiedCommunication license, which did not have an authorization code in the pre-upgrade environment.

  The same reporting method applies to subsequent reporting - if reporting is required. After initial synchronization, refer to the output of **show license status** or **show license all** commands to know if and by when reporting is required. In the output check fields `Next report push` and `Next ACK deadline`. You will also receive system messages when reporting is required.

Show Commands Before and After Migration

show version Before and After Migration

```
------------------------------------------------------------------------------------------------------------
show version Before Migration
------------------------------------------------------------------------------------------------------------
```

The output here shows the software version before upgrade.

```
Device# show version
Cisco IOS XE Software, Version 16.12.04 Cisco IOS Software [Gibraltar],
ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version 16.12.4, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 25-Jun-20 12:56 by mcpre
<output truncated>
```

```
------------------------------------------------------------------------------------------------------------
show version After Migration
------------------------------------------------------------------------------------------------------------
```

The output here shows the software version after migration, and an excerpt of the licensing-related system messages that are displayed when the system restarts with the new image.

```
Device# show version
Cisco IOS XE Software, Version 17.4.1a Cisco IOS Software [Bengaluru],
ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version 17.4.1a, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 17-Dec-20 22:38 by mcpre
<output truncated>


<output truncated>
Press RETURN to get started!

*Jan 19 07:09:06.615: %SMART_LIC-6-RESERVED_INSTALLED:
Specific License Reservation Authorization code installed for
udi PID:C1111-8PLTEEAWB,SN:FGL214391JK
*Jan 19 07:09:06.616: %SMART_LIC-6-EXPORT_CONTROLLED:
Usage of export controlled features is not allowed
*Jan 19 07:09:07.174: %SMART_LIC-6-EXPORT_CONTROLLED:
Usage of export controlled features is allowed for feature hseck9
*Jan 19 07:09:09.163: %SMART_LIC-6-REPORTING_REQUIRED:
A Usage report acknowledgement will be required in 365 days.
<output truncated>
```

show license summary Before and After Migration

```
------------------------------------------------------------------------------------------------------------
show license summary Before Migration
------------------------------------------------------------------------------------------------------------
```

The output before migration shows that two licenses are AUTHORIZED, and one license is NOT AUTHORIZED. The uck9 license is *not* an export-controlled or enforced license, so all licenses will be migrated and all of the them will be displayed as IN USE.

```
Device# show license summary

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED
```

```
License Authorization:
  Status: NOT AUTHORIZED

License Usage:
  License                 Entitlement tag             Count Status
  -----------------------------------------------------------------------------
  Cisco 1100 Series wi... (ISR_1100_8P_Foundation...)     1 AUTHORIZED
                          (ISR_1100_8P_UnifiedCom...)     1 NOT AUTHORIZED
  hseck9                  (ISR_1100_8P_Hsec)              1 AUTHORIZED
```

---

show license summary After Migration

The output after migration shows that all three licenses have been migrated and are displayed with status IN USE.

```
Device# show license summary

License Reservation is ENABLED

License Usage:
  License                 Entitlement Tag             Count Status
  -----------------------------------------------------------------
  hseck9                  (ISR_1100_8P_Hsec)              1 IN USE
  uck9                    (ISR_1100_8P_UnifiedCom...)     1 IN USE
  FoundationSuiteK9       (ISR_1100_8P_Foundation...)     1 IN USE
```

show license status Before and After Migration

---

show license status Before Migration

The output before migration shows that default transport type is displayed - but because the licenses on this product instance are reserved licenses (SLR is effective), the transport type will be set to *off* after migration, to continue operating in an air-gapped network.

```
Device# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED
License Reservation is ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Jan 19 06:27:47 2021 UTC

License Authorization:
```

```
  Status: NOT AUTHORIZED

License Conversion:
  Automatic Conversion Enabled: False
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>
```

```
---------------------------------------------------------------------------------------------------
show license status After Migration
---------------------------------------------------------------------------------------------------
```

The output after migration shows that the product instance is now in the Smart Licensing Using Policy environment (`Smart Licensing Using Policy: Status: ENABLED`).

The transport type is set to Off (`Type: Transport Off`). This means the product instance cannot communicate with CSSM or anything outside the network.

For now, the default policy is effective. (When no other policy is available, the product instance applies the CISCO default policy). If a custom policy is available in CSSM the same will be installed after initial synchronization. The synchronization will also address the reporting that the current policy requires (`Next ACK deadline: Jan 19 07:09:09 2022 UTC`).

```
Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED
License Reservation is ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Transport Off

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
```

```
Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Jan 19 07:09:09 2022 UTC
  Reporting push interval: 30  days
  Next ACK push check: <none>
  Next report push: Jan 19 07:11:09 2021 UTC
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>
```

show license usage Before and After Migration

```
----------------------------------------------------------------------------------------------------
show license usage Before Migration
----------------------------------------------------------------------------------------------------
```

The output before migration shows all the licenses that are being used.

All licenses that have export status NOT RESTRICTED will have enforcement type NOT ENFORCED after migration. (This includes the one that has status NOT AUTHORIZED before migration).

The licenses that has export status RESTRICTED - ALLOWED, will continue to display the same after migration, and also have enforcement type EXPORT RESTRICTED.

All available authorization codes will be migrated. This includes the SLR authorization code for the ISR_1100_8P_FoundationSuite license (Reservation status: SPECIFIC INSTALLED), and the SLR authorization code for the export-controlled ISR_1100_8P_Hsec license (Reservation status: SPECIFIC EXPORT AUTHORIZATION KEY INSTALLED).

An SLR authorization code is not installed for the ISR_1100_8P_UnifiedCommunication license (Reservation status: NOT INSTALLED) there is therefore no code to migrate - but the license will be migrated.

```
Device# show license usage

License Authorization:
  Status: NOT AUTHORIZED

Cisco 1100 Series with 8 LAN Ports, Cisco One Foundation Suite (ISR_1100_8P_FoundationSuite):

  Description: Cisco 1100 Series with 8 LAN Ports, Cisco One Foundation Suite
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1

(ISR_1100_8P_UnifiedCommunication):
  Description:
  Count: 1
  Version: 1.0
  Status: NOT AUTHORIZED
  Export status: NOT RESTRICTED
  Reservation:
    Reservation status: NOT INSTALLED
```

```
hseck9 (ISR_1100_8P_Hsec):
  Description: Export Controlled Feature hseck9
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: Export Controlled Feature hseck9
  Reservation:
    Reservation status: SPECIFIC EXPORT AUTHORIZATION KEY INSTALLED
    Total reserved count: UNLIMITED

---------------------------------------------------------------------------------------------------
show license usage After Migration
---------------------------------------------------------------------------------------------------
```

The output after migration shows that all licenses that were being used, have been migrated, and all available authorization codes have also been migrated.

```
Device# show license usage

License Authorization:
  Status: Not Applicable

hseck9 (ISR_1100_8P_Hsec):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC EXPORT AUTHORIZATION KEY INSTALLED
    Total reserved count: UNLIMITED

uck9 (ISR_1100_8P_UnifiedCommunication):
  Description: uck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: uck9
  Feature Description: uck9
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: NOT INSTALLED

FoundationSuiteK9 (ISR_1100_8P_FoundationSuite):
  Description: FoundationSuiteK9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: FoundationSuiteK9
  Feature Description: FoundationSuiteK9
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1
```

show platform hardware throughput level and **show platform hardware throughput crpto** Before and After Migration

```
------------------------------------------------------------------------------------------------------------
show platform hardware throughput level and show platform hardware throughput crypto Before
 Migration
------------------------------------------------------------------------------------------------------------
```

The output before migration shows that the Cisco Express Forwarding (CEF) throughput and crypto throughput is unthrottled. The available HSECK9 license authorizes the use of unthrottled crypto throughput. There will therefore be no change in this configuration after migration.

```
Device# show platform hardware throughput level
The current throughput level is unthrottled

Device# show platform hardware throughput crypto
The current crypto level is unthrottled
```

```
------------------------------------------------------------------------------------------------------------
show platform hardware throughput level and show platform hardware throughput crypto After
 Migration
------------------------------------------------------------------------------------------------------------
```

The output after migration shows that the CEF throughput and crypto configuration is the same after migration.

```
Device# show platform hardware throughput level
The current throughput level is unthrottled

Device# show platform hardware throughput crypto
The current crypto level is unthrottled
```

show platform software cerm-information Before and After Migration

```
------------------------------------------------------------------------------------------------------------
show platform software cerm-information Before Migration
------------------------------------------------------------------------------------------------------------
```

The output before migration shows the throughput level is unthrottled. There will be no change in this configuration after migration.

```
Device# show platform software cerm-information
Crypto Export Restrictions Manager(CERM) Information:
 CERM functionality: DISABLED
```

```
------------------------------------------------------------------------------------------------------------
show platform software cerm-information After Migration
------------------------------------------------------------------------------------------------------------
```

The output after migration shows the CERM configuration is the same after migration.

```
Device# show platform software cerm-information
Crypto Export Restrictions Manager(CERM) Information:
 CERM functionality: DISABLED
```

show license authorization After Migration

```
------------------------------------------------------------------------------------------------------------
show license authorization Before Migration
------------------------------------------------------------------------------------------------------------
```

The **show license authorization** command is not available in the Smart Licensing environment. But for the purpose of verification before migration, the **show license usage** output above shows that the required authorization is in place. You could also use the **show license reservation** command to note the authorization code before migration, and check that the same is displayed after migration..

```
------------------------------------------------------------------------------------------------------
show license authorization After Migration
------------------------------------------------------------------------------------------------------
```

The output after migration shows that all available authorization codes have been migrated and honored (`Status: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC`, `Last Confirmation code: 0708eeec`).

```
Device# show license authorization

Overall status:
  Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
      Status: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
      Last Confirmation code: 0708eeec

Specified license reservations:
  Cisco 1100 Series with 8 LAN Ports,
Cisco One Foundation Suite (ISR_1100_8P_FoundationSuite):
    Description: Cisco 1100 Series with 8 LAN Ports,
Cisco One Foundation Suite
    Total reserved count: 1
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
        Authorization type: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
        License type: PERPETUAL
          Term Count: 1
  ISR_1100_8P_Hsec (ISR_1100_8P_Hsec):
    Description: Cisco 1100 Series with 8 LAN Ports,
U.S. Export Restriction Compliance license
    Total reserved count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
        Authorization type: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available


Derived Licenses:
  Entitlement Tag: regid.2017-08.com.cisco.ISR_1100_8P_Hsec,
1.0_34a5e7e7-722a-41ab-bdad-d53d5a3cac14
  Entitlement Tag: regid.2018-12.com.cisco.ISR_1100_8P_UnifiedCommunication,
1.0_55775cb5-538d-482e-b57f-fc8af02f93a3
  Entitlement Tag: regid.2017-04.com.cisco.ISR_1100_8P_FoundationSuite,
1.0_6f4a1f6f-b607-45cb-8bd0-d672ac06a314
```

Required Tasks After Migration

1. Complete topology implementation.

In this example, we're implementing the No Connectivity to CSSM and No CSLU topology. The corresponding workflow to follow is: Workflow for Topology: No Connectivity to CSSM and No CSLU, on page 45.

When migrating from SLR, the transport type is automatically set to **off**. The sample output of the **show license status** command after migration shows that this is done.

An export-controlled license is being used and the corresponding authorization code for this has been migrated. SLAC does not have to be installed again after upgrade.

This completes topology implementation to work in an air-gapped network.

2. Synchronize license usage with CSSM, verify synchronization, and check subsequent reporting requirements.

   For this topology, the RUM report must be saved to a file (on the product instance) and uploaded it to CSSM (from a workstation that has connectivity to the internet, and CSSM). The ACK must then be downloaded and installed on the product instance.

   a. Synchronize license usage with CSSM

      In the sample configuration shown below, the RUM report is saved to the flash memory of the product instance, in a file called *usage_report*. It is then transferred to a TFTP location for upload to CSSM:

```
Device# license smart save usage unreported file usage_report
Device# dir bootflash:
Directory of bootflash:/

73441   drwx            40960  Jan 19 2021 07:26:57 +00:00  tracelogs
23      -rw-             3950  Jan 19 2021 07:26:26 +00:00  usage_report
48961   drwx             4096  Jan 19 2021 07:09:15 +00:00  .installer
122401  drwx             4096  Jan 19 2021 07:08:36 +00:00  license_evlog
106082  drwx             4096  Jan 19 2021 07:08:23 +00:00  .geo
13      -rw-              30  Jan 19 2021 07:08:21 +00:00  throughput_monitor_params
171361  drwx             4096  Jan 19 2021 04:17:00 +00:00  .rollback_timer
11      -rw-        542523052  Jan 19 2021 04:14:17 +00:00
c1100-universalk9.16.12.04.SPA.bin

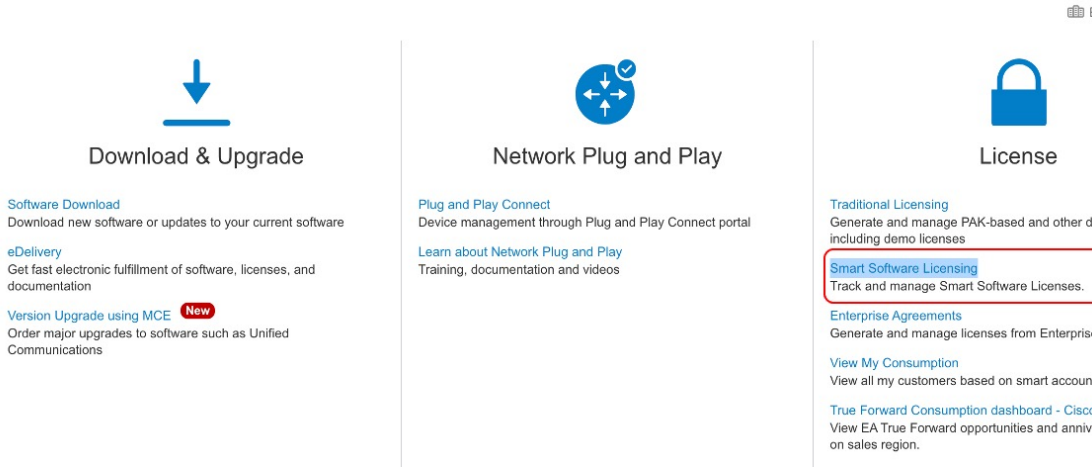
2908606464 bytes total (1558736896 bytes free)
<output truncated>


Device# copy bootflash:usage_report tftp://10.8.0.6//user01/usage_report
Address or name of remote host [10.8.0.6]?
Destination filename [/user01/usage_report]?
!!
3950 bytes copied in 0.012 secs (329167 bytes/sec)
```

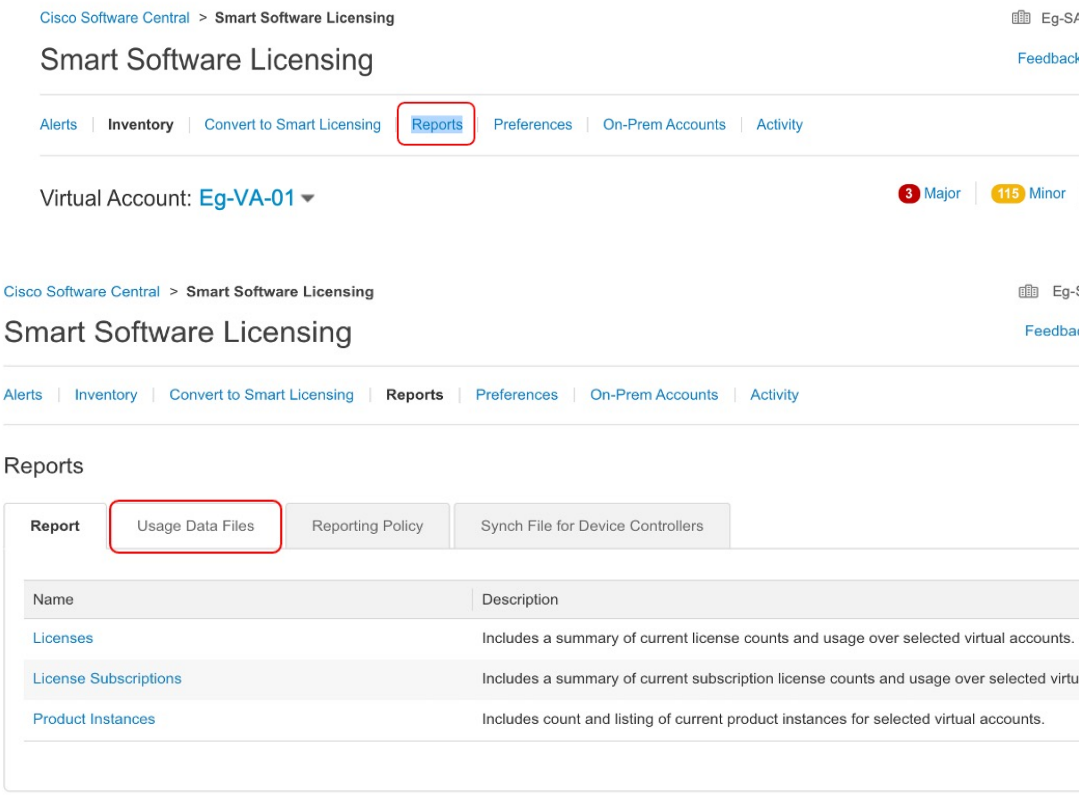
      In the screenshots and sample configuration shown below, the RUM report is uploaded to CSSM. After it is processed, the ACK is downloaded and installed on the product instance.

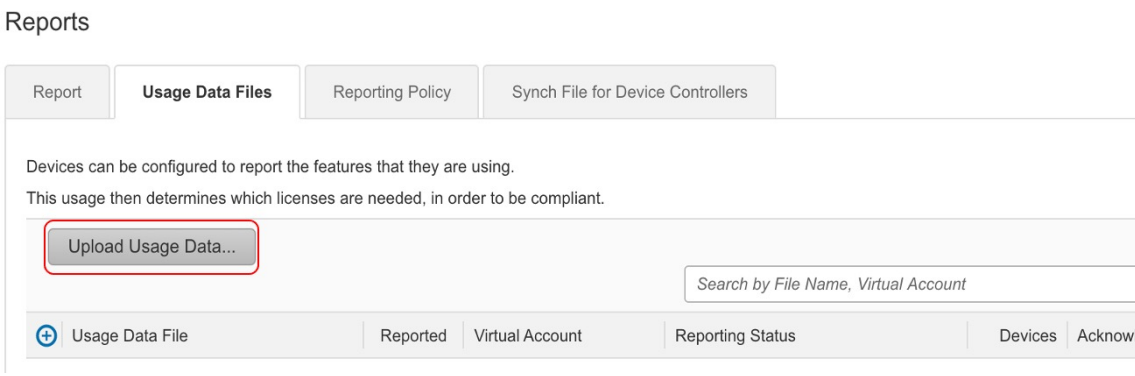
      The ACK is also furnished with a custom policy - as shown in the system messages that are displayed after the ACK is installed on the product instance.

      - Log in to the CSSM Web UI and select the **Smart Software Licensing** link.

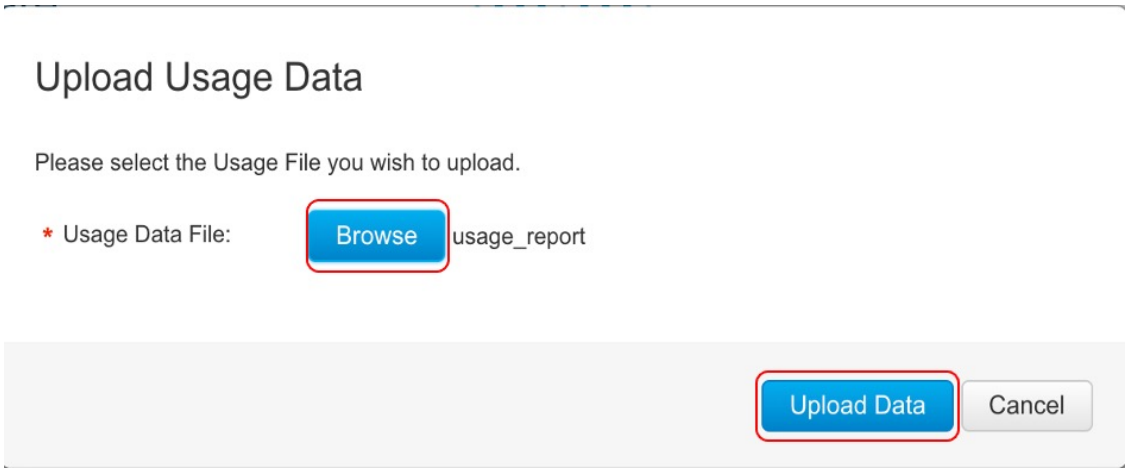


• Click**Reports** > **Usage Data Files** > **Upload Usage Data**, to upload the RUM report.

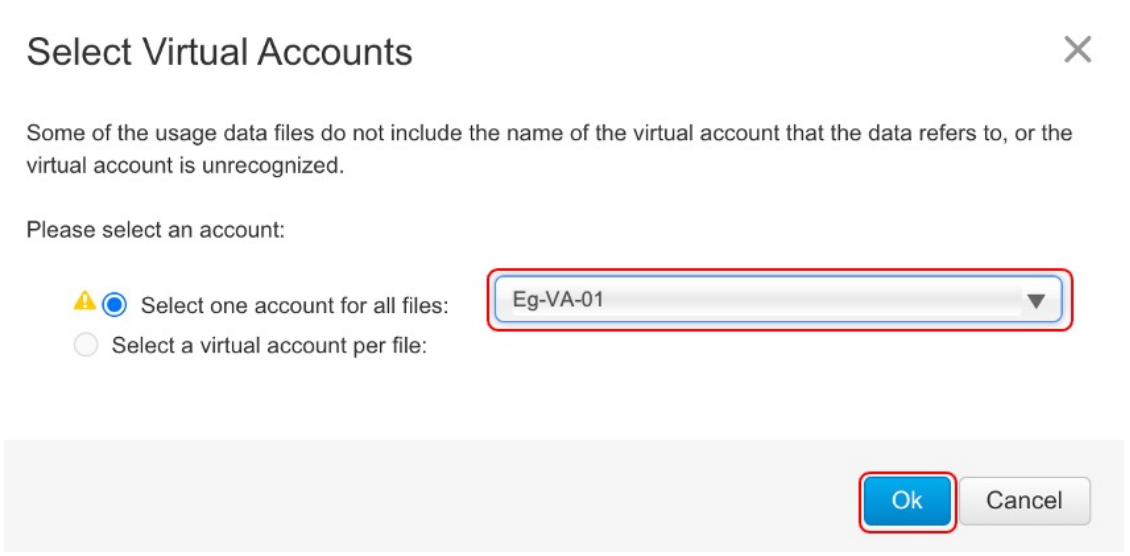


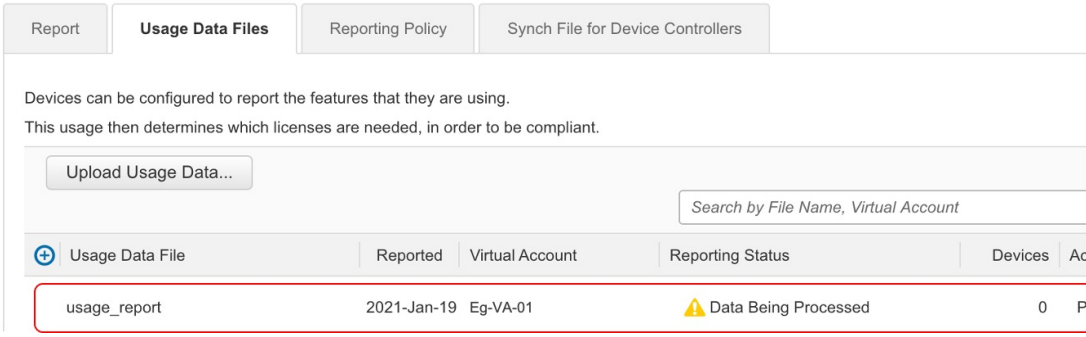


- Click **Browse** to locate the file, and the click **Upload Data**, to upload the RUM report:

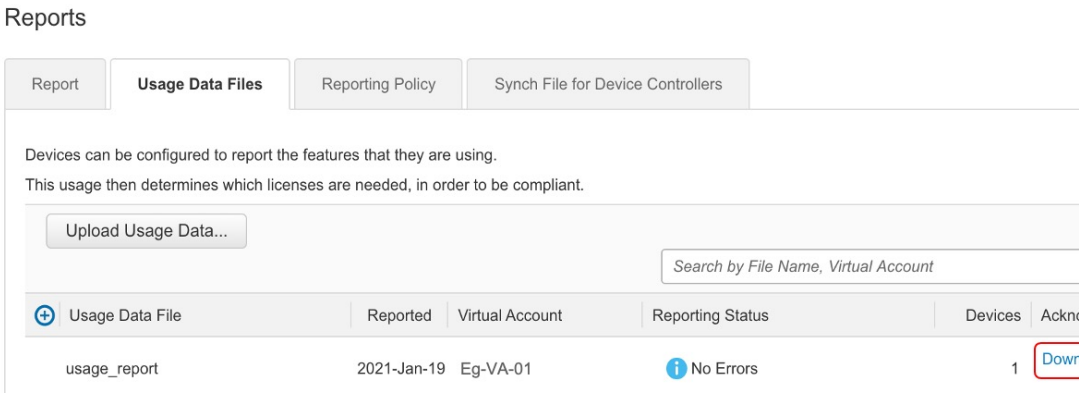


- Select the Virtual Account that will receive the RUM report and then wait for the ACK to appear in the Acknowledgement column:





- Wait for the reporting status to change to **No Errors** and then download the ACK:



- Copy the file from the downloaded location, save it in the flash memory of the product instance (**copy** *source* **bootflash:***file-name*), and install the ACK on the product instance:

```
Device# copy tftp://10.8.0.6//user01 bootflash:ACK_usage_report.txt

Device# license smart import bootflash: ACK_usage_report.txt
Import Data Successful
Device#
*Jan 19 07:50:33.311: %SIP-1-LICENSING: SIP service is Up. License report
acknowledged.
*Jan 19 07:50:33.667: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled
 features is allowed for feature hseck9
*Jan 19 07:50:34.131: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
 was successfully installed
```

b. Verify synchronization and check updated policy to know about subsequent reporting requirements.

In the sample output below, the following fields help verify synchronization:

- The updated timestamp here: `Policy in use: Installed On Jan 19 07:50:34 2021 UTC`
- The updated timestamp here: `Last ACK received: Jan 19 07:50:33 2021 UTC`

If subsequent reporting is required, this is indicated in the policy and system messages are displayed. You then have to upload the RUM report as shown in Step 2 above (including all substeps). In the sample output, the following fields provide information about if and when reporting is required:

- `Next report push: Jan 19 07:51:04 2021 UTC`

- Next ACK deadline: Feb 18 07:50:34 2021 UTC

```
Device# show license all
Smart Licensing Status
======================

Smart Licensing is ENABLED
License Reservation is ENABLED

License Conversion:
  Automatic Conversion Enabled: False
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Transport Off

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Installed On Jan 19 07:50:34 2021 UTC
  Policy name: SLP Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 150 (Customer Policy)
    Report on change (days): 120 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Usage Reporting:
  Last ACK received: Jan 19 07:50:33 2021 UTC
  Next ACK deadline: Feb 18 07:50:34 2021 UTC
  Reporting push interval: 30  days
  Next ACK push check: <none>
  Next report push: Jan 19 07:51:04 2021 UTC
  Last report push: <none>
  Last report file write: <none>
```

```
Trust Code Installed: <none>

License Usage
=============

hseck9 (ISR_1100_8P_Hsec):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC EXPORT AUTHORIZATION KEY INSTALLED
    Total reserved count: UNLIMITED

uck9 (ISR_1100_8P_UnifiedCommunication):
  Description: uck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: uck9
  Feature Description: uck9
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: NOT INSTALLED

FoundationSuiteK9 (ISR_1100_8P_FoundationSuite):
  Description: FoundationSuiteK9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: FoundationSuiteK9
  Feature Description: FoundationSuiteK9
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1

Product Information
===================
UDI: PID:C1111-8PLTEEAWB,SN:FGL214391JK

Agent Version
=============
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
======================
Overall status:
  Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
      Status: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
      Last Confirmation code: 0708eeec

Specified license reservations:
  Cisco 1100 Series with 8 LAN Ports, Cisco One Foundation Suite
```

```
(ISR_1100_8P_FoundationSuite):
    Description: Cisco 1100 Series with 8 LAN Ports, Cisco One Foundation Suite
    Total reserved count: 1
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
        Authorization type: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
        License type: PERPETUAL
          Term Count: 1
  ISR_1100_8P_Hsec (ISR_1100_8P_Hsec):
    Description: Cisco 1100 Series with 8 LAN Ports, U.S. Export Restriction Compliance
 license
    Total reserved count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
        Authorization type: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available


Derived Licenses:
  Entitlement Tag:
regid.2017-08.com.cisco.ISR_1100_8P_Hsec,1.0_34a5e7e7-722a-41ab-bdad-d53d5a3cac14
  Entitlement Tag:
regid.2018-12.com.cisco.ISR_1100_8P_UnifiedCommunication,1.0_55775cb5-538d-482e-b57f-fc8af02f93a3

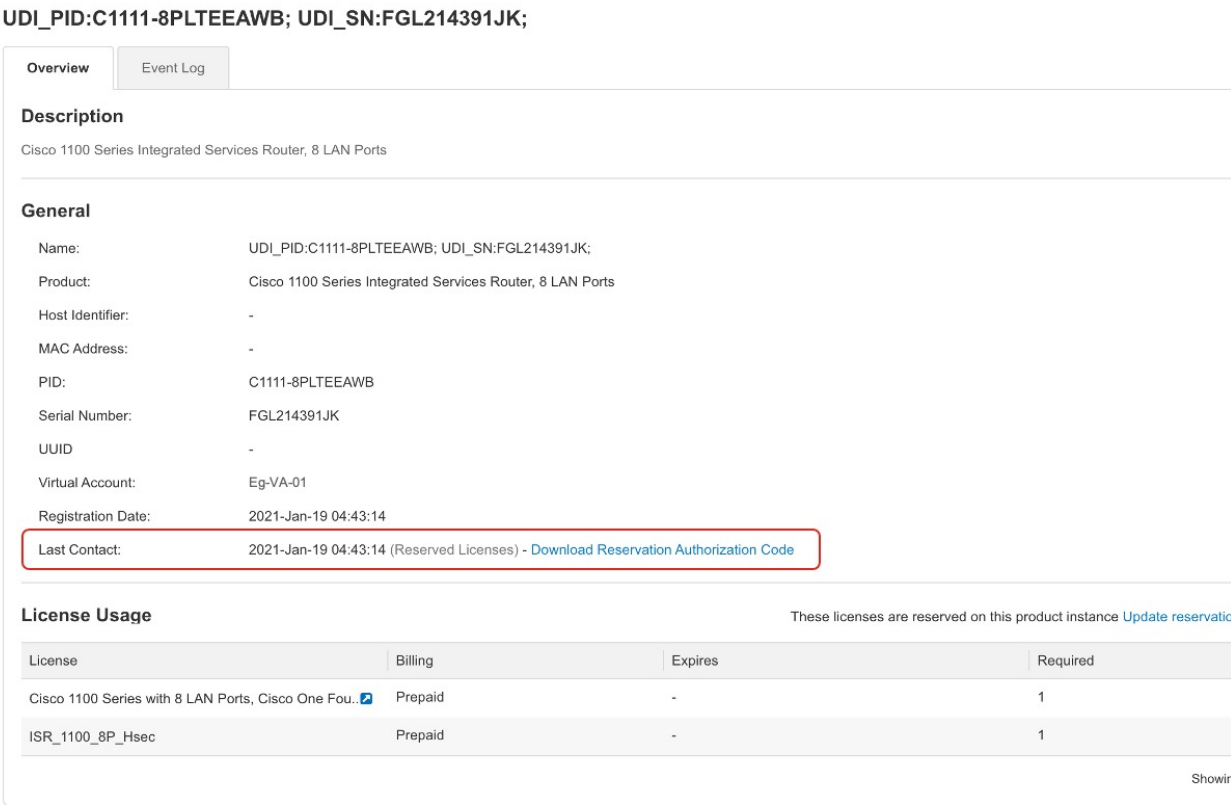
  Entitlement Tag:
regid.2017-04.com.cisco.ISR_1100_8P_FoundationSuite,1.0_6f4a1f6f-b607-45cb-8bd0-d672ac06a314
```

CSSM Web UI Before and After Migration

Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**. In the applicable Smart Account and Virtual Account, go to **Inventory** > **Product Instances** to display all the product instances.

CSSM Web UI Before Migration

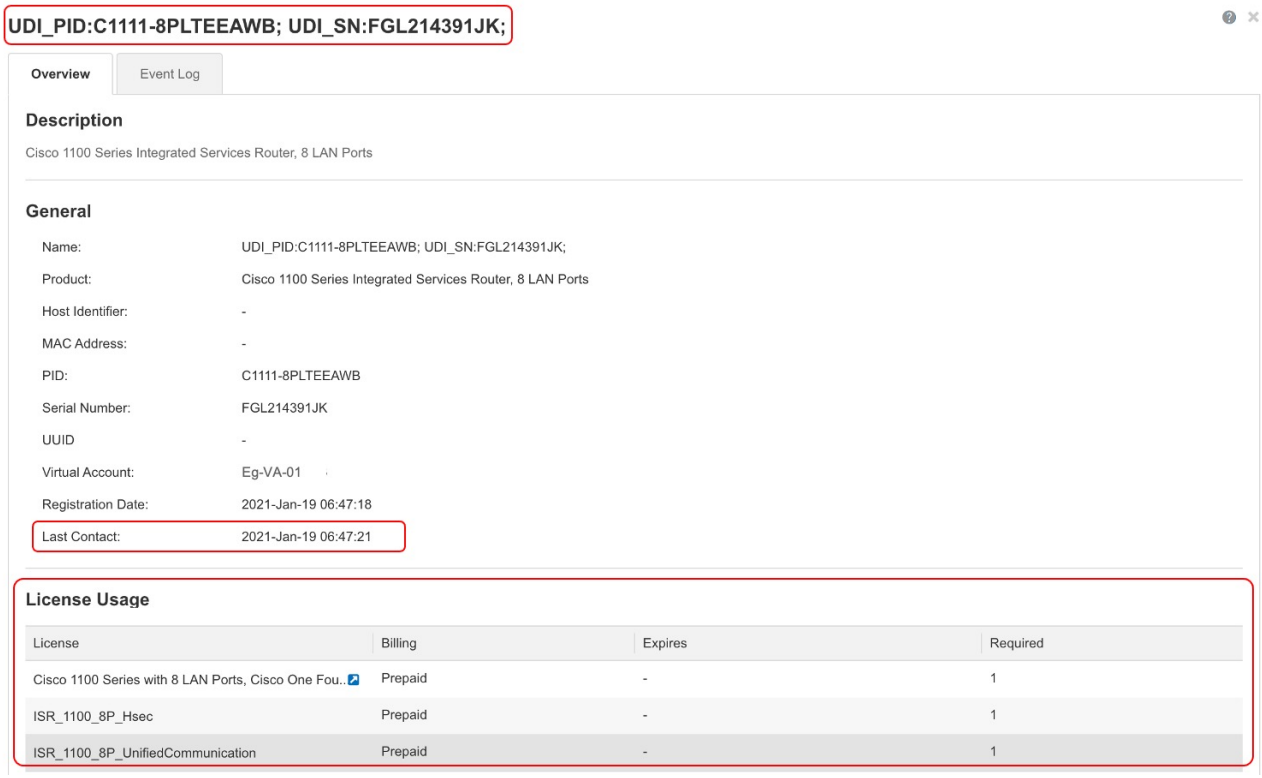
From the **Product Instances** tab, click on the UDI to display detailed license usage information as shown below.



CSSM Web UI After Migration

From the **Product Instances** tab, click on the UDI to display detailed license usage information as shown below.

After upgrade to Smart Licensing Using Policy, and after the requisite RUM report is uploaded the **Last Contact** field is updated.



Example: Smart Licensing (SLR With Throughput >250 Mbps, Without Export-Controlled License) to Smart Licensing Using Policy

The following is an example of a **Cisco Cloud Services Router 1000v** migrating from Smart Licensing, where Specific License Reservation (SLR) licenses are being used, to Smart Licensing Using Policy. The software version on the product instance is upgraded from Cisco IOS XE Gibraltar 16.12.2 (CSRv .bin image) to Cisco IOS XE Bengaluru 17.6.1 (Catalyst 8000V software image) for Smart Licensing Using Policy support.



Important All Cisco Cloud Services Routers 1000v and Cisco Integrated Services Virtual Routers where throughput greater than 250 Mbps is configured, have the export-control flag in CSSM enabled to allow throughput greater than 250 Mbps - and not an HSECK9 license. The product instance in this example also has throughput greater than 250 Mbps, further, it is using reserved licenses. So its SLR code does not include an HSECK9 license, rather, the export-control flag in CSSM is enabled.

U.S. export control regulations no longer allow the use of the export control flag as a way of authorizing throughput greater than 250 Mbps. SLAC installation is therefore required in the Smart Licensing Using Policy environment. (See Authorization Code, on page 4).

If throughput is lesser than or equal to 250 Mbps, SLAC installation is not required.

When upgrading a product instance as in this example, we recommend updating the SLR authorization code to include the applicable HSECK9 license *before* upgrading the product instance, so that you have uninterrupted throughput after upgrade. This example shows you how to do it this way. If you upgrade the software image without performing this task 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.

The following is a summary of what to expect after upgrade for this example:

- Enforcement type after migration: The reserved licenses on the product instance are being updated prior to upgrade, to include an HSECK9 license in the SLR authorization code. See section *Required Tasks Before Migration* below. Two licenses are therefore available on the product instance before upgrade. The HSECK9 license will be available after migration and have enforcement type: EXPORT RESTRICTED. The remaining license will be available with enforcement type: NOT ENFORCED, after migration.
- Transport type after migration: Since this an upgrade from SLR, when the software version is upgraded, the transport type will be set **off**.
- Device-Led Conversion (DLC): DLC does not apply to the licenses in this scenario, because they are authorized and reserved licenses from the earlier Smart Licensing environment (they are already Smart licenses).
- Reporting after migration: For initial synchronization, the RUM report will be manually uploaded to CSSM and the corresponding ACK will be installed on the product instance.

  The same reporting method applies to subsequent reporting - if reporting is required. After initial synchronization, refer to the output of **show license status** or **show license all** commands to know if and by when reporting is required. In the output check fields `Next report push` and `Next ACK deadline`. You will also receive system messages when reporting is required.

Required Tasks *Before* Migration

When using throughput greater than 250 Mbps with the export control flag enabled in CSSM, ensure uninterrupted throughput on upgrade to Smart Licensing Using Policy, by adding an HSECK9 license to the SLR code *before* you upgrade the software version on the product instance.



Note At this point the product instance is still in the earlier Smart Licensing environment, therefore the corresponding commands apply.

1. Display licenses that are currently available on the product instance.

```
Device# show version
Cisco IOS XE Software, Version 16.12.02
Cisco IOS Software [Gibraltar], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 16.12.2, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Thu 22-Jul-21 10:23 by mcpre

<output truncated>
```

```
Device# show license summary
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED

License Authorization:
```

```
  Status: AUTHORIZED - RESERVED

License Usage:
  License                  Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  CSR 1KV AX 10G           (ax_10G)                          1 AUTHORIZED


Device# show license reservation
License reservation: ENABLED

Overall status:
  Active: PID:CSR1000V,SN:95QS2T1KUJX
      Reservation status: SPECIFIC INSTALLED on Jul 09 21:10:37 2021 UTC
      Export-Controlled Functionality: ALLOWED
      Last Confirmation code: 4372613e

Specified license reservations:
  CSR 1KV AX 10G (ax_10G):
    Description: CSR 1KV AX 10G
    Total reserved count: 1
    Term information:
      Active: PID:CSR1000V,SN:95QS2T1KUJX
        License type: PERPETUAL
          Term Count: 1
```

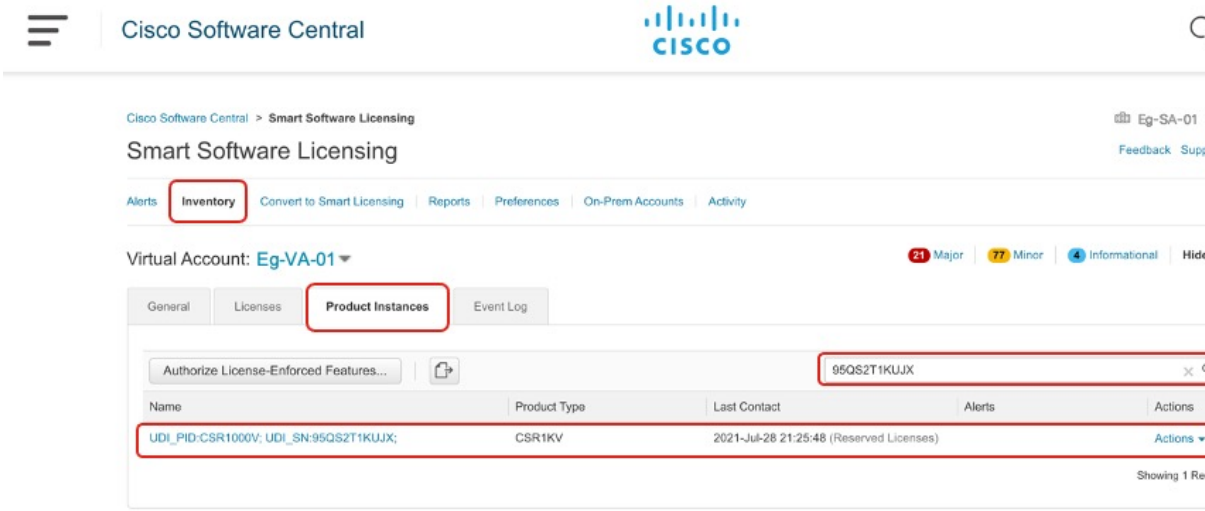
2. Update the reservation code in CSSM.
   a. Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**.

      Log in using the username and password provided by Cisco.

   b. In the corresponding Smart Account and Virtual Account, navigate to **Inventory** > **Licences**, ensure that a positive balance of the applicable DNA HSECK9 license (Router US Export Lic for DNA) is available.

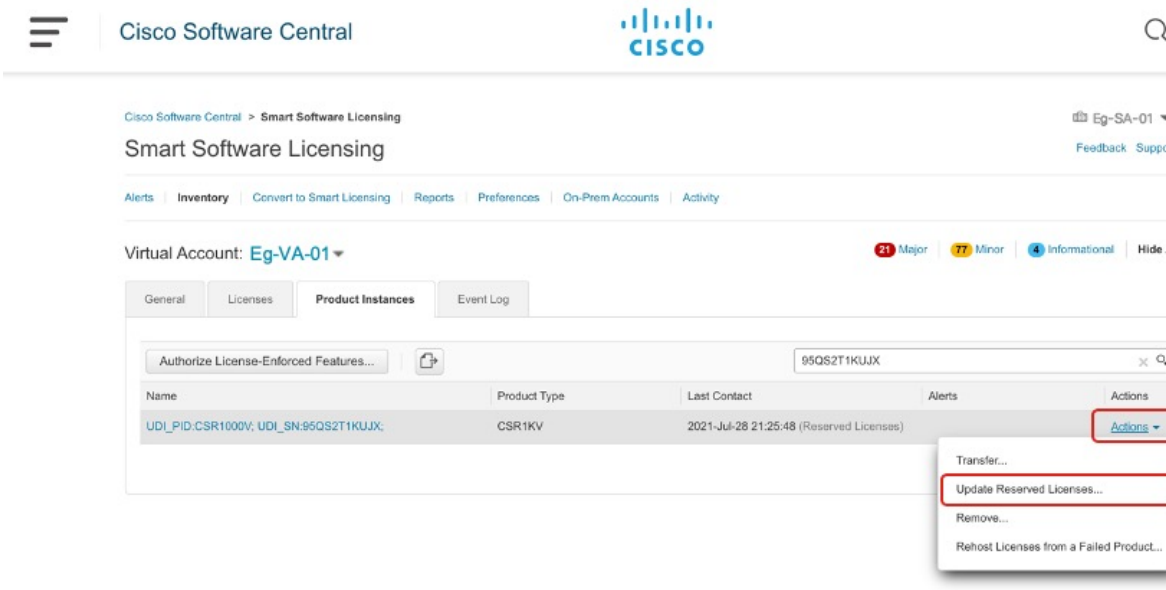
   c. Click the **Product Instances** tab use the search function to locate the product instance

      In this example, we're using the serial number (95QS2T1KUJX) to locate the product instance.



   d. From the **Actions** column of the located product instance, select **Update Reserved Licenses**.

      The **Update Reservation License** window is displayed.

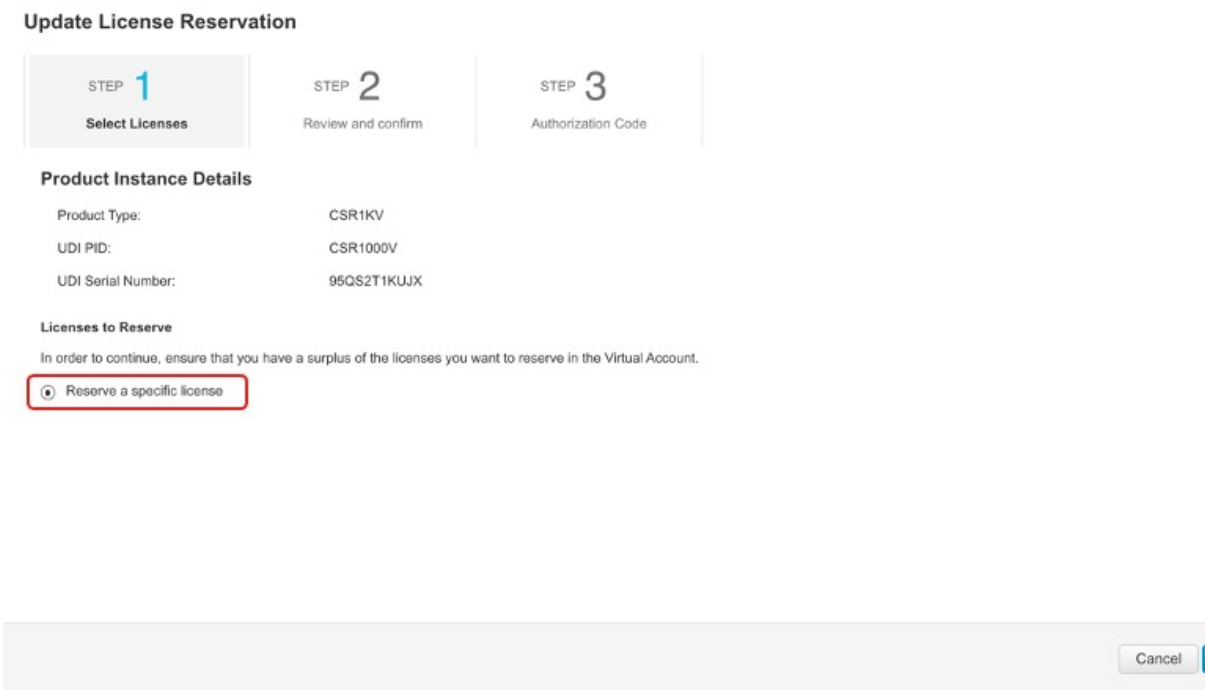


e. Select the **Reserve a specific license** radio button.

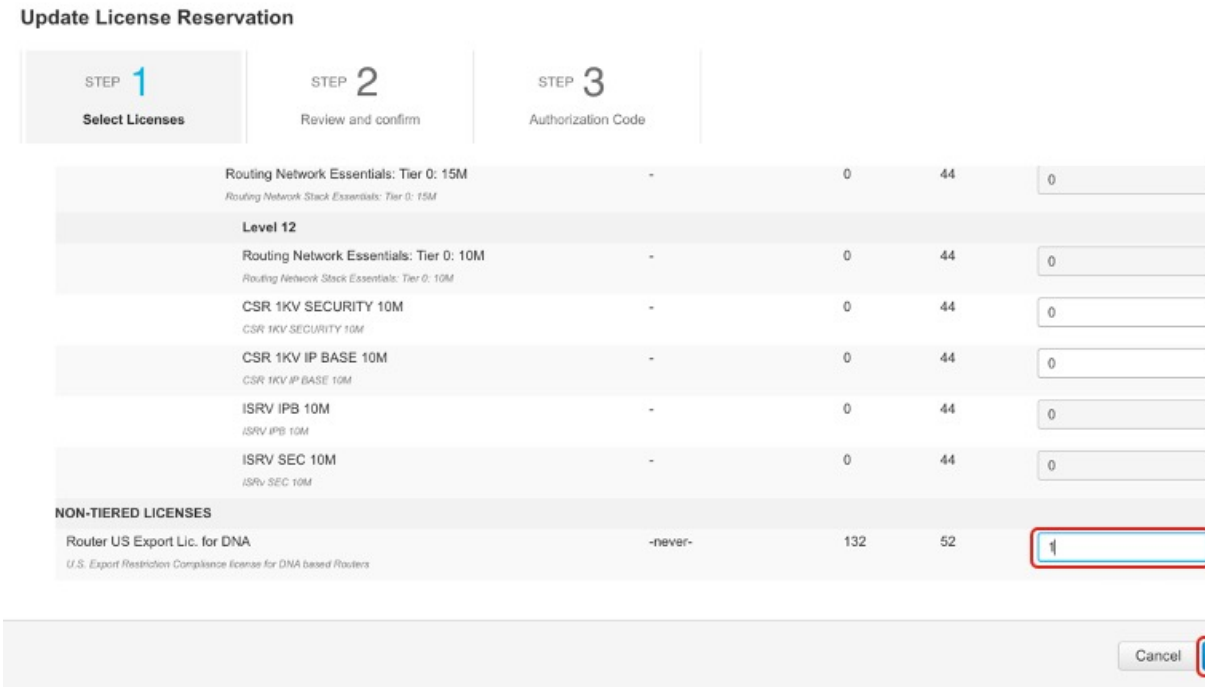
A table with all available licenses on the product instance is displayed and an HSECK9 license is automaticaly included in the list since this Smart Account and Virtual Account has a positive balance of HSECK9 licenses.

Ensure that you select the correct HSECK9 license for a product instance, see HSECK9 License Mapping Table for Routing Product Instances, on page 231.

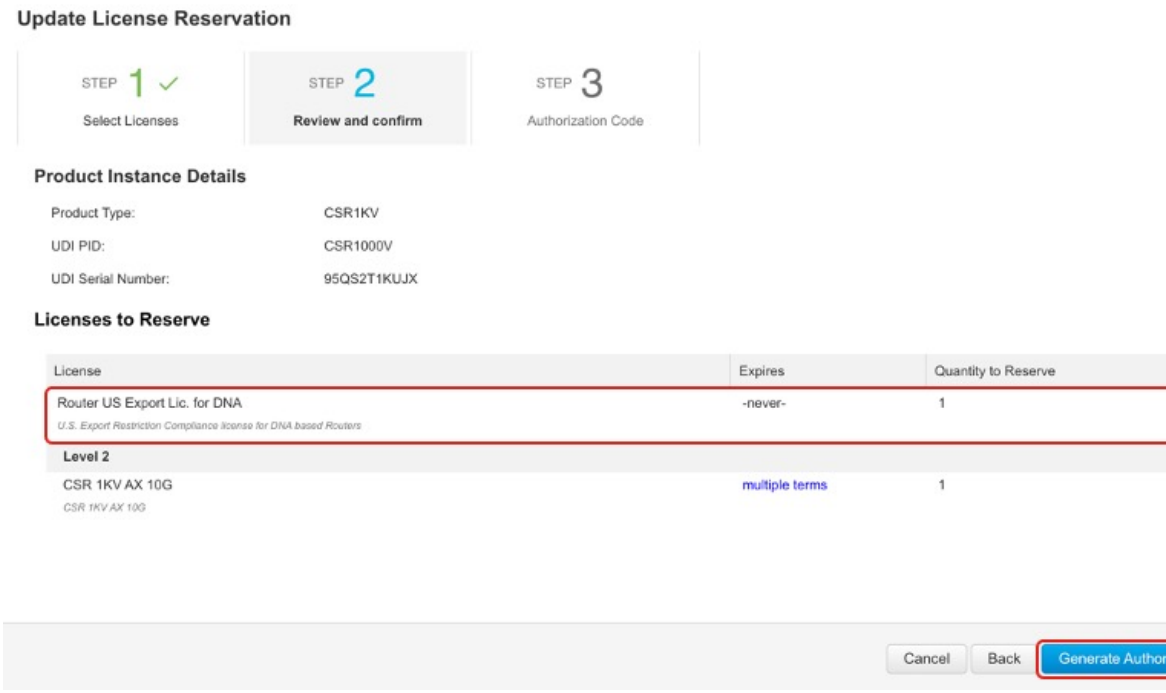
In this example, the "Router US Export Lic for DNA" is selected. (All virtual platforms use this HSECK9 license; this is also called the "DNA_HSEC"license). Other product instances, such as an ISR 1000 or ISR 4000 may require a different product-specific HSECK9 license.



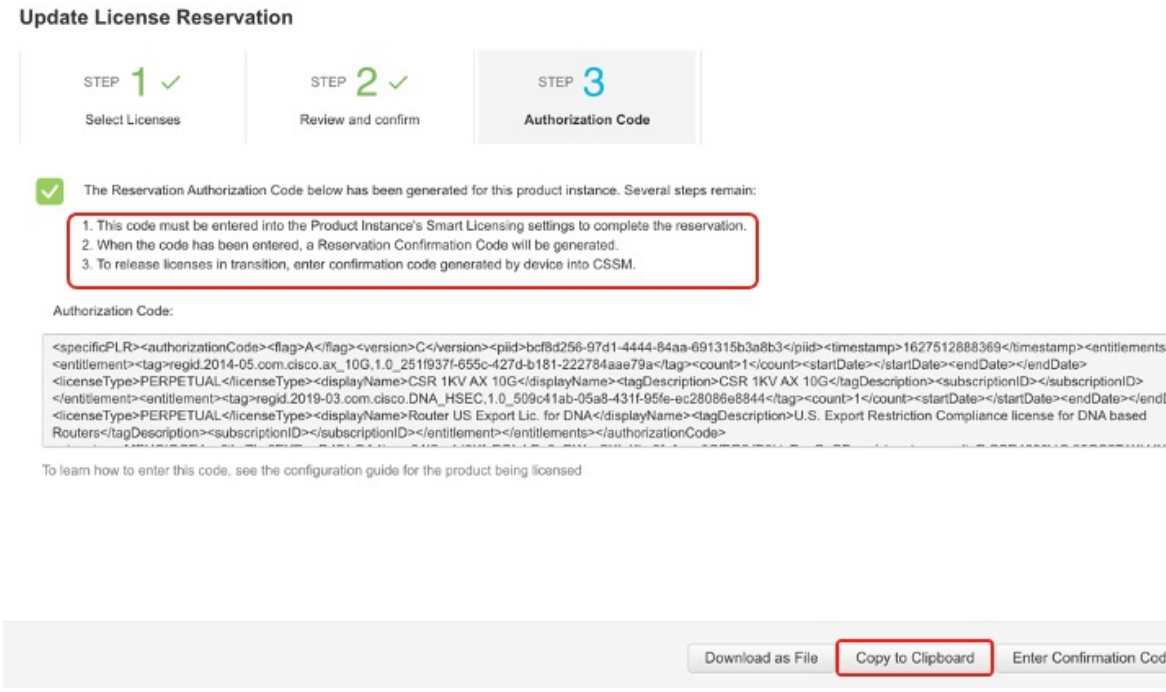
f. In the corresponding **Reserve** column, enter `1` and click **Next**.



g. Click **Generate Authorization Code**.



h. Click **Copy to Clipboard** and save the authorization code in a file.



Note Do not click **Close** yet. Keep this window open and proceed to next step.

3. Save and install the authorization code on the product instance.
   a. On the product instance, enter the **copy***source***bootflash:***file name* command in privileged EXEC mode, to save the authorization code file in the bootflash of the product instance. For example:

      ```
      Device# copy tftp://10.8.0.6/bootflash:slr_code_02
      ```

   b. On the product instance, enter the **license smart reservation install file** {**bootflash:***filename* command in privileged EXEC mode, to install the authorization code. For example:

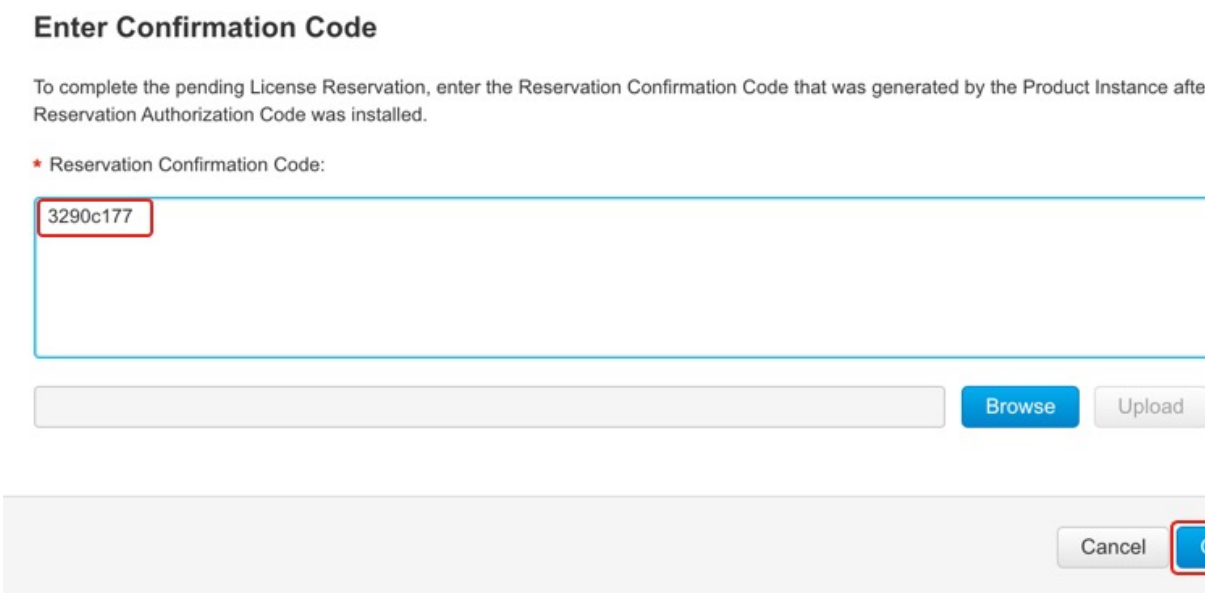
      ```
      Device# license smart reservation install file bootflash:slr_code_02
      Reservation install file successful
      Last Confirmation code UDI: PID:CSR1000V,SN:95QS2T1KUJX
          Confirmation code: 3290c177
      ```

   c. Copy the confirmation code.

4. Enter the confirmation code in CSSM, and then verify the list of licences on the product instance
   a. Go back to the **Update Reservation License** window in the CSSM Web UI and click **Enter Confirmation Code**.

      The **Enter Confirmation Code** window is displayed.

   b. Paste the confirmation code and click **OK**.



   c. On the product instance, enter the **show license reservation** command in privileged EXEC mode.

      Along with the existing ax_10G license, a DNA_HSEC license and the new confirmation code is displayed:

      ```
      Device# show license reservation
      License reservation: ENABLED

      Overall status:
        Active: PID:CSR1000V,SN:95QS2T1KUJX
            Reservation status: SPECIFIC INSTALLED on Jul 28 20:46:46 2021 UTC
            Export-Controlled Functionality: ALLOWED
            Last Confirmation code: 3290c177
      ```

```
Specified license reservations:
  CSR 1KV AX 10G (ax_10G):
    Description: CSR 1KV AX 10G
    Total reserved count: 1
    Term information:
      Active: PID:CSR1000V,SN:95QS2T1KUJX
        License type: PERPETUAL
          Term Count: 1
  Router US Export Lic. for DNA (DNA_HSEC):
    Description: U.S. Export Restriction Compliance license for DNA based Routers
    Total reserved count: 1
    Term information:
      Active: PID:CSR1000V,SN:95QS2T1KUJX
        License type: PERPETUAL
          Term Count: 1
```



Note This is now a product instance where the SLR authorization code includes authorization for an HSECK9 license and will be honored after upgrade. SLAC installation after upgrade is therefore not required.

5. Reload the device with a software version that supports Smart Licensing Using Policy.

   The product instance comes up with the previously configured (pre-upgrade) throughput. See section *Show Commands After Migration* below.

Show Commands After Migration

show version After Migration

```
------------------------------------------------------------------------------------------------------------
show version After Migration
------------------------------------------------------------------------------------------------------------
```

The output here shows the software version after upgrade. Further, note that the software version installed is the Catalyst 8000V software image.

```
Device# show version
Cisco IOS XE Software, Version 17.6.1
Cisco IOS Software [Bengaluru], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 17.6.1
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Sat 24-Jul-21 11:21 by mcpre

<output truncated>

ROM: IOS-XE ROMMON

Router uptime is 1 minute
Uptime for this control processor is 2 minutes
System returned to ROM by reload
System image file is "bootflash:c8000v-universalk9.SSA.bin"
Last reload reason: Reload Command
```

show show license summary After Migration

```
------------------------------------------------------------------------------------------------------------
show license summary After Migration
------------------------------------------------------------------------------------------------------------
```

The output here shows that the export-controlled HSECK9 license and the ax_10G have been migrated.

```
Device# show licence summary
License Reservation is ENABLED

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  hseck9                  (DNA_HSEC)                        1 IN USE
  ax_10G                  (ax_10G)                          1 IN USE
```

show license usage After Migration

```
------------------------------------------------------------------------------------------------------------
show license usage After Migration
------------------------------------------------------------------------------------------------------------
```

The output here shows the enforcement types for the all the migrated licenses. The HSECK9 licenses has `Enforcement type: EXPORT RESTRICTED`. The ax_10G, which is not an export-controlled license has enforcement type `Enforcement type: NOT ENFORCED`.

```
Device# show license usage
License Authorization:
  Status: Not Applicable

hseck9 (DNA_HSEC):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Export
  Reservation:
    Reservation status: SPECIFIC EXPORT AUTHORIZATION KEY INSTALLED
    Total reserved count: UNLIMITED

ax_10G (ax_10G):
  Description: ax_10G
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: ax_10G
  Feature Description: ax_10G
  Enforcement type: NOT ENFORCED
  License type: Subscription
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1
```

show license authorization After Migration

```
------------------------------------------------------------------------------------------------------------
show license authorization After Migration
------------------------------------------------------------------------------------------------------------
```

The output here shows that the SLR authorization code included as part of an HSECK9 license has been honored (`Last Confirmation code: 3290c177`).

```
Device# show license authorization
Overall status:
  Active: PID:CSR1000V,SN:95QS2T1KUJX
      Status: SPECIFIC INSTALLED on Jul 28 20:46:46 2021 UTC
      Last Confirmation code: 3290c177

Specified license reservations:
  CSR 1KV AX 10G (ax_10G):
    Description: CSR 1KV AX 10G
    Total reserved count: 1
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:CSR1000V,SN:95QS2T1KUJX
        Authorization type: SPECIFIC INSTALLED on Jul 28 20:46:46 2021 UTC
        License type: PERPETUAL
          Term Count: 1
  Router US Export Lic. for DNA (DNA_HSEC):
    Description: U.S. Export Restriction Compliance license for DNA based Routers
    Total reserved count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:CSR1000V,SN:95QS2T1KUJX
        Authorization type: SPECIFIC INSTALLED on Jul 28 20:46:46 2021 UTC
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available


Derived Licenses:
  Entitlement Tag: regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844

  Entitlement Tag: regid.2014-05.com.cisco.ax_10G,1.0_251f937f-655c-427d-b181-222784aae79a
```

show platform hardware throughput level After Migration

```
------------------------------------------------------------------------------------------------------------
show platform hardware throughput level After Migration
------------------------------------------------------------------------------------------------------------
```

The output here shows that throughput of 1250 Mbps has been retained after migration.

```
Device# show platform hardware throughput level
The current throughput level is 10000000 kb/s
```

show license status After Migration

```
------------------------------------------------------------------------------------------------------------
show license status After Migration
------------------------------------------------------------------------------------------------------------
```

The output after migration shows that the product instance is now in the Smart Licensing Using Policy environment (`Smart Licensing Using Policy: Status: ENABLED`).

The transport type is set to Off (`Type: Transport Off`). This means the product instance cannot communicate with CSSM or anything outside the network.

For now, the default policy is effective. (When no other policy is available, the product instance applies the CISCO default policy). If a custom policy is available in CSSM the same will be installed after initial synchronization. The synchronization will also address the reporting that the current policy requires (`Next ACK deadline: Oct 26 21:17:32 2021 UTC`).

```
Device# show license status
Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: <none>
  Virtual Account: <none>
License Reservation is ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Transport Off

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Oct 26 21:17:32 2021 UTC
  Reporting push interval: 30  days
  Next ACK push check: <none>
  Next report push: Jul 28 21:19:32 2021 UTC
  Last report push: <none>
  Last report file write: <none>
```

```
Trust Code Installed: <none>
```

Required Tasks After Migration

1. Complete topology implementation.

   In this example, we're implementing the No Connectivity to CSSM and No CSLU topology. The corresponding workflow to follow is: Workflow for Topology: No Connectivity to CSSM and No CSLU, on page 45.

   When migrating from SLR, the transport type is automatically set to **off**. The sample output of the **show license status** command after migration shows that this is done.

   An export-controlled license is being used and the corresponding authorization code for this has been migrated. SLAC does not have to be installed again after upgrade.

   This completes topology implementation to work in an air-gapped network.

2. Synchronize license usage with CSSM, verify synchronization, and check subsequent reporting requirements.

   For this topology, the RUM report must be saved to a file (on the product instance) and uploaded it to CSSM (from a workstation that has connectivity to the internet, and CSSM). The ACK must then be downloaded and installed on the product instance.

   a. Synchronize usage information with CSSM.

      - In the sample configuration shown below, the RUM report is saved to the flash memory of the product instance, in a file called *usage_report*. It is then transferred to a TFTP location for upload to CSSM:

        ```
        Device# license smart save usage unreported file usage_report
        Device# dir bootflash:
        Directory of bootflash:/

        23      -rw-             3950  Jan 19 2021 07:26:26 +00:00  usage_report

        <output truncated>


        Device# copy bootflash:usage_report tftp://10.8.0.6//user01/usage_report
        Address or name of remote host [10.8.0.6]?
        Destination filename [/user01/usage_report]?
        !!
        3950 bytes copied in 0.012 secs (329167 bytes/sec)
        ```

      - Upload the RUM report to CSSM. After it is processed, download the ACK. See Uploading Data or Requests to CSSM and Downloading a File, on page 214

      - Copy the file from the downloaded location, save it in the flash memory of the product instance (**copy** *source* **bootflash:***file-name*), and install the ACK on the product instance:

        ```
        Device# copy tftp://10.8.0.6//user01 bootflash:ACK_usage_report.txt

        Device# license smart import bootflash: ACK_usage_report.txt
        Import Data Successful
        ```

b. Verify synchronization and check updated policy to know about subsequent reporting requirements.

In the output of the **show license all** privileged EXEC command, the updated time stamp in the `Last ACK received:` field of helps verify that synchronization is complete.

If subsequent reporting is required, this is indicated in the policy and system messages are displayed. You then have to upload the RUM report as shown in Step 2 above (including all substeps). The following fields of the **show license all** privileged EXEC command provide information about if and when reporting is required:

- `Next ACK deadline:`
- `Next report push:`

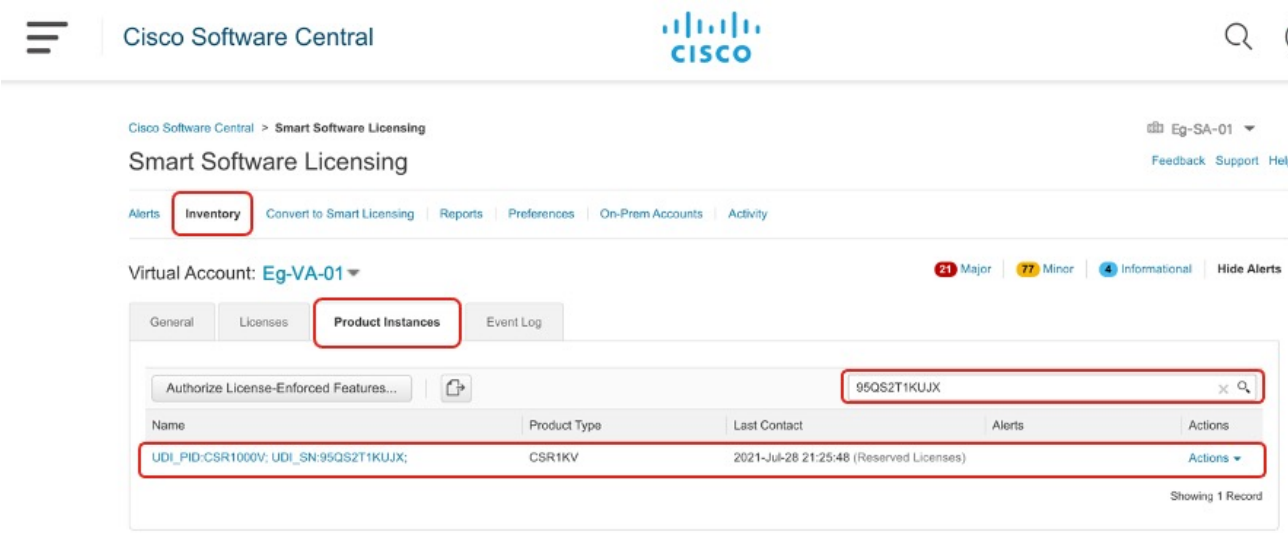
CSSM Web UI Before and After Migration

Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**. In the applicable Smart Account and Virtual Account, go to **Inventory** > **Product Instances** to display all the product instances.

CSSM Web UI Before Migration

From the **Product Instances** tab, click on the UDI to display detailed license usage information as shown below.

In the Smart Licensing environment, SLR licenses are displayed with the label "(Reserved Licenses)" in the Last Contact field:



CSSM Web UI After Migration

From the **Product Instances** tab, click on the UDI to display detailed license usage information.

Note Even though a Catalyst 8000V software image is installed on the product instance, the PID does not change. So the PID for this product instance continues to be PID:CSR1000V,SN:95QS2T1KUJX. You can also verify this with the **show license udi** command before and after upgrade.

After upgrade to Smart Licensing Using Policy, and after the requisite RUM report is uploaded the **Last Contact** field is updated.

Example: Smart Licensing (Evaluation Licenses) to Smart Licensing Using Policy

The following is an example of a **Cisco 4351 Integrated Services Router** with evaluation licenses, migrating from Smart Licensing to Smart Licensing Using Policy. The software version on the product instance is upgraded from Cisco IOS XE Gibraltar 16.12.4 to Cisco IOS XE Bengaluru 17.4.1a. The following is a summary of what to expect after upgrade for this example:

- Enforcement type after migration: Before migration, all the licenses are in evaluation mode. All licenses that are being used will be migrated and they will all have enforcement type NOT ENFORCED after migration.

  A SLAC is being installed *after* migration in this example, to use an export-controlled license in the Smart Licensing Using Policy environment. See the detailed steps under subsection *Required Tasks After Migration* below. This is only to illustration how to request and install SLAC after upgrade and is not a requirement.

- Transport type after migration: When migrating evaluation licenses the system automatically sets the default transport type (**cslu**). This can be changed depending on the topology that is finally implemented; any one of the Supported Topologies, on page 15 may be implemented.

  The *Connected Directly to CSSM* topology (using transport type **smart** to connect to CSSM) is being implemented in this example.

Note In this example, all the licenses being used on the product instance are in evaluation mode, and hence the automatic setting of the default transport type. If yours is a scenario where even one of the licenses being used is registered and authorized, the transport type configuration will be retained, and evaluation licenses, if any, are also migrated, as unenforced licenses (An export-controlled license, that is HSECK9, does not support evaluation mode).

- Device-Led Conversion (DLC): DLC does not apply to the licenses in this scenario, because they are evaluation licenses from the earlier Smart Licensing environment (they are already Smart licenses).

- Reporting after migration: For initial synchronization, a topology will be implemented after the software version is upgraded and the corresponding reporting method will be followed. If a custom policy is available in CSSM, it will be installed on the product instance as part of this synchronization. Subsequent reporting requirements will then depend on the updated policy. If a custom policy is not available, subsequent reporting requirements will be as per the default policy.

Show Commands Before and After Migration

show version Before and After Migration

```
------------------------------------------------------------------------------------------------------------
show version Before Migration
------------------------------------------------------------------------------------------------------------
```

The output here shows the software version before upgrade.

```
Device# show version
Cisco IOS XE Software, Version 16.12.04
Cisco IOS Software [Gibraltar], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 16.12.4, RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 09-Jul-20 21:44 by mcpre
```

```
------------------------------------------------------------------------------------------------------------
show version After Migration
------------------------------------------------------------------------------------------------------------
```

The output here shows the software version after migration, followed by an excerpt of the licensing-related system messages that are displayed when the system restarts with the new image.

```
Device# show version
Cisco IOS XE Software, Version 17.4.1a
Cisco IOS Software [Bengaluru], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 17.4.1a, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Fri 18-Dec-20 05:04 by mcpre

Press RETURN to get started!
*Jan 21 01:06:50.905: %ISR_THROUGHPUT-6-LEVEL:
Throughput level has been set to 400000 kbps
*Jan 21 01:06:53.874: %SMART_LIC-6-AGENT_ENABLED:
Smart Agent for Licensing is enabled
*Jan 21 01:06:54.485: %SMART_LIC-6-EXPORT_CONTROLLED:
Usage of export controlled features is not allowed
*Jan 21 01:07:34.924: %SYS-5-RESTART: System restarted --
*Jan 21 01:08:05.933: %CALL_HOME-6-CALL_HOME_ENABLED:
Call-home is enabled by Smart Agent for Licensing.
*Jan 21 01:08:07.186: %SMART_LIC-6-REPORTING_REQUIRED:
A Usage report acknowledgement will be required in 365 days.
*Jan 21 01:10:32.210: %SMART_LIC-3-COMM_FAILED:
Communications failure with the Cisco Smart License Utility (CSLU) :
Unable to resolve server hostname/domain name
```

show license summary Before and After Migration

```
------------------------------------------------------------------------------------------------------------
show license summary Before Migration
------------------------------------------------------------------------------------------------------------
```

The output before migration shows that all licenses are in Evaluation or EVAL MODE. They will all be displayed as IN USE after migration (There is no notion of an evaluation mode in the Smart Licensing Using Policy environment).

```
Device# show license summary

Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: NOT ALLOWED
```

```
License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 89 days, 23 hours, 58 minutes, 0 seconds

License Usage:
  License                 Entitlement tag             Count Status
  -----------------------------------------------------------------------------
                          (ISR_4351_Application)          1 EVAL MODE
                          (ISR_4351_UnifiedCommun...)     1 EVAL MODE
                          (ISR_4351_Security)             1 EVAL MODE
                          (ISR_4351_400M_Performance)     1 EVAL MODE
```

```
-------------------------------------------------------------------------------------------------------------
show license summary After Migration
-------------------------------------------------------------------------------------------------------------
```

The output after migration shows that all four licenses have been migrated and are displayed with status IN USE.

```
Device# show license summary

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  throughput              (ISR_4351_400M_Performance)       1 IN USE
  appxk9                  (ISR_4351_Application)            1 IN USE
  uck9                    (ISR_4351_UnifiedCommun...)       1 IN USE
  securityk9              (ISR_4351_Security)               1 IN USE
```

show license status Before and After Migration

```
-------------------------------------------------------------------------------------------------------------
show license status Before Migration
-------------------------------------------------------------------------------------------------------------
```

The output before migration shows that the licenses are unregistered.

Evaluation licenses are unregistered and therefore the default transport type in the Smart Licensing environment is effective (**callhome**). After migration, the default in the Smart Licensing Using Policy will be effective.

```
Device# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: NOT ALLOWED

License Authorization:
  Status: EVAL MODE
```

```
  Evaluation Period Remaining: 89 days, 23 hours, 57 minutes, 0 seconds

License Conversion:
  Automatic Conversion Enabled: False
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>
```

---

show license status After Migration

The output after migration shows that the product instance is now in the Smart Licensing Using Policy environment (`Smart Licensing Using Policy: Status: ENABLED`).

The transport type is set to CSLU (`Type: cslu`), which is the default in the Smart Licensing Using Policy environment.

For now, the default policy is effective. (When no other policy is available, the product instance applies the CISCO default policy). A custom policy, if available, will be applied after a topology is implemented and initial synchronization is completed.

```
Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: cslu
  Cslu address: <empty>
  Proxy:
    Not Configured

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
```

```
Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Jan 21 01:08:07 2022 UTC
  Reporting push interval: 30  days
  Next ACK push check: <none>
  Next report push: Jan 21 01:10:07 2021 UTC
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>
```

show license usage Before and After Migration

---

show license usage Before Migration

The output before migration shows that all the licenses being used have `Export status: NOT RESTRICTED`. The export status will be the same after migration. Additionally they will all have enforcement type NOT ENFORCED.

```
Device# show license usage

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 89 days, 23 hours, 55 minutes, 44 seconds

(ISR_4351_Application):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: NOT RESTRICTED

(ISR_4351_UnifiedCommunication):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: NOT RESTRICTED

(ISR_4351_Security):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: NOT RESTRICTED

(ISR_4351_400M_Performance):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: NOT RESTRICTED
```

---

show license usage After Migration

The output after migration shows that all the licenses are unenforced (`Export status: NOT RESTRICTED`, `Enforcement type: NOT ENFORCED`).

```
Device# show license usage

License Authorization:
  Status: Not Applicable

throughput (ISR_4351_400M_Performance):
  Description: throughput
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: throughput
  Feature Description: throughput
  Enforcement type: NOT ENFORCED
  License type: Perpetual

appxk9 (ISR_4351_Application):
  Description: appxk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: appxk9
  Feature Description: appxk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

uck9 (ISR_4351_UnifiedCommunication):
  Description: uck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: uck9
  Feature Description: uck9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

securityk9 (ISR_4351_Security):
  Description: securityk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: securityk9
  Feature Description: securityk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual
```

show platform hardware throughput level Before and After Migration

```
-------------------------------------------------------------------------------------------------------
show platform hardware throughput level Before Migration
-------------------------------------------------------------------------------------------------------
```

This command displays the currently configured throughput. The sample output shows that the throughput is set to 400000 kbps. This is authorised by the performance license (in the **show license** output, see `Feature:`

`throughput`), which allows for increased throughput. The configured throughput will therefore be retained after migration.

```
Device# show platform hardware throughput level
The current throughput level is 400000 kb/s
```

```
------------------------------------------------------------------------------------------------------------
show platform hardware throughput level After Migration
------------------------------------------------------------------------------------------------------------
```

The output after migration shows the throughput configuration is the same after migration.

```
Device# show platform hardware throughput level
The current throughput level is 400000 kb/s
```

show platform software cerm-information Before and After Migration

```
------------------------------------------------------------------------------------------------------------
show platform software cerm-information Before Migration
------------------------------------------------------------------------------------------------------------
```

The output before migration shows that CERM functionality is enabled. Without an HSECK9 license, only 1000 secure tunnels and 250 Mbps of crypto bandwidth is supported. There will be no change in this configuration after migration.

```
Device# show platform software cerm-information

Crypto Export Restrictions Manager(CERM) Information:
 CERM functionality: ENABLED

 ---------------------------------------------------------------
 Resource   Maximum Limit  Available
 ---------------------------------------------------------------
 Number of tunnels       1000   1000
 Number of TLS sessions  1000   1000

 Resource reservation information:
 D - Dynamic
 ---------------------------------------------------------------------------
 Client  Tunnels    TLS Sessions
 ---------------------------------------------------------------------------
 VOICE     0       0
 IPSEC     0       N/A
 SSLVPN    0       N/A

 Statistics information:
 Failed tunnels:            0
 Failed sessions:           0
 Failed encrypt pkts:                          0
 Failed encrypt pkt bytes:                     0
 Failed decrypt pkts:                          0
 Failed decrypt pkt bytes:                     0
```

```
------------------------------------------------------------------------------------------------------------
show platform software cerm-information After Migration
------------------------------------------------------------------------------------------------------------
```

The output after migration shows the CERM configuration is the same after migration.

```
Device# show platform software cerm-information

Crypto Export Restrictions Manager(CERM) Information:
 CERM functionality: ENABLED
```

```
---------------------------------------------------------------
Resource   Maximum Limit  Available
---------------------------------------------------------------
Number of tunnels       1000   1000
Number of TLS sessions  1000   1000

Resource reservation information:
D - Dynamic
---------------------------------------------------------------------------
Client  Tunnels    TLS Sessions
---------------------------------------------------------------------------
VOICE     0       0
IPSEC     0       N/A
SSLVPN    0       N/A

Statistics information:
Failed tunnels:            0
Failed sessions:           0
Failed encrypt pkts:                        0
Failed encrypt pkt bytes:                   0
Failed decrypt pkts:                        0
Failed decrypt pkt bytes:                   0
```

Required Tasks After Migration

1. Complete topology implementation.

   In this example, we're implementing the Connected Directly to CSSM, on page 18 topology with the transport type **smart**. The corresponding workflow to follow is: Workflow for Topology: Connected Directly to CSSM, on page 36.

   a. Set-Up Smart Account.

      In this example, the evaluation licenses are already in the Smart Licensing environment. Smart Account and Virtual Account set-up is already complete.

   b. Set-Up product instance connection to CSSM

      The sample configuration shows the required configuration for a source interface for HTTP connections, and two name servers, for name and address resolution:

      ```
      Device(config)# ip http client source-interface gigabitethernet 0/0/2
      Device(config)# ip name-server 209.165.201.1 209.165.200.225
      ```

      Refer to Setting Up a Connection to CSSM , on page 177 for any other steps that may be required for your set-up.

   c. Configure a connection method and transport type.

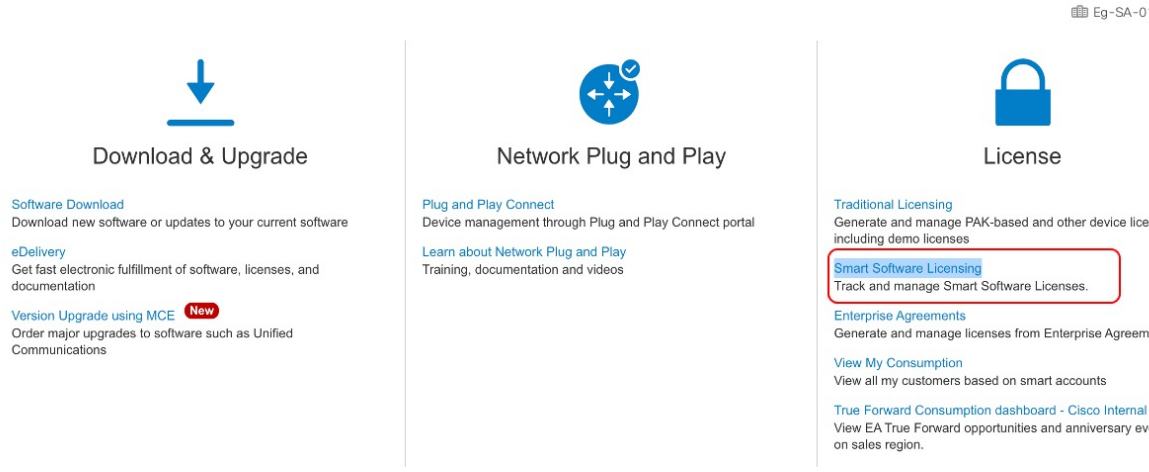
      The sample configuration below shows the required configuration to use Smart transport:

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

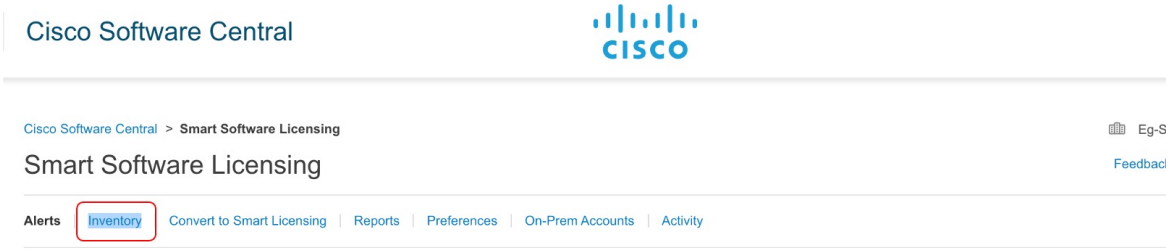
   d. Establish trust with CSSM.

      The following steps show how the token is generated and installed, and how successful trust establishment results in the provision of a policy from CSSM. (After successful trust establishment, the policy is automatically installed on all product instances of that Virtual Account):

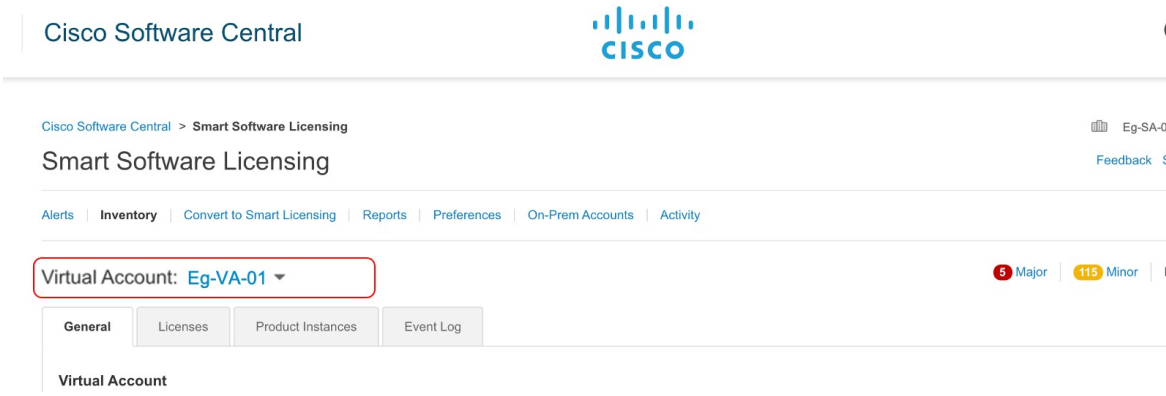
Log in to the CSSM Web UI at https://software.cisco.com and click on **Smart Software Licensing**:



Click on the **Inventory** tab:



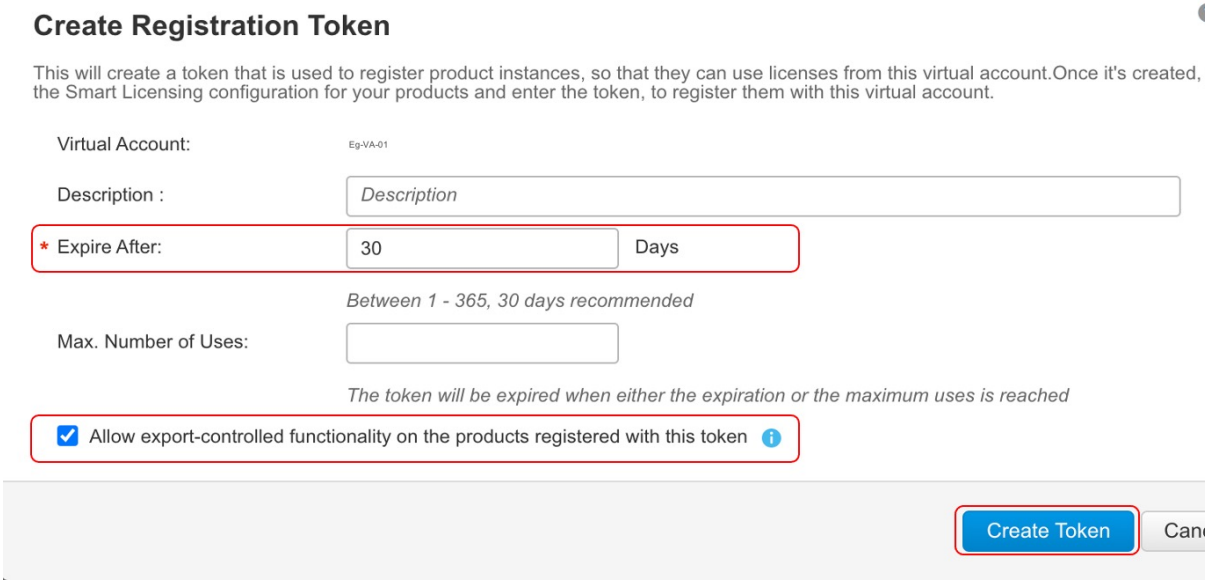
Ensure that the correct Virtual Account is selected, and click on the **General** tab:



Click on **New Token**; the **Create Registration Token** window is displayed.

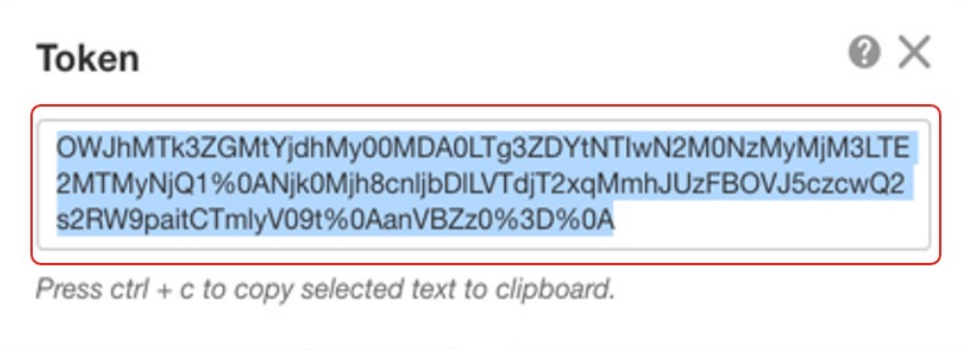


Enter the number of days for which the token must be active, and enable the export-controlled functionality check box.



Note The export-controlled functionality check box is being checked here because a SLAC is being installed after this. (SLAC installation steps are shown below). If an export-controlled license is not required, the checkbox may be left unchecked.

Copy the token to clipboard. Alternatively, you can also click **Actions** and download the token as a `.txt` file.



Install the trust code.

The sample configuration below shows the required configuration to install the trust code.

Note The system messages that are displayed after trust code installation show: a) successful trust code installation, b) new policy installation, and c) license usage synchronization with CSSM (since communication with CSSM has been restored, the product instance has automatically send the requisite RUM report):

```
Device# license smart trust idtoken
$T2xqMmhJUzFBOVJ5czcwQ2s2RW9paitCTmlyV09t%0AanVBZz0%3D%0A local

*Jan 21 03:37:14.577: %SMART_LIC-5-COMM_RESTORED: Communications with Cisco Smart
Software Manager (CSSM) restored
*Jan 21 03:37:15.404: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
was successfully installed
*Jan 21 03:37:15.588: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code
 was successfully installed on P:ISR4351/K9,S:FDO21512BJB.
*Jan 21 03:42:03.106: %SIP-1-LICENSING: SIP service is Up. License report acknowledged.
*Jan 21 03:42:03.761: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
was successfully installed
```

2. Synchronize license usage with CSSM, verify synchronization, and check subsequent reporting requirements.

   System messages in the previous step show that synchronization is complete. In the sample output below, the following fields help verify synchronization:

   - The updated timestamp here: `Policy in use: Installed On Jan 21 03:42:03 2021 UTC`
   - The updated timestamp here: `Last ACK received: Jan 21 03:42:02 2021 UTC`

   In the *Connected Directly to CSSM* topology, the *product instance* sends the next RUM report to CSSM, based on the policy. In the sample output, the following fields provide this information:

   - `Next report push: Feb 20 03:38:01 2021 UTC`
   - `Next ACK deadline: Mar 22 03:42:02 2021 UTC`

```
Device# show license status
Utility:
  Status: DISABLED

Smart Licensing Using Policy:
```

```
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Policy:
  Policy in use: Installed On Jan 21 03:42:03 2021 UTC
  Policy name: SLP Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 150 (Customer Policy)
    Report on change (days): 120 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: Jan 21 03:42:02 2021 UTC
  Next ACK deadline: Mar 22 03:42:02 2021 UTC
  Reporting push interval: 30  days
  Next ACK push check: <none>
  Next report push: Feb 20 03:38:01 2021 UTC
  Last report push: Jan 21 03:38:01 2021 UTC
  Last report file write: <none>

Trust Code Installed: Jan 21 03:37:15 2021 UTC
```

3. Manually request and auto-install SLAC to use an export-controlled license. The **license smart authorization request** is supported on all enterprise routing product instances. (Additionally, alternative commands are available for certain product instances. For details, see Manually Requesting and Auto-Installing a SLAC , on page 201)

```
Device# license smart authorization request replace hseck9 local
Device#
*Jan 21 03:58:37.558: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS:
A new licensing authorization code was successfully installed on
PID:ISR4351/K9,SN:FDO21512BJB
*Jan 21 03:58:39.196: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was
successfully installed
*Jan 21 03:59:37.087: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
 is allowed for feature hseck9
*Jan 21 04:04:10.751: %SIP-1-LICENSING: SIP service is Up. License report acknowledged.
```

```
*Jan 21 04:04:10.979: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
 is allowed for feature hseck9
*Jan 21 04:04:11.614: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was
successfully installed

Device# show license summary
License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  throughput              (ISR_4351_400M_Performance)       1 IN USE
  hseck9                  (ISR_4351_Hsec)                   1 IN USE
  appxk9                  (ISR_4351_Application)            1 IN USE
  uck9                    (ISR_4351_UnifiedCommun...)       1 IN USE
  securityk9              (ISR_4351_Security)               1 IN USE

Device# show license all
Smart Licensing Status
======================

Smart Licensing is ENABLED

License Conversion:
  Automatic Conversion Enabled: False
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Installed On Jan 21 04:04:11 2021 UTC
  Policy name: SLE Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 150 (Customer Policy)
    Report on change (days): 120 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
```

```
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Usage Reporting:
  Last ACK received: Jan 21 04:04:10 2021 UTC
  Next ACK deadline: Mar 22 04:04:10 2021 UTC
  Reporting push interval: 30  days
  Next ACK push check: <none>
  Next report push: Feb 20 04:00:10 2021 UTC
  Last report push: Jan 21 04:00:10 2021 UTC
  Last report file write: <none>

Trust Code Installed: Jan 21 03:37:15 2021 UTC

License Usage
=============

throughput (ISR_4351_400M_Performance):
  Description: throughput
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: throughput
  Feature Description: throughput
  Enforcement type: NOT ENFORCED
  License type: Perpetual

hseck9 (ISR_4351_Hsec):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Perpetual

appxk9 (ISR_4351_Application):
  Description: appxk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: appxk9
  Feature Description: appxk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

uck9 (ISR_4351_UnifiedCommunication):
  Description: uck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: uck9
  Feature Description: uck9
  Enforcement type: NOT ENFORCED
  License type: Perpetual
```

```
securityk9 (ISR_4351_Security):
  Description: securityk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: securityk9
  Feature Description: securityk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

Product Information
===================
UDI: PID:ISR4351/K9,SN:FDO21512BJB

Agent Version
=============
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
======================
Overall status:
  Active: PID:ISR4351/K9,SN:FDO21512BJB
      Status: SMART AUTHORIZATION INSTALLED on Jan 21 03:58:37 2021 UTC
      Last Confirmation code: 76c6a69b

Authorizations:
  ISR_4351_Hsec (ISR_4351_Hsec):
    Description: U.S. Export Restriction Compliance license for 4350 series
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:ISR4351/K9,SN:FDO21512BJB
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available


Derived Licenses:
  Entitlement Tag:
regid.2015-01.com.cisco.ISR_4351_400M_Performance,1.0_79a9ccb4-d7c3-46fd-9980-7efe247c90e5

  Entitlement Tag:
regid.2015-01.com.cisco.ISR_4351_Application,1.0_601ccfff-5601-4293-98d2-2f653d864ce0
  Entitlement Tag:
regid.2014-12.com.cisco.ISR_4351_UnifiedCommunication,1.0_a04fec0e-e944-4096-bcf8-05d6e9a0a6d3

  Entitlement Tag:
regid.2014-12.com.cisco.ISR_4351_Security,1.0_df7d8d7f-b71a-4d3d-a9ab-aec7828a37a7
```

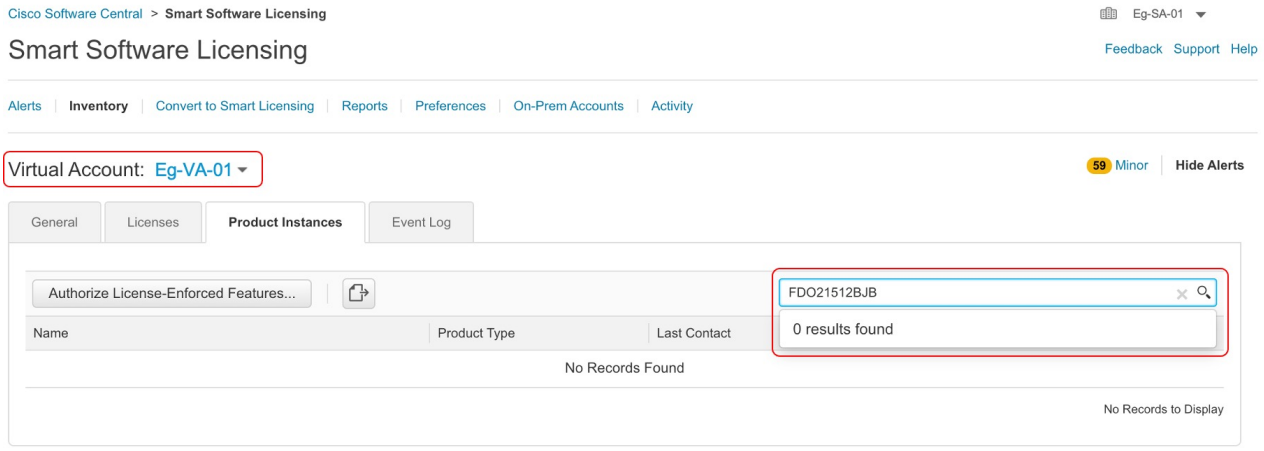
CSSM Web UI Before and After Migration

Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**. In the applicable Smart Account and Virtual Account, go to **Inventory** > **Product Instances** to display all the product instances.

CSSM Web UI Before Migration

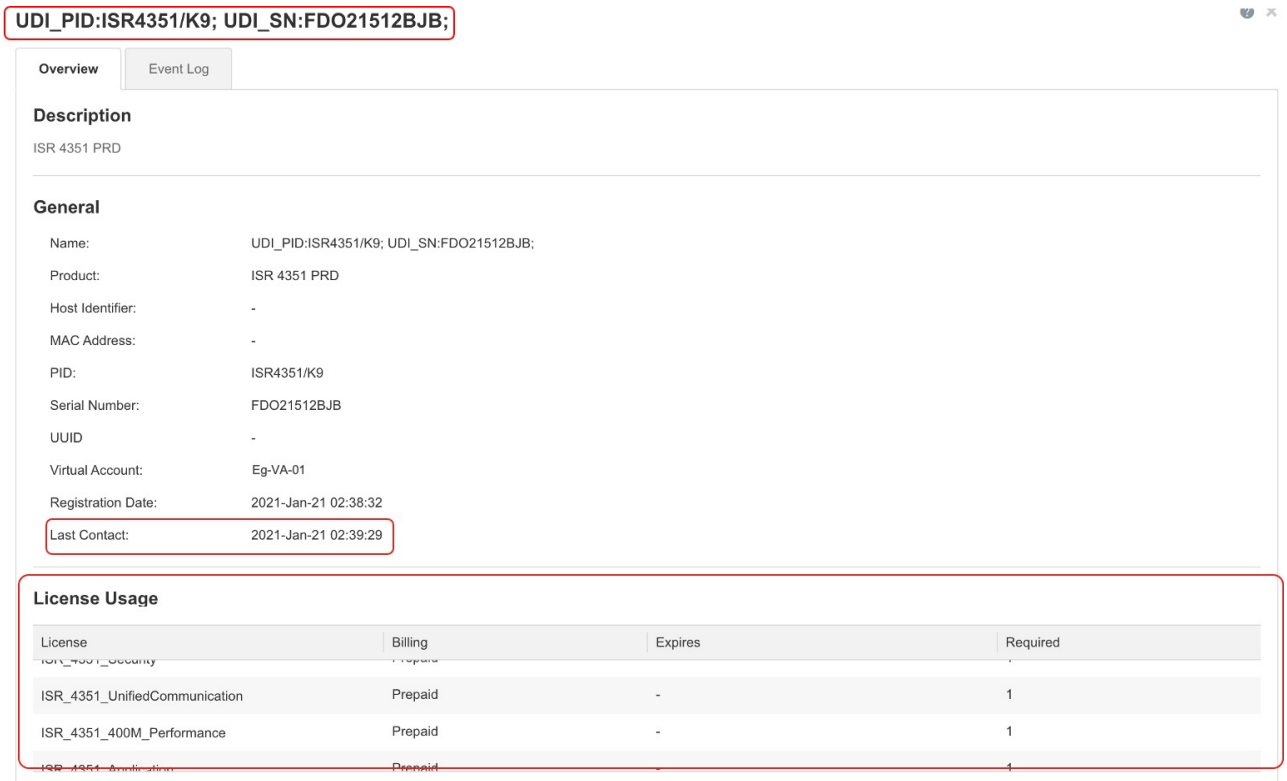
In the **Product Instances** tab area, use the search function to locate the product instance. You will see that no search results are found. This is because all the licenses on this product instance are evaluation licenses, which means the product instance had had no prior communication with CSSM.

(The notion of evaluation licenses does not exist in the Smart Licensing Using Policy environment and all the evaluation licenses will be migrated - this is displayed in the post-migration screenshot.)



CSSM Web UI After Migration

From the **Product Instances** tab, click on the UDI to display detailed license usage information as shown below.



Example: Cisco Software Licensing (PAK Licenses) to Smart Licensing Using Policy

The following is an example of a **Cisco 1000 Series Integrated Services Router** with Product Authorization Keys (PAK) licenses, which falls under the Cisco Software Licensing (CSL) licensing model, to Smart Licensing Using Policy. The software version on the product instance is upgraded from Cisco IOS XE Fuji 16.9.1 to Cisco IOS XE Amsterdam 17.3.2.

Note While this example is meant to highlight migration of PAK licenses, there are also Right-to-Use (RTU) licenses available on the product instance. The example clarifies what happens to the RTU licenses in the course of the migration process as well.

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 159.

The following is a summary of what to expect after upgrade for this example:

- Enforcement type after migration: A total of seven licenses are available on the product instance prior to migration. Only three of these are licenses are being used (**show license feature**, Enabled = yes) and and the enforcement type for these will be as follows:
  - `hseck9`: This is an HSECK9 PAK license and is an export-controlled license. It will be honored after migration and will have enforcement type EXPORT RESTRICTED. A SLAC does not have to be installed after migration. See this point about an HSECK9 PAK license here: How Upgrade Affects Enforcement Types for Existing Licenses, on page 54.
  - `appxk9` and `securityk9`: These two remaining licenses that are being used, are RTU licenses. These will also be migrated will have enforcement type NOT ENFORCED after migration.

    In this example, the `appxk9` and `securityk9` are RTU licenses - but they can also be PAK licenses. You can use the **show license feature** command to clarify. If the `RightToUse` column in the output displays `yes`, it means that they are RTU licenses. If the `RightToUse` column in the output displays `no`, they are PAK licenses.

  `ipbasek9` and `internal_services`: These are default licenses that are always available on the product instance. They will be migrated, but not displayed.

  `FoundationSuiteK9` and `throughput`: These are RTU licenses. RTU licenses that are *not* being used (**show license feature**: Enabled = no, and **show license**: License State: Active, Not in Use, EULA not accepted), will not be migrated.

- Transport type after migration: A transport type is not applicable to PAK licenses. The default transport type (**cslu**) is therefore effective after migration. After the software image is upgraded, you can implement a topology that uses CSLU, or you can implement any one of the other supported topologies and configure the transport type accordingly.

  The *Connected Directly to CSSM* topology with transport type **smart** is implemented in this example.

- Device-Led Conversion (DLC): DLC applies to this scenario, because PAK and RTU licenses are not *Smart* licenses. The *Required Tasks After Migration* section below shows how to verify the status of the DLC.

- Reporting after migration: License usage information and DLC data is being sent as part of the initial synchronization.

  After initial synchronization is completed, subsequent reporting for PAK licenses is required only if there is a change in license consumption. The output of the **show license status** command (`Next report push` and `Next ACK deadline` fields) can be used to know if and by when reporting is required. You will also receive system messages when reporting is required. The topology you implement determines the reporting *method* you can use.

Show Commands Before and After Migration

The licensing related commands available in the Cisco Software Licensing environment (with PAK licenses in this case), and in the Smart Licensing Using Policy environment are not all the same. Where the same command is not available, the closest equivalents have been used in the sample output below.

show version Before and After Migration

```
---------------------------------------------------------------------------------------------------------
show version Before Migration
---------------------------------------------------------------------------------------------------------
```

The output here shows the software version before upgrade.

```
Device# show version
Cisco IOS XE Software, Version 16.09.01
Cisco IOS Software [Fuji], ISR Software (ARMV8EB_LINUX_IOSD-UNIVERSALK9_IAS-M), Version
16.9.1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 17-Jul-18 17:13 by mcpre
<output truncated>
```

```
---------------------------------------------------------------------------------------------------------
show version After Migration
---------------------------------------------------------------------------------------------------------
```

The output here shows the software version after migration, followed by an excerpt of the licensing-related system messages that are displayed when the system restarts with the new image.

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
17.3.2, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Sat 31-Oct-20 11:31 by mcpre
<output truncated>

Press RETURN to get started!
*Jan 20 00:05:21.185: %ISR_THROUGHPUT-6-UNTHROTTLED: Crypto level is unthrottled
*Jan 20 00:05:23.766: %SMART_LIC-6-AGENT_ENABLED: Smart Agent for Licensing is enabled
*Jan 20 00:05:26.654: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
is not allowed
*Jan 20 00:05:32.135: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
is allowed for feature hseck9
*Jan 20 00:05:39.261: %SYS-5-RESTART: System restarted --
*Jan 20 00:06:10.308: %CALL_HOME-6-CALL_HOME_ENABLED: Call-home is enabled by Smart Agent
for Licensing.
*Jan 20 00:06:11.574: %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement will
 be required in 365 days.
<output truncated>
```

show license feature Before Migration and **show license summary** After Migration

---

show license feature Before Migration

The output before migration shows all the licenses available on the product instance.

Note the licenses that are enabled (Enabled = yes). These are all the licenses that will be available after migration.

In addition, the two default licenses (ipbasek9 and internal_service) will be available after upgrade but not displayed. Default licenses will be available irrespective of whether they are enabled or not.

```
Device# show license feature

Feature name        Enforcement  Evaluation  Subscription  Enabled  RightToUse
appxk9              yes          yes         no            yes      yes
securityk9          yes          yes         no            yes      yes
ipbasek9            no           no          no            no       no
FoundationSuiteK9   yes          yes         no            no       yes
hseck9              yes          no          no            yes      no
throughput          yes          yes         no            no       yes
internal_service    yes          no          no            no       no
```

---

show license summary After Migration

The output after migration shows that the three licenses that were enabled, have been migrated and are displayed with status `IN USE`.

```
Device# show license summary

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  hseck9                  (ISR_1100_8P_Hsec)                1 IN USE
  appxk9                  (ISR_1100_8P_Application)         1 IN USE
  securityk9              (ISR_1100_8P_Security)            1 IN USE
```

show license Before Migration and **show license usage** After Migration

---

show license Before Migration

The output before migration shows the state of all the licenses that are available on the product instance.

Licenses that are displayed with `License State: Active, Not in Use, EULA not accepted` will not be migrated. All other licenses, including the default ipbasek9 and internal_service will be migrated.

```
Device# show license

Index 1 Feature: appxk9
 Period left: Life time
 License Type: Permanent
 License State: Active, In Use
 License Count: Non-Counted
```

```
 License Priority: Medium
Index 2 Feature: securityk9
 Period left: Life time
 License Type: Permanent
 License State: Active, In Use
 License Count: Non-Counted
 License Priority: Medium
Index 3 Feature: ipbasek9
Index 4 Feature: FoundationSuiteK9
 Period left: Not Activated
 Period Used: 0  minute  0  second
 License Type: EvalRightToUse
 License State: Active, Not in Use, EULA not accepted
 License Count: Non-Counted
 License Priority: None
Index 5 Feature: hseck9
 Period left: Life time
 License Type: Permanent
        License State: Active, In Use
 License Count: Non-Counted
 License Priority: Medium
Index 6 Feature: throughput
 Period left: Not Activated
 Period Used: 0  minute  0  second
 License Type: EvalRightToUse
 License State: Active, Not in Use, EULA not accepted
 License Count: Non-Counted
 License Priority: None
Index 7 Feature: internal_service

------------------------------------------------------------------------------------------------------
show license usage After Migration
------------------------------------------------------------------------------------------------------
```

The output after migration shows that the HSECK9 PAK license is honored (`Export status: RESTRICTED - ALLOWED`), and has enforcement type: `EXPORT RESTRICTED`.

All the other licenses are unenforced and have enforcement type: `NOT ENFORCED`.

```
Device# show license usage

License Authorization:
  Status: Not Applicable

hseck9 (ISR_1100_8P_Hsec):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Perpetual

appxk9 (ISR_1100_8P_Application):
  Description: appxk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: appxk9
  Feature Description: appxk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual
```

```
securityk9 (ISR_1100_8P_Security):
  Description: securityk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: securityk9
  Feature Description: securityk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual
```

show license all Before and After Migration

show license all Before Migration

The output before migration shows detailed information for all the available licenses on the product instance.

```
Device# show license all

License Store: Primary License Storage
StoreIndex: 0  Feature: hseck9                          Version: 1.0
 License Type: Permanent
 License State: Active, In Use
 Lock type: Node locked
 Vendor info: <UDI><PID>C1111-8PLTEEAWB</PID><SN>FGL214391J3</SN></UDI>
 License Addition: Exclusive
 License Generation version: 0x8100000
 License Count: Non-Counted
 License Priority: Medium
StoreIndex: 1  Feature: securityk9                      Version: 1.0
 License Type: Permanent
 License State: Active, In Use
 Lock type: Node locked
 Vendor info: <UDI><PID>C1111-8PLTEEAWB</PID><SN>FGL214391J3</SN></UDI>
 License Addition: Exclusive
 License Generation version: 0x8100000
 License Count: Non-Counted
 License Priority: Medium
StoreIndex: 2  Feature: appxk9                          Version: 1.0
 License Type: Permanent
 License State: Active, In Use
 Lock type: Node locked
        Vendor info: <UDI><PID>C1111-8PLTEEAWB</PID><SN>FGL214391J3</SN></UDI>
 License Addition: Exclusive
 License Generation version: 0x8100000
 License Count: Non-Counted
 License Priority: Medium
License Store: Built-In License Storage
StoreIndex: 0  Feature: appxk9                          Version: 1.0
 License Type: EvalRightToUse
 License State: Inactive
     Evaluation total period: 8  weeks 4  days
     Evaluation period left: 8  weeks 4  days
     Period used: 0  minute  0  second
 Lock type: Non Node locked
 Vendor info: <UDI><PID>NOTLOCKED</PID><SN>NOTLOCKED</SN></UDI><T>RTU</T>
 License Addition: Additive
 License Generation version: 0x8200000
 License Count: Non-Counted
 License Priority: None
```

```
StoreIndex: 1  Feature: securityk9                        Version: 1.0
 License Type: EvalRightToUse
 License State: Inactive
     Evaluation total period: 8  weeks 4  days
     Evaluation period left: 8  weeks 4  days
            Period used: 0  minute  0  second
 Lock type: Non Node locked
 Vendor info: <UDI><PID>NOTLOCKED</PID><SN>NOTLOCKED</SN></UDI><T>RTU</T>
 License Addition: Additive
 License Generation version: 0x8200000
 License Count: Non-Counted
 License Priority: None
StoreIndex: 2  Feature: FoundationSuiteK9                 Version: 1.0
 License Type: EvalRightToUse
 License State: Active, Not in Use, EULA not accepted
     Evaluation total period: 8  weeks 4  days
     Evaluation period left: 8  weeks 4  days
     Period used: 0  minute  0  second
 Lock type: Non Node locked
 Vendor info: <UDI><PID>NOTLOCKED</PID><SN>NOTLOCKED</SN></UDI><T>RTU</T>
 License Addition: Additive
 License Generation version: 0x8200000
 License Count: Non-Counted
 License Priority: None
StoreIndex: 3  Feature: throughput                        Version: 1.0
 License Type: EvalRightToUse
 License State: Active, Not in Use, EULA not accepted
     Evaluation total period: 8  weeks 4  days
            Evaluation period left: 8  weeks 4  days
     Period used: 0  minute  0  second
 Lock type: Non Node locked
 Vendor info: <UDI><PID>NOTLOCKED</PID><SN>NOTLOCKED</SN></UDI><T>RTU</T>
 License Addition: Additive
 License Generation version: 0x8200000
 License Count: Non-Counted
 License Priority: None

------------------------------------------------------------------------------------------------------
show license all After Migration
------------------------------------------------------------------------------------------------------
```

The output after migration shows that the product instance is now in the Smart Licensing Using Policy environment (`Smart Licensing Using Policy: Status: ENABLED`).

Since PAK licenses do not have a transport type in the pre-upgrade environment, the default transport type is effective after upgrade (`Type: cslu`).

For now, the default policy is effective (Under `Policy:` see `CISCO default`). When no other policy is available, the product instance applies the CISCO default policy). A custom policy, if available, will be applied after a topology is implemented and initial synchronization is completed.

Under `License Authorizations`, you can ignore `Status: NOT INSTALLED`, since SLAC installation is not required for an HSECK9 PAK license. (Under `License Usage`, note `Export status: RESTRICTED - ALLOWED`. This shows that the license is honored after migration.

```
Device# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

License Conversion:
  Automatic Conversion Enabled: False
```

```
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: cslu
  Cslu address: <empty>
  Proxy:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Jan 20 00:06:11 2022 UTC
  Reporting push interval: 30  days
  Next ACK push check: <none>
  Next report push: Jan 20 00:08:11 2021 UTC
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage
=============

hseck9 (ISR_1100_8P_Hsec):
  Description: hseck9
  Count: 1
```

```
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Perpetual

appxk9 (ISR_1100_8P_Application):
  Description: appxk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: appxk9
  Feature Description: appxk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

securityk9 (ISR_1100_8P_Security):
  Description: securityk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: securityk9
  Feature Description: securityk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

Product Information
===================
UDI: PID:C1111-8PLTEEAWB,SN:FGL214391J3

Agent Version
=============
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
======================
Overall status:
  Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
      Status: NOT INSTALLED
      Status:PAK

Legacy License Info:
  regid.2017-04.com.cisco.ISR_1100_8P_Application,
  1.0_c4cf42aa-2d60-4f4e-83dd-c5c9672132c9:
    DisplayName: appxk9
    Description: appxk9
    Total available count: 1
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
        License type: PERPETUAL
          Term Count: 1

  regid.2017-04.com.cisco.ISR_1100_8P_Security,
  1.0_6b61b693-0daa-42d4-8cee-930de5c1b37c:
    DisplayName: securityk9
    Description: securityk9
    Total available count: 1
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
        License type: PERPETUAL
```

```
        Term Count: 1

  regid.2017-08.com.cisco.ISR_1100_8P_Hsec,
  1.0_34a5e7e7-722a-41ab-bdad-d53d5a3cac14:
    DisplayName: hseck9
    Description: hseck9
    Total available count: 1
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
        License type: PERPETUAL
          Term Count: 1
```

show platform hardware throughput crypto Before and After Migration

```
------------------------------------------------------------------------------------------------------------
show platform hardware throughput crypto Before Migration
------------------------------------------------------------------------------------------------------------
```

The output before migration shows that the crypto throughput is unthrottled. The available HSECK9 PAK license authorizes the use of unthrottled crypto throughput. There will therefore be no change in this configuration after migration. (On a Cisco 1000 Series Integrated Services Router, throughput is unthrottled by default. The HSECK9 license provides unthrottled *crypto* throughput).

```
Device# show platform hardware throughput crypto
The current crypto level is unthrottled
```

```
------------------------------------------------------------------------------------------------------------
show platform hardware throughput crypto After Migration
------------------------------------------------------------------------------------------------------------
```

The output after migration shows that crypto throughput configuration is the same after migration.

```
Device# show platform hardware throughput crypto
The current crypto level is unthrottled
```

show platform software cerm-information Before and After Migration

```
------------------------------------------------------------------------------------------------------------
show platform software cerm-information Before Migration
------------------------------------------------------------------------------------------------------------
```

The output before migration shows that CERM functionality is enabled. There will be no change in this configuration after migration.

```
Device# show platform software cerm-information
Crypto Export Restrictions Manager(CERM) Information:
 CERM functionality: DISABLED
```

```
------------------------------------------------------------------------------------------------------------
show platform software cerm-information After Migration
------------------------------------------------------------------------------------------------------------
```

The output after migration shows the CERM configuration is the same after migration.

```
Device# show platform software cerm-information
Crypto Export Restrictions Manager(CERM) Information:
 CERM functionality: DISABLED
```

Required Tasks After Migration

1. Complete topology implementation.

   In this example, we're implementing the Connected Directly to CSSM, on page 18 topology with the transport type **smart**. The corresponding workflow to refer to is: Workflow for Topology: Connected Directly to CSSM, on page 36.

   a. Set-Up Smart Account.

      The Smart Account and Virtual Account set-up is already completed and not shown in this example.

   b. Set-Up product instance connection to CSSM

      Refer to Setting Up a Connection to CSSM , on page 177 for steps that may be required for your set-up.

   c. Configure a connection method and transport type.

      The sample configuration below shows the required configuration to use Smart transport:

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

   d. Establish trust with CSSM.

      The token *generation* process is not shown here, but must be completed. See Generating a New Token for a Trust Code from CSSM, on page 211. Generate one token for each *Virtual Account* you have. You can use same token for all the product instances that are part of one Virtual Account, as long as it has not expired. Token expiry corresponds to the **Expire After** field that you fill when generating a token.

      Install the trust code.

      The sample configuration below shows how to install the trust code, followed by system messages. The system messages show confirmation that the use of export-controlled features is allowed, new policy installation, and successful trust code installation:

      ```
      Device# license smart trust idtoken
      V0p1dCtxVXY2ZUxBQ29XYUU2Zys3dzI2aU5ZNDc1%0AQW9URT0%3D%0A all
      Device#
      *Jan 20 02:47:00.173: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of exportcontrolled
      features is allowed for feature hseck9
      *Jan 20 02:47:00.202: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
      was successfully installed
      *Jan 20 02:47:00.392: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code
       was successfully installed on P:C1111-8PLTEEAWB,S:FGL214391J3.
      ```

   This completes topology implementation.

2. Check the status of the DLC.

   You can monitor DLC progress by entering the **show platform software license dlc** command in command in privileged EXEC mode. DLC is complete when the output displays the following: `DLC Process Status: Completed`, `DLC Conversion Status: SUCCESS`. The DLC data will be sent to CSSM as part of usage reporting, in the next step.

   The first instance of the sample output below shows the status of the DLC process soon after the software version was upgraded. The second instance of the sample output shows the status of the DLC process after around an hour.

```
Device# show platform software license dlc
Index 1  Feature:           appxk9
 Permanent License:  1
 EVAL RTU License:   0
 RTU License:        0
 Paper License:      0
Index 2  Feature:           securityk9
 Permanent License:  1
 EVAL RTU License:   0
 RTU License:        0
 Paper License:      0
Index 3  Feature:           hseck9
 Permanent License:  1
 EVAL RTU License:   0
 RTU License:        0
 Paper License:      0

DLC Process Status: Not Complete
```

```
<<<<AFTER APPROXIMATELY AN HOUR>>>>>
```

```
Device# show platform software license dlc
Index 1  Feature:           appxk9
 Permanent License:  1
 EVAL RTU License:   0
 RTU License:        0
 Paper License:      0
Index 2  Feature:           securityk9
 Permanent License:  1
 EVAL RTU License:   0
 RTU License:        0
 Paper License:      0
Index 3  Feature:           hseck9
 Permanent License:  1
 EVAL RTU License:   0
 RTU License:        0
 Paper License:      0

DLC Process Status: Completed
DLC Conversion Status: SUCCESS
```

3. Synchronize license usage with CSSM, verify synchronization, and check subsequent reporting requirements.

   For this topology you can synchronize usage by entering the **license smart sync** command in privileged EXEC mode. This manually synchronizes (sends and receives) any pending data with CSSM.

   The sample configuration below shows this, followed by system messages that show successful synchronization and confirm that the use of export-controlled features is allowed.

   The successful synchronization is indicated by successful policy installation. (A custom policy can be enclosed in a RUM ACK and a RUM ACK is sent by CSSM in response to a RUM report that has been sent).

   ```
   Device# license smart sync all
   *Jan 20 02:51:36.650: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
    is allowed for feature hseck9
   *Jan 20 02:51:36.689: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was
   successfully installed
   ```

   Verify synchronization by entering the **show license all** command in privileged EXEC mode. In the sample output below, the following fields help verify synchronization:

   - The updated timestamp here: `Policy in use: Installed On Jan 20 02:51:36 2021 UTC`

- The updated timestamp here: `Last ACK received: Jan 20 02:51:36 2021 UTC`

In the *Connected Directly to CSSM* topology, the *product instance* sends the next RUM report to CSSM, based on the policy. In the sample output, the following fields provide this information:

- `Next ACK deadline: Feb 19 02:51:36 2021 UTC`
- `Next report push: Feb 19 02:47:36 2021 UTC`

```
Device# show license all
Smart Licensing Status
======================

Smart Licensing is ENABLED

License Conversion:
  Automatic Conversion Enabled: False
  Status: Successful on Jan 20 03:17:23 2021 UTC

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Installed On Jan 20 02:51:36 2021 UTC
  Policy name: SLP Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 150 (Customer Policy)
    Report on change (days): 120 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 30 (Customer Policy)
```

```
    Report on change (days): 30 (Customer Policy)

Usage Reporting:
  Last ACK received: Jan 20 02:51:36 2021 UTC
  Next ACK deadline: Feb 19 02:51:36 2021 UTC
  Reporting push interval: 30  days
  Next ACK push check: <none>
  Next report push: Feb 19 02:47:36 2021 UTC
  Last report push: Jan 20 02:47:36 2021 UTC
  Last report file write: <none>

Trust Code Installed: Jan 20 02:47:00 2021 UTC

License Usage
=============

hseck9 (ISR_1100_8P_Hsec):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Perpetual

appxk9 (ISR_1100_8P_Application):
  Description: appxk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: appxk9
  Feature Description: appxk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

securityk9 (ISR_1100_8P_Security):
  Description: securityk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: securityk9
  Feature Description: securityk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

Product Information
===================
UDI: PID:C1111-8PLTEEAWB,SN:FGL214391J3

Agent Version
=============
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
======================
Overall status:
  Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
      Status: NOT INSTALLED
      Status:PAK
```

```
Legacy License Info:

regid.2017-04.com.cisco.ISR_1100_8P_Application,1.0_c4cf42aa-2d60-4f4e-83dd-c5c9672132c9:

    DisplayName: appxk9
    Description: appxk9
    Total available count: 1
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
        License type: PERPETUAL
          Term Count: 1

  regid.2017-04.com.cisco.ISR_1100_8P_Security,1.0_6b61b693-0daa-42d4-8cee-930de5c1b37c:

    DisplayName: securityk9
    Description: securityk9
    Total available count: 1
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
        License type: PERPETUAL
          Term Count: 1

  regid.2017-08.com.cisco.ISR_1100_8P_Hsec,1.0_34a5e7e7-722a-41ab-bdad-d53d5a3cac14:
    DisplayName: hseck9
    Description: hseck9
    Total available count: 1
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
        License type: PERPETUAL
          Term Count: 1
```

Migration for this scenario is complete.

CSSM Web UI Before and After Migration

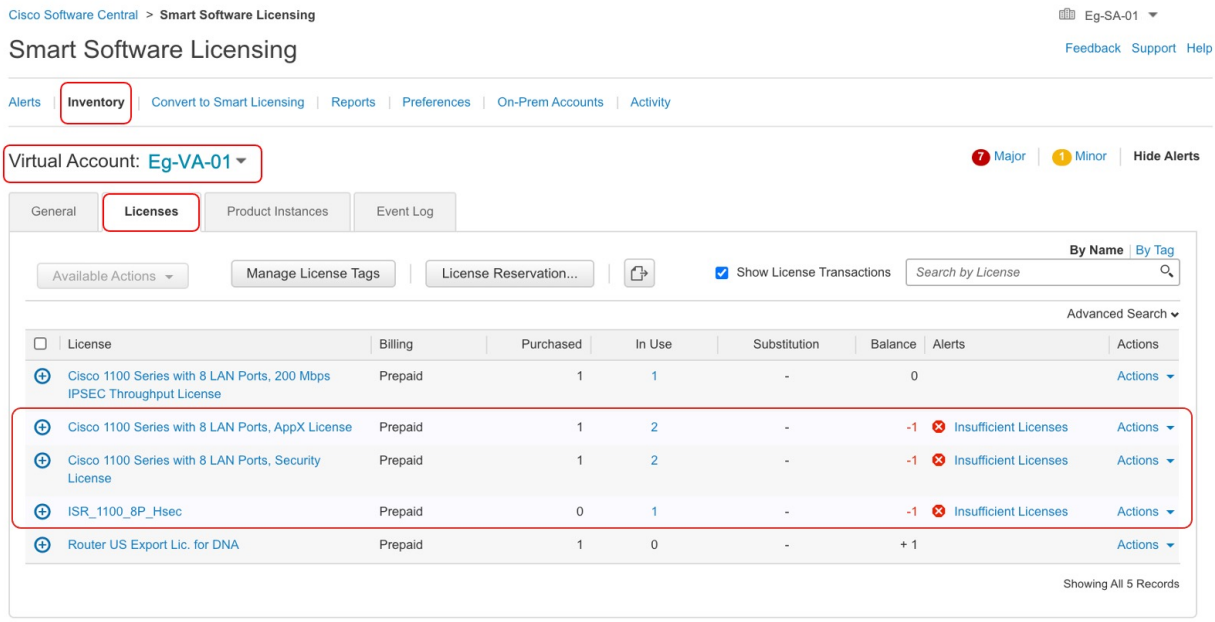
Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**.

CSSM Web UI Before Migration

In the applicable Smart Account and Virtual Account, go to **Inventory** > **Licenses** to display available licenses.

The following screenshot shows how licenses are displayed for the product instance, before upgrade.

Since they are not Smart licenses, they are displayed as Insufficient Licenses. For this same reason, their count is negative.

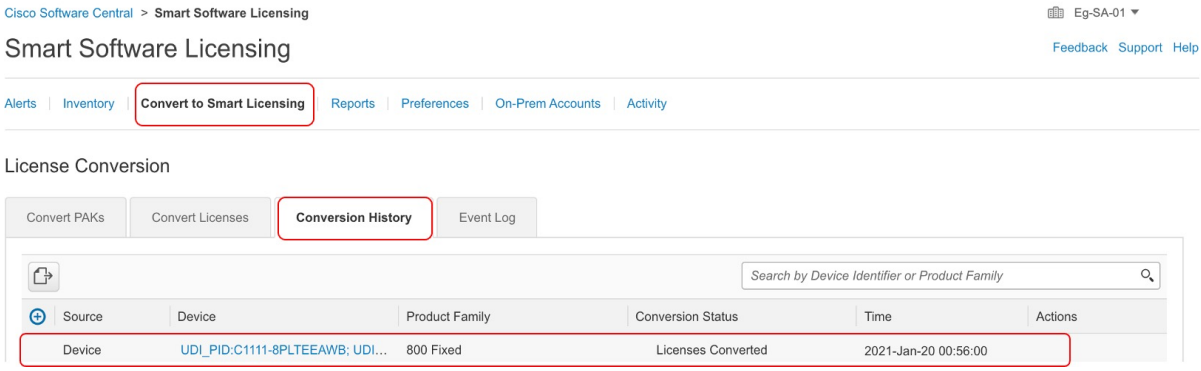


CSSM Web UI After Migration

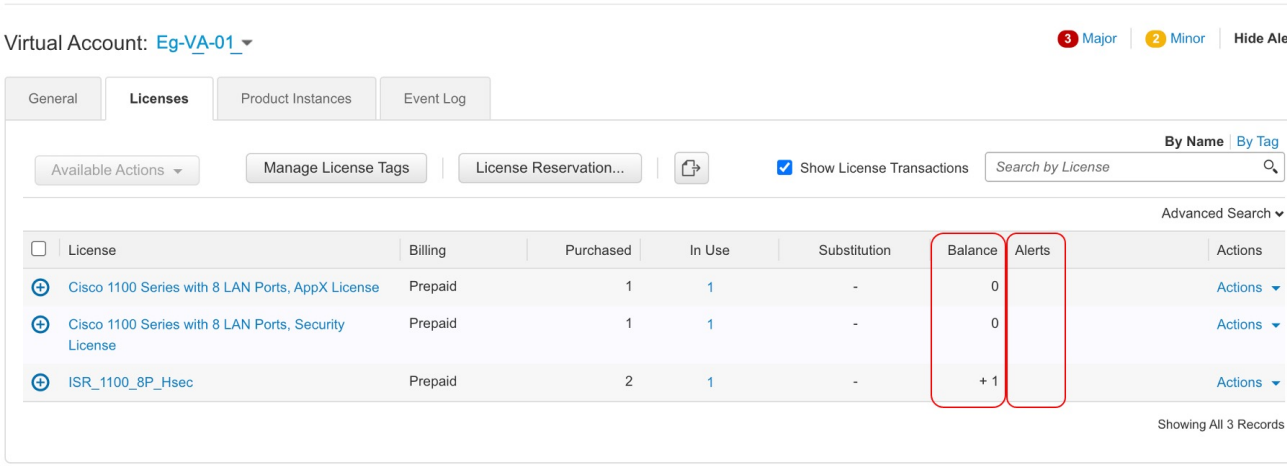
In the applicable Smart Account, go to **Convert to Smart Licensing** > **Conversion History** to verify conversion status.

The following screenshot shows how licenses are displayed for the product instance, after upgrade.

Successful DLC is reflected in the “Conversion Status” column.



Click on the product instance in the **Device** column displays license usage details for that product instance – this is displayed in the following screenshot. (The **Alerts** column no longer displays “Insufficient Licenses” and the count for all licenses is updated in the **Balance** column):



Example: Cisco Software Licensing (RTU Licenses) to Smart Licensing Using Policy

The following is an example of a **Cisco 4351 Integrated Services Router** with Right-to-Use (RTU) licenses, which falls under the Cisco Software Licensing (CSL) licensing model, to Smart Licensing Using Policy. The software version on the product instance is upgraded from Cisco IOS XE Gibraltar 16.19.6 to Cisco IOS XE Bengaluru 17.3.2. The following is a summary of what to expect after upgrade for this example:

- Enforcement type after migration: A total of 10 licenses are available on the product instance prior to migration.

  `appxk9`, `uck9`, `securityk9`, and `throughput`: Only these four licenses are being used (**show license feature**, Enabled = yes) and will be migrated. They are all RTU licenses (**show license feature** RightToUse = yes). Since none of them are export-controlled, they willl have enforcement type NOT ENFORCED after migration.

  `ipbasek9` and `internal_services`: These are default licenses that are always available on the product instance. They will be migrated, but not displayed.

  `FoundationSuiteK9`, `AdvUCSuiteK9`, `cme-srst`: These are RTU licenses. RTU licenses that are *not* being used (**show license feature**: Enabled = no, and **show license**: License State: Active, Not in Use, EULA not accepted), will not be migrated.

  `hseck9`: This is an export-controlled license and requires a PAK license in the RTU environment - but in this example, the requisite PAK license is not available. This license will therefore not be migrated.

- Transport type after migration: A transport type is not applicable to RTU licenses. The default transport type (**cslu**) is therefore effective after migration. After the software image is upgraded, you can implement a topology that uses CSLU, or any one of the other supported topologies and configure the transport type accordingly.

  The *Connected to CSSM Through CSLU (with product instance-initiated communication)* topology with transport type **cslu** is implemented in this example.

- Device-Led Conversion (DLC): DLC applies to this scenario, because RTU licenses are not *Smart* licenses. The *Required Tasks After Migration* section below shows how to verify the status of the DLC.

- Reporting after migration: License usage information and DLC data is being sent as part of the initial synchronization.

  After initial synchronization is completed, subsequent reporting for RTU licenses depends on the license being used. The output of the **show license status** command (`Next report push` and `Next ACK deadline` fields) can be used to know if and by when reporting is required. You will also receive system messages when reporting is required. The topology you implement determines the reporting *method* you can use.

Show Commands Before and After Migration

The licensing related commands available in the Cisco Software Licensing environment (with RTU licenses in this case) and in the Smart Licensing Using Policy environment are not all the same. Where the same command is not available, the closest equivalents have been used in the sample output below.

show version Before and After Migration

```
------------------------------------------------------------------------------------------------------------------
show version Before Migration
------------------------------------------------------------------------------------------------------------------
```

The output here shows the software version before upgrade.

```
Device# show version
Cisco IOS XE Software, Version 16.09.06
Cisco IOS Software [Fuji],
ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 16.9.6, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Thu 27-Aug-20 02:41 by mcpre

<output truncated>
```

```
------------------------------------------------------------------------------------------------------------------
show version After Migration
------------------------------------------------------------------------------------------------------------------
```

The output here shows the software version after migration, followed by an excerpt of the licensing-related system messages that are displayed when the system restarts with the new image.

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam],
ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 17.3.2, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Sat 31-Oct-20 13:21 by mcpre

<output truncated>


Press RETURN to get started!

*Jan 29 18:18:31.506: %ISR_THROUGHPUT-6-LEVEL: Throughput level has been set to 400000 kbps
*Jan 29 18:18:34.482: %SMART_LIC-6-AGENT_ENABLED: Smart Agent for Licensing is enabled
*Jan 29 18:18:34.980: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
is not allowed.
*Jan 29 18:19:04.089: %SYS-5-RESTART: System restarted --
*Jan 29 18:19:41.554: %CALL_HOME-6-CALL_HOME_ENABLED: Call-home is enabled by Smart Agent
for Licensing.
*Jan 29 18:19:42.803: %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement will
```

```
 be required in 365 days.
```

show license feature Before Migration and **show license summary** After Migration

```
---------------------------------------------------------------------------------------------------------
show license feature Before Migration
---------------------------------------------------------------------------------------------------------
```

The output before migration shows all the licenses available on the product instance.

Note the licenses that are enabled (Enabled = yes). These are all the licenses that will be available after migration.

In addition, the two default licenses (ipbasek9 and internal_service) will be available after upgrade but not displayed. Default licenses are available irrespective of whether they are enabled or not.

```
Device# show license feature

Feature name         Enforcement  Evaluation  Subscription   Enabled  RightToUse
appxk9               yes          yes         no             yes      yes
uck9                 yes          yes         no             yes      yes
securityk9           yes          yes         no             yes      yes
ipbasek9             no           no          no             no       no
FoundationSuiteK9    yes          yes         no             no       yes
AdvUCSuiteK9         yes          yes         no             no       yes
cme-srst             yes          yes         no             no       yes
hseck9               yes          no          no             no       no
throughput           yes          yes         no             yes      yes
internal_service     yes          no          no             no       no
```

```
---------------------------------------------------------------------------------------------------------
show license summary After Migration
---------------------------------------------------------------------------------------------------------
```

The output after migration shows that all the licenses that were enabled (Enabled = yes) before upgrade have been migrated and are displayed with status IN USE.

The default licenses (ipbasek9, internal_service) are not displayed even though they are also migrated.

```
Device# show license summary

License Usage:
  License              Entitlement Tag               Count Status
  -----------------------------------------------------------------
  throughput           (ISR_4351_400M_Performance)       1 IN USE
  appxk9               (ISR_4351_Application)            1 IN USE
  uck9                 (ISR_4351_UnifiedCommun...)       1 IN USE
  securityk9           (ISR_4351_Security)               1 IN USE
```

show license Before Migration and **show license all** After Migration

```
---------------------------------------------------------------------------------------------------------
show license Before Migration
---------------------------------------------------------------------------------------------------------
```

The output before migration shows the state of all the licenses that are available on the product instance.

Note all licenses that have `License State: Active, In Use`. These are the licenses that are displayed with Enabled = yes in the sample output of the **show license feature** privileged EXEC command above. These and the default licenses will be migrated.

Licenses that are displayed with `License State: Active, Not in Use, EULA not accepted` will not be migrated.

```
Device# show license

Index 1 Feature: appxk9
 Period left: 8  weeks 3  days
 Period Used: 5  minutes 27 seconds
 License Type: EvalRightToUse
 License State: Active, In Use
 License Count: Non-Counted
 License Priority: Low
Index 2 Feature: uck9
 Period left: 8  weeks 3  days
 Period Used: 5  minutes 27 seconds
 License Type: EvalRightToUse
 License State: Active, In Use
 License Count: Non-Counted
 License Priority: Low
Index 3 Feature: securityk9
 Period left: 8  weeks 3  days
 Period Used: 5  minutes 27 seconds
 License Type: EvalRightToUse
 License State: Active, In Use
 License Count: Non-Counted
 License Priority: Low
Index 4 Feature: ipbasek9
Index 5 Feature: FoundationSuiteK9
        Period left: Not Activated
 Period Used: 0  minute  0  second
 License Type: EvalRightToUse
 License State: Active, Not in Use, EULA not accepted
 License Count: Non-Counted
 License Priority: None
Index 6 Feature: AdvUCSuiteK9
 Period left: Not Activated
 Period Used: 0  minute  0  second
 License Type: EvalRightToUse
 License State: Active, Not in Use, EULA not accepted
 License Count: Non-Counted
 License Priority: None
Index 7 Feature: cme-srst
 Period left: Not Activated
 Period Used: 0  minute  0  second
 License Type: EvalRightToUse
 License State: Active, Not in Use, EULA not accepted
 License Count: 0/0  (In-use/Violation)
 License Priority: None
Index 8 Feature: hseck9
Index 9 Feature: throughput
 Period left: 8  weeks 3  days
        Period Used: 5  minutes 26 seconds
 License Type: EvalRightToUse
 License State: Active, In Use
 License Count: Non-Counted
 License Priority: Low
Index 10 Feature: internal_service
```

---

show license all After Migration

The output after migration shows that the product instance is now in the Smart Licensing Using Policy environment (`Smart Licensing Using Policy: Status: ENABLED`).

Section `Transport`: Since RTU licenses do not have a transport type in the pre-upgrade environment, the default transport type is effective after upgrade (`Type: cslu`).

Section `Policy`: For now, the default policy is effective (Under `Policy:` see `CISCO default`). When no other policy is available, the product instance applies the CISCO default policy). A custom policy, if available, will be applied after a topology is implemented and initial synchronization is completed.

Section `License Usage`: There are no export-controlled and all licenses have `Enforcement type: NOT ENFORCED`.

```
Device# show license all
Smart Licensing Status
======================

Smart Licensing is ENABLED

License Conversion:
  Automatic Conversion Enabled: False
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: cslu
  Cslu address: <empty>
  Proxy:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
```

```
Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Jan 29 18:19:42 2022 UTC
  Reporting push interval: 30  days
  Next ACK push check: <none>
  Next report push: Jan 29 18:21:42 2021 UTC
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage
=============

throughput (ISR_4351_400M_Performance):
  Description: throughput
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: throughput
  Feature Description: throughput
  Enforcement type: NOT ENFORCED
  License type: Perpetual

appxk9 (ISR_4351_Application):
  Description: appxk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: appxk9
  Feature Description: appxk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

uck9 (ISR_4351_UnifiedCommunication):
  Description: uck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: uck9
  Feature Description: uck9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

securityk9 (ISR_4351_Security):
  Description: securityk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: securityk9
  Feature Description: securityk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

Product Information
===================
UDI: PID:ISR4351/K9,SN:FDO210305DQ

Agent Version
```

```
=============
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
======================
Overall status:
  Active: PID:ISR4351/K9,SN:FDO210305DQ
      Status: NOT INSTALLED

Purchased Licenses:
  No Purchase Information Available


Derived Licenses:
  Entitlement Tag: regid.2015-01.com.cisco.ISR_4351_400M_Performance,
1.0_79a9ccb4-d7c3-46fd-9980-7efe247c90e5
  Entitlement Tag: regid.2015-01.com.cisco.ISR_4351_Application,
1.0_601ccfff-5601-4293-98d2-2f653d864ce0
  Entitlement Tag: regid.2014-12.com.cisco.ISR_4351_UnifiedCommunication,
1.0_a04fec0e-e944-4096-bcf8-05d6e9a0a6d3
  Entitlement Tag: regid.2014-12.com.cisco.ISR_4351_Security,
1.0_df7d8d7f-b71a-4d3d-a9ab-aec7828a37a7
```

show platform hardware throughput level Before and After Migration

```
-------------------------------------------------------------------------------------------------------------
show platform hardware throughput level Before Migration
-------------------------------------------------------------------------------------------------------------
```

This command displays the currently configured throughput. The sample output shows that the throughput is set to 400000 kbps. This is authorised by the performance license (in the **show license** output, see `Feature: throughput`), which allows for increased throughput. The configured throughput will therefore be retained after migration.

```
Device# show platform hardware throughput level
The current throughput level is 400000 kbps
```

```
-------------------------------------------------------------------------------------------------------------
show platform hardware throughput level After Migration
-------------------------------------------------------------------------------------------------------------
```

The sample output shows that throughput configuration is retained after migration.

```
Device# show platform hardware throughput level
The current throughput level is 400000 kbps
```

Required Tasks After Migration

1. Complete topology implementation.

   In this example, we're implementing the Connected to CSSM Through CSLU, on page 16 (Product Instance-Initiated Communication) topology with the transport type **cslu**. The corresponding workflow to refer to is: Workflow for Topology: Connected to CSSM Through CSLU, on page 33 > Tasks for Product Instance-Initiated Communication.

   a. CSLU Installation

      CSLU installation is not shown here, but must be completed

Download the file from Smart Software Manager > **Smart Licensing Utility**.

Refer to Cisco Smart License Utility Quick Start Setup Guide for help with installation and set-up.

b. CSLU Preference Settings

CSLU settings are not shown here, but must be completed

Logging into Cisco (CSLU Interface), on page 166

Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 166

Adding a Product-Initiated Product Instance in CSLU (CSLU Interface), on page 167

c. Product Instance Configuration

Configure all required commands to ensure network reachability. Refer to Ensuring Network Reachability for Product Instance-Initiated Communication, on page 167 for steps that may be required for your set-up.

```
Device(config)# ip route 192.168.0.1 255.255.0.0 192.168.255.1
```

Ensure that transport type is set to **cslu**.

CSLU is the default transport type, since this has not been changed, it does not have to be reconfigured. (See the sample output of the **show license all** privileged EXEC command above).

Specify how you want CSLU to be discovered, and synchronize with CSLU to send and receive pending data.

In this example, we're configuring the CSLU URL. Enter the **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* command in global configuration mode. For `<cslu_ip_or_host>`, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

The system message that is displayed after configuration is completed, shows that the communication with CSLU is established now.

```
Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi
*Jan 29 18:36:35.457: %SMART_LIC-5-COMM_RESTORED: Communications with Cisco Smart
License Utility (CSLU) restored.
```

This completes topology implementation.

2. Check the status of the DLC.

You can monitor DLC progress by entering the **show platform software license dlc** command in command in privileged EXEC mode. DLC is complete when the output displays the following: `DLC Process Status: Completed`, `DLC Conversion Status: SUCCESS`. The DLC data will be sent to CSSM as part of usage reporting, in the next step.

The first instance of the sample output below shows the status of the DLC process soon after the software version was upgraded. The second instance of the sample output shows the status of the DLC process after around an hour.

```
Device# show platform software license dlc

Index 1  Feature:           appxk9
 Permanent License:  0
 EVAL RTU License:   1
 RTU License:        0
 Paper License:      0
Index 2  Feature:           uck9
```

```
 Permanent License:  0
 EVAL RTU License:   1
 RTU License:        0
 Paper License:      0
Index 3  Feature:           securityk9
 Permanent License:  0
 EVAL RTU License:   1
 RTU License:        0
 Paper License:      0
Index 4  Feature:           throughput
 Permanent License:  0
 EVAL RTU License:   1
 RTU License:        0
 Paper License:      0

DLC Process Status: Not Complete

<<<<AFTER 1 HOUR>>>>>

Device# show platform software license dlc

Index 1  Feature:           appxk9
 Permanent License:  0
 EVAL RTU License:   1
 RTU License:        0
 Paper License:      0
Index 2  Feature:           uck9
 Permanent License:  0
 EVAL RTU License:   1
 RTU License:        0
 Paper License:      0
Index 3  Feature:           securityk9
 Permanent License:  0
 EVAL RTU License:   1
 RTU License:        0
 Paper License:      0
Index 4  Feature:           throughput
 Permanent License:  0
 EVAL RTU License:   1
 RTU License:        0
 Paper License:      0

DLC Process Status: Completed
DLC Conversion Status: SUCCESS
```

3. Synchronize license usage with CSSM, verify synchronization, and check subsequent reporting requirements.

   For this topology you can synchronize usage by entering the **license smart sync** command in privileged EXEC mode. This manually synchronizes (sends and receives) any pending data with CSLU. CSLU in turn synchronizes with CSSM.

   The sample configuration below shows this, followed by system messages that show successful synchronization.

```
Device# license smart sync all
*Jan 29 18:40:37.836: %SIP-1-LICENSING: SIP service is Up. License report acknowledged.
*Jan 29 18:40:38.484: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was
successfully installed
```

   Verify synchronization by entering the **show license status** (or even **show license all**) command in privileged EXEC mode.

In the sample output below, the following fields help verify that synchronization has been completed:

- The updated timestamp here: `Policy in use: Installed On Jan 29 18:40:38 2021 UTC`
- The updated timestamp here: `Last ACK received: Jan 29 18:40:37 2021 UTC`

In the *Connected to CSSM Through CSLU* topology with Product Instance-Initiated Communication, the *product instance* sends the next RUM report to CSSM, based on the policy. In the sample output, the following fields provide this information:



Note Reporting is not required until the policy or system messages indicate that it is. Here, after initial synchronization, the updated policy shows that reporting is not required.

- Next report push: <none>
- Next ACK deadline: <none>

```
Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  Proxy:
    Not Configured

Policy:
  Policy in use: Installed On Jan 29 18:40:38 2021 UTC
  Policy name: SLP Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 25 (Customer Policy)
    Reporting frequency (days): 25 (Customer Policy)
    Report on change (days): 25 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 15 (Customer Policy)
    Reporting frequency (days): 15 (Customer Policy)
    Report on change (days): 15 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 35 (Customer Policy)
    Report on change (days): 35 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Miscellaneous:
```

```
    Custom Id: <empty>

  Usage Reporting:
    Last ACK received: Jan 29 18:40:37 2021 UTC
    Next ACK deadline: <none>
    Reporting push interval: 0 (no reporting)
    Next ACK push check: <none>
    Next report push: <none>
    Last report push: Jan 29 18:36:38 2021 UTC
    Last report file write: <none>

  Trust Code Installed: <none>
```

CSSM Web UI and CSLU UI Before and After Migration

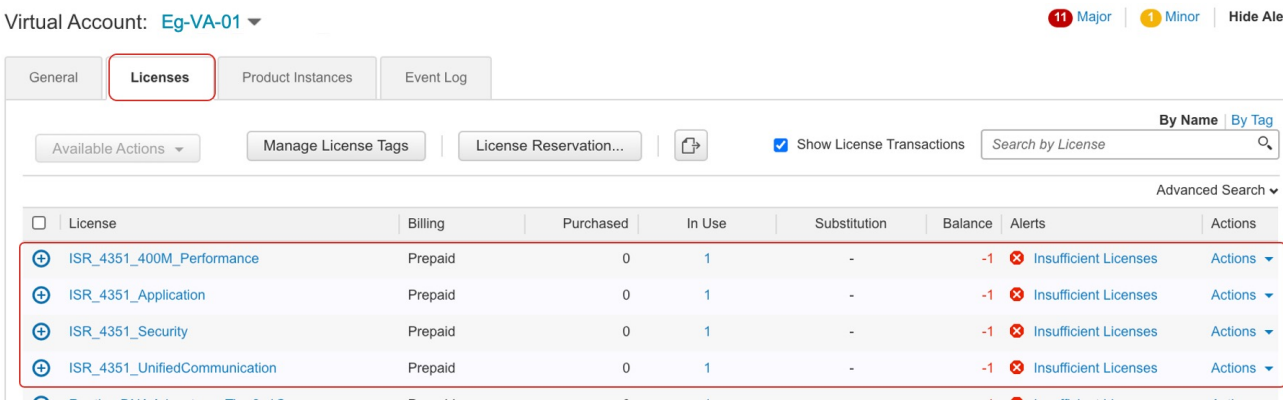
CSSM Web UI Before Migration

Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**.

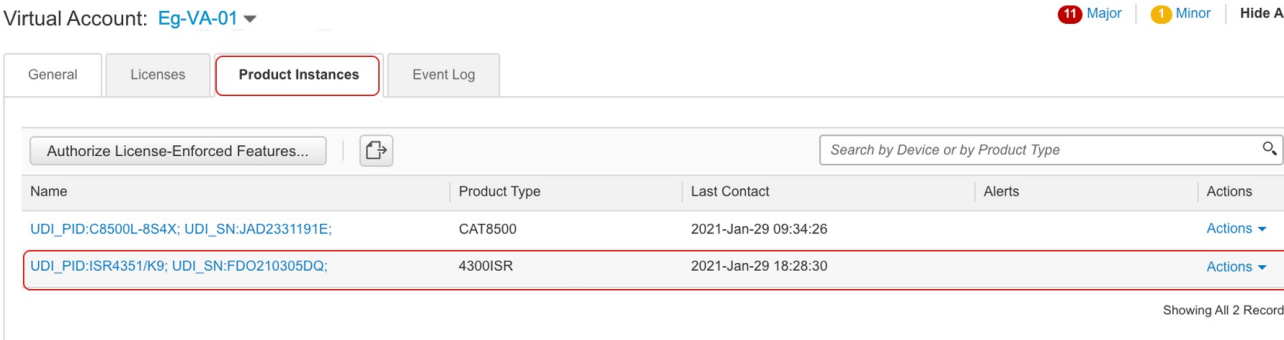
In the applicable Smart Account and Virtual Account, go to **Inventory** > **Licenses** to display available licenses.

The following screenshot shows how licenses are displayed for the product instance, before upgrade.

Since they are not Smart licenses, they are displayed as Insufficient Licenses. For this same reason, their count is negative.



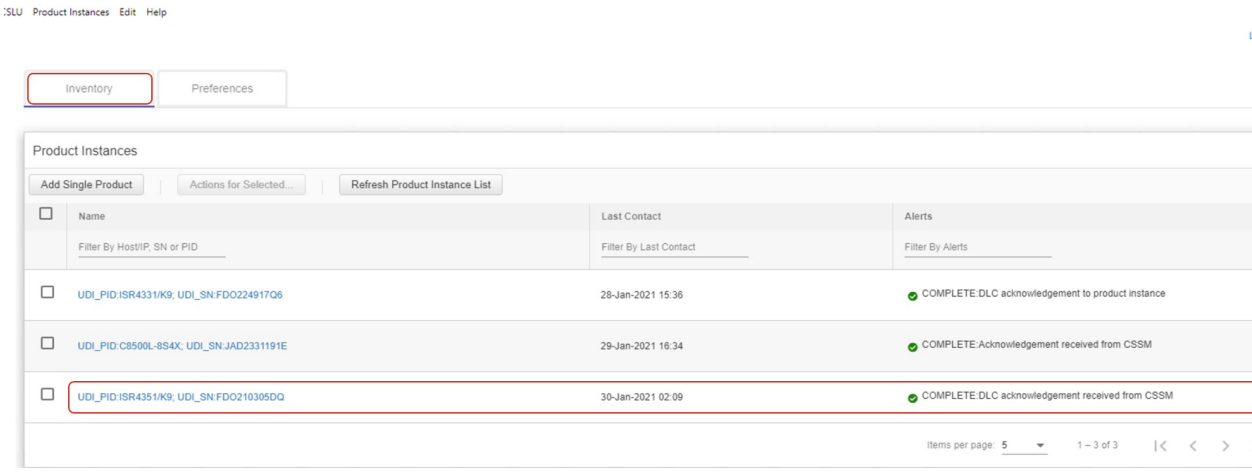
Next, click on the **Product Instances** tab to display information about the product instance that will be migrated.



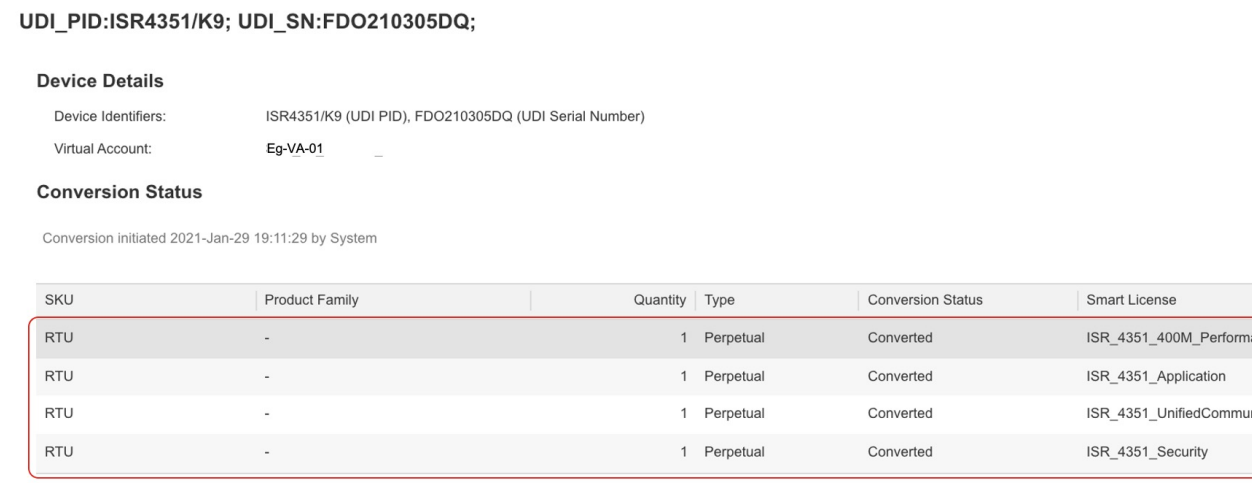
CSLU UI After Migration

In the *CSLU UI*, click the **Inventory** tab to display the Product Instances table.

See the **Alerts** column for the product instance (ISR4351/K9:FDO210305DQ in this example) that was migrated. Information about successful DLC converation is provided here - this displayed in the following screenshot:



Click on the product instance in the **Name** column to display license usage details for the product instance – this is displayed in the following screenshot:



You can also verify the same on the CSSM Web UI: Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**. In the applicable Smart Account, go to **Convert to Smart Licensing** > **Conversion History** to verify conversion status. Successful DLC is reflected in the "Conversion Status" column.

Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy

If you are using a version of SSM On-Prem that is earlier than the minimum required version (See Cisco Smart Software Manager On-Prem (SSM On-Prem), on page 14), you can use this section as an outline of

the process and sequence you have to follow to update the SSM On-Prem version, the product instance, and any other tasks like SLAC installation, if applicable.

1. Upgrade SSM On-Prem.

   Upgrade to the minimum required Version 8, Release 202102 or a later version.

   Refer to the Cisco Smart Software Manager On-Prem Migration Guide.

2. Generate SLAC in CSSM and import it into SSM On-Prem (Only if Applicable).

   If you are using a CSR 1000v or ISRv *with throughput greater than 250 Mbps*, an HSECK9 license will be required in the Smart Licensing Using Policy environment. (U.S. export control regulations no longer allow the use of the export control flag to authorize throughput greater than 250 Mbps).

   Complete this procedure before you upgrade the product instanceSubmitting an Authorization Code Request (SSM On-Prem UI, Disconnected Mode), on page 191.

3. Upgrade the product instance.

   For information about the minimum required software version, see Cisco Smart Software Manager On-Prem (SSM On-Prem), on page 14.

   For information about the upgrade procedure, see Upgrading the Software Version, on page 58.

4. Re-Register a local account with CSSM

   Online and Offline options are available. Refer to the Cisco Smart Software Manager On-Prem Migration Guide > *Re-Registering a local Account (Online Mode)* or *Manually Re-Registering a Local Account (Offline Mode)* .

   Once re-registration is complete, the following events occur automatically:

   - SSM On-Prem responds with new transport URL that points to the tenant in SSM On-Prem.
   - The transport type configuration on the product instance changes from from **call-home** or **smart**, to **cslu**. The transport URL is also updated automatically.

5. Request and install SLAC on applicable product instances: Manually Requesting and Auto-Installing a SLAC , on page 201.

   If you performed step 2 for a product instance, you must complete this step to request and install SLAC on the product instance (for an HSECK9 license).

6. Save configuration changes on the product instance, by entering the **copy running-config startup-config** command in privileged EXEC mode.

7. Clear older On-Prem Smart Licensing certificates on the product instance and reload the product instance. Do not save configuration changes after this.

Note This step is required only if the software version running on the product instance is Cisco IOS XE Amsterdam 17.3.x or Cisco IOS XE Bengaluru 17.4.x.

Enter the **licence smart factory reset** and then the **reload** commands in privileged EXEC mode.

```
Device# licence smart factory reset
Device# reload
```

8. If Device-Led Conversion (DLC) applies, wait an hour for DLC data collection to be completed.

   If the product instance was using Right-To-Use (RTU) or Product Authorization Keys (PAK) licenses prior to product instance upgrade, wait for an hour before you proceed to the next step. By waiting for an hour, you can send DLC data as part of initial usage report. If you do not wait, you have to repeat Step 9 and Step 10.

   If the product instance was NOT using PAK or RTU licenses prior to product instance upgrade, skip this step and proceed to the next step.

9. Perform usage synchronization.

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

      ```
      Device(config)# license smart sync local
      ```

      You can verify this in the SSM On-Prem UI. Go to **Inventory** > **SL Using Policy**. In the **Alerts** column, the following message is displayed: Usage report from product instance.

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

      - Option 1:

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

      - Option 2:

        SSM On-Prem is not connected to CSSM. See: Exporting and Importing Usage Data (SSM On-Prem UI), on page 192.

   After you synchronize usage with CSSM, wait for a few minutes for the device to receive the ACK from SSM On-Prem. To verify that the product instance has received the ACK, enter the **show license status** command in privileged EXEC mode, and in the output, check the date for the `Last ACK received` field.

10. If DLC was applicable in Step 8, verify DLC completion and synchronize the local account.

    a. Verify DLC completion.

       In SSM On-Prem UI, navigate to the **On-Prem Admin Workspace**, and click the **Support Centre** widget. Look for the following events in the **Event Log** tab: `DLC request sent to CSSM` and `DLC acknowledgement received from CSSM`.

       On the product instance, enter the **show license all** privileged EXEC command and check the timestamp in the `License Conversion` section of the output.

       ```
       Device# show license all
       Smart Licensing Status
       ======================

       Smart Licensing is ENABLED

       License Conversion:
         Automatic Conversion Enabled: False
         Status: Successful on Aug 11 05:42:21 2021 UTC

       <output truncated>
       ```

On the product instance, enter the the **show platform software license dlc** privileged EXEC command, check `DLC Process Status` and `DLC Conversion Status` fields; they should display `Completed` and `SUCCESS`, respectively.

Note If DLC was applicable and *you did not wait for one hour* before usage synchronization, then DLC data is not included in the RUM report and status "Completed" is not displayed in the output below. You then have to repeat Steps 9 and 10 before you can see this status.

```
Device# show platform software license dlc
Index 1  Feature:           appxk9
 Permanent License:  1
 EVAL RTU License:   0
 RTU License:        0
 Paper License:      0
Index 2  Feature:           securityk9
 Permanent License:  1
 EVAL RTU License:   0
 RTU License:        0
 Paper License:      0
Index 3  Feature:           hseck9
 Permanent License:  1
 EVAL RTU License:   0
 RTU License:        0
 Paper License:      0

DLC Process Status: Completed

DLC Conversion Status: SUCCESS
```

b. Synchronize the local account in SSM On-Prem with CSSM, by using the **Synchronization** widget in SSM On-Prem.

Result:

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

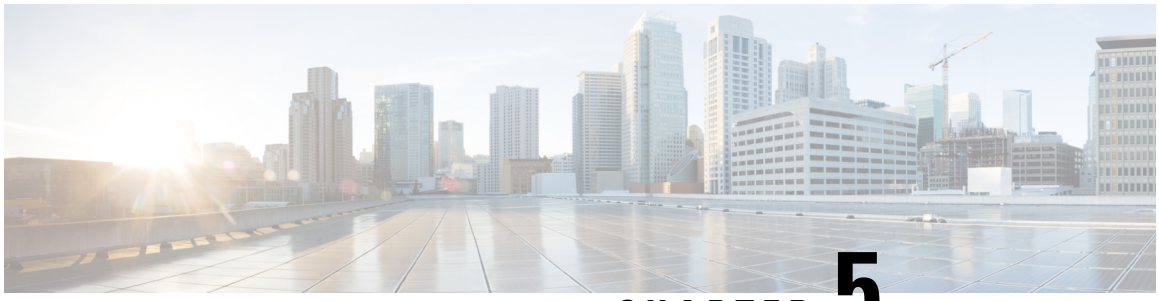
For subsequent reporting, you have the following options:

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

    To know when the product instance will be sending the next RUM report, enter the **show license all** command in privileged EXEC mode and in the output, check the `Next report push:` field.
  - Enter the **license smart sync** privileged EXEC command, for ad hoc or on-demand synchronization between the product instance and SSM On-Prem.
- To synchronize usage information with CSSM:
  - Schedule periodic synchronization with CSSM. In the SSM On-Prem UI, navigate to **Reports** > **Usage Schedules** > **Synchronization schedule with Cisco**. Enter the following frequency information and save:

- **Days**: Refers to how *often* synchronization occurs. For example, if you enter 2, synchronization occurs once every two days.
- **Time of Day:**: Refers to the time at which synchronization occurs, in the 24-hour notation system. For example, if you enter 14 hours and 0 minutes, synchronization occurs at 2 p.m. (1400) in your local time zone.

- Upload and download the required files for reporting: Exporting and Importing Usage Data (SSM On-Prem UI), on page 192).



CHAPTER 5

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, on page 153
- Snapshots for PAK Licenses , on page 159
- Permanent License Reservation in the Smart Licensing Using Policy Environment, on page 161

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, on page 231.

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, on page 353.

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 8: 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, on page 199 and Installing a File on the Product Instance, on page 215. • **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, on page 239, 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, on page 199 and Installing a File on the Product Instance, on page 215 • **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 9: Licensing Model Where HSECK9 License is Used and Release Matrix

Release	Licensing Model Available with the Release	PAK HSECK9 Supported?	SLR in Suppo
<=16.9	PAK	Yes	Not ap
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, on page 59. 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, on page 221.
- If you have a PAK license on a product instance and you want to remove it, see: Removing a PAK License, on page 223.
- 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, on page 224.

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)

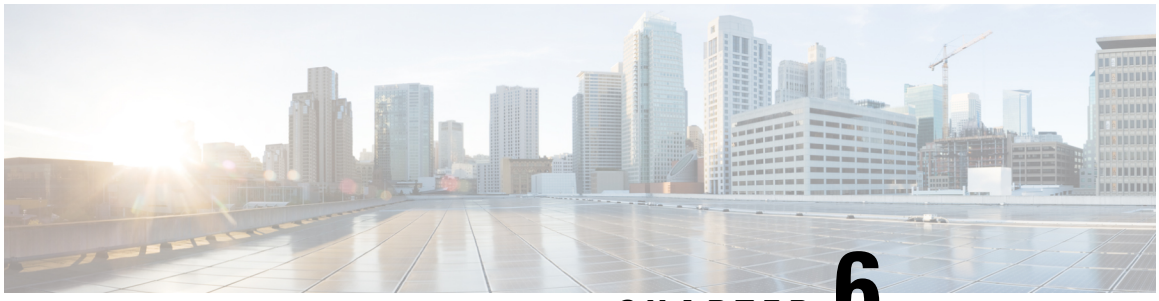
How an Existing PLR is Handled - Upgrade and Downgrade

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, on page 228.
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, on page 228.

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, on page 225.
- If you performing a .bin upgrade on a Cisco Cloud Services Router 1000v Router and want to continue using PLR, see: Upgrading a PLR, on page 228.
- If you want to deactive a PLR, see: Deactivating a PLR, on page 230.



CHAPTER 6

Task Library for Smart Licensing Using Policy

This section is a group of tasks that apply to Smart Licensing Using Policy.

If you are implementing a particular topology, refer to the corresponding workflow. See *How to Configure Smart Licensing Using Policy: Workflows by Topology* to know the sequential order of tasks that apply.

- Logging into Cisco (CSLU Interface), on page 166
- Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 166
- Adding a Product-Initiated Product Instance in CSLU (CSLU Interface), on page 167
- Ensuring Network Reachability for Product Instance-Initiated Communication, on page 167
- Adding a CSLU-Initiated Product Instance in CSLU (CSLU Interface), on page 169
- Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 170
- Ensuring Network Reachability for CSLU-Initiated Communication, on page 171
- Export to CSSM (CSLU Interface), on page 175
- Import from CSSM (CSLU Interface), on page 176
- Requesting SLACs for Multiple Product Instances (CSLU Interface), on page 176
- Setting Up a Connection to CSSM , on page 177
- Configuring Smart Transport Through an HTTPs Proxy, on page 180
- Configuring the Call Home Service for Direct Cloud Access, on page 181
- Configuring the Call Home Service for Direct Cloud Access through an HTTPs Proxy Server, on page 184
- Assigning a Smart Account and Virtual Account (SSM On-Prem UI), on page 185
- Validating Devices (SSM On-Prem UI), on page 186
- Ensuring Network Reachability for Product Instance-Initiated Communication, on page 186
- Retrieving the Transport URL (SSM On-Prem UI), on page 189
- Submitting an Authorization Code Request (SSM On-Prem UI, Connected Mode), on page 190
- Submitting an Authorization Code Request (SSM On-Prem UI, Disconnected Mode), on page 191
- Exporting and Importing Usage Data (SSM On-Prem UI), on page 192
- Adding One or More Product Instances (SSM On-Prem UI), on page 193
- Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 194
- Generating and Downloading SLAC from CSSM to a File, on page 199
- Manually Requesting and Auto-Installing a SLAC , on page 201
- Generating and Saving a SLAC Request on the Product Instance, on page 203
- Removing and Returning an Authorization Code, on page 204
- Returning SLAC for an HSECK9 License That Is In-Use, on page 209
- Entering a Return Code in CSSM and Removing the Product Instance, on page 210

• Generating a New Token for a Trust Code from CSSM, on page 211
• Establishing Trust with an ID Token, on page 212
• Downloading a Policy File from CSSM, on page 213
• Uploading Data or Requests to CSSM and Downloading a File, on page 214
• Installing a File on the Product Instance, on page 215
• Setting the Transport Type, URL, and Reporting Interval, on page 216
• Enabling the Utility Mode, on page 219
• Continue Using a PAK License, on page 221
• Removing a PAK License, on page 223
• Removing a PAK License on a Failed Product Instance, on page 224
• Activating a PLR, on page 225
• Upgrading a PLR, on page 228
• Deactivating a PLR, on page 230
• HSECK9 License Mapping Table for Routing Product Instances, on page 231
• Converting a Device-Specific HSECK9 License, on page 239
• Sample Resource Utilization Measurement Report, on page 247

Logging into Cisco (CSLU Interface)

Depending on your needs, when working in CSLU, you can either be in connected or disconnected mode. To work in the connected mode, complete these steps to connect with Cisco.

Procedure

Step 1 From the CSLU Main screen, click **Login to Cisco** (located at the top right corner of the screen).

Step 2 Enter: **CCO User Name** and **CCO Password**.

Step 3 In the CSLU Preferences tab, check that the Cisco connectivity toggle displays “Cisco Is Available”.

Configuring a Smart Account and a Virtual Account (CSLU Interface)

Both the Smart Account and Virtual Account are configured through the Preferences tab. Complete the following steps to configure both Smart and Virtual Accounts for connecting to Cisco.

Procedure

Step 1 Select the **Preferences Tab** from the CSLU home screen.

Step 2 Perform these steps for adding both a Smart Account and Virtual Account:

a) In the Preferences screen navigate to the **Smart Account** field and add the **Smart Account Name**.

b) Next, navigate to the **Virtual Account** field and add the **Virtual Account Name**.

If you are connected to CSSM (In the Preferences tab, **Cisco is Available**), you can select from the list of available SA/VAs.

If you are not connected to CSSM (In the Preferences tab, **Cisco Is Not Available**), enter the SA/VAs manually.

Note
SA/VA names are case sensitive.

Step 3 Click **Save**. The SA/VA accounts are saved to the system

Only one SA/VA pair can reside on CSLU at a time. You cannot add multiple accounts. To change to another SA/VA pair, repeat Steps 2a and 2b then Save. A new SA/VA account pair replaces the previous saved pair

Adding a Product-Initiated Product Instance in CSLU (CSLU Interface)

Complete these steps to add a device-created Product Instance using the Preferences tab.

Procedure

Step 1 Select the **Preferences** tab.
Step 2 In the Preferences screen, de-select the **Validate Device** check box.
Step 3 Set the **Default Connect Method** to **Product Instance Initiated** and then click **Save**.

Ensuring Network Reachability for Product Instance-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for product instance-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps my be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Before you begin

Supported topologies: Connected to CSSM Through CSLU (product instance-initiated communication).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding SLP_VRF`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 5	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 6	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables auto-negotiation operation for the speed and duplex parameters of an interface.
Step 7	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.
Step 8	**ip http client source-interface** *interface-type-number* **Example:** `Device(config)# ip http client source-interface gigabitethernet0/0`	Configures a source interface for the HTTP client.
Step 9	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf SLP_VRF 192.168.0.1 255.255.0.0 192.168.255.1`	(Required) Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.

	Command or Action	Purpose
Step 10	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# ip name-server vrf SLP_VRF 173.37.137.85`	Configures Domain Name System (DNS) on the VRF interface.
Step 11	**license smart vrf** *vrf_string* **Example:** `Device(config)# Device(config)# license smart vrf SLP_VRF`	Configures the VRF name that is used by the product instance. The product instance uses the VRF to send licensing-related data to CSSM, CSLU, or SSM On-Prem. Ensure that the product instance is one that supports VRF and that you configure the transport type as **smart** or **cslu**, with the corresponding URL.
Step 12	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Configures the source interface for the DNS domain lookup. **Note** If you configure this command on a Layer 3 physical interface, it is automatically removed from running configuration in case the port mode is changed or if the device reloads. The only available workaround is to reconfigure the command. Starting with Cisco IOS XE Dublin 17.12.1, this issue is resolved.
Step 13	**ip domain name** *domain-name* **Example:** `Device(config)# ip domain name example.com`	Configure DNS discovery of your domain. In accompanying example, the name-server creates entry `cslu-local.example.com`.

Adding a CSLU-Initiated Product Instance in CSLU (CSLU Interface)

Using the CSLU interface, you can configure the connect method to be CSLU Initiated. This connect method (mode) enables CSLU to retrieve product instance information from the product instance.

Note The default Connect Method is set in the **Preferences** tab.

Complete these steps to add a product instance from the **Inventory** tab

Procedure

Step 1 Go to the **Inventory** tab and from the Product Instances table, select **Add Single Product**.

Step 2 Enter the **Host** (IP address of the Host).

Step 3 Select the **Connect Method** and select one of the CSLU Initiated connect methods.

Step 4 In the right panel, click **Product Instance Login Credentials**. The left panel of the screen changes to show the User Name and Password fields.

Step 5 Enter the product instance **User Name** and **Password**.

Step 6 Click **Save**.

The information is saved to the system and the device is listed in the Product Instances table with the Last Contact listed as never.

Collecting Usage Reports: CSLU Initiated (CSLU Interface)

CSLU also allows you to manually trigger the gathering of usage reports from devices.

After configuring and selecting a product instance (selecting **Add Single Product**, filling in the **Host** name and selecting a CSLU-initiated connect method), click **Actions for Selected** > **Collect Usage**. CSLU connects to the selected product instances and collects the usage reports. These usage reports are stored in CSLU's local library. These reports can then be transferred to Cisco if CSLU is connected to Cisco, or (if you are not connected to Cisco) you can manually trigger usage collection by selecting **Data** > **Export to CSSM**.

If you are working in CSLU-initiated mode, complete these steps to configure CSLU to collect RUM reports from product instances.

Procedure

Step 1 Click the **Preference** tab and enter a valid **Smart Account** and **Virtual Account**, and then selectan appropriate CSLU-initiated collect method. (If there have been any changes in Preferences, make sure you click **Save**).

Step 2 Click the **Inventory** tab and select one or more product instances.

Step 3 Click **Actions for Selected** > **Collect Usage**.

RUM reports are retrieved from each selected device and stored in the CSLU local library. The Last Contacted column is updated to show the time the report was received, and the Alerts column shows the status.

If CSLU is currently logged into Cisco the reports will be automatically sent to the associated Smart Account and Virtual Account in Cisco and Cisco will send an acknowledgement to CSLU as well as to the product instance. The acknowledgement will be listed in the alerts column of the Product Instance table. To manually transfer usage reports Cisco, from the CSLU main screen select **Data** > **Export to CSSM**.

Step 4 From the **Export to CSSM** modal, select the local directory where the reports are to be stored. (<CSLU_WORKING_Directory>/data/default/rum/unsent)

At this point, the usage reports are saved in your local directory (library). To upload these usage reports to Cisco, follow the steps described in Uploading Data or Requests to CSSM and Downloading a File, on page 214.

Note
The Windows operating system can change the behavior of a usage report file properties by dropping the extension when that file is renamed. The behavior change happens when you rename the downloaded file and the renamed file drops the extension. For example, the downloaded default file named `UD_xxx.tar` is renamed to `UD_yyy`. The file loses its TAR extension and cannot function. To enable the usage file to function normally, after re-naming a usage report file, you must also add the TAR extension back to the file name, for example `UD_yyy.tar`.

Ensuring Network Reachability for CSLU-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for CSLU-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps may be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Before you begin

Supported topologies: Connected to CSSM Through CSLU (CSLU-initiated communication).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new model** **Example:** `Device(config)# aaa new model`	(Required) Enable the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa authentication login default local** **Example:** `Device(config)# aaa authentication login default local`	(Required) Sets AAA authentication to use the local username database for authentication.

	Command or Action	Purpose
Step 5	**aaa authorization exec default local** **Example:** `Device(config)# aaa authorization exec default local`	Sets the parameters that restrict user access to a network. The user is allowed to run an EXEC shell.
Step 6	ip routing **Example:** `Device(config)# ip routing`	Enables IP routing.
Step 7	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300`	(Optional) Specifies the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The device sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 8	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Enables DNS-based hostname-to-address translation on your device. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS). **Note** Note If you configure this command on a Layer 3 physical interface, it is automatically removed from running configuration in case the port mode is changed or if the device reloads. The only available workaround is to reconfigure the command. Starting with Cisco IOS XE Dublin 17.12.1, this issue is resolved.
Step 9	**ip domain name** *name* **Example:** `Device(config)# ip domain name vrf Mgmt-vrf cisco.com`	Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).
Step 10	**no username** *name* **Example:** `Device(config)# no username admin`	(Required) Clears the specified username, if it exists. For *name* , enter the same username you will create in the next step. This ensures that a duplicate of the username you are going to create in the next step does not exist.

	Command or Action	Purpose
		If you plan to use REST APIs for CSLU-initiated retrieval of RUM reports, you have to log in to CSLU. Duplicate usernames may cause the feature to work incorrectly if there are duplicate usernames in the system.

Step 11	**username** *name* **privilege** *level* **password** *password*
	Example:
	`Device(config)# username admin privilege 15`
	`password 0 lab`
		(Required) Establishes a username-based authentication system.
		The **privilege** keyword sets the privilege level for the user. A number between 0 and 15 that specifies the privilege level for the user.
		The password allows access to the name argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.
		This enables CSLU to use the product instance native REST.
		Note
		Enter this username and password in CSLU (Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 170 → *Step 4. f.* CSLU can then collect RUM reports from the product instance.

Step 12	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.
Step 13	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding Mgmt-vrf`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 14	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 15	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables auto-negotiation operation for the speed and duplex parameters of an interface.
Step 16	**no shutdown** **Example:**	Restarts a disabled interface.

	Command or Action	Purpose
	`Device(config-if)# no shutdown`	
Step 17	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.
Step 18	**ip http server** **Example:** `Device(config)# ip http server`	(Required) Enables the HTTP server on your IP or IPv6 system, including a Cisco web browser user interface. The HTTP server uses the standard port 80, by default.

Step 19	**ip http authentication local**
	Example:
	`ip http authentication local`
	`Device(config)#`
		(Required) Specifies a particular authentication method for HTTP server users.
		The **local** keyword means that the login user name, password and privilege level access combination specified in the local system configuration (by the username global configuration command) should be used for authentication and authorization.

Step 20	**ip http secure-server** **Example:** `Device(config)# ip http server`	(Required) Enables a secure HTTP (HTTPS) server. The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.
Step 21	**ip http max-connections** **Example:** `Device(config)# ip http max-connections 16`	(Required) Configures the maximum number of concurrent connections allowed for the HTTP server. Enter an integer in the range from 1 to 16. The default is 5.
Step 22	**ip tftp source-interface** *interface-type-number* **Example:** `Device(config)# ip tftp source-interface GigabitEthernet0/0`	Specifies the IP address of an interface as the source address for TFTP connections.
Step 23	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.
Step 24	**logging host** **Example:** `Device(config)# logging host 172.25.33.20 vrf Mgmt-vrf`	Logs system messages and debug output to a remote host.
Step 25	**end** **Example:**	Exits the global configuration mode and enters priveleged EXEC mode.

	Command or Action	Purpose
	`Device(config)# end`	
Step 26	**show ip http server session-module** **Example:** `Device# show ip http server session-module`	(Required) Verifies HTTP connectivity. In the output, check that `SL_HTTP` is active. Additionally, you can also perform the following checks : • From device where CSLU is installed, verify that you can ping the product instance. A successful ping confirms that the product instance is reachable. • From a Web browser on the device where CSLU is installed verify `https://<product-instance-ip>/`. This ensures that the REST API from CSLU to the product instance works as expected.

Export to CSSM (CSLU Interface)

This option can be used as a part of a manual download procedure when you want the workstation isolated for security purposes.

Procedure

Step 1 Go to the **Preferences** tab, and turn off the **Cisco Connectivity** toggle switch.

The field switches to “Cisco Is Not Available”.

Step 2 From the main menu in the CSLU home screen navigate to **Data** > **Export to CSSM**.

Step 3 Select the file from the modal that opens and click **Save**. You now have the file saved.

Note
At this point you have a DLC file, RUM file, or both.

Step 4 From a workstation that has connectivity to Cisco, and complete the following: Uploading Data or Requests to CSSM and Downloading a File, on page 214.

Once the file is downloaded, you can import it into CSLU, see Import from CSSM (CSLU Interface), on page 176

Import from CSSM (CSLU Interface)

Once you have received the ACK or other file (such as an authorization code) from Cisco, you are ready to upload that file to your system. This procedure can be used for workstations that are offline. Complete these steps to select and upload files from Cisco.

Procedure

Step 1 Ensure that you have downloaded the file to a location that is accessible to CSLU.

Step 2 From the main menu in the CSLU home screen, navigate to **Data** > **Import from CSSM**.

Step 3 An Import from CSSM modal open for you to either:

- Drag and Drop a file that resides on your local drive, or
- Browse for the appropriate *.xml file, select the file and click **Open**.

If the upload is successful, you will get message indicating that the file was successfully sent to the server. If the upload is not successful, you will get an import error.

Step 4 When you have finished uploading, click the **x** at the top right corner of the modal to close it.

Requesting SLACs for Multiple Product Instances (CSLU Interface)

The **Authorization Code Request** menu option is specifically used to manually request SLACs for multiple Product Instances.

Before you begin

Supported topologies:

- Connected to CSSM Through CSLU
- CSLU Disconnected from CSSM

Procedure

Step 1 From the Product Instance table, select the **Product Instances** for authorization code request.

Step 2 With one or more Product Instances selected, select the **Authorization Code Request** option from the Available Actions menu.

Step 3 In the modal it describes that steps to take, click **Accept**

The upload modal opens to select a CSV file for uploading. (local)

Step 4 Next, follow these steps that are also described in the modal.

a) Upload the file to Cisco by following this directory path: **software.cisco.com** > **Smart Software Licensing** > **Inventory** > **Product Instances** > **Authorize License Enforced Features**

b) Follow the steps shown on the screen:

1. Select **Multiple Product Instances**.

   If multiple Product Instances, you can click **Choose File** to upload or **Download a Template** (csv file template) for future uploads.

2. In the next panel, **select licenses**.

3. Review and Confirm your **license selections**

4. Create the **Authorization Code** to be downloaded

c) After the file and selected licenses have uploaded to Cisco, **download the authorization codes** (as a file) for those Product Instances selected back to CSLU.

Step 5 Select **Upload From Cisco (in the CSLU interface)**

If CSLU is In Product-Initiated mode: The uploaded codes are now applied to the Product Instances the next time the Product Instance contacts CSLU.

If CSLU is in a CSLU initiated mode: The uploaded codes are now applied to the Product Instances the next time the CSLU runs an update.

Setting Up a Connection to CSSM

The following steps show how to set up a Layer 3 connection to CSSM to verify network reachability. Steps marked as "(Required)" are required for all product instances, all other steps may be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:**	Specifies the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The

	Command or Action	Purpose
	`Device(config)# ip name-server 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230`	first server specified is the primary server. The device sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 4	**ip name-server vrf Mgmt-vrf** *server-address 1...server-address 6* **Example:** `Device(config)# ip name-server vrf SLP_VRF 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230`	(Optional) Configures DNS on the VRF interface. You can specify up to six name servers. Separate each server address with a space. **Note** This command is an alternative to the **ip name-server** command.
Step 5	**license smart vrf** *vrf_string* **Example:** `Device(config)# Device(config)# license smart vrf SLP_VRF`	Configures the VRF name that is used by the product instance. The product instance uses the VRF to send licensing-related data to CSSM, CSLU, or SSM On-Prem. Ensure that the product instance is one that supports VRF and that you configure the transport type as **smart** or **cslu**, with the corresponding URL.
Step 6	**ip domain lookup source-interface** *interface-type interface-number* **Example:** `Device(config)# ip domain lookup source-interface Vlan100`	Configures the source interface for the DNS domain lookup.
Step 7	**ip domain name** *domain-name* **Example:** `Device(config)# ip domain name example.com`	Configures the domain name.
Step 8	**ip host tools.cisco.com** *ip-address* **Example:** `Device(config)# ip host tools.cisco.com 209.165.201.30`	Configures static hostname-to-address mappings in the DNS hostname cache if automatic DNS mapping is not available.

Step 9	**interface** *interface-type-number*
	Example:
	`Device(config)# interface Vlan100`
	`Device(config-if)# ip address 192.0.2.10 255.255.255.0`
	`Device(config-if)# exit`
		Configures a Layer 3 interface. Enter an interface type and number or a VLAN.

Step 10	**ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**] **Example:**	(Required) Activates the NTP service (if it has not already been activated) and enables the system to synchronize the system software

	Command or Action	Purpose

	`Device(config)# ntp server 198.51.100.100 version 2 prefer`	clock with the specified NTP server. This ensures that the device time is synchronized with CSSM.
		Use the **prefer** keyword if you need to use this command multiple times and you want to set a preferred server. Using this keyword reduces switching between servers.
		Tip
		After you complete this configuration, use the **show license tech** to verify if the clock has actually synchronized. If successfully synchronized, the `Clock sync-ed with NTP` field is set to `True`. If not synchronized, this field is set to `False`.
		If the clock is not synchronized, your **attempts** at trust establishment or requesting SLAC and so on, are not reflected in the **show license tech** output. For example:
		`Trust Establishment:`
		`  Attempts: Total=0, Success=0, Fail=0`
		`  Ongoing Failure: Overall=0`
		`Communication=0`

Step 11	**switchport access vlan** *vlan_id*
	Example:
	`Device(config)# interface GigabitEthernet1/0/1`
	`Device(config-if)# switchport access vlan 100`
	`Device(config-if)# switchport mode access`
	`Device(config-if)# exit`
	`OR`
	`Device(config)#`
		Enables the VLAN for which this access port carries traffic and sets the interface as a nontrunking nontagged single-VLAN Ethernet interface.
		Note
		This step is to be configured only if the switchport access mode is required. The **switchport access vlan** command may apply to Catalyst switching product instances, for example, and for routing product instances you may want to configure the **ip address** *ip-address mask* command instead.

Step 12	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route 192.0.2.0 255.255.255.255 192.0.2.1`	Configures a route on the device. You can configure either a static route or a dynamic route.
Step 13	**ip http client source-interface** *interface-type-number* **Example:** `Device(config)# ip http client source-interface Vlan100`	(Required) Configures a source interface for the HTTP client. Enter an interface type and number or a VLAN.

	Command or Action	Purpose
Step 14	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 15	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Configuring Smart Transport Through an HTTPs Proxy

To use a proxy server to communicate with CSSM when using the Smart transport mode, complete the following steps:

Note *Authenticated* HTTPs proxy configurations are not supported.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**license smart transport smart** **Example:** `Device(config)# license smart transport smart`	Enables Smart transport mode.
Step 4	**license smart url default** **Example:** `Device(config)# license smart transport default`	Automatically configures the Smart URL (https://smartreceiver.cisco.com/licservice/license). For this option to work as expected, the transport mode in the previous step must be configured as **smart**.
Step 5	**license smart proxy** {**address** *address_hostname* | **port** *port_num*} **Example:**	Configures a proxy for the Smart transport mode. When a proxy is configured, licensing messages are sent to the proxy along with the final destination URL (CSSM). The proxy sends

	Command or Action	Purpose
	`Device(config)# license smart proxy address 192.168.0.1` `Device(config)# license smart proxy port 3128`	the message on to CSSM. Configure the proxy IP address and port information separately: • **address** *address_hostname*: Specifies the proxy address. Enter the IP address or hostname of the proxy server. • **port** *port_num*: Specifies the proxy port. Enter the proxy port number. Note the change in the criteria for the acceptance of proxy servers, starting with Cisco IOS XE Bengaluru 17.6.1: only the status code of the proxy server response is verified by the system and not the reason phrase. The RFC format is `status-line = HTTP-version SP status-code SP reason-phrase CRLF`. For more information about the status line, see section 3.1.2 of RFC 7230.
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 7	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Configuring the Call Home Service for Direct Cloud Access

The Call Home service provides email-based and web-based notification of critical system events to CSSM. To configure the transport mode, enable the Call Home service, and configure a destination profile (A destination profile contains the required delivery information for an alert notification. At least one destination profile is required.), complete the following steps:

Note All steps are required unless specifically called-out as "(Optional)".

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**license smart transport callhome** **Example:** `Device(config)# license smart transport callhome`	Enables Call Home as the transport mode.
Step 4	**license smart url** *url* **Example:** `Device(config)# license smart url https://tools.cisco.com/its/service/oddce/services/DDCEService`	For the **callhome** transport mode, configure the CSSM URL exactly as shown in the example.
Step 5	**service call-home** **Example:** `Device(config)# service call-home`	Enables the Call Home feature.
Step 6	**call-home** **Example:** `Device(config)# call-home`	Enters Call Home configuration mode.
Step 7	**contact-email-address** *email-address* **Example:** `Device(config-call-home)# contact-email-addr username@example.com`	Assigns customer's email address and enables Smart Call Home service full reporting capability and sends a full inventory message from Call-Home TAC profile to Smart Call Home server to start full registration process. You can enter up to 200 characters in email address format with no spaces.

Step 8	**profile** *name*
	Example:
	`Device(config-call-home)# profile CiscoTAC-1`
	`Device(config-call-home-profile)#`
		Enters the Call Home destination profile configuration submode for the specified destination profile.
		By default:
		• The CiscoTAC-1 profile is inactive. To use this profile with the Call Home service, you must enable the profile.
		• The CiscoTAC-1 profile sends a full report of all types of events subscribed in the profile. The alternative is to additionally configure `Device(cfg-call-home-profile)# anonymous-reporting-only` anonymous-reporting-only. When this is

	Command or Action	Purpose
		set, only crash, inventory, and test messages will be sent. Use the **show call-home profile all** command to check the profile status.
Step 9	**active** **Example:** `Device(config-call-home-profile)# active`	Enables the destination profile.

Step 10	**destination transport-method http** {**email** |**http**}
	Example:
	`Device(config-call-home-profile)# destination transport-method http`
	AND
	`Device(config-call-home-profile)# no destination transport-method email`
		Enables the message transport method. In the example, Call Home service is enabled via HTTP and transport via email is disabled.
		
		The **no** form of the command disables the method.

Step 11	**destination address** { **email** *email_address* |**http** *url*}
	Example:
	`Device(config-call-home-profile)# destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`
	AND
	`Device(config-call-home-profile)# no destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`
		Configures the destination e-mail address or URL to which Call Home messages are sent. When entering a destination URL, include either **http://** (default) or **https://**, depending on whether the server is a secure server.
		
		In the example provided here, a **http://** destination URL is configured; and the **no** form of the command is configured for **https://**.

Step 12	**exit** **Example:** `Device(config-call-home-profile)# exit`	Exits Call Home destination profile configuration mode and returns to Call Home configuration mode.
Step 13	**exit** **Example:** `Device(config-call-home)# end`	Exits Call Home configuration mode and returns to privileged EXEC mode.
Step 14	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.
Step 15	**show call-home profile** {*name* |**all**}	Displays the destination profile configuration for the specified profile or all configured profiles.

Configuring the Call Home Service for Direct Cloud Access through an HTTPs Proxy Server

The Call Home service can be configured through an HTTPs proxy server. This configuration requires no user authentication to connect to CSSM.

Note Authenticated HTTPs proxy configurations are not supported.

To configure and enable the Call Home service through an HTTPs proxy, complete the following steps:

Note All steps are required unless specifically called-out as "(Optional)".

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**license smart transport callhome** **Example:** `Device(config)# license smart transport callhome`	Enables Call Home as the transport mode.
Step 4	**service call-home** **Example:** `Device(config)# service call-home`	Enables the Call Home feature.
Step 5	**call-home** **Example:** `Device(config)# call-home`	Enters Call Home configuration mode.
Step 6	**http-proxy** *proxy-address* **proxy-port** *port-number* **Example:**	Configures the proxy server information to the Call Home service. Note the change in the criteria for the acceptance of proxy servers, starting with Cisco

	Command or Action	Purpose
	`Device(config-call-home)# http-proxy 198.51.100.10 port 5000`	IOS XE Bengaluru 17.6.1: only the status code of the proxy server response is verified by the system and not the reason phrase. The RFC format is `status-line = HTTP-version SP status-code SP reason-phrase CRLF`. For more information about the status line, see section 3.1.2 of RFC 7230.
Step 7	**exit** **Example:** `Device(config-call-home)# exit`	Exits Call Home configuration mode and enters global configuration mode.
Step 8	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.
Step 9	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Assigning a Smart Account and Virtual Account (SSM On-Prem UI)

You can use this procedure to import one or more product instances along with corresponding Smart Account and Virtual Account information, into the SSM On-Prem database. This enables SSM On-Prem to map product instances that are part of local virtual accounts (other than the default local virtual account), to the correct license pool in CSSM:

Before you begin

Supported topologies: SSM On-Prem Deployment (product instance-initiated communication).

Procedure

Step 1 Log into the SSM On-Prem and select the **Smart Licensing** workspace.

Step 2 Navigate to **Inventory** > **SL Using Policy** > **Export/Import All** > **Import Product Instances List**

The **Upload Product Instances** window is displayed.

Step 3 Click **Download** to download the .csv template file and enter the required information for all the product instances in the template.

Step 4 Once you have filled-out the template, click **Inventory** > **SL Using Policy** > **Export/Import All** > **Import Product Instances List**.

The **Upload Product Instances** window is displayed.

Step 5 Now, click **Browse** and upload the filled-out .csv template.

Smart Account and Virtual Account information for all uploaded product instances is now available in SSM On-Prem.

Validating Devices (SSM On-Prem UI)

When device validation is enabled, RUM reports from unknown product instances (not in the SSM On-Prem database) are rejected.

By default, devices are not validated. Complete the following steps to enable it:

Before you begin

Supported topologies: SSM On-Prem Deployment (product instance-initiated communication).

Procedure

Step 1 In the **On-Prem License Workspace** window, click **Admin Workspace** and log in, if prompted.

The **On-Prem Admin Workspace** window is displayed.

Step 2 Click the **Settings** widget.

The **Settings** window is displayed.

Step 3 Navigate to the **CSLU** tab and turn-on the **Validate Device** toggle switch.

RUM reports from unknown product instances will now be rejected. If you haven't already, you must now add the required product instances to the SSM On-Prem database before sending RUM reports. See Assigning a Smart Account and Virtual Account (SSM On-Prem UI), on page 185

Ensuring Network Reachability for Product Instance-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for product instance-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps my be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Note Ensure that you configure steps 14, 15, and 16 exactly as shown below. These commands must be configured to ensure that the correct trustpoint is used and that the necessary certificates are accepted for network reachability.

Before you begin

Supported topologies: SSM On-Prem Deployment(product instance-initiated communication).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding SLP_VRF`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 5	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 6	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables auto-negotiation operation for the speed and duplex parameters of an interface.
Step 7	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.

	Command or Action	Purpose
Step 8	**ip http client source-interface** *interface-type-number* **Example:** `Device(config)# ip http client source-interface gigabitethernet0/0`	Configures a source interface for the HTTP client.
Step 9	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf SLP_VRF 192.168.0.1 255.255.0.0 192.168.255.1`	(Required) Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.
Step 10	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# ip name-server vrf SLP_VRF 198.51.100.1`	Configures Domain Name System (DNS) on the VRF interface.
Step 11	**license smart vrf** *vrf_string* **Example:** `Device(config)# Device(config)# license smart vrf SLP_VRF`	Configures the VRF name that is used by the product instance. The product instance uses the VRF to send licensing-related data to CSSM, CSLU, or SSM On-Prem. Ensure that the product instance is one that supports VRF and that you configure the transport type as **smart** or **cslu**, with the corresponding URL.
Step 12	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Configures the source interface for the DNS domain lookup.
Step 13	**ip domain name** *domain-name* **Example:** `Device(config)# ip domain name example.com`	Configure DNS discovery of your domain. In the accompanying example, the name-server creates entry `cslu-local.example.com`.

Step 14	**crypto pki trustpoint SLA-TrustPoint**
	Example:
	`Device(config)# crypto pki trustpoint SLA-TrustPoint`
	`Device(ca-trustpoint)#`
		(Required) Declares that the product instance should use trustpoint "SLA-TrustPoint" and enters the ca-trustpoint configuration mode. The product instance does not recognize any trustpoints until you declare a trustpoint using this command.

Step 15	enrollment terminal **Example:**	(Required) Specifies the certificate enrollment method.

	Command or Action	Purpose
	`Device(ca-trustpoint)# enrollment terminal`	
Step 16	**revocation-check none** **Example:** `Device(ca-trustpoint)# revocation-check none`	(Required) Specifes a method that is to be used to ensure that the certificate of a peer is not revoked. For the SSM On-Prem Deployment topology, enter the **none** keyword. This means that a revocation check will not be performed and the certificate will always be accepted.

Step 17	**exit**
	Example:
	`Device(ca-trustpoint)# exit`
	`Device(config)# exit`
		Exits the ca-trustpoint configuration mode and then the global configuration mode and returns to privileged EXEC mode.

Step 18	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Retrieving the Transport URL (SSM On-Prem UI)

You must configure the transport URL on the product instance when you deploy the product instance-initiated communication with SSM On-Prem deployment. This task show you how to easily copy the complete URL including the tenant ID from SSM On-Prem.

Before you begin

Supported topologies: SSM On-Prem Deployment (product instance-initiated communication).

Procedure

Step 1 Log into SSM On-Prem and select the **Smart Licensing** workspace.

Step 2 Navigate to the **Inventory** tab and from the dropdown list of local virtual accounts (top right corner), select the *default local virtual account*. When you do, the area under the **Inventory** tab displays **Local Virtual Account: Default**.

Step 3 Navigate to the **General** tab.

The **Product Instance Registration Tokens** area is displayed.

Step 4 In the **Product Instance Registration Tokens** area click **CSLU Transport URL**.

The **Product Registration URL** pop-window is displayed.

Step 5 Copy the entire URL and save it in an accessible place.

You will require the URL when you configure the transport type and URL on the product instance.

Step 6 Configure the transport type and URL. See: Setting the Transport Type, URL, and Reporting Interval, on page 216.

Submitting an Authorization Code Request (SSM On-Prem UI, Connected Mode)

This procedure shows you how to install SLAC for export-controlled and enfored licenses when SSM On-Prem is connected to CSSM. Here you begin by sending the SLAC request from the product instance, to SSM On-Prem. You must then synchronize SSM On-Prem with CSSM. CSSM processes the request and the response is send back to SSM On-Prem. Finally, the response is sent from SSM On-Prem to the product instance and the SLAC is installed on the device.

Before you begin

Supported topologies: SSM On-Prem Deployment (Product instance-initiated communication).

Ensure that you have an adequate positive balance of the necessary export-controlled or enforced licenses in your Smart Account and Virtual Account in CSSM.

Procedure

Step 1 On the product instance, configure the following command: **license smart authorization request** {**add** | **replace**} *feature_name* {**all** | **local** }

This sends the SLAC request to SSM On-Prem.

Specify if you want to add to or replace an existing SLAC:

- **add**: Adds the requested license to an existing SLAC. The new authorization code will contain all the licences of the existing SLAC, and the requested license.
- **replace**: Replaces the existing SLAC. The new SLAC will contain only the requested license. All licenses in the existing SLAC are returned. When you enter this keyword, the product instance checks if these existing licenses are in-use. If they are, an error message is displayed, telling you to first disable the corresponding feature.

For *feature_name*, enter the name of the license for which you want to request an addition or a replacement of the SLAC. For example, enter `hseck9` for the HSECK9 license.

Specify the device by entering one of these options:

- **all**: Gets the authorization code for *all* devices in a High Availability set-up
- **local**: Gets the authorization code for the *active* device in a High Availability set-up. This is the default option.

Step 2 Log into SSM On-Prem.

Step 3 In the SSM On-Prem UI, Smart Licensing workspace, nagivate to **Reports** > **Usage Schedules** > **Synchronize now with Cisco**

The SLAC request is sent to CSSM. CSSM processes the request and sends a SLAC response back to SSM On-Prem, which sends the response to the product instance. It is automatically installed on the product instance.

You can monitor the event log in SSM On-Prem UI to know when the SLAC has been sent to the product instance.

Step 4 On the product instance, enter the **show license authorization** command in privileged EXEC mode to display SLAC information.

Submitting an Authorization Code Request (SSM On-Prem UI, Disconnected Mode)

With the SSM On-Prem Deployment topology, if SSM On-Prem is not connected to CSSM, the authorization codes required for export-controlled and enfored licenses must be generated in CSSM and imported into SSM On-Prem before the product instance can request the same.

This procedure shows you the steps you have to complete in SSM On-Prem (to submit the request and then import SLAC), points you to the procedure you have to complete in CSSM (to generate and download SLAC), and to the procedure you have to complete on the product instance (to finally request and install SLAC).

Before you begin

Supported topologies:

- SSM On-Prem Deployment (SSM On-Prem-initiated communication)
- SSM On-Prem Deployment (Product instance-initiated communication).

Ensure that you have an adequate positive balance of the necessary export-controlled or enforced licenses in your Smart Account and Virtual Account in CSSM.

Procedure

Step 1 Log into SSM On-Prem and select **Smart Licensing**.

Step 2 Navigate to **Inventory** > **SL Using Policy**. Select all the product instances for which you want to request SLAC.

Step 3 Click **Actions for Selected…** > **Authorization Code Request**.

The **Authorization Request Information** pop-up window is displayed.

Step 4 Click **Accept** and save the .csv file when prompted.

The generated .csv file contains the list of selected product instances along with required device information, in the required format, to generate the SLAC in CSSM. Save this file in a location that is accessible when you are working on the CSSM Web UI (in the next step).

Step 5 Complete this task in CSSM: Uploading Data or Requests to CSSM and Downloading a File, on page 214.

You can use the above procedure to generate SLAC for a single product instance and for multiple product instances. For the SSM On-Prem Deployment topology, follow the steps to generate SLAC for multiple product instances.

Step 6 Return to the SSM On-Prem UI and navigate to **Inventory** > **SL Using Policy**.

Step 7 Click **Export/Import All…** > **Import From Cisco**.

Import the file download from CSSM at the end of the procedure in Step 5 above.

To verify import, under **Inventory** > **SL Using Policy**, see the Alerts column. The following message is displayed: Authorization message received from CSSM.

Step 8 Complete this task on the product instance: Manually Requesting and Auto-Installing a SLAC , on page 201.

This task shows you how to request and install SLAC from SSM On-Prem.

Exporting and Importing Usage Data (SSM On-Prem UI)

You can use this procedure to complete usage synchronization between SSM On-Prem and CSSM when SSM On-Prem is disconnected from CSSM.

Before you begin

Supported topologies:

- SSM On-Prem Deployment (SSM On-Prem-initiated communication)
- SSM On-Prem Deployment (product instance-initiated communication).

Reporting data must be available in SSM On-Prem. You must have either pushed the nessary reporting data from the product instance to SSM On-Prem (product instance-initiated communication) or retrieved the necessary reporting data from the product instance (SSM On-Prem-initiated communication).

Procedure

Step 1 Log into SSM On-Prem and select **Smart Licensing**.

Step 2 Navigate to **Inventory** > **SL Using Policy** tab.

Step 3 In the **SL Using Policy** tab area, click **Export/Import All...** > **Export Usage to Cisco**.

This generates one .tar file with *all* the usage reports available in the SSM On-Prem server.

Step 4 Complete this task in CSSM: Uploading Data or Requests to CSSM and Downloading a File, on page 214.

At the end of this task you will have an ACK file to import into SSM On-Prem.

Step 5 Again navigate to the **Inventory** > **SL Using Policy** tab.

Step 6 In the **SL Using Policy** tab area, click **Export/Import All...** > **Import From Cisco** . Upload the .tar ACK file.

To verify ACK import, in the **SL Using Policy** tab area check the **Alerts** column of the corresponding product instance. The following message is displayed: Acknowledgement received from CSSM.

Adding One or More Product Instances (SSM On-Prem UI)

You can use this procedure to add one product instance or to import and add multiple product instances. It enables SSM On-Prem to retrieve information from the product instance.

Before you begin

Supported topologies: SSM On-Prem Deployment (SSM On-Prem-initiated communication).

Procedure

Step 1 Log into the SSM On-Prem UI and click **Smart Licensing**.

Step 2 Navigate to **Inventory** tab. Select a local virtual account from the drop-down list in the top right corner.

Step 3 Navigate to the **SL Using Policy** tab.

Step 4 Add a single product or import multiple product instances (*choose one*).

- **To add a single product instance**:
  - **a.** In the **SL Using Policy** tab area, click **Add Single Product**.
  - **b.** In the **Host** field, enter the IP address of the host (product instance).
  - **c.** From the **Connect Method** dropdown list, select an appropriate SSM On-Prem-initiated connect method.

    The available connect methods for SSM On-Prem-initiated communication are: NETCONF, RESTCONF, and REST API.
  - **d.** In the right panel, click **Product Instance Login Credentials**.

    The **Product Instance Login Credentials** window is displayed

    Note
    You need the login credentials if a product instance requires a SLAC. Further, you must have also added a valid Smart Account and Virtual Account before any SLAC requests can be serviced.
  - **e.** Enter the **User ID** and **Password**, and click **Save**.

    This is the same user ID and password that you configured as part of commands required to establish network reachability (Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 194).

    Once validated, the product instance is displayed in the listing in the **SL Using Policy** tab area.
- **To import multiple product instances:**
  - **a.** In **SL Using Policy** tab, click **Export/Import All...** > **Import Product Instances List**.

The **Upload Product Instances** window is displayed.

b. Click **Download** to download the predefined .csv template.

c. Enter the required information for all the product instances in the .csv template.

In the template, ensure that you provide **Host**, **Connect Method** and **Login Credentials** for all product instances.

The available connect methods for SSM On-Prem-initiated communication are: NETCONF, RESTCONF, and REST API.

Login credentials refer to the user ID and password that you configured as part of commands required to establish network reachability (Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 194).

d. Again navigate to **Inventory** > **SL Using Policy** tab. Click **Export/Import All....** > **Import Product Instances List**.

The **Upload Product Instances** window is displayed.

e. Now upload the filled-out .csv template.

Once validated, the product instances are displayed in the listing in the **SL Using Policy** tab.

Ensuring Network Reachability for SSM On-Prem-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for SSM On-Prem-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps may be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:



Note Ensure that you configure steps 25, 26, and 27 exactly as shown below. These commands must be configured to ensure that the correct trustpoint is used and that the necessary certificates are accepted for network reachability.

Before you begin

Supported topologies: SSM On-Prem Deployment (SSM On-Prem-initiated communication).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new model** **Example:** `Device(config)# aaa new model`	(Required) Enable the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa authentication login default local** **Example:** `Device(config)# aaa authentication login default local`	(Required) Sets AAA authentication to use the local username database for authentication.
Step 5	**aaa authorization exec default local** **Example:** `Device(config)# aaa authorization exec default local`	Sets the parameters that restrict user access to a network. The user is allowed to run an EXEC shell.
Step 6	ip routing **Example:** `Device(config)# ip routing`	Enables IP routing.
Step 7	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300`	(Optional) Specifies the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The device sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 8	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Enables DNS-based hostname-to-address translation on your device. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS). **Note** If you configure this command on a Layer 3 physical interface, it is automatically removed from running configuration in case the port

	Command or Action	Purpose
		mode is changed or if the device reloads. The only available workaround is to reconfigure the command. Starting with Cisco IOS XE Dublin 17.12.1, this issue is resolved.
Step 9	**ip domain name** *name* **Example:** `Device(config)# ip domain name vrf Mgmt-vrf cisco.com`	Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).
Step 10	**no username** *name* **Example:** `Device(config)# no username admin`	(Required) Clears the specified username, if it exists. For *name* , enter the same username you will create in the next step. This ensures that a duplicate of the username you are going to create in the next step does not exist. If you plan to use REST APIs for SSM On-Prem-initiated retrieval of RUM reports, you have to log in to SSM On-Prem. Duplicate usernames may cause the feature to work incorrectly if there are present in the system.

Step 11	**username** *name* **privilege** *level* **password** *password*
	Example:
	`Device(config)# username admin privilege 15`
	`password 0 lab`
		(Required) Establishes a username-based authentication system.
		The **privilege** keyword sets the privilege level for the user. A number between 0 and 15 that specifies the privilege level for the user.
		The password allows access to the name argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.
		This enables SSM On-Prem to use the product instance native REST.
		Note
		Enter this username and password in SSM On-Prem (Adding One or More Product Instances (SSM On-Prem UI), on page 193). This enables SSM On-Prem to collect RUM reports from the product instance.

Step 12	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.

	Command or Action	Purpose
Step 13	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding Mgmt-vrf`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 14	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 15	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables auto-negotiation operation for the speed and duplex parameters of an interface.
Step 16	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Restarts a disabled interface.
Step 17	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.
Step 18	**ip http server** **Example:** `Device(config)# ip http server`	(Required) Enables the HTTP server on your IP or IPv6 system, including a Cisco web browser user interface. The HTTP server uses the standard port 80, by default.

Step 19	**ip http authentication local**
	Example:
	`ip http authentication local`
	`Device(config)#`
		(Required) Specifies a particular authentication method for HTTP server users.
		The **local** keyword means that the login user name, password and privilege level access combination specified in the local system configuration (by the username global configuration command) should be used for authentication and authorization.

Step 20	**ip http secure-server** **Example:** `Device(config)# ip http server`	(Required) Enables a secure HTTP (HTTPS) server. The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.
Step 21	**ip http max-connections** **Example:** `Device(config)# ip http max-connections 16`	(Required) Configures the maximum number of concurrent connections allowed for the HTTP server. Enter an integer in the range from 1 to 16. The default is 5.

	Command or Action	Purpose
Step 22	**ip tftp source-interface** *interface-type-number* **Example:** `Device(config)# ip tftp source-interface GigabitEthernet0/0`	Specifies the IP address of an interface as the source address for TFTP connections.
Step 23	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.
Step 24	**logging host** **Example:** `Device(config)# logging host 172.25.33.20 vrf Mgmt-vrf`	Logs system messages and debug output to a remote host.

Step 25	**crypto pki trustpoint SLA-TrustPoint**
	Example:
	`Device(config)# crypto pki trustpoint SLA-TrustPoint`
	`Device(ca-trustpoint)#`
		(Required) Declares that the product instance should use trustpoint "SLA-TrustPoint" and enters the ca-trustpoint configuration mode. The product instance does not recognize any trustpoints until you declare a trustpoint using this command.

Step 26	enrollment terminal **Example:** `Device(ca-trustpoint)# enrollment terminal`	Required) Specifies the certificate enrollment method.
Step 27	**revocation-check none** **Example:** `Device(ca-trustpoint)# revocation-check none`	(Required) Specifes a method that is to be used to ensure that the certificate of a peer is not revoked. For the SSM On-Prem Deployment topology, enter the **none** keyword. This means that a revocation check will not be performed and the certificate will always be accepted.

Step 28	**end**
	Example:
	`Device(ca-trustpoint)# exit`
	`Device(config)# end`
		Exits the ca-trustpoint configuration mode and then the global configuration mode and returns to privileged EXEC mode.

Step 29	**show ip http server session-module** **Example:** `Device# show ip http server session-module`	(Required) Verifies HTTP connectivity. In the output, check that `SL_HTTP` is active. Additionally, you can also perform the following checks : • From device where SSM On-Prem is installed, verify that you can ping the product instance. A successful ping

	Command or Action	Purpose
		confirms that the product instance is reachable. • From a Web browser on the device where SSM On-Prem is installed verify `https://<product-instance-ip>/`. This ensures that the REST API from SSM On-Prem to the product instance works as expected.
Step 30	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Generating and Downloading SLAC from CSSM to a File

To generate a SLAC in CSSM and download it to a file, perform the following steps in CSSM:

Before you begin

Supported topologies:

- No Connectivity to CSSM and No CSLU
- CSLU Disconnected from CSSM
- SSM On-Prem Deployment (product instance-initiated and SSM On-Prem-initiated communication)

You can use this procedure to generate SLAC for a single product instance and for multiple product instances.

If it is for a single product instance, you will require the PID and Serial number to complete this task. On the product instance, enter the **show license udi** command in privileged EXEC mode and keep this information handy.

If it is for multiple product instances, have the .csv file (with necessary product instance information) saved in an accessible location.

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com, and click **Manage licenses**.

Log in using the username and password provided by Cisco. The **Smart Software Licensing** page is displayed.

Step 2 Click the **Inventory** tab.

Step 3 Click the **Product Instances** tab.

Step 4 Click the **Authorize License Enforced Features** tab.

Step 5 Generate SLAC for a single product instance or for multiple product instances (*choose one*).

- **To generate SLAC for a single product instance:**
  a. Enter the **PID** and **Serial Number**.

     Note
     Do not populate any of the other fields.

  b. Choose the license, and in the corresponding **Reserve** column, and enter `1`.

     Ensure that you choose the correct license for a PID. See the HSECK9 License Mapping Table for Routing Product Instances, on page 231 for reference.

  c. Click **Next**

  d. Click **Generate Authorization Code**.

  e. Download the authorization code and save as a .csv file.

  f. Install the file on the product instance. See Installing a File on the Product Instance, on page 215.

- **To generate SLAC for multiple product instances (you will have a .csv file to upload in this case)**:
  a. From the dropdown list that says “Single Device” (by default), change the selection to “Multiple Devices”.

  b. Click **Browse** and navigate to the .csv file, which contains the list of product instances that require SLAC.

  c. Once uploaded, the list of devices is displayed in CSSM. All the devices will have the checkbox enabled (implying that you want to request a SLAC for all of them), and click **Next**.

  d. Specify the quantity licenses required for each product instance, and click **Next**.

     Note
     If you are requesting SLAC for export-controlled or enforced licenses in the Smart Licensing Using Policy environment only one SLAC is required for each product instance.

  e. From the **Device Type** dropdown list, select **DNA On-Prem**, and click **Continue**.

  f. Click **Reserve Licenses**.

     The **Download Authorization Codes** button is displayed.

  g. Click **Download Authorization Codes** to download this .csv file, which has SLACs for all product insances in step c. above. Click **Close**.

  h. You can now import this .csv file to SSM On-Prem. Return to Submitting an Authorization Code Request (SSM On-Prem UI, Disconnected Mode), on page 191 and complete the remaining steps to import this file.

Manually Requesting and Auto-Installing a SLAC

To request CSSM, or CSLU, or SSM On-Prem for a SLAC and have it automatically installed on the product instance, perform the following steps on the product instance:

Before you begin

Supported topologies:

- Connected to CSSM Through CSLU
- Connected Directly to CSSM
- SSM On-Prem Deployment (product instance-initiated communication)

Before you proceed, check the following as well:

- The product instance on which you are requesting the SLAC is connected CSSM, CSLU, or SSM On-Prem.
- The transport type is set accordingly (**smart** for CSSM, and **cslu** for CSLU). Enter the **show license all** command in privileged EXEC mode. In the output, check field `Transport: .`
- If you are directly connected to CSSM, a trust code is installed. Enter the **show license all** command in privileged EXEC mode. In the output check field `Trust Code Installed:`
- In case of an SSM On-Prem Deployment where SSM On-Prem is in a disconnected mode, the product instance requests SSM On-Prem for SLAC in this task, so the required SLAC file must be available in the SSM On-Prem server before you begin with this task. See Submitting an Authorization Code Request (SSM On-Prem UI, Disconnected Mode), on page 191

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted
Step 2	**license smart authorization request** { **add** | **replace** } *feature_name* { **all** | **local** } **Example:** `Device# license smart authorization request replace hseck9 local`	The **license smart authorization request** command requests a SLAC from CSSM or CSLU (CSLU in-turn fetches it from CSSM), or SSM On-Prem. A SLAC is returned and automatically installed on the product instance. Specify if you want to add to or replace an existing SLAC: • **add**: Adds the requested license to an existing SLAC. The new authorization code will contain all the licences of the existing SLAC, and the requested license.

	Command or Action	Purpose
		Do not use this option even though it is available on the CLI, for any of the supported product instances that are within the scope of this document. Use the replace option in all scenarios. • **replace**: Requests SLAC if it is not already installed, or replaces an existing SLAC. When you enter this keyword, the product instance checks if these existing licenses are in-use. If they are, an error message is displayed, telling you to first disable the corresponding feature. A device requires only one SLAC. For *feature_name*, enter the name of the license for which you want to request an addition or a replacement of the SLAC. Specify the device by entering one of these options: • **all**: Gets the authorization code for *all* devices in a High Availability set-up • **local**: Gets the authorization code for the *active* device in a High Availability set-up. This is the default option. Alternatively, use one of the following methods to request and install a SLAC - note the supported platforms for each option: • Only on Cisco 1000, 4000 Series Integrated Services Routers, Catalyst 8200 Edge Platforms, and 8300 Edge Platforms: **license feature** *feature_name*: Enables the feature and automatically request the code. `Device(config)# license feature hseck9` • Only on Catalyst 8000V Edge Software, Cisco Cloud Services Router 1000v, Cisco Integrated Services Virtual Routers: **platform hardware throughput level MB** {**500** |**1000** | **2500** | **5000**}: Requests and installs the requisite SLAC. This is supported only with the throughput value keywords specified here (greater than 250 MB).

	Command or Action	Purpose
		`Device(config)# platform hardware throughput level MB 5000`
Step 3	**show license authorization** **Example:** `Device# show license authorization`	Displays the authorization code (SLAC) installed on the product instance.

Generating and Saving a SLAC Request on the Product Instance

To generate and then save a SLAC request for an HSECK9 key to a file on the product instance, complete the following task:

Note This method of requesting a SLAC is supported starting with Cisco IOS XE Cupertino 17.7.1a only.

Before you begin

Supported topologies: No Connectivity to CSSM and No CSLU

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted
Step 2	**license smart authorization request** {**add** | **replace**} *feature_name* {**all**| **local**} **Example:** `Device# license smart authorization request replace hseck9 local`	Generates a SLAC request with the required license and UDI details. Specify if you want to add to or replace an existing SLAC: • **add**: Adds the requested license to an existing SLAC. The new authorization code will contain all the licences of the existing SLAC, and the requested license. **Note** Do not use this option even though it is available on the CLI, for any of the supported product instances that are within the scope of this document. Use the replace option in all scenarios. • **replace**: Requests an authorization code (SLAC) if it is not already installed, or

	Command or Action	Purpose
		replaces an existing one. When you enter this keyword, the product instance checks if these existing licenses are in-use. If they are, an error message is displayed, telling you to first disable the corresponding feature. A device requires only one SLAC. For *feature_name*, enter the name of the license for which you want to request an addition or a replacement of the SLAC. Specify the device by entering one of these options: • **all**: Gets the SLAC for *all* devices in a High Availability set-up • **local**: Gets the SLAC for the *active* device in a High Availability set-up. This is the default option.
Step 3	**license smart authorization request save** *path* **Example:** `Device# license smart authorization request save bootflash:slac.txt`	Saves the required UDI and license details for the SLAC request in a .txt file, in the specified location.
Step 4	Upload the file to the CSSM Web UI, and then download the file containing the SLAC code.	Complete this task: Uploading Data or Requests to CSSM and Downloading a File, on page 214.
Step 5	Install the file on the product instance.	Complete this task: Installing a File on the Product Instance, on page 215.

Removing and Returning an Authorization Code

This task shows how you can remove an authorization code for a license and return it to your license pool in CSSM. The authorization code on the device can be any one of the following: a Smart Licensing Authorization Code (SLAC), a Specific License Reservation (SLR) authorization code, a Product Activation Key (PAK), a Permanent License Reservation (PLR) authorization code.

You may want to remove and return an authorization code on a product instance under these circumstances:

- You no longer want to use the cryptographic feature, which requires an HSECK9 license.
- You want to return a device for Return Material Authorization (RMA), or decommission it permanently. As part of the RMA or decommision process you must perform a factory reset. But before you perform a factory reset, remove the authorization code and return the license to your license pool in CSSM.

Note Not all authorization codes require you to perform the entire procedure. Further, on some product instances, you cannot remove and return the code yourself. Note the specific guidelines provided under "**Before you begin**" for each kind of authorization code and the differences in the prerequisites between product instances.

Before you begin

Supported topologies: all

- To return *a SLAC* for an HSECK9 license:
  - On Cisco 1000, 4000 Series Integrated Services Routers, first disable the HSECK9 license for which SLAC is installed. Next, save configuration changes and reload the device for the status of the HSECK9 license to be displayed as NOT IN USE.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# no license feature hseck9
% use 'write' command to disable 'hseck9' license on next boot
Device(config)# end
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Device# reload
Proceed with reload? [confirm]
.
.
.
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Jan 29 07:10:00 2023 UTC
  Virtual Account: Eg-VA
License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  hseck9                  (ISR_4331_Hsec)                   0 NOT IN USE
  booster_performance     (ISR_4331_BOOST)                  1 IN USE
  appxk9                  (ISR_4331_Application)            1 IN USE
  uck9                    (ISR_4331_UnifiedCommun...)       1 IN USE
  securityk9              (ISR_4331_Security)               1 IN USE
```

  After the above prerequsite is met, perform the remaining steps to remove and return the SLAC as show in the procedure below.

  - On Cisco Catalyst 8200 and 8300 Edge Platforms, first configure the throughput to lesser than 250 Mbps. This can be a tier-based value or a numeric value. Next, disable the HSECK9 license for which SLAC is installed. Lastly, save configuration changes and reload the device for the status of the HSECK9 license to be displayed as NOT IN USE.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# platform hardware throughput crypto ?
  100M  100 mbps bidirectional thput
  10M   10 mbps bidirectional thput
  15M   15 mbps bidirectional thput
  1G    2 gbps aggregate thput
  2.5G  5 gbps aggregate thput
  250M  250 mbps bidirectional thput
```

```
  25M   25 mbps bidirectional thput
  500M  1gbps aggregate thput
  50M   50 mbps bidirectional thput
  T0    T0(up to 15 mbps) bidirectional thput
  T1    T1(up to 100 mbps) bidirectional thput
  T2    T2(up to 2 gbps) aggregate thput
  T3    T3(up to 5 gbps) aggregate thput
Device(config)# platform hardware throughput crypto 10M

Device(config)# no license feature hseck9
% use 'write' command to disable 'hseck9' license on next boot
Device(config)# end
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
*Jan 31 05:13:22.556: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private
 config file
*Jan 31 05:13:22.563: %CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE: Setting crypto bidir
throughput to: 10000 kbps

Device# reload
Proceed with reload? [confirm]
.
.
.
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Jan 29 07:10:00 2023 UTC
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag     Count Status
  -----------------------------------------------------------
  network-advantage_10M   (ESR_P_10M_A)           1 IN USE
  dna-advantage_10M       (DNA_P_10M_A)           1 IN USE
  Router US Export Lic... (DNA_HSEC)              0 NOT IN USE
```

After the above prerequsite is met, perform the remaining steps to remove and return the SLAC as show in the procedure below.

- On Catalyst 8000V Edge Software, (including Cisco Cloud Services Router 1000v and Cisco Integrated Services Virtual Routers where the .bin image is upgraded to a Catalyst 8000V software image), first configure the throughput to lesser than 250 Mbps. This can be a tier-based value or a numeric value. You do not have to reload the device for the changes to take effect.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# platform hardware throughput level MB ?
  100    Mbps
  1000   Mbps
  10000  Mbps
  15     Mbps
  25     Mbps
  250    Mbps
  2500   Mbps
  50     Mbps
  500    Mbps
  5000   Mbps
  T0     Tier0(up to 15M throughput)
  T1     Tier1(up to 100M throughput)
  T2     Tier2(up to 1G throughput)
```

```
  T3      Tier3(up to 10G throughput)
  T4      Tier4(unthrottled)

Device(config)# platform hardware throughput level MB T1
The current throughput level is 100000 kb/s
Device(config)# end
```

After the above prerequsite is met, perform the remaining steps to remove and return the SLAC as show in the procedure below.

- On Catalyst 8500 Edge Platforms, you cannot disable the HSECK9 license yourself. To return a SLAC, you must open a case instead. Go to Support Case Manager. Click **Open New Case** and select **Software Licensing**. Select the applicable category and click **Open Case**. Ensure that you provide the Smart Account, Virtual Account, device UDI information in the case. The licensing team will contact you to start the process or for any additional information.

  The steps in the procedure below do not apply to this platform.

- To return *an SLR authorization code*, complete the procedure below. The steps are the same regardless of whether the SLR authorization code includes an HSECK9 license or not.
- To return *a PAK*, see: Removing a PAK License, on page 223.
- To return *a PLR authorization code*, see: Deactivating a PLR, on page 230.

Procedure

	Command or Action	Purpose

Step 1	**license smart authorization return** {**all** | **local**} {**offline** [*path*] | **online**}
	Example:
	`Device# license smart authorization return local online`
	
	`OR`
	
	`Device# license smart authorization return local offline`
	`Enter this return code in Cisco Smart Software Manager portal:`
	`UDI: PID:C8300-1N1S-4T2X,SN:FDO2349A00R`
	`Return code: CrMfaJ-9odPW7-gr2DzP-t3srpf-ATqzGS-wGF3c6-U3Kg77-GdiABx-gud`
	`*Jan 31 05:18:00.804: %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code has been removed from PID:C8300-1N1S-4T2X,SN:FDO2349A00R.`
	
	`OR`
	
	`Device# license smart authorization return local offline bootflash:return-code.txt`
		Returns an authorization code back to the license pool in CSSM. A return code is displayed after you enter this command.
		Specify the product instance:
		• **all**: Performs the action for all connected product instances in a High Availability set-up.
		• **local**: Performs the action for the active product instance. This is the default option.
		Specify if you are connected to CSSM or not:
		• If connected to CSSM, enter **online**. The code is automatically returned to CSSM and a confirmation is returned and installed on the product instance. If you choose this option, the return code is automatically submitted to CSSM.
		• If not connected to CSSM, enter **offline**.
		If you choose the offline option, you must complete the additional step of submitting this to CSSM.

	Command or Action	Purpose
		• Copy the return code from the CLI or from a saved file and enter it in CSSM: Entering a Return Code in CSSM and Removing the Product Instance, on page 210. For software versions prior to 17.7.1a, you can use only this procedure to return the code. • Specify a path to save the file and upload the file to CSSM. This procedure to return the code is available starting with 17.7.1a: Uploading Data or Requests to CSSM and Downloading a File, on page 214. The file format can be any readable format. For example: `Device# license smart authorization return local offline bootflash:return-code.txt`. **Note** In case of an SSM On-Prem Deployment, use only the **online** option; the **offline** option is not supported.

Step 2	**show license all**
	Example:
	`Device# show license all`
	`.`
	`.`
	`.`
	`License Authorizations`
	`==========`
	`Overall status:`
	`Active:`
	`PID:C8300-1N1S-4T2X,SN:FDO2349A00R`
	`Status: NOT INSTALLED`
	`Last return code:`
	`CrMfaJ-9odPW7-gr2DzP-t3srpf-ATqzGS-wGF3c6-U3Kg77-GdiABx-gud`
	`.`
	`.`
	`.`
		Displays licensing information. Check the `License Authorizations` header in the output. If the return process is completed correctly, the `Last return code:` field displays the return code.

Step 3	**show license summary**
	Example:
	`Device# show license summary`
	`Account Information:`
	`Smart Account: Eg-SA As of Jan 31 05:31:20 2023 UTC`
	`Virtual Account: Eg-VA`
		Displays all the licenses available on the product instance. In the accompanying example, the HSECK9 license is no longer displayed.

	Command or Action	Purpose
	License Usage: License Tag Count Status Entitlement network-advantage_10M (ESR_P_10M_A) 1 IN USE dna-advantage_10M (DNA_P_10M_A) 1 IN USE	

Returning SLAC for an HSECK9 License That Is In-Use

To return an HSECK9 license that is being used (license status is IN-USE), you have to initiate a forced return of the Smart Licensing Authorization Code (SLAC).

Note Returning an HSECK9 license, throttles throughput on the device to 250 Mbps.

Before you begin

Supported topologies: all

The forced return option for SLAC is available only on these devices: Catalyst 8000V Edge Software, Catalyst 8200 Series Edge Platforms, Catalyst 8300 Series Edge Platforms, and Cisco 1000 Series Integrated Services Routers.

This option is not available on Catalyst 8500 Series Edge Platforms. This option is also not available on devices that do not support the HSECK9 license.

Follow these steps to initiate a forced return:

Procedure

	Command or Action	Purpose

Step 1	**license smart authorization return force-reload**
	Example:
	`Device# license smart authorization return force-reload`
	`Attention!!! This command will forcibly remove HSECK9 authorization code. Device will reload automatically if you continue.`
	`Do you want to continue? [yes/no]:yes`
		Forces the the device to return the SLAC. A return code is displayed after you enter this command.
		Note
		On a Catalyst 8000V Edge device the keyword is **force**. This is because a reload is not required on virtual platforms.

Step 2	Check that the return process is completed	• If the device has connectivity to the internet and Cisco SSM:

	Command or Action	Purpose

		For virtual platforms, the return code is automatically updated in Cisco SSM, and the device does not reload.
		For physical platforms, after reload is complete and connectivity is restored, the return code is automatically updated in Cisco SSM.
		Verify the return by accessing the coressponding Smart Account and Virtual Account in Cisco SSM.
		• If the device is offline and has no connectivity to the internet, then you must manually copy and enter the return code in Cisco SSM, to complete the return process. See Entering a Return Code in CSSM and Removing the Product Instance, on page 210.
		You can find the code in the output of the **show license authorization** privileged EXEC command.
		`Device# show license authorization`
		`Overall status:`
		`Active:`
		`PID:C8300-1N1S-4T2X,SN:FDO2349A00R`
		`Status: NOT INSTALLED`
		`Last return code:`
		`CtMfaJ-9odRW7-gr2DzP-t3srpf-AKpqGS-wGF3c6-U3Kg77-GdiABx-gud`
		`<output truncated>`
		Once the SLAC return process is complete, the HSECK9 license is automatically returned to the license pool in Cisco SSM and throughput on the device is throttled to 250 Mbps.

Entering a Return Code in CSSM and Removing the Product Instance

If you return an authorization code by configuring configured **license smart authorization return** {**all** | **local**} **offline**, you must manully enter the return code in CSSM, to complete the return process.

You can use this procedure for all authorization codes (SLAC, SLR, PLR, etc.)

Before you begin

Supported topologies: No Connectivity to CSSM and No CSLU

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com, and click **Manage licenses**.

Log in using the username and password provided by Cisco. The **Smart Software Licensing** page is displayed.

Step 2 Click the **Inventory** tab.

Step 3 From the **Virtual Account** drop-down list, choose your virtual account.

Step 4 Click the **Product Instances** tab.

The list of product instances that are available is displayed.

Step 5 Locate the required product instance from the product instances list. Optionally, you can enter a name or product type string in the search tab to locate the product instance.

Step 6 In the **Actions** column of the product instance, from the Actions dropdown list, select **Remove**.

The **Remove Reservation** window is displayed.

Step 7 In the **Reservation Return Code** field, enter the return code.

The license is returned to the license pool. The Remove Reservation window is automatically closed and you return to the Product Instances tab.

Note
If you want to only return the license, your task ends here. If you also want to remove the product instance from CSSM, continue to the next step.

Step 8 In the **Actions** column of the product instance, from the Actions dropdown list, *again* select **Remove**.

The **Confirm Remove Product** Instance window is displayed.

Step 9 Click **Remove Product Instance**.

The product instance is removed from CSSM and no longer consumes any licenses.

Generating a New Token for a Trust Code from CSSM

To generate a token to request a trust code, complete the following steps.

Generate one token for each *Virtual Account* you have. You can use same token for all the product instances that are part of one Virtual Account.

Before you begin

Supported topologies: Connected Directly to CSSM

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com, and click **Manage licenses**.

Log in using the username and password provided by Cisco. The **Smart Software Licensing** page is displayed.

Step 2 Click the **Inventory** tab.

Step 3 From the **Virtual Account** drop-down list, choose the required virtual account

Step 4 Click the **General** tab.

Step 5 Click **New Token**. The **Create Registration Token** window is displayed.

Step 6 In the **Description** field, enter the token description

Step 7 In the **Expire After** field, enter the number of days the token must be active.

Step 8 (Optional) **In the Max. Number of Uses** field, enter the maximum number of uses allowed after which the token expires.

Note
If you enter a value here, ensure that you stagger the installation of the trust code during the next part of the process. If you want to simultaneously install the trust code on a large number of product instances, we recommend that you leave this field blank. Entering a limit here and simultaneously installing it on a large number of devices causes a bottleneck in the processing of these requests in CSSM and installation on some devices may fail, with the following error: `Failure Reason: Server error occurred: LS_LICENGINE_FAIL_TO_CONNECT`.

Step 9 Click **Create Token**.

Step 10 You will see your new token in the list. Click **Actions** and download the token as a `.txt` file.

Establishing Trust with an ID Token

To establish a trusted connection with CSSM, complete the following steps:

Before you begin

Supported topologies: Connected Directly to CSSM

Before you peform this task, ensure that you have generated and downloaded an ID token file from CSSM: Generating a New Token for a Trust Code from CSSM, on page 211.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted

	Command or Action	Purpose
Step 2	**license smart trust idtoken** *id_token_value* {**local** | **all**} [**force**] **Example:** `Device# license smart trust idtoken NGMwMjk5mYtNZaxMS00NzMZmtgWm all force`	Submits the trust request and establishes a trusted connection with CSSM. For *id_token_value*, enter the token you generated in CSSM. Enter one of following options: • **local**: Submits the trust request only for the active device in a High Availability set-up. This is the default option. • **all**: Submits the trust request for all devices in a High Availability set-up. Enter the **force** keyword to submit a trust code request despite an existing trust code on the product instance. Trust codes are node-locked to the UDI of the product instance. If a UDI already has a trust code (a trusted connection with CSSM), CSSM does not allow a new trust code for same UDI. Entering the **force** keyword sets a force flag in the message sent to CSSM to create a new trust code even if one already exists.

Step 3	**show license status**
	Example:
	`<output truncated>`
	`Trust Code Installed:`
	`  Active: PID:C9500-24Y4C,SN:CAT2344L4GH`
	`    INSTALLED on Sep 04 01:01:46 2020 EDT`
	`  Standby: PID:C9500-24Y4C,SN:CAT2344L4GJ`
	`    INSTALLED on Sep 04 01:01:46 2020 EDT`
		Displays date and time if trust code is installed. Date and time are in the local time zone. See field `Trust Code Installed:`.

Downloading a Policy File from CSSM

If you have requested a custom policy or if you want to apply a policy that is different from the default that is applied to the product instance, complete the following task:

Before you begin

Supported topologies:

- No Connectivity to CSSM and No CSLU
- CSLU Disconnected from CSSM

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com, and click **Manage licenses**.

Log in using the username and password provided by Cisco. The **Smart Software Licensing** page is displayed.

Step 2 Follow this directory path: **Reports** > **Reporting Policy**.

Step 3 Click **Download**, to save the `.xml` policy file.

You can now install the file on the product instance. See Installing a File on the Product Instance, on page 215

Uploading Data or Requests to CSSM and Downloading a File

You can use this task to:

- To upload a RUM report to CSSM and download an ACK.
- To upload a SLAC request file and download a SLAC code file.

  This method is supported starting with Cisco IOS XE Cupertino 17.7.1a
- To upload a SLAC return file.

  This method is supported starting with Cisco IOS XE Cupertino 17.7.1a

To upload a file to CSSM and download file when the product instance is not connected to CSSM or when CSLU or SSM On-Prem are not connect to CSSM, complete the following task:

Before you begin

Supported topologies:

- No Connectivity to CSSM and No CSLU
- CSLU Disconnected from CSSM
- SSM On-Prem Deployment (Product instance-initiated communication and SSM On-Prem-initiated communication)

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com, and click **Manage licenses**.

Log in using the username and password provided by Cisco. The **Smart Software Licensing** page is displayed.

Step 2 Select the **Smart Account** (upper left-hand corner of the screen) that will receive the report.

Step 3 Select **Smart Software Licensing** → **Reports** → **Usage Data Files**.

Step 4 Click **Upload Usage Data**. Browse to the file location (RUM report in tar format), select, and click **Upload Data**.

Upload a RUM report (`.tar` format), or a SLAC request file (`.txt` format), or a SLAC return request file (`.txt` format).

You cannot delete a file after it has been uploaded. You can however upload another file, if required.

Step 5 From the Select Virtual Accounts pop-up, select the **Virtual Account** that will receive the uploaded file. The file is uploaded to Cisco and is listed in the Usage Data Files table in the Reports screen showing the File Name, time is was Reported, which Virtual Account it was uploaded to, the Reporting Status, Number of Product Instances reported, and the Acknowledgement status.

Step 6 In the Acknowledgement column, click **Download** to save the ACK or SLAC file for the report or request you uploaded.

You may have to wait for the file to appear in the Acknowledgement column. If there many RUM reports or requests to process, CSSM may take a few minutes.

After you download the file, import and install the file on the product instance, or transfer it to CSLU or SSM On-Prem.

Installing a File on the Product Instance

To install a SLAC, or policy, or ACK on the product instance, complete the following task:

Before you begin

Supported topologies: No Connectivity to CSSM and No CSLU

You must have the corresponding file saved in a location that is accessible to the product instance.

- For a SLAC, see Generating and Downloading SLAC from CSSM to a File, on page 199 or Uploading Data or Requests to CSSM and Downloading a File, on page 214 (There are multiple ways to obtain a SLAC file in an air-gapped network).
- For a policy, see Downloading a Policy File from CSSM, on page 213.
- For an ACK, see Uploading Data or Requests to CSSM and Downloading a File, on page 214.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted

	Command or Action	Purpose
Step 2	**copy** *source* **bootflash:***file-name* **Example:** `Device# copy tftp://10.8.0.6/user01/example.txt bootflash:`	Copies the file from its source location or directory to the flash memory of the product instance. • *source*: This is the location of the source file or directory to be copied. The source can be either local or remote • **bootflash:**: This is the destination for boot flash memory.
Step 3	**license smart import bootflash:** *file-name* **Example:** `Device# license smart import bootflash:example.txt`	Imports and installs the file on the product instance. After installation, a system message displayed - this indicates the type of file you just installed. For a SLAC, the product instance ensures that this new file correctly accounts for all the licenses in-use. On successful installation, the new code replaces any existing code.
Step 4	**show license all** **Example:** `Device# show license all`	Displays license authorization, policy and reporting information for the product instance.

Setting the Transport Type, URL, and Reporting Interval

To configure the mode of transport for a product instance, complete the following task:

Before you begin

Supported topologies: all

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	

	Command or Action	Purpose
Step 3	**license smart transport** {**automatic** | **callhome** | **cslu** | **off** | **smart**} **Example:** `Device(config)# license smart transport cslu`	Selects the type of message transport the product instance will use. Choose from the following options: • **automatic**: Sets the transport mode to default, which is CSLU. • **callhome**: Enables Call Home as the transport mode. • **cslu**: This is the default transport mode. Enter this keyword if you are using CSLU *or* SSM On-Prem, with product instance-initiated communication. **Note** The same transport mode applies to both CSLU *and* SSM On-Prem, but the URLs are different. See **cslu***cslu_or_on-prem_url* in the next step. • **off**: Disables all communication from the product instance. • **smart**: Enables Smart transport. **Note** If you are changing the transport method from **callhome** to **smart** you do not have to disable the call-home profile "CiscoTAC-1" for Smart Licensing Using Policy to work as expected.
Step 4	**license smart url** {*url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *smart_url*} **Example:** `Device(config)# license smart url cslu http://192.168.0.1:8182/cslu/v1/pi`	Sets the URL that is used for the configured transport mode. Depending on the transort mode you've chosen in the previous step, configure the corresponding URL here: • *url*: If you have configured the transport mode as **callhome**, configure this option. Enter the CSSM URL exactly as follows: `https://tools.cisco.com/its/service/oddce/services/DDCEService` The **no license smart url** *url* command reverts to the default URL. • **cslu** *cslu_or_on-prem_url*: If you have configured the transport mode as **cslu**, configure this option, with the URL for CSLU or SSM On-Prem, as applicable: • If you are using CSLU, enter the URL as follows:

	Command or Action	Purpose

		`http://<cslu_ip_or_host>:8182/cslu/v1/pi`
		For `<cslu_ip_or_host>`, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.
		The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`
		• If you are using SSM On-Prem, enter the URL as follows:
		`http://<ip>/cslu/v1/pi/<tenant ID>`
		For <ip>, enter the hostname or the IP address of the server where you have installed SSM On-Prem. The <tenantID> must be the default local virtual account ID.
		Tip
		You can retrieve the entire URL from SSM On-Prem. See Retrieving the Transport URL (SSM On-Prem UI), on page 189
		The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`
		• **default**: Depends on the configured transport mode. Only the **smart** and **cslu** transport modes are supported with this option.
		If the transport mode is set to **cslu**, and you configure **license smart url default**, the CSLU URL is configured automatically (`https://cslu-local:8182/cslu/v1/pi`).
		If the transport mode is set to **smart**, and you configure **license smart url default**, the Smart URL is configured automatically (`https://smartreceiver.cisco.com/licservice/license`).

	Command or Action	Purpose
		• **smart** *smart_url*: If you have configured the transport type as **smart**, configure this option. Enter the URL exactly as follows: `https://smartreceiver.cisco.com/licservice/license` When you configure this option, the system automatically creates a duplicate of the URL in **license smart url** *url*. You can ignore the duplicate entry, no further action is required. The **no license smart url smart***smart_url* command reverts to the default URL. • **utility** *smart_url*: Although available on the CLI, this option is not supported.
Step 5	**license smart usage interval** *interval_in_days* **Example:** `Device(config)# license smart usage interval 40`	(Optional) Sets the reporting interval in days. By default the RUM report is sent every 30 days. The valid value range is 1 to 3650. If you are using the utility mode, we recommend a reporting interval of seven days or less. This ensures that the 30- day ACK requirement, which applies to a product instance in the utility mode, is met in timely manner. If you do not configure an interval, the reporting interval is determined entirely by the policy.

Enabling the Utility Mode

You must enable this mode on the product instance for all supported topologies - only if you have an MSLA.

Before you begin

Supported topologies:

- Connected Directly to CSSM
- Connected to CSSM Through CSLU, CSLU Disconnected from CSSM (Product Instance-Initiated and CSLU-Initiated Communication)
- SSM On-Prem Deployment (Product Instance-Initiated and SSM On-Prem-Initiated Communication)
- No Connectivity to CSSM and No CSLU

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	
Step 3	**license smart utility** **Example:** `Device (config)# license smart utility`	Enables the utility mode on the product instance to indicate that an MSLA will be used. Enabling it causes the following to occur: • The system checks the transport type and URL. The %SMART_LIC-4-UTILITY_TRANSPORT_NOT_CONFIG system message is displayed if this settings is not configured correctly. • RUM reports include a flag to indicate that the product instance is in the utility mode. When utility mode is first enabled, the RUM report has the utility flag set. If a subscription exists in the Smart Account and Virtual Account, the subscription IDs are returned in the RUM ACK. Subsequent RUM reports include the subscription IDs. The subscription IDs are also returned in every RUM ACK. The %SMART_LIC-4-UTILITY_SUBSCRIPTION_LICENSE message is displayed if the utility mode is enabled and a license without a subscription ID is being used on the product instance. • A policy that is specific to the utility mode is set on the product instance. The utility policy states that a RUM ACK must be installed every 30 days. The %SMART_LIC-4-UTILITY_NO_ACK system message is displayed if an ACK is past due.

	Command or Action	Purpose
		• An informational message, %SMART_LIC-3-UTILITY_STARTED is displayed; it indicates that the utility mode is enabled and a subscription ID is available.
Step 4	**exit** **Example:** `Device (config)# exit`	Exits the global configuration mode and returns to the privileged EXEC mode.
Step 5	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Continue Using a PAK License

If you have a PAK license and you want to continue using it on the product instance, complete the following steps:

Note This procedure is applicable to all licenses that are PAK-fufilled - including HSECK9.

Before you begin

Supported topologies: all

Procedure

Step 1 Upgrade the software version on the product instance to a release where the system takes a snapshot of the PAK license.

For the system to take snapshot of the PAK license, you must upgrade to one of the following releases:

- 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.
- Cisco IOS XE Cupertino 17.7.1 and later releases of the 17.7.x train, and all releases of subsequent trains, that is, Cisco IOS XE Cupertino 17.8.x, Cisco IOS XE Cupertino 17.9.x, and until Cisco IOS XE Dublin 17.10.x.

For upgrade information, see:

Product Series	Supports PAK ?	Link to Upgrade Information
Cisco 1000 Series Integrated Services Routers	Yes	How to Install and Upgrade the Software
Cisco 4000 Series Integrated Services Routers	Yes	How to Install and Upgrade the Software
Cisco ASR 1000 Series Aggregation Services Routers	Yes	Software Upgrade Processes Supported by Cisco ASR 1000 Series Routers
Cisco Cloud Services Router 1000v	Yes	Upgrading the Cisco IOS XE Software
Catalyst 8000V Edge Software	Yes - but, only in case of a .bin upgrade from a CSR1000v to Catalyst 8000V Edge Software	Upgrading the Cisco IOS XE Software

After upgrade, enter the **show platform software sl-infra pak-info** command in privileged EXEC mode to display and verify that a snapshot has been taken.

Step 2 Verify that DLC is completed.

The system triggers the DLC. After DLC, the PAK-fulfilled license is available in your Smart Account. On the product instance, enter the **show license all** command to verify that it continues to be *identified* as a PAK-fulfilled license. For example, an HSECK9 PAK that has been snapshotted, continues to be displayed with `Status:PAK`.

The DLC process is triggered automatically on the product instance when you upgrade to a release that supports Smart Licensing Using Policy. DLC data is collected one hour after the product instance is upgraded to a software version that supports Smart Licensing Using Policy.

The DLC process is completed after an ACK is installed on the product instance. (The ACK is available once usage synchronization is completed - this is the next step.)

```
Device# show platform software license dlc

<output truncated>

DLC Process Status: Completed

DLC Conversion Status: SUCCESS
```

Step 3 Synchronize license usage with CSSM.

Follow the method that applies to the topology you have implemented and ensure that a RUM report is sent to CSSM.

Results:

- A snaphot of the PAK license is available and continues to be honored even after the PAK-managing library is discontinued.

- The license count is deposited in the Smart Account and Virtual Account in CSSM.
- Usage of the license is reported to CSSM.

Removing a PAK License

If you have a PAK license on a product instance and you want to remove the license, complete the following steps:



Note This procedure is applicable to all licenses that are PAK-fufilled - including HSECK9.

After you have completed this task, multiple options are available with respect to what you can do with the device and the license that is returned to the license pool in CSSM. These are described in the "**Results**" section at the end of the task.

Before you begin

Supported topologies: all

Procedure

Step 1 Verify that DLC is completed.

The system triggers the DLC. After DLC, the PAK-fulfilled license is available in your Smart Account. On the product instance, enter the **show license all** command to verify that it continues to be *identified* as a PAK-fulfilled license. For example, an HSECK9 PAK, continues to be displayed with `Status:PAK`.

The DLC process is triggered automatically on the product instance when you upgrade to a release that supports Smart Licensing Using Policy. DLC data is collected one hour after the product instance is upgraded to a software version that supports Smart Licensing Using Policy.

The DLC process is completed after an ACK is installed on the product instance. (The ACK is available once usage synchronization is completed - this is the next step.)

```
Device# show platform software license dlc

<output truncated>

DLC Process Status: Completed

DLC Conversion Status: SUCCESS
```

Step 2 Perform factory reset

Depending on your product instance, refer to the corresponding link:

Product Series	Link to Factory Reset Information
Cisco 1000 Series Integrated Services Routers	Using the factory reset Commands
Cisco 4000 Series Integrated Services Routers	Factory Reset

Product Series	Link to Factory Reset Information
Cisco ASR 1000 Series Aggregation Services Routers	Factory Reset
Cisco Cloud Services Router 1000v	Performing a Factory Reset
Catalyst 8000V Edge Software	Performing a Factory Reset

Step 3 Reload the product instance if the PAK license included an HSECK9 license.

This step is not required if the PAK license did not include an HSECK9 license.

After you have performed factory reset in the previous step, this reload enables the device to come-up without the HSECK9 license.

Step 4 Synchronize license usage with CSSM

Follow the method that applies to the topology you have implemented and ensure that a RUM report is sent to CSSM. Sending the RUM report accomplishes the following:

- Notifies CSSM that no licenses are being consumed on the product instance.
- The PAK-fulfilled license is returned to the license pool in CSSM and is *available* as a Smart license. For example, if what you had was a "PAK-fulfilled securityk9" license, it is now available for use as a "securityk9" license.

Results:

You now have the following options:

- Use the PAK-fulfilled license, on *the same* product instance, as a regular Smart license.

  To use the license on the product instance, configure the license using the applicable commands. Reporting requirements for the license will be the same as any other license - as per the policy, or, if system messages indicate that it is.

- Use the PAK-fulfilled license, on *another* product instance, as a regular Smart license.

  To use the license on another product instance, configure the license using the applicable commands for that product instance. Reporting requirements for the license will be the same as any other license - as per the policy, or, if system messages indicate that it is.

- Continue using the product instance.
- Remove the product instance from CSSM if you want to decommission the product instance or perform a Return Material Authrization (RMA).

Removing a PAK License on a Failed Product Instance

This task shows you how to return a PAK license on a product instance, which is not working at all (you cannot access the console to configure any Cisco IOS commands).

To return a PAK license on a failed product instance, you must open a case. Go to Support Case Manager. Click **OPEN NEW CASE** > Select **Software Licensing**.

After you have opened a case, the support team will contact you to initiate the return process and remove the product instance from CSSM.

Activating a PLR

To activate PLR on a supporting product instance, complete the following steps:

Some of the steps in this procedure must be performed on the product instance and some of them, on the CSSM Web UI. Steps that must be performed on the CSSM Web UI are prefixed with "(CSSM)" to avoid confusion. All other steps must be performed on the product instance.

Before you begin

- Ensure that you have a user role with proper access rights to a Smart Account and the required Virtual Accounts in CSSM.
- Ensure that your Smart Account is enabled for PLR.

  To check if it is enabled, login to CSSM https://software.cisco.com, and click **Manage licenses**. Click the **Inventory** tab. Select your Virtual Account. Click the **Licenses** tab. If the **License Reservation** button is enabled, then your Smart account is enabled for PLR. If it is greyed-out or not available, open a case in Support Case Manager (SCM).
- Ensure that the software version running on the product instance is Cisco IOS XE Dublin 17.10.1a or later. Enter the **show version** command in privileged EXEC mode, to confirm.

Procedure

Step 1 **configure terminal**

Example:

```
Device#configure terminal
```

Enters the global configuration mode.

Step 2 **license smart reservation**

Example:

```
Device(config)# license smart reservation
```

Enables the reservation mode.

Step 3 **exit**

Example:

```
Device(config)# exit
```

Exits the global configuration mode and enters the privileged EXEC mode.

Step 4 **license smart reservation request local**

Example:

```
Device# license smart reservation request local
Enter this request code in the Cisco Smart Software Manager portal:
UDI: PID:C8000V,SN:96QKIABBZ1H
Request code: DB-ZC8000V:96QKIABBZ1H-AYk3ndtp6-F1
```

Generates a reservation request code on the product instance.

You have to paste this in the CSSM Web UI, in a later step. You can save it in a .txt or other accessible file.

Step 5 (CSSM) Go to https://software.cisco.com and click **Manage licenses**. Log in using the username and password provided by Cisco.

The **Smart Software Licensing** page is displayed.

Step 6 (CSSM) Click the **Inventory** tab. Select your Virtual Account. Click the **Licenses** tab, and then click the **License Reservation** button.

The system displays the **Smart License Reservation** dialog box.

Tip
If the Smart Account and Virtual Account are not enabled for PLR, then the **License Reservation** button is not enabled. If this is the case, you must open a support case in Support Case Manager (SCM), to get it enabled.

Step 7 (CSSM) For **Step 1: Enter Request Code**, enter the request code in the **Reservation Request Code** text box. Click **Next**.

Enter the reservation request code that you generated on the product instance in Step 3.

After you click **Next**, the system displays the **Step 2: Select Licenses** dialog box.

Step 8 (CSSM) For **Step 2: Select Licenses**, select **C8000v PLR**. Click **Next**.

After you click **Next**, the system displays a list of licenses for selection.

Step 9 (CSSM) Enter the **Quantity to Reserve** as `1` and leave the **Expires** column blank. Click **Next**.

After you click **Next**, the system displays the **Step 3: Review and Confirm** dialog box.

Step 10 (CSSM) In the **Step 3: Review and Confirm** dialog box, click the **Generate Authorization Code** button.

After you click the **Generate Authorization Code**button, the system displays the **Step 4: Authorization Code** dialog box.

Step 11 (CSSM) In the **Step 4: Authorization Code** dialog box, either click **Copy to Clipboard** or **Download as File**. Click **Close**.

Copies the PLR authorization code to clipboard or downloads it as a file.

If you download it to a file, you must transfer the saved file to a flash drive or network resource (for example, a TFTP server), because you must install it on the product instance in the next step.

Step 12 **license smart reservation install** *PLR-Code*

Example:

```
Device# license smart reservation install
DA3Ks9-WM4yzT-Y7UAbh-GGXUwr-qARDsq-sjJs9e-Z3Xqix-TKcsy9-z6
Reservation install successful
```

Installs Version 3 of the PLR code and displays a success message.

Tip

Version 3 of the PLR code always starts with the letter “D” and is 58 characters long.

Step 13 **show license reservation**

Example:

```
Device# show license reservation
License reservation: ENABLED
Overall status:
   Active: PID:C8000V,SN:96QKIABBZ1H
   Reservation status: UNIVERSAL INSTALLED on Oct 25 17:50:48 2022 UTC
```

Displays license reservation information.

When a PLR code is installed on the product instance, the reservation status in the output of this command displays `UNIVERSAL INSTALLED`.

Step 14 **configure terminal**

Example:

```
Device# configure terminal
```

Enters the global configuration mode.

Step 15 **platform hardware throughput level MB** {**100** | **1000** | **10000** | **15** | **25** | **50** | **250** | **2500** | **50** | **500** | **5000**}

Example:

```
Device(config)# platform hardware throughput level MB 1000
```

Configures the throughput level.

At a minimum, you must have configured a network-stack license already. Otherwise the command is not recognized as a valid one on the command line interface.

Note
If you configure a throughput that is greater than 250 Mbps, you do not have to install SLAC. The PLR code authorizes a throughput of greater than 250 Mbps.

Step 16 **exit**

Example:

```
Device(config)# exit
```

Exits the global configuration mode and enters the privileged EXEC mode.

Step 17 **show platform hardware throughput level MB**

Example:

```
Device# show platform hardware throughput level MB
The current throughput level is 2000000 kb/s
```

Displays the currently running throughput on the device.

Upgrading a PLR

To upgrade the PLR version code to continue using PLR in the Smart Licensing Using Policy environement, complete the following steps:

Some of the steps in this procedure must be performed on the product instance and some of them, on the CSSM Web UI. Steps that must be performed on the CSSM Web UI are prefixed with "(CSSM)" to avoid confusion. All other steps must be performed on the product instance.

Before you begin

- Supported topologies: Not applicable
- The following settings are assumed because you have an existing, older version of the PLR code:
  - You have a user role with proper access rights to a Smart Account and the required Virtual Accounts in CSSM.
  - Your Smart Account is enabled for PLR.
- Ensure that you have performed a .bin upgrade of the software version on the product instance to Cisco IOS XE Dublin 17.10.1a or later. Enter the **show version** command in privileged EXEC mode, to confirm.



Note If the throughput level on the product instance was greater than 250 Mbps before upgrade, then on upgrade, it is set *to* 250 Mbps. A system message as shown below is also displayed, but you can ignore it. The procedure below shows you how to upgrade the PLR code to Version 3, which automatically restores throughput.

```
%SMART_LIC-6-RESERVE_AUTH_FAILED: Failed to validate the Universal
 Reservation
Authorization Code for udi PID:CSR1000V,SN:9QLBLATKXM4. Changing to
 the unregistered state.
```

Procedure

Step 1 (CSSM) Go to https://software.cisco.com and click **Manage licenses**. Log in using the username and password provided by Cisco.

Logs in to the CSSM Web UI.

Step 2 (CSSM) Click the **Inventory** tab. Select your Virtual Account. Click the **Product Instances** tab.

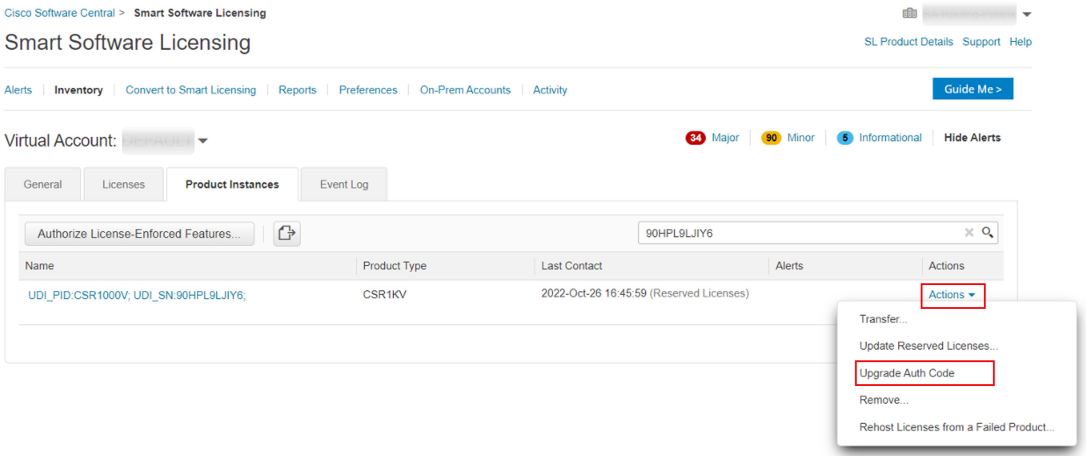
A list of product instances is displayed.

Step 3 (CSSM) Locate the product instance for which you are upgrading the PLR code and click on the corresponding **Actions** dropdown.

A list of available actions is displayed.

Step 4 (CSSM) Select **Upgrade Auth Code**.

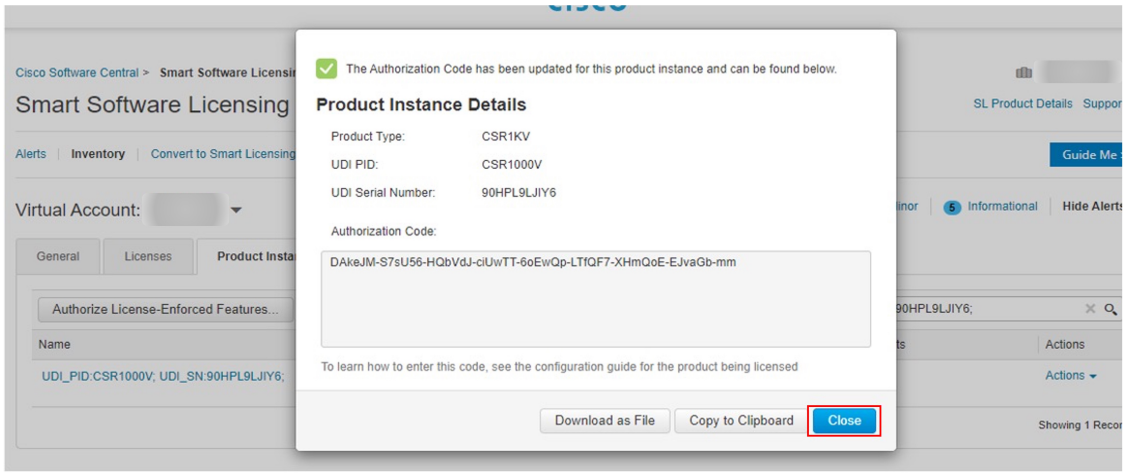
Example:



The **Product Instance Details** pop-up window is displayed.

Step 5 (CSSM) either click **Copy to Clipboard** or **Download as File**. Click **Close**.

Example:



Copies the PLR authorization code to clipboard or downloads it as a file.

If you download it to a file, you must transfer the saved file to a flash drive or network resource (for example, a TFTP server), because you must install it on the product instance in the next step.

Step 6 **license smart reservation install** *PLR-Code*

Example:

```
Device# license smart reservation
DA3Ks9-WM4yzT-Y7UAbh-GGXUwr-qARDsq-sjJs9e-Z3Xqix-TKcsy9-z6

Reservation install successful
```

Installs Version 3 of the PLR code and displays a success message. Any existing older PLR code version is deleted during the process.

If the throughput level on the product instance was greater than 250 Mbps before software version upgrade, the throughput level is now restored.

Tip
Version 3 of the PLR code always starts with the letter “D” and is 58 characters long.

Step 7 **show platform hardware throughput level MB**

Example:

```
Device# show platform hardware throughput level MB
The current throughput level is 2000000 kb/s
```

Displays the currently running throughput on the device.

Step 8 **show license reservation**

Example:

```
Device# show license reservation
License reservation: ENABLED
Overall status:
      Active: PID:CSR1000V,SN:9QLBLATKXM4
      Status: UNIVERSAL INSTALLED on Oct 25 20:54:08 2022 UTC
```

Displays license reservation information.

When a PLR code is installed on the product instance, the reservation status in the output of this command displays `UNIVERSAL INSTALLED`.

Deactivating a PLR

To deactivate PLR on a supporting product instance, complete the following steps:

Some of the steps in this procedure must be performed on the product instance and some of them, on the CSSM Web UI. Steps that must be performed on the CSSM Web UI are prefixed with "(CSSM)" to avoid confusion. All other steps must be performed on the product instance.

Before you begin

Supported topologies: Not applicable

Procedure

Step 1 **license smart reservation return local**

Example:

```
Device# license smart reservation return local
This command will remove the license authorization code.
Some features may not function properly.

Do you want to continue? [yes/no]:
Enter this return code in Cisco Smart Software Manager portal:
```

```
UDI: PID:CSR1000V,SN:9QLBLATKXM4
    Return code: CNcjZD-aGrAPP-SpCkkD-nZtES8-46zCDq-jZP
```

Generates a reservation return request code on the product instance.

You have to paste this in the CSSM Web UI, in a later step. You can save it in a .txt or other accessible file.

Step 2 (CSSM) Go to https://software.cisco.com and click **Manage licenses**. Log in using the username and password provided by Cisco.

Logs in to the CSSM Web UI.

Step 3 (CSSM) Click the **Inventory** tab. Select your Virtual Account. Click the **Product Instances** tab.

A list of product instances is displayed.

Step 4 (CSSM) Locate the product instance for which you are upgrading the PLR code and click on the corresponding **Actions** dropdown.

Step 5 (CSSM) Select **Remove Product Instance**. Paste the return code you generated in Step 1 in the text box. Click **Remove**.

If greater than 250 Mbps throughput was running with PLR, then throughput is set to 250 Mbps. It throughput was less than or equal to 250 Mbps, it remains unchanged.

Step 6 **configure terminal**

Example:

```
Device# configure terminal
```

Enters the global configuration mode.

Step 7 **no license smart reservation**

Example:

```
Device (config)# no license smart reservation
```

Disables the reservation mode.

Step 8 **exit**

Example:

```
Device (config)# exit
```

Exits the global configuration mode and enters the privileged EXEC mode.

HSECK9 License Mapping Table for Routing Product Instances

When you generate a SLAC in CSSM (Generating and Downloading SLAC from CSSM to a File, on page 199), you must select the correct license name for the PID. This table is provides a ready reference of the PID ↔ license name mapping for Cisco Aggregation, Integrated, and Cloud Service Routers.

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
ISR1K -8P	C1111-8P	ISR_1100_8P_Hsec	Use **ISR_1100_8P_Hsec**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, If the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses, on page 153
	C1111-8PLTEEA		
	C1111-8PLTELA		
	C1111-8PWE		
	C1111-8PWB		
	C1111-8PWA		
	C1111-8PWZ		
	C1111-8PWN		
	C1111-8PWQ		
	C1111-8PWC		
	C1111-8PWR		
	C1111-8PWK		
	C1111-8PWS		
	C1111-8PLTEEAWE		
	C1111-8PLTEEAWB		
	C1111-8PLTEEAWA		
	C1111-8PLTEEAWR		
	C1111-8PLTELAWZ		
	C1111-8PLTELAWN		
	C1111-8PLTELAWQ		
	C1111-8PLTELAWC		
	C1111-8PLTELAWK		
	C1111-8PLTELAWD		
	C1111-8PLTELAWA		
	C1111-8PLTELAWE		
	C1111-8PLTELAWS		
	C1116-8P		
	C1116-8PLTEEA		
	C1117-8P		
	C1117-8PM		

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
	C1117-8PLTEEA		
	C1117-8PLTELA		
	C1117-8PMLTEEA		
	C1117-8PWE		
	C1117-8PWA		
	C1117-8PWZ		
	C1117-8PMWE		
	C1117-8PLTEEAWE		
	C1117-8PLTELAWE		
	C1117-8PLTELAWZ		
	C1111X-8P		
	C1112-8P		
	C1112-8PLTEEA		
	C1113-8P		
	C1113-8PM		
	C1113-8PLTEEA		
	C1113-8PLTELA		
	C1113-8PMLTEEA		
	C1113-8PWE		
	C1113-8PWA		
	C1113-8PWZ		
	C1113-8PMWE		
	C1113-8PLTEEAWE		
	C1113-8PLTELAWE		
	C1113-8PLTELAWZ		
	C1114-8P		
	C1114-8PLTEEA		
	C1115-8P		
	C1115-8PLTEEA		
	C1115-8PM		

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
	C1115-8PMLTEEA		
	C1118-8P		
	C1121-8PLTEPWE		
	C1121-8PLTEPWB		
	C1121-8PLTEPWZ		
	C1121-8PLTEPWQ		
	C1121-8PLTEP		
	C1121X-8PLTEP		
	C1121-8P		
	C1121X-8P		
	C1161-8P		
	C1161X-8P		
	C1161-8PLTEP		
	C1161X-8PLTEP		
	C1126-8PLTEP		
	C1127-8PLTEP		
	C1127-8PMLTEP		
	C1126X-8PLTEP		
	C1127X-8PLTEP		
	C1127X-8PMLTEP		
	C1128-8PLTEP		
	C1121X-8PLTEPWE		
	C1121X-8PLTEPWB		
	C1121X-8PLTEPWZ		
	C1121X-8PLTEPWA		

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
ISR1K - 4P	C1111-4P	ISR_1100_4P_Hsec	Use **ISR_1100_4P_Hsec**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, if the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses, on page 153
	C1111-4PLTEEA		
	C1111-4PLTELA		
	C1111-4PWE		
	C1111-4PWB		
	C1111-4PWA		
	C1111-4PWZ		
	C1111-4PWN		
	C1111-4PWQ		
	C1111-4PWC		
	C1111-4PWR		
	C1111-4PWK		
	C1111-4PWD		
	C1111X-4P		
	C1116-4P		
	C1116-4PLTEEA		
	C1116-4PLTEEAWE		
	C1116-4PWE		
	C1117-4P		
	C1117-4PLTEEA		
	C1117-4PLTELA		
	C1117-4PLTEEAWE		
	C1117-4PLTEEAWA		
	C1117-4PLTELAWZ		
	C1117-4PWE		
	C1117-4PWA		
	C1117-4PWZ		
	C1117-4PM		
	C1117-4PMLTEEA		
	C1117-4PMLTEEAWE		

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
	C1117-4PMWE		
	C1101-4P		
	C1101-4PLTEP C1101-4PLTEPWE		
	C1101-4PLTEPWB		
	C1101-4PLTEPWD		
	C1101-4PLTEPWZ		
	C1101-4PLTEPWA		
	C1101-4PLTEPWH		
	C1101-4PLTEPWQ		
	C1101-4PLTEPWR		
	C1101-4PLTEPWN		
	C1101-4PLTEPWF		
	C1109-4PLTE2P		
	C1109-4PLTE2PWB		
	C1109-4PLTE2PWD		
	C1109-4PLTE2PWE		
	C1109-4PLTE2PWZ		
	C1109-4PLTE2PWA		
	C1109-4PLTE2PWH		
	C1109-4PLTE2PWQ		
	C1109-4PLTE2PWR		
	C1109-4PLTE2PWN		
	C1109-4PLTE2PWF		
	C1118-4P		
	C1121-4P		
	C1121-4PLTEP		

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
ISR1K-2P	C1109-2PLTEGB	ISR_1100_2P_Hsec	Use **ISR_1100_2P_Hsec**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, if the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses, on page 153
	C1109-2PLTEUS		
	C1109-2PLTEVZ		
	C1109-2PLTEJN		
	C1109-2PLTEAU		
	C1109-2PLTEIN		
ISR4200	ISR4221/K9	ISR4220_HSEC	Use **ISR4220_HSEC**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, if the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses, on page 153
	ISR4221X/K9		

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
ISR4300	ISR4321/K9	ISR_4321_Hsec	Use **ISR_4321_Hsec**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, if the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses, on page 153
	ISR4331/K9	ISR_4331_Hsec	Use **ISR_4331_Hsec**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, if the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses, on page 153
	ISR4351/K9	ISR_4531_Hsec	Use **ISR_4531_Hsec**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, if the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses, on page 153

Product Family	PID	License Name to Use for Cisco IOS XE Bengaluru 17.5.x and Earlier Releases	License Name to Use for Cisco IOS XE Bengaluru 17.6.1 and Later Releases
ISR4400	ISR4431/K9	ISR_4400_Hsec	Use **ISR_4400_Hsec**, if using the offline mode or downgrading to an earlier software release for installation and then reverting to 17.6.1 or later. Use **Router US Export Lic for DNA**, if the device-specific HSECK9 license is converted. For more information, see Phasing Out of Device-Specific HSECK9 Licenses, on page 153
	ISR4451/K9		
	ISR4451-X/K9		
	ISR4461/K9		
C8300	C8300-1N1S-4T2X	Router US Export Lic for DNA	Router US Export Lic for DNA (No change)
	C8300-1N1S-6T		
	C8300-2N2S-4T2X		
	C8300-2N2S-6T		
	C8300-1N1S-4G2X		
	C8300-1N1S-6G		
	C8300-2N2S-4G2X		
	C8300-2N2S-6G		
C8200	C8200-1N-4T		
	C8200-1N-1G		
ISR1100	ISR1100-6G		
	ISR1100X-6G		
C8500	C8500-12X4QC		
	C8500-12X		
	C8500L-8S4X		
C8000V	C8000V		
CSR1000V	CSR1000V		
ISRV	ISRV		

Converting a Device-Specific HSECK9 License

This task shows you how to convert *unused* device-specific HSECK9 licenses like *ISR_1100_8P_Hsec* or *ISR_4321_Hsec* to *Router US Export Lic for DNA* (DNA_HSEC) license. For the complete list of device-specific

HSECK9 licenses that you can convert, see: HSECK9 License Mapping Table for Routing Product Instances, on page 231.

To perform this task you will require a device from which you can access the internet.

Before you begin

Depending on the number of device-specific HSECK9 licenses you want to convert, order the corresponding number of spare upgrade-license PIDs on Cisco commerce workspace (CCW). Use part number DNA-HSEC-UPGD=. The unit list price for this PID is USD 0.00.

Note Ensure that the correct Smart Account and Virtual Account is mentioned in the order. The account must be the same as the Virtual Account where the device-specific HSECK9 license (which you are going to convert) is deposited.

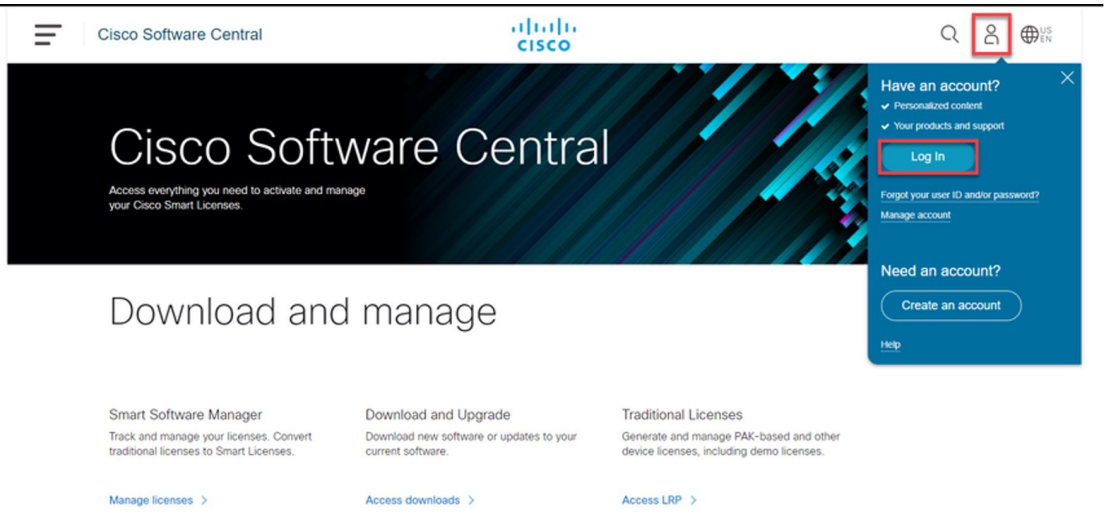
Procedure

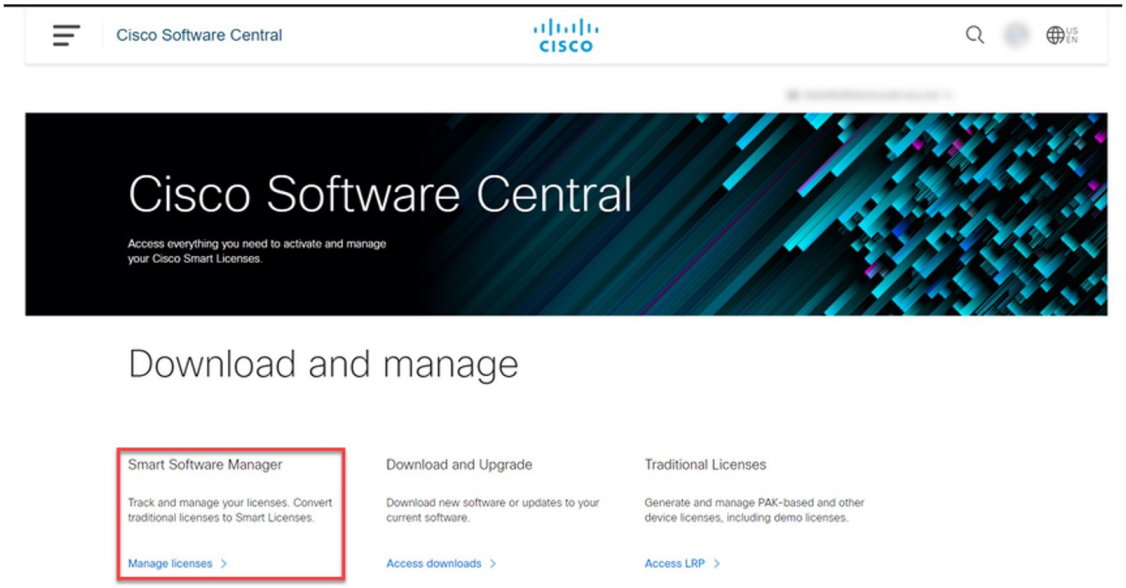
Step 1 Go to https://software.cisco.com and click **Manage licenses**.

Log in by the using username and password provided by Cisco.

The **Smart Software Licensing** page is displayed.

Example:



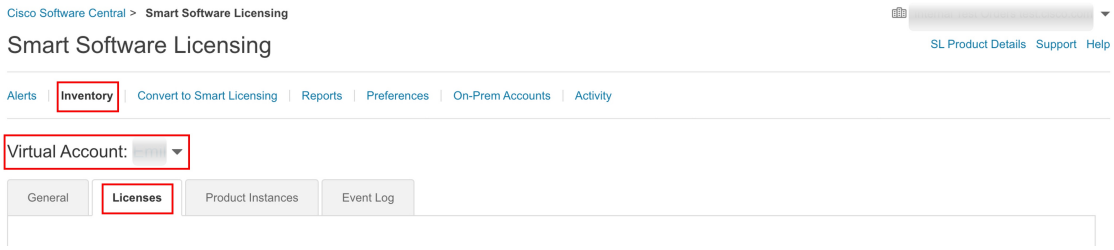


Step 2 Click the **Inventory** tab.

Step 3 From the **Virtual Account** drop-down list, choose the applicable Virtual Account.

Step 4 Click the **Licenses** tab.

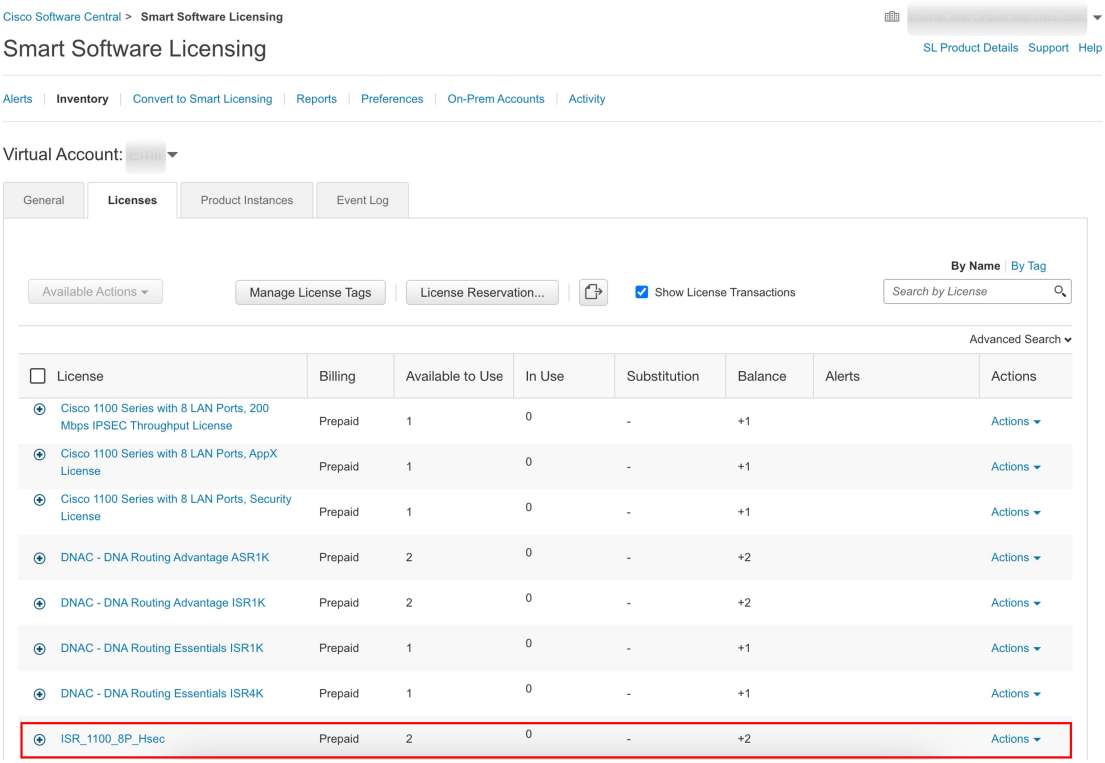
Example:



Step 5 Ensure that the device-specific HSECK9 license and the *Router US Export Lic for DNA* licenses are in this same Virtual Account.

Use the search bar and locate the device-specific HSECK9 license. In the accompanying sample screenshot this is the “ISR_1100_8P_Hsec” HSECK9 license and there are two of them.

Example:

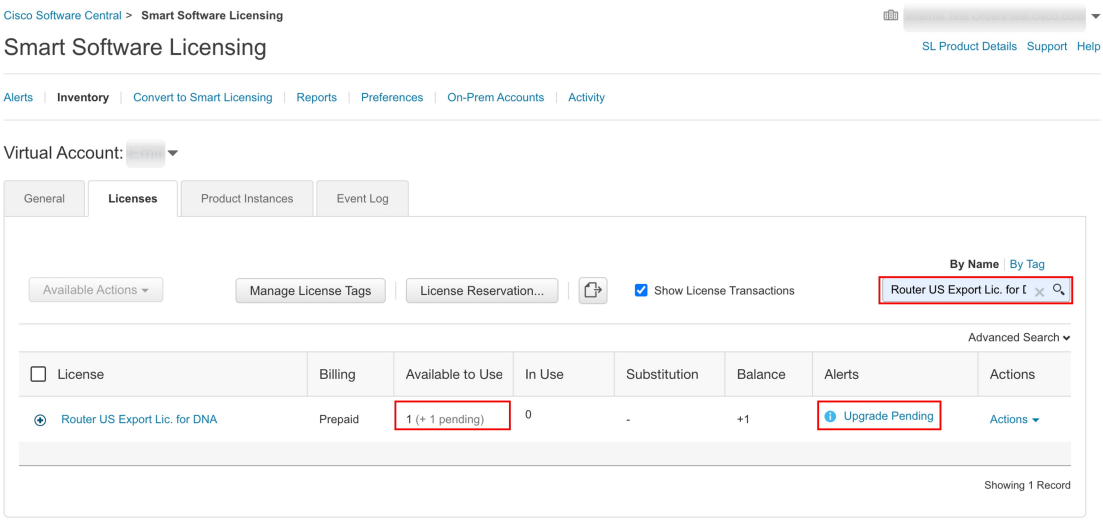


Again use the search bar and locate *Router US Export Lic for DNA*. In the **Alerts** column for this license check that "Upgrade Pending" is displayed. This confirms that you have the correct spare upgrade-license PID. Further, the **Available to Use** column displays the number of PIDs that are pending upgrade, within parentheses. In the accompanying sample screenshot there is one license pending.

step

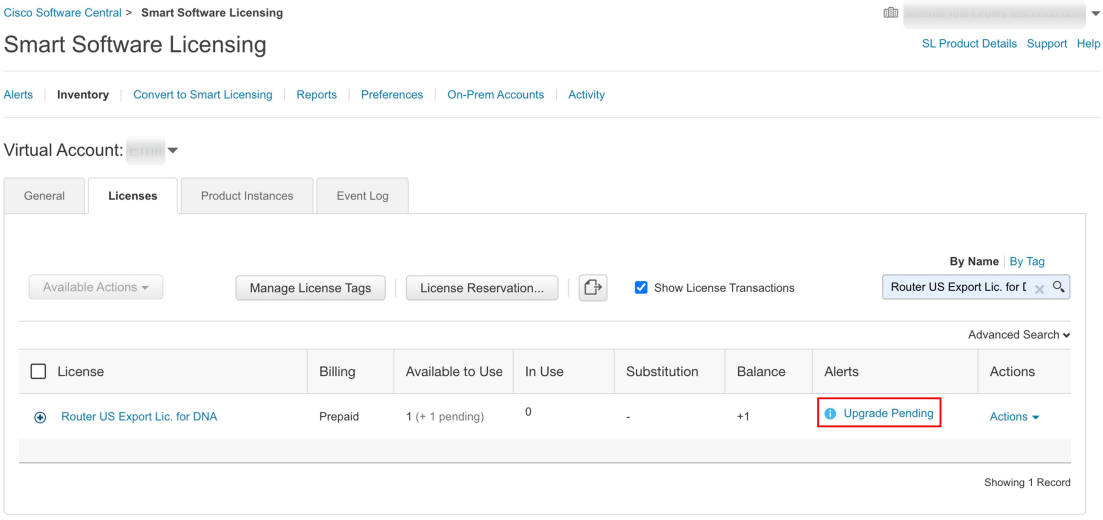
Note
Although there are two device-specific HSECK9 licenses in the sample screenshot, only one of them is converted in this example, because only one upgrade-license PID is available. Also note that if there are different device-specific HSECK9 licenses in your virtual account (for example, ISR_1100_8P_Hsec *and* ISR4220_HSEC) you can choose the one you want to convert to DNA_HSEC.

Example:



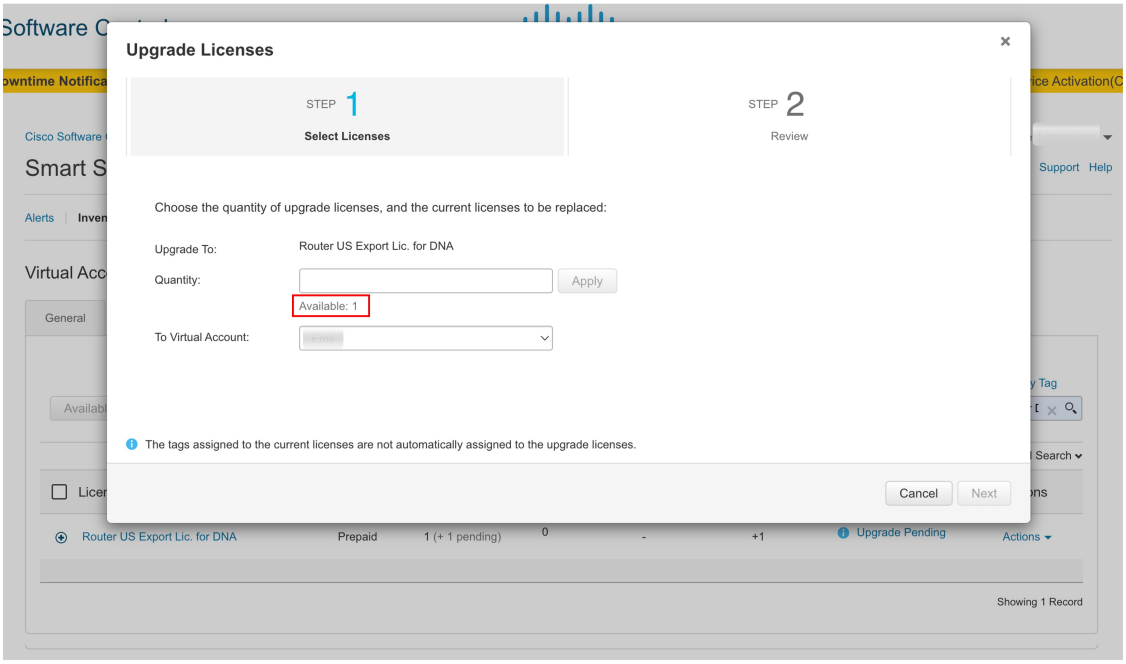
Step 6 Click **Upgrade Pending**.

Example:



The **Upgrade Licences** pop-up window is displayed. Below the *Quantity* field, the number of available upgrade licenses is displayed.

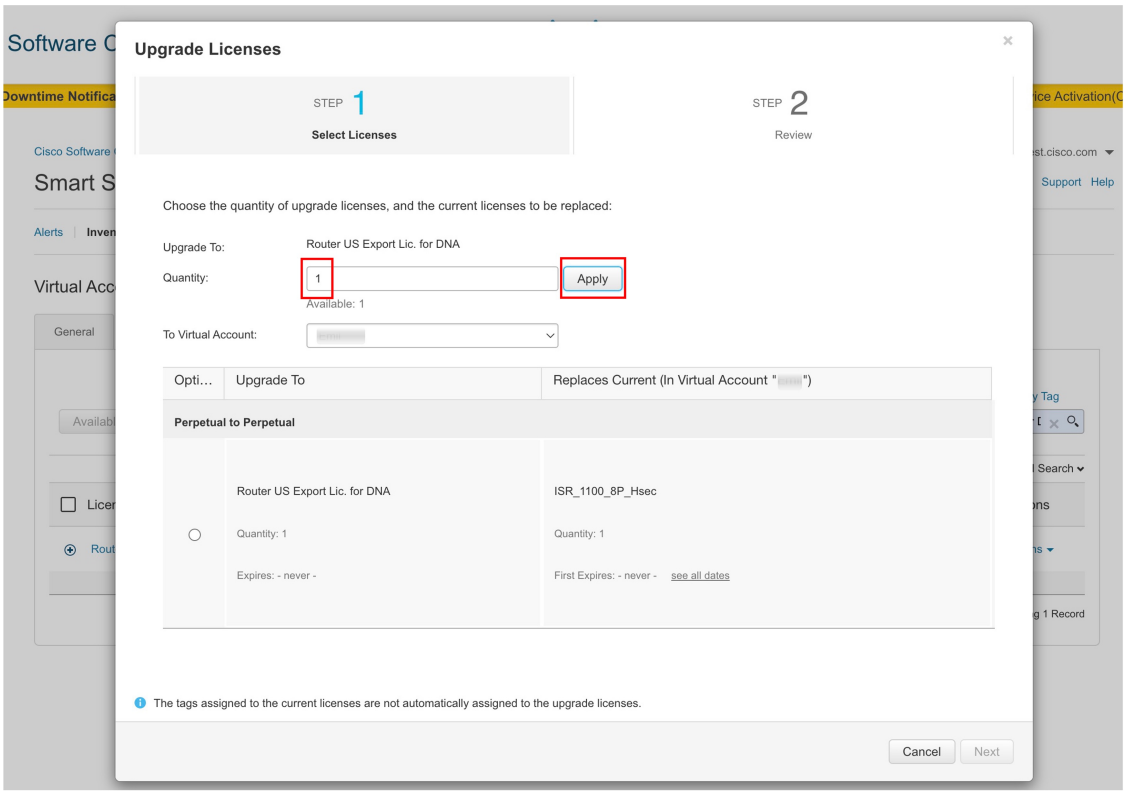
Example:



Step 7 In the **Quantity** field, enter the number of upgrade licenses that you want to convert and then click **Apply**.

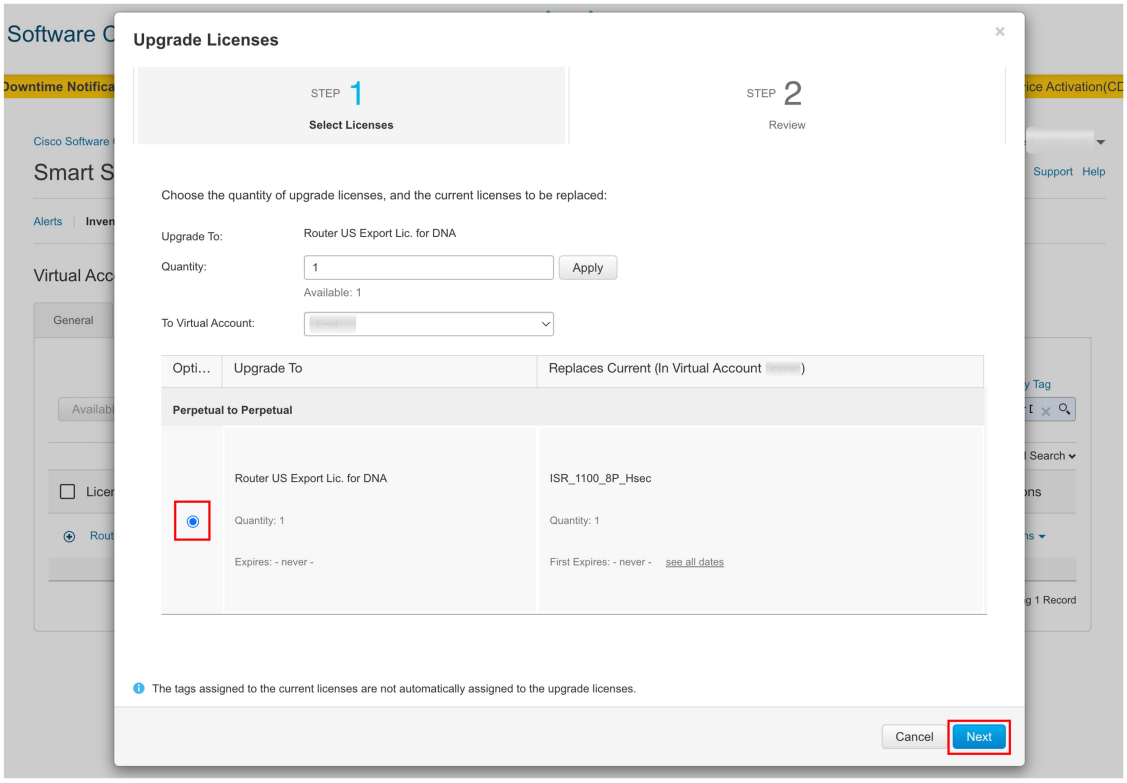
The quantity of *Router US Export Lic for DNA* licenses and number of device-specific HSECK9 licenses that will be replaced are displayed in a table in the same window.

Example:



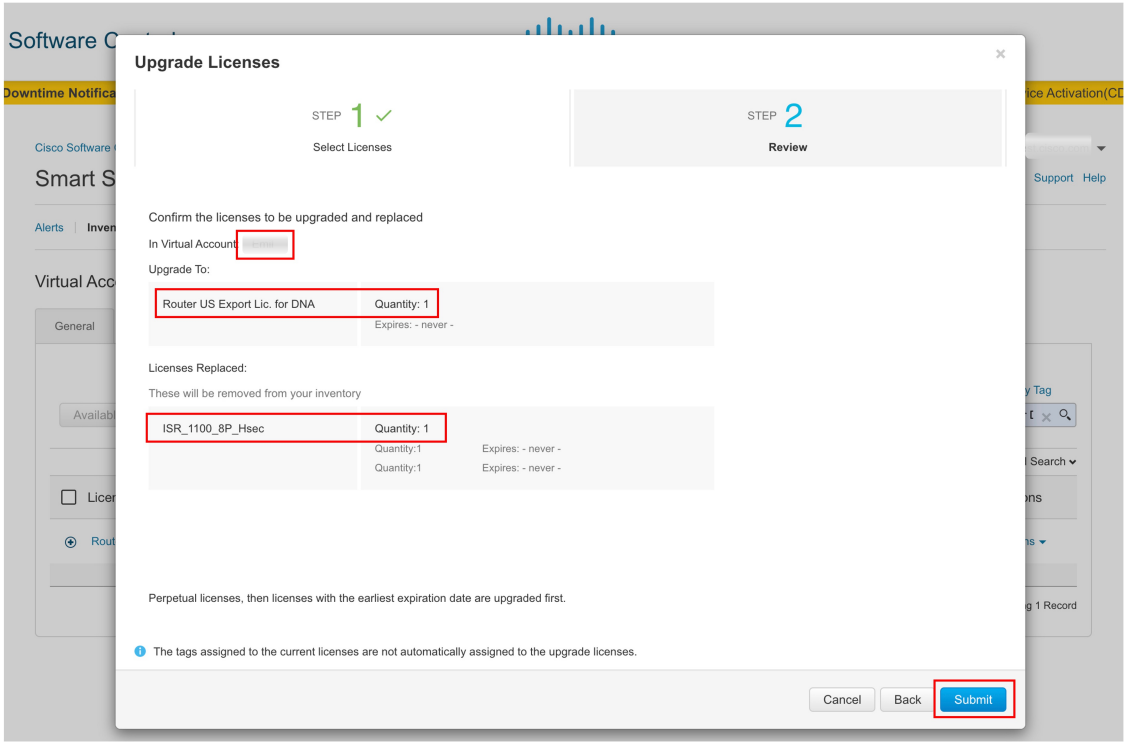
Step 8 Select the radio button and click **Next**.

Example:



Step 9 Review all the information and click **Submit**.

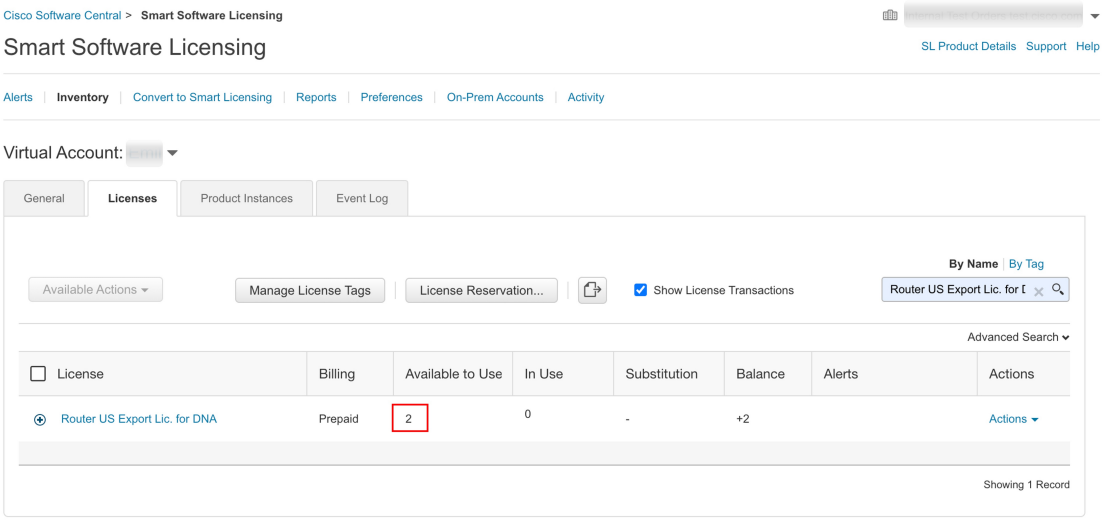
Example:



Step 10 In the **Licenses** tab, again use the search bar and locate *Router US Export Lic for DNA*. Check the **Available to Use** column for an updated count.

In the accompanying sample screenshot the number of *Router US Export Lic for DNA* licenses has increased from one to two.

Example:



What to do next

To use the *Router US Export Lic for DNA* HSECK9 license, install SLAC (on the device) according to the topology you have implemented.

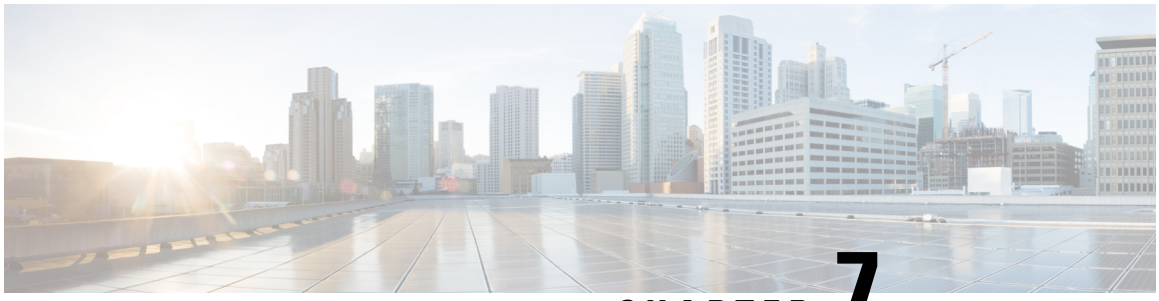
Sample Resource Utilization Measurement Report

The following is a sample Resource Utilization Measurement (RUM) report, in XML format (See RUM Report and Report Acknowledgement). Several such reports may be concatenated to form one report.

```
<?xml version="1.0" encoding="UTF-8"?>
  <smartLicense>
```

[redacted]

```
  </smartLicense>
```



CHAPTER 7

Command Reference for Smart Licensing Using Policy

This section provides complete command syntax information for Smart Licensing commands.

- license smart (global config), on page 249
- license smart (privileged EXEC), on page 264
- show license all, on page 272
- show license authorization, on page 278
- show license data, on page 286
- show license eventlog, on page 287
- show license history message, on page 290
- show license reservation, on page 290
- show license rum, on page 291
- show license status, on page 298
- show license summary, on page 307
- show license tech, on page 309
- show license udi, on page 320
- show license usage, on page 321
- show platform software sl-infra, on page 324

license smart (global config)

To configure licensing-related settings such as the mode of transport and URL that the product instance uses to communicate with Cisco Smart Software Manager (CSSM), or Cisco Smart Licensing Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), the usage reporting interval, the information that must be exluded or included in a license usage report (RUM report), a VRF to send licensing data, enter the **license smart** command in global configuration mode. Use the **no** form of the command to revert to default values.

license smart { **custom_id** *ID* | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** { **automatic** | **callhome** | **cslu** | **off** | **smart** } | **url** { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **id** *id* | **name** *name* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] | **vrf** *vrf_string* }

no license smart { **custom_id** | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** | **url** { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **id** *id* | **name** *name* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] | **vrf** *vrf_string* }

Syntax Description

custom_id *ID*	Although visible on the CLI, this option is not supported.
enable	Although visible on the CLI, configuring this keyword has no effect. Smart Licensing is always enabled.
privacy { **all**	**hostname**	**version** }	Sets a privacy flag to prevent the sending of the specified data privacy related information. When the flag is disabled, the corresponding information is sent in a message or offline file created by the product instance. Depending on the topology this is sent to one or more components, including CSSM, CSLU, and SSM On-Prem. *All data privacy settings are disabled by default*. You must configure the option you want to exclude from all communication: • **all**: All data privacy related information is excluded from any communication. The **no** form of the command causes all data privacy related information to be sent in a message or offline file. **Note** The Product ID (PID) and serial number are *included in the RUM report* regardless of whether data privacy is enabled or not. • **hostname**: Excludes hostname information from any communication. When hostname privacy is enabled, the *UDI* of the product instance is displayed on the applicable user interfaces (CSSM, CSLU, and SSM On-Prem). The **no** form of the command causes hostname information to be sent in a message or offline file. The hostname is displayed on the applicable user interfaces (CSSM, CSLU, and SSM On-Prem). • **version**: Excludes the Cisco IOS-XE software version running on the product instance and the Smart Agent version from any communication. The **no** form of the command causes version information to be sent in a message or offline file.

proxy { **address** *address_hostname* | **port** *port* }	Configures a proxy for license usage synchronization with CSLU or CSSM. This means that you can use this option to configure a proxy only if the transport mode is **license smart transport smart** (CSSM), or **license smart transport cslu** (CSLU). However, you cannot configure a proxy for license usage synchronization in an SSM On-Prem deployment, which also uses **license smart transport cslu** as the transport mode. When a proxy is configured, messages are sent to the proxy along with the final destination URL (CSSM). The proxy sends the message on to CSSM. Configure the following options: • **address** *address_hostname*: Configures the proxy address. For *address_hostname*, enter the enter the IP address or hostname of the proxy. • **port** *port*: Configures the proxy port. For *port*, enter the proxy port number.
reservation	Enables the reservation mode for Permanent License Reservation (PLR) in the Smart Licensing Using Policy environment. In the Smart Licensing Using Policy environment, PLR is supported starting from Cisco IOS XE Dublin 17.10.1 only. The product instances that support PLR are only Catalyst 8000V Edge Software and Cloud Services Router 1000v on which a .bin upgrade to Catalyst 8000V Edge Software is performed. The **no** form of the command disables reservation. You must enable the reservation mode using this keyword before you can access the privileged EXEC commands used to cancel, install, request, and return a PLR code.
server-identity-check	Enables or disables the HTTP secure server identity check.

transport { **automatic** | **callhome** | **cslu** | **off** | **smart** }	Configures the mode of transport the product instance uses to communicate with CSSM. Choose from the following options: • **automatic**: Sets the transport mode **cslu**. • **callhome**: Enables Call Home as the transport mode. • **cslu**: Enables CSLU as the transport mode. This is the default transport mode. **Note** The same transport mode applies to both CSLU *and* SSM On-Prem, but the URLs are different. See **cslu***cslu_or_on-prem_url* in the following row. • **off**: Disables all communication from the product instance. • **smart**: Enables Smart transport.

url { *url* | **cslu** *cslu_or_on-prem_url* | **default**
| **smart** *smart_url* | **utility** *secondary_url* }

Sets URL that is used for the configured transport mode. Choose from the following options:

- *url*: If you have configured the transport mode as **callhome**, configure this option. Enter the CSSM URL exactly as follows:

  `https://tools.cisco.com/its/service/oddce/services/DDCEService`

  The **no license smart url** *url* command reverts to the default URL.

- **cslu** *cslu_or_on-prem_url*: If you have configured the transport mode as **cslu**, configure this option, with the URL for CSLU or SSM On-Prem, as applicable:

  - If you are using CSLU, enter the URL as follows:

    `http://<cslu_ip_or_host>:8182/cslu/v1/pi`

    For `<cslu_ip_or_host>`, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

    The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`

  - If you are using SSM On-Prem, enter the URL as follows:

    `http://<ip>/cslu/v1/pi/<tenant ID>`

    For <ip>, enter the hostname or the IP address of the server where you have installed SSM On-Prem. The <tenantID> must be the default local virtual account ID.

    Tip
    You can retrieve the entire URL from SSM On-Prem. See Retrieving the Transport URL (SSM On-Prem UI), on page 189

    The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`

- **default**: Depends on the configured transport mode. Only the **smart** and **cslu** transport modes are supported with this option.

  If the transport mode is set to **cslu**, and you configure **license smart url default**, the CSLU URL is configured automatically (`https://cslu-local:8182/cslu/v1/pi`).

  If the transport mode is set to **smart**, and you configure

license smart url default, the Smart URL is configured automatically (`https://smartreceiver.cisco.com/licservice/license`).

- **smart** *smart_url*: If you have configured the transport type as **smart**, configure this option. Enter the URL exactly as follows:

  `https://smartreceiver.cisco.com/licservice/license`

  When you configure this option, the system automatically creates a duplicate of the URL in **license smart url** *url*. You can ignore the duplicate entry, no further action is required.

  The **no license smart url smart***smart_url* command reverts to the default URL.

- **utility** *smart_url*: Although available on the CLI, this option is not supported.

usage { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* }	Provides usage reporting settings. You can set the following options: • **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value*: Defines strings for inclusion in data models, for telemetry. Up to 4 strings (or tags) may be defined. For *tag_value*, enter the string value for each tag that you define. • **interval** *interval_in_days*: Sets the reporting interval days. By default the RUM report is sent every 30 days. The valid value range is 1 to 3650. If you set the value to zero, RUM reports are not sent, regardless of what the applied policy dictates - this applies to a topology where CSLU or CSSM may be on the receiving end. If you set a value that is greater than zero and the transport type is set to **off**, then, between the *interval_in_days* and the policy value for `Ongoing reporting frequency(days):`, the lower of the two values is applied. For example, if *interval_in_days* is set to 100, and the value in the in the policy says `Ongoing reporting frequency (days):90`, RUM reports are sent every 90 days. If you do not set an interval, and the default is effective, the reporting interval is determined entirely by the policy value. For example, If the default value is effective and only unenforced licenses are in use, if the policy states that reporting is not required, then RUM reports are not sent. If you are using the utility mode, we recommend a reporting interval of seven days or less. This ensures that the 30- day ACK requirement, which applies to a product instance in the utility mode, is met in timely manner.

utility [**customer_info** { **city** *city* | **country** *country* | **id** *id* | **name** *name* | **postalcode** *postalcode* | **state** *state* | **street** *street* }]	Enables the utility mode on the product instance. The utility mode must be enabled if you have an MSLA and use licenses with subscription IDs. When enabled, all communication to and from the product instance is flagged accordingly. For a product instance in the utility mode, you can optionally include the additional information in a RUM report. This information is not used by Cisco. To include optional information in the RUM report, enter the **customer_info** keyword, followed by one or more of the following options: • **city** *city* • **country** *country* • **id** *id*: Enter a user-defined ID • **name** *name*: Enter a user-defined name. • **postalcode** *postalcode* • **state** *state* • **street** *street* The no form of the **license smart utility** command disables the utility mode.
vrf *vrf_string*	Configures a Virtual Routing and Forwarding (VRF) name that is used by the product instance. The product instance uses the VRF to send licensing-related data to CSSM, CSLU, or SSM On-Prem. For *vrf_string*, enter the VRF name you have defined. Ensure that the following requirements are met: • The product instance is one that supports VRF. • The transport type is **smart** or **cslu**, with the corresponding URL.

Command Default

Starting from Cisco IOS XE Amsterdam 17.3.2, Smart Licensing Using Policy is enabled by default.

Command Modes

Global config (Device(config)#)

Command History

Release	Modification
This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2	This command was introduced.

Release	Modification
Cisco IOS XE Amsterdam 17.3.2	The following keywords and variables were introduced with Smart Licensing Using Policy: • Under the **url**keyword, these options were introduced: { **cslu** *cslu_url* | **smart** *smart_url* } • Under the **transport** keyword, these options were introduced: { **cslu** | **off** } Further, the default transport type was changed from **callhome**, to **cslu**. • **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } The following keywords and variables under the **license smart** command are deprecated and no longer available on the CLI: **enable**and **conversion automatic**.
Cisco IOS XE Amsterdam 17.3.3	SSM On-Prem support was introduced. For product instance-initiated communication in an SSM On-Prem deployment, the existing [**no**]**license smart url cslu***cslu_or_on-prem_url* command supports the configuration of a URL for SSM On-Prem as well. But the required URL format for SSM On-Prem is: `http://<ip>/cslu/v1/pi/<tenant ID>`. The corresponding transport mode that must be configured is also an existing command (**license smart transport cslu**).
Cisco IOS XE Cupertino 17.7.1a	If version privacy is disabled (**no license smart privacy version** global configuration command), the Cisco IOS-XE software version running on the product instance and the Smart Agent version is *included* in the RUM report. To exclude version information from the RUM report, version privacy must be enabled (**license smart privacy version**).

Release	Modification
Cisco IOS XE Cupertino 17.9.1a	• Support for the **utility** keyword was introduced. Configure the **license smart utility** command to enable the utility mode on the product instance. The utility mode must be enabled if you have an MSLA and use licenses with subscription IDs. • A new mechanism to send all data privacy related information was introduced. This information is no longer included in a RUM report. If data privacy is disabled (**no license smart privacy** {**all** | **hostname** | **version**} global configuration command), data privacy related information is sent in a separate sync message or offline file. • Support for sending hostname information was introduced. If the privacy setting for the hostname is disabled (**no license smart privacy hostname** global configuration command), hostname information is sent from the product instance, in a separate sync message, or offline file. Depending on the topology you have implemented, the hostname information is received by CSSM, CSLU, or SSM On-Prem. It is also displayed on the corresponding user interface. • The **vrf** *vrf_string* keyword was introduced. On a product instance where VRF is supported, you can configure the **license smart vrf** *vrf_string* command to send all licensing data to CSSM, or CSLU, or SSM On-Prem.
Cisco IOS XE Dublin 17.10.1	Support for the **reservation** keyword was introduced. The [**no**] **license smart reservation** command enables or disables the reservation mode on supported product instances.

Usage Guidelines

Data Privacy Settings

When you disable a privacy setting, the topology you have implemented determines the recipient and how the information reaches its destination:

- The recipient of the information may be one or more of the following: CSSM, CSLU, and SSM On-Prem. The privacy setting has no effect on a controller (Cisco DNA Center).

  In case of the **hostname** keyword, after the hostname information is received by CSSM, CSLU, or SSM On-Prem, it is also displayed on the corresponding UIs – as applicable. If you then *enable* privacy, the corresponding UIs revert to displaying the UDI of the product instance.

- How the information is sent.

  - In case of a topology where the product instance initiates communication, the product instance initiates the sending of this information in a message, to CSSM, or CSLU, or SSM On-Prem.

    The product instance sends the hostname sent every time one of the following events occur: the product instance boots up, the hostname changes, there is a switchover in a High Availability set-up.

  - In case of a topology where CSLU or SSM On-Prem initiate communication, the corresponding component initiates the retrieval of privacy information from the product instance.

The hostname is retrieved at the frequency you configure in CSLU or SSM On-Prem.

- In case of a topology where the product instance is in an air-gapped network, privacy information is included in the offline file that is generated when you enter the **license smart save usage** privileged EXEC command.

Note For all topologies, data privacy related information is *not* included in the RUM report.

Data privacy related information it is not stored by the product instance *prior* to sending or saving. This ensures that if and when information is sent, it is consistent with the data privacy setting at the time of sending or saving.

Communication failure and reporting

The reporting interval that you configure (**license smart usage interval** *interval_in_days* command), determines the date and time at which the product instance sends out the RUM report. If the scheduled interval coincides with a communication failure, the product instance attempts to send out the RUM report for up to four hours after the scheduled time has expired. If it is still unable to send out the report (because the communication failure persists), the system resets the interval to 15 minutes. Once the communication failure is resolved, the system reverts the reporting interval to the value that you last configured.

The system message you may see in case of a communicatin failure is %SMART_LIC-3-COMM_FAILED. See the *Troubleshooting Smart Licensing Using Policy* section for information about resolving this error and restoring the reporting interval value.

Proxy server acceptance

When configuring the **license smart proxy** {**address** *address_hostname* | **port***port*} command, note the change in the criteria for the acceptance of proxy servers, starting with Cisco IOS XE Bengaluru 17.6.1: only the status code of the proxy server response is verified by the system and not the reason phrase. The RFC format is `status-line = HTTP-version SP status-code SP reason-phrase CRLF`, where the status code is a three-digit numeric code. For more information about the status line, see section 3.1.2 of RFC 7230.

Setting the Utility Mode

If the utility mode is enabled (**license smart utility**) and a license without a subscription ID is in use, the %SMART_LIC-4-UTILITY_SUBSCRIPTION_LICENSE system message is generated - once, for every license, and 30 days after the use of the license without the subscription ID is detected.

To remedy the situation, ensure that subscription IDs are deposited in the correct Smart Account and Virtual Account in CSSM. This enables all communication to be flagged accordingly.

To support the utility mode, the transport type must be set to one of the following options only:

- **smart**, if the product instance is directly connected to CSSM).
- **cslu**, if the product instance is connected to CSSM via CSLU or SSM On-Prem.
- **off**, if the product instance is in an air-gapped network.

Using a VRF

When you use the **license smart vrf** *vrf_string* global configuration command, the topology you implement must be one where the product instance is connected to CSSM, or CSLU, or SSM-OnPrem. (The supported transport types when using a VRF are **smart** and **cslu** only.)

Further, if connected to CSSM via CSLU or SSM On-Prem, you must implement a topology where the product instance initiates communication. CSLU or SSM On-Prem can be connected to CSSM or disconnected from it.

In order to use a VRF to send licensing data, other supporting VRF configuration may also be required. This will depend on your network. For more information, see IP Routing: Protocol-Independent Configuration Guide, Cisco IOS XE 17.

Sample VRF configuration is provided in the *Examples* section below.

Examples

- Examples for Data Privacy, on page 261
- Examples for Transport Type and URL, on page 262
- Examples for Usage Reporting Options, on page 263
- Example for Using VRF, on page 263

Examples for Data Privacy

The following examples show how to configure data privacy related information using **license smart privacy** command in global configuration mode. The accompanying **show license status** output displays the privacy options that are enabled and those that are disabled.

Note The output of the **show** command only tells you if a particular option is enabled or disabled.

Here, no data privacy related information information is sent:

```
Device# configure terminal
Device(config)# license smart privacy all
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: ENABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

Here, hostname is included and version information is excluded in the message initiated from the product instance. The product instance is directly connected to CSSM (transport type is **smart**, with the corresponding URL).

```
Device# configure terminal
Device(config)# license smart privacy version
Device(config)# no license smart privacy hostname
```

```
Device(config)# exit

Device# show license all
<output truncated>

Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

<output truncated>
```

Examples for Transport Type and URL

The following examples show how to configure some of the transport types using the **license smart transport** and the **license smart url** commands in global configuration mode. The accompanying **show license all** output displays configured information.

Transport **cslu**:

```
Device# configure terminal
Device(config)# license smart transport cslu
Device(config)# license smart url default
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  Proxy:
    Not Configured
<output truncated>
```

Transport **smart**:

```
Device# configure terminal
Device(config)# license smart transport smart
Device(config)# license smart url smart https://smartreceiver.cisco.com/licservice/license
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured
<output truncated>
```

Examples for Usage Reporting Options

The following examples show how to configure some of the usage reporting settings using the **license smart usage** command in global configuration mode. The accompanying **show running-config** output displays configured information.

Configuring the **customer-tag** option:

```
Device# configure terminal
Device(config)# license smart usage customer-tags tag1 SA/VA:01
Device(config)# exit
Device# show running-config | include tag1
license smart usage customer-tags tag1 SA/VA:01
```

Configuring a narrower reporting interval than the currently applied policy:

```
Device# show license status
<output truncated>
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Dec 21 12:02:21 2020 PST
Reporting push interval: 30 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 22 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>

Device# configure terminal
Device(config)# license smart usage interval 20
Device(config)# exit
Device# show license status
<output truncated>

Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Nov 22 12:02:21 2020 PST
Reporting push interval: 20 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 12 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>
```

Example for Using VRF

Here, *SLP_VRF* is used to send licensing data from the product instance. The **license smart vrf** *vrf_string* command is used to specify the VRF that will be used to send licensing data. The rest of the supporting configuration is for example purposes.

```
Device (config)# vrf definition SLP_VRF
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# exit
Device(config-vrf)# interface GigabitEthernet 0/0/0
Device (config-if)# no shutdown
Device (config-if)# vrf forwarding SLP_VRF
Device (config-if)# ip address 192.168.0.47 255.255.0.0
Device (config-if)# exit
Device (config)# ip route vrf SLP_VRF 0.0.0.0 0.0.0.0 192.168.0.1
Device (config)# ip name-server vrf SLP_VRF 173.37.137.85
```

```
Device (config)# license smart transport smart
Device (config)# license smart url https://smartreceiver.cisco.com/licservice/license
Device (config)# license smart vrf SLP_VRF
Device (config)# ip http client source-interface GigabitEthernet 0/0/0
```

license smart (privileged EXEC)

To configure licensing functions such as requesting or returning authorization codes, saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, establishing trust with Cisco Smart Software Manager (CSSM), synchronizing the product instance with CSSM, or Cisco Smart License Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), and removing licensing information from the product instance, enter the **license smart** command in privileged EXEC mode with the corresponding keyword or argument.

license smart { **authorization** { **request** { **add** | **replace** | **save** *filepath_filename* } *feature_name* { **all** | **local** } [*request_count*] | **return** { **all** | **force-reload** [**no-prompt**] | **local** } { **offline** [*filepath_filename*] | **online** } } | **clear eventlog** | **export return** { **all** | **local** } *feature_name* | **factory reset** | **import** *filepath_filename* | **renew** { **ID** | **auth** } | **reservation** { **cancel** [**all** | **local**] | **install** { *plr_code* | **file** *filepath_filename* } | **request** { **all** | **local** | **universal** } | **return** [**all** | **authorization** { *return_code* | **file** *filepath_filename* } | **local**] } | **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *filepath_filename* } } | **sync** { **all** | **local** } | **trust idtoken** *id_token_value* { **local** | **all** } [**force**] }

Syntax Description

smart	Provides options for Smart Licensing.
authorization	Provides the option to request for, or return, authorization codes.
request	Requests an authorization code from CSSM, CSLU (CSLU in-turn fetches it from CSSM), or SSM On-Prem and installs it on the product instance.
add	Adds the requested license to the existing authorization code. The new authorization code will contain all the licenses of the existing authorization code and the requested license. **Note** Do not use this option even though it is available on the CLI, for any of the supported product instances that are within the scope of this document. Use the replace option in all scenarios.
replace	Requests SLAC if it is not already installed, or replaces an existing SLAC. When you enter this option, the product instance verifies if licenses that correspond to the authorization codes that will be removed, are in-use. If licenses are being used, an error message tells you to first disable the corresponding features. A device requires only one SLAC.
save *filepath_filename*	Saves the authorization code request to a file. For *filepath_filename*, specify the absolute path to the file, including the filename.
feature_name	Name of the license for which you are requesting an authorization code.

all	Performs the action for all product instances in a High Availability configuration.
local	Performs the action for the *active* product instance. This is the default option.
request_count	Enter the license request count. Enter a value between 0 and 4294967295.
return	Returns an authorization code back to the license pool in CSSM.
force-reload [**no-prompt**]	Forces the SLAC on the device to be returned even if the HSECK9 license is in-use. Use the optional **no-prompt** keyword to skip the confirmation prompt that follows the entry of the command. On virtual product instances, the keyword displayed on the CLI is **force** . The **no-prompt** is not available because a reload is not required. If these keywords are not displayed on the CLI, it means that either the option to forcibly return SLAC is not supported on the product instance, or the HSECK9 license is not supported on the product instance.
offline *filepath_filename*	Means the product instance is not connected to CSSM. The authorization code is returned offline. This option requires you to print the return code to a file. For *file_path*, specify the location of the file where you have saved the return code.
online	Means that the product instance is in a connected mode. The authorization code is returned to CSLU or CSSM directly.
clear eventlog	Clears all event log files from the product instance.
export return	Returns the authorization key for an export-controlled license.
factory reset	Clears all saved Smart Licensing information from the product instance.
import *filepath_filename*	Imports a file on to the product instance. The file may be that of an authorization code, a trust code, or, or a policy. For *filepath_filename*, specify the location, including the filename.

{ **reservation** { **cancel** [**all** | **local**] | **install** { *plr_code* | **file** *filepath_filename* } | **request** { **all** | **local** | **universal** } | **return** [**all** | **authorization** { *return_code* | **file** *filepath_filename* } | **local**] } }	Configures reservation settings. You must specify one of these options: • **cancel** [**all** | **local**]: Cancels a reservation request before the authorization code is installed. Use this if you have generated a PLR request code, but dont want to use it. If you have already installed a PLR code, you must use the **return** option instead. • **install** {*plr_code* | **file** *filepath_filename*}: Installs the PLR code. Any older PLR code version, if it exists, is deleted during the installation process. You must first generate a reservation request code on the product instance, enter the request code in CSSM, generate the PLR authorization code in CSSM, copy it from CSSM, and then use this keyword to install it on the product instance. • **request** { **all** | **local** | **universal** }: Generates a reservation request code on the product instance. **Note** Although visible on the CLI, the **universal** keyword is deprecated and not supported. To generate a reservation request code, specify **all** to perform the action for all product instances in a High Availability configuration, or **local** to perform the action on the active product instance. • **return** [**all** | **authorization** | **local**]: Returns a PLR authorization code that was installed. After you configure this command, a return code is displayed on the CLI, you must enter this return code in CSSM to complete the return process.
save	Provides options to save RUM reports or trust code requests.
trust-request *filepath_filename*	Saves the trust code request for the active product instance in the specified location. For *filepath_filename*, specify the absolute path to the file, including the filename.
usage { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *filepath_filename* }	Saves RUM reports (license usage information) in the specified location. You must specify one of these options: • **all**: Saves all RUM reports. • **days** *days*: Saves RUM report for the last *n* number of days (excluding the current day). Enter a number. The valid range is 0 to 4294967295. For example, if you enter 3, RUM reports of the last three days are saved. • **rum-Id** *rum-ID*: Saves a specified RUM ID. The valid value range is 0 to 18446744073709551615. • **unreported**: Saves all unreported RUM reports. **file** *filepath_filename*: Saves the specified usage information to a file. Specify the absolute path to the file, including the filename.

sync { **all** | **local** }	Synchronizes with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. This includes uploading pending RUM reports, downloading the ACK response, any pending authorization codes, trust codes, and policies for the product instance. Specify the product instance by entering one of these options: • **all**: Performs synchronization for all the product instances in a High Availability set-up. If you choose this option, the product instance also sends the list of all the UDIs in the synchronization request. • **local**: Performs synchronization only for the active product instance sending the request, that is, its own UDI. This is the default option.
trust idtoken *id_token_value*	Establishes a trusted connection with CSSM. To use this option, you must first generate a token in the CSSM portal. Provide the generated token value for *id_token_value*.
force	Submits a trust code request even if a trust code already exists on the product instance. A trust code is node-locked to the UDI of a product instance. If the UDI is already registered, CSSM does not allow a new registration for the same UDI. Entering the **force** keyword overrides this behavior.

Command Default

Starting from Cisco IOS XE Amsterdam 17.3.2, Smart Licensing Using Policy is enabled by default.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2	This command was introduced.

Release	Modification
Cisco IOS XE Amsterdam 17.3.2	The following keywords and variables were introduced with Smart Licensing Using Policy: • **authorization** { **request** { **add** | **replace** } *feature_name* { **all** | **local** } | **return** { **all** | **local** } { **offline** [*path*] | **online** } } • **import** *file_path* • **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* } } • **sync** { **all** | **local** } • **trust idtoken** *id_token_value* { **local** | **all** } [**force**] The following keywords and variables under the **license smart** command are deprecated and no longer available on the CLI: • **register idtoken** *token_id* [**force**] • **renew id** { **ID** | **auth** } • **debug** { **error** | **debug** | **trace** | **all** } • **mfg reservation** { **request** | **install** | **install file** | **cancel** } • **conversion** { **start** | **stop** }
Cisco IOS XE Amsterdam 17.3.3	Support for SSM On-Prem was introduced. You can perform licensing-related tasks such as requesting or returning authorization codes, saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, synchronizing the product instance, and removing licensing information from the product instance in an SSM On-Prem deployment.
Cisco IOS XE Cupertino 17.7.1a	The following enhancements were introduced in this release: • The **save** *path* keyword and variable were added to the **license smart authorization request** command string. You can use this option to generate a SLAC request and save it to a file. The new options are displayed as follows: **license smart authorization request** { **add** | **replace** | **save** *path* } *feature_name* { **all** | **local** } [*request_count*] • The existing **license smart save usage** command was enhanced to automatically include a trust code request if it doesn't already exist.
Cisco IOS XE Dublin 17.10.1	The **reservation** keyword was restored. You can cancel, install, request, and return a PLR code.
Cisco IOS XE Dublin 17.15.1	The **force-reload** [**no-prompt**] keywords were introduced.

Usage Guidelines

Requesting a Trust Code in an Air-Gapped Network

Starting with Cisco IOS XE Cupertino 17.7.1a if a trust code is not available on the product instance, the product instance automatically includes a trust code request in the RUM report when you enter the **license smart save usage** command. This supported in a standalone set-up, 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. CSSM includes the trust code in the ACK which is available for download from the CSSM Web UI. You then have to install the ACK on the product instance. You can verify trust code installation by entering the **show license status** command in privileged EXEC mode - check for the updated timestamp in the `Trust Code Installed` field.

Overwriting a Trust Code

Use cases for the **force** option when configuring the **license smart trust idtoken** command:

- You use same token for all the product instances that are part of one Virtual Account. If the product instance has moved from one account to another (for instance, because it was added to a High Availability set-up, which is part of another Virtual Account), then there may be an existing trust code you have to overwrite.
- There is already a factory-installed trust code on the product instance, but you want to implement a topology where the product instance is directly connected to CSSM. A factory-installed trust code cannot be used for secure communication with CSSM. You must generate an ID token in the CSSM Web UI and download a trust code file. When you install this new trust code, you must overwrite the existing factory-installed trust code.

Requesting and Returning SLAC in an Air-Gapped Network

Starting with Cisco IOS XE Cupertino 17.7.1a, you can request and install a SLAC without having to enter the required PIDs or generating a SLAC in the CSSM Web UI. Instead, save a SLAC request in a file on the product instance by configuring the **license smart authorization request** command, followed by the **license smart authorization request save** commands. Upload the SLAC request file, to CSSM (in the same location and just as you would, a RUM report). After the request is processed, a SLAC file is available on the CSSM Web UI. Download, and import the SLAC file into the product instance.

Similarly, to return a SLAC configure the **license smart authorization return** command with the **offline** keyword to save the file. Upload the file to CSSM (in the same location and just as you would, a RUM report).

You can verify authorization code installation by entering the **show license authorization** command in privileged EXEC mode.

Removing Licensing Information

Entering the **licence smart factory reset** command removes all licensing information (except the licenses in-use) from the product instance, including any authorization codes, RUM reports etc. Therefore, we recommend the use of this command only if the product instance is being returned (Return Material Authrization, or RMA), or being decommissioned permanently. We also recommend that you send a RUM report to CSSM, before you remove licensing information from the product instance - this is to ensure that CSSM has up-to-date usage information.

Authorization Codes in an SSM On-Prem Deployment

Before you enter the **license smart authorization request** command on the product instance to request SSM On-Prem for SLAC, ensure that the following requirements are met.

- The product instance must be added to SSM On-Prem. The process of addition validates and maps the product instance to the applicable Smart Account and Virtual account in CSSM. See Assigning a Smart Account and Virtual Account (SSM On-Prem UI), on page 185.

- The authorization codes required for export-controlled and enfored licenses must be generated in CSSM and imported into SSM On-Prem. See Submitting an Authorization Code Request (SSM On-Prem UI, Disconnected Mode), on page 191.

Examples

- Example: Requesting a SLAC and Returning a SLAC (Connected Directly to CSSM), on page 270
- Example: Requesting a SLAC and Returning a SLAC (No Connectivity to CSSM and No CSLU), on page 271
- Example: Saving Licensing Usage Information, on page 272
- Example: Installing a Trust Code, on page 272

Example: Requesting a SLAC and Returning a SLAC (Connected Directly to CSSM)

The following example shows how to request CSSM for a SLAC and also how to return a SLAC to CSSM. Here the product instance is a Cisco 4000 Series Integrated Services Router and is configured to communicate with CSSM.

Requesting and installing a SLAC:

```
Device# license smart authorization request replace hseck9 all
*Sep 23 17:41:10.938: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing
authorization code
was successfully installed on PID:ISR4331/K9,SN:FDO224917Q6
*Sep 23 17:41:12.929: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was
successfully
installed

Device# show license authorization
Overall status:
  Active: PID:ISR4331/K9,SN:FDO224917Q6
Status: SMART AUTHORIZATION INSTALLED on Sep 23 17:41:10 2020 UTC
      Last Confirmation code: 5fd33d79

Authorizations:
  ISR_4331_Hsec (ISR_4331_Hsec):
    Description: U.S. Export Restriction Compliance license for 4330 series
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:ISR4331/K9,SN:FDO224917Q6
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

Returning a SLAC to CSSM:

```
Device# license smart authorization return all online

Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:ISR4331/K9,SN:FDO224917Q6
    Return code: CPo1Sb-CHc1jc-dFu2Fj-R9qkZc-V46wAG-7KWxKB-8vmQgp-4xZAE4-BAS

*Sep 23 17:46:12.284: %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code
```

```
has been
removed from PID:ISR4331/K9,SN:FDO224917Q6.
```

Example: Requesting a SLAC and Returning a SLAC (No Connectivity to CSSM and No CSLU)

The following example shows how to request CSSM for a SLAC and also how to return a SLAC to CSSM from a product instance in an air-gapped network. Here the product instance is a Cisco 4000 Series Integrated Services Router. The software version running on the product instance is Cisco IOS XE Cupertino 17.7.1a, which introduces support for a more simplified way of requesting and returning SLAC in an air-gapped network.

Requesting a SLAC

```
Device# license smart authorization request replace hseck9 local
Device# license smart authorization request save bootflash:slac.txt
```

After the above steps, upload the file to CSSM and download the file containing the SLAC code, and install it on the product instance. For the steps you have to complete in CSSM, see Uploading Data or Requests to CSSM and Downloading a File, on page 214. Once the file is downloaded, continue as follows:

```
Device# copy tftp://10.8.0.6/user01/slac_code.txt bootflash:
Device# license smart import bootflash:slac_code.txt
```

Returning a SLAC

```
Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Oct 29 17:19:04 2021 UTC
  Virtual Account: EG-VA

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  booster_performance     (ISR_4431_BOOST)                  1 IN USE
  appxk9                  (ISR_4400_Application)            1 IN USE
  AdvUCSuiteK9            (ISR_4400_AdvancedUCSuite)        1 IN USE
  Router US Export Lic... (DNA_HSEC)                        0 NOT IN USE
  ISR_4400_Hsec           (ISR_4400_Hsec)                   0 NOT IN USE

Device# license smart authorization return local offline bootflash:auth_return.txt
*Nov  3 05:12:06.515: %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code
has been removed from PID:ISR4431/K9,SN:FOC22446T0U.
```

After the above steps, upload the file to CSSM. For the steps you have to complete in CSSM, see Uploading Data or Requests to CSSM and Downloading a File, on page 214. A file is available for download after this, but import and installation of this file is optional.

```
Device# show license authorization
Overall status:
  Active: PID:ISR4431/K9,SN:FOC22446T0U
      Status: NOT INSTALLED
      Last return code: CqAMzh-nsjvdh-ZZCnYK-4pELCF-cZgySA-yBiYgg-qBxfdM-ykmGMs-QAT

Purchased Licenses:
  No Purchase Information Available


Device# show license summary
Account Information:
  Smart Account: Eg-SA As of Nov 03 05:02:01 2021 UTC
  Virtual Account: Eg-VA
```

```
License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  booster_performance     (ISR_4431_BOOST)                  1 IN USE
  appxk9                  (ISR_4400_Application)            1 IN USE
  AdvUCSuiteK9            (ISR_4400_AdvancedUCSuite)        1 IN USE
```

Example: Saving Licensing Usage Information

The following example shows how you can save license usage information on the product instance. You can use this option to fulfil reporting requirements in an air-gapped network. In the example, the file is first save to flash memory and then copied to a TFTP location:

```
 Device> enable
Device# license smart save usage unreported file flash:RUM-unrep.txt
Device# copy flash:RUM-unrep.txt tftp://192.168.0.1//auto/tftp-user/user01/
Address or name of remote host [192.168.0.1]?
Destination filename [//auto/tftp-user/user01/RUM-unrep.txt]?
!!
15128 bytes copied in 0.161 secs (93963 bytes/sec)
```

After you save RUM reports to a file, you must upload it to CSSM (from a workstation that has connectivity to the internet, and Cisco).

Example: Installing a Trust Code

The following example shows how to install a trust code even if one is already installed on the product instance. This requires connectivity to CSSM. The accompanying **show license status** output shows sample output after successful installation:

Before you can install a trust code, you must generate an ID token and download the corresponding file from CSSM.

Use the **show license status** command (`Trust Code Installed:`) to verify results.

```
Device> enable
Device# license smart trust idtoken
NGMwMjk5mYtNZaxMS00NzMZmtgWm local force
Device# show license status
<output truncated>
Trust Code Installed:
  Active: PID:C9500-24Y4C,SN:CAT2344L4GH
    INSTALLED on Sep 04 01:01:46 2020 EDT
  Standby: PID:C9500-24Y4C,SN:CAT2344L4GJ
    INSTALLED on Sep 04 01:01:46 2020 EDT
<output truncated>
```

show license all

To display all licensing information enter the **show license all** command in Privileged EXEC mode. This command displays status, authorization, UDI, and usage information, all combined.

show license all

This command has no arguments or keywords.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2	Command output was updated to display information relating to Smart Licensing Using Policy. Command output no longer displays Smart Account and Virtual account information.
Cisco IOS XE Cupertino 17.7.1a	The output of the command was enhanced to display the following information: • RUM report statistics, in section `Usage Report Summary`. • Smart Account and Virtual Account information, in section `Account Information`.

Usage Guidelines

This command concatenates the output of other **show license** commands, enabling you to display different kinds of licensing information together. For field descriptions, refer to the corresponding commands in the links provided below.

The `Smart Licensing Status` and `Account Information` sections of the **show license all** command corresponds with the output of the show license status, on page 298 command.

The `License Usage` section of the **show license all** command corresponds with the output of the show license usage, on page 321 command.

The `Product Information` section of the **show license all** command corresponds with the output of the show license udi, on page 320 command.

The `Agent Version` section of the **show license all** command displays the Smart Agent version and is available only in this command.

The `License Authorizations` section of the **show license all** command corresponds with the output of the show license authorization, on page 278 command.

The `Usage Report Summary` section of the **show license all** command corresponds with the output in the show license tech, on page 309 command.

Examples

- Example: show license all (Catalyst 8200 Series Edge Platform), on page 274
- Example: show license all (Cisco 4000 Series Integrated Services Routers), on page 276

Example: show license all (Catalyst 8200 Series Edge Platform)

The following is sample output of the **show license all** command, on a product instance where the software version is Cisco IOS XE Cupertino 17.7.1a. Note the addition of the two new sections in this release: `Account Information` and `Usage Report Summary`:

```
Device# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

License Conversion:
  Automatic Conversion Enabled: True
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: <none>
  Virtual Account: <none>

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: cslu
  Cslu address: <empty>
  Proxy:
    Not Configured
  VRF:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
```

```
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Jan 30 10:27:22 2022 UTC
  Reporting push interval: 30  days
  Next ACK push check: <none>
  Next report push: Nov 01 15:11:57 2021 UTC
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage
=============

network-advantage_250M (ESR_P_250M_A):
  Description: network-advantage_250M
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage_250M
  Feature Description: network-advantage_250M
  Enforcement type: NOT ENFORCED
  License type: Perpetual

dna-advantage_250M (DNA_P_250M_A):
  Description: dna-advantage_250M
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage_250M
  Feature Description: dna-advantage_250M
  Enforcement type: NOT ENFORCED
  License type: Subscription

Product Information
===================
UDI: PID:C8200-1N-4T,SN:FGL2447LGZ1

Agent Version
=============
Smart Agent for Licensing: 5.3.15_rel/49

License Authorizations
======================
Overall status:
  Active: PID:C8200-1N-4T,SN:FGL2447LGZ1
      Status: NOT INSTALLED

Purchased Licenses:
  No Purchase Information Available

Usage Report Summary:
=====================
Total: 6,  Purged: 0
Total Acknowledged Received: 0,  Waiting for Ack: 0
Available to Report: 6  Collecting Data: 2
```

Example: show license all (Cisco 4000 Series Integrated Services Routers)

The following is sample output from the **show license all** command.

```
Device# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Sep 23 22:08:22 2020 UTC

License Authorization:
  Status: AUTHORIZED - RESERVED on Sep 23 22:08:22 2020 UTC

License Conversion:
  Automatic Conversion Enabled: False
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Miscellaneus:
  Custom Id: <empty>

License Usage
=============

ISR_4400_Application (ISR_4400_Application):
  Description: AppX License for Cisco ISR 4400 Series
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1

ISR_4400_UnifiedCommunication (ISR_4400_UnifiedCommunication):
  Description: Unified Communications License for Cisco ISR 4400 Series
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Reservation:
```

```
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1

ISR_4400_Security (ISR_4400_Security):
  Description: Security License for Cisco ISR 4400 Series
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1

ISR_4431_1G_Performance (ISR_4431_1G_Performance):
  Description: Performance on Demand License for 4430 Series
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1

hseck9 (ISR_4400_Hsec):
  Description: Export Controlled Feature hseck9
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: Export Controlled Feature hseck9
  Reservation:
    Reservation status: SPECIFIC EXPORT AUTHORIZATION KEY INSTALLED
    Total reserved count: UNLIMITED

Product Information
===================
UDI: PID:ISR4431/K9,SN:FOC21030CHG

Agent Version
=============
Smart Agent for Licensing: 4.11.5_rel/41

Reservation Info
================
License reservation: ENABLED

Overall status:
  Active: PID:ISR4431/K9,SN:FOC21030CHG
      Reservation status: SPECIFIC INSTALLED on Sep 23 22:08:22 2020 UTC
      Export-Controlled Functionality: ALLOWED
      Last Confirmation code: ea24d89a

Specified license reservations:
  ISR_4400_Application (ISR_4400_Application):
    Description: AppX License for Cisco ISR 4400 Series
    Total reserved count: 1
    Term information:
      Active: PID:ISR4431/K9,SN:FOC21030CHG
        License type: PERPETUAL
          Term Count: 1
  ISR_4400_Hsec (ISR_4400_Hsec):
    Description: U.S. Export Restriction Compliance license for 4400 series
    Total reserved count: 1
```

```
  Term information:
    Active: PID:ISR4431/K9,SN:FOC21030CHG
      License type: PERPETUAL
        Term Count: 1
ISR_4400_Security (ISR_4400_Security):
  Description: Security License for Cisco ISR 4400 Series
  Total reserved count: 1
  Term information:
    Active: PID:ISR4431/K9,SN:FOC21030CHG
      License type: PERPETUAL
        Term Count: 1
ISR_4400_UnifiedCommunication (ISR_4400_UnifiedCommunication):
  Description: Unified Communications License for Cisco ISR 4400 Series
  Total reserved count: 1
  Term information:
    Active: PID:ISR4431/K9,SN:FOC21030CHG
      License type: PERPETUAL
        Term Count: 1
ISR_4431_1G_Performance (ISR_4431_1G_Performance):
  Description: Performance on Demand License for 4430 Series
  Total reserved count: 1
  Term information:
    Active: PID:ISR4431/K9,SN:FOC21030CHG
      License type: PERPETUAL
        Term Count: 1
```

show license authorization

To display authorization-related information for (export-controlled and enforced) licenses, enter the **show license authorization** command in privileged EXEC mode.

show license authorization

This command has no arguments or keywords.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2	This command was introduced.

Examples

The following are sample outputs of the **show license authorization** command, on various Cisco product instances. See Table 10: show license authorization Field Descriptions, on page 279 for information about fields shown in the display.

- HSECK9 on Cisco 4000 Series Integrated Services Router, on page 281
- HSECK9 PAK on Cisco 1000 Series Integrated Services Router, on page 282
- HSECK9 SLR on Cisco 1000 Series Integrated Services Router, on page 283
- No HSEC, SLAC on Cisco 4000 Series Integrated Services Router, on page 285

For information about *when* SLAC is required, see Authorization Code, on page 4.

Table 10: show license authorization Field Descriptions

Field		Description
Overall Status	Header for UDI information for all product instances in the set-up, the type of authorization that is installed, and configuration errors, if any. In a High Availability set-up, all UDIs in the set-up are listed.	
	Active: Status:	The active product instance UDI, followed by the status of the authorization code installation for this UDI. If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.
	Standby: Status:	The standby product instance UDI, followed by the status of the authorization code installation for this UDI. If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.
	Member: Status:	The member product instance UDI, followed by the status of the authorization code installation for this UDI. If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.
	ERROR:	Configuration errors or discrepancies in the High Availability set-up, if any.

Field		Description
Authorizations	Header for detailed license authorization information. All licenses, their enforcement types, and validity durations are displayed. Errors are displayed for each product instance if its authorization or mode does not match what is installed on the active. This section is displayed only if the product instance is using a license that requires one of these authorization codes: SLAC, SLR, PAK, RTU. This section is not displayed if a PLR authorization code is installed on the product instance.	
	():	License name and a shortened form of the license name.
	Description	License description.
	Total available count:	Total count of licenses that are available to consume. This includes licenses of all durations (perpetual and subscription), including expired subscription licenses, for all the product instances in a High Availability setup.
	Enforcement type	Enforcement type for the license. This may be one of the following: • Enforced • Not enforced • Export Restricted (same as export-controlled) For more information about enforcement types, see License Enforcement Types, on page 3.
	Term information:	

Field		Description
		Header providing license duration information. The following fields maybe included under this header: • Active: The active product instance UDI, followed by the status of the authorization code installation for this UDI. • Authorization type: Type of authorization code installed and date of installation. The type can be: SLAC, UNIVERSAL, SPECIFIED, PAK, RTU. • Start Date: Displays validity start date if the license is for a specific term or time period. • Start Date: Displays validity end date if the license is for a specific term or time period. • Term Count: License count. • Subscription ID: Displays ID if the license is for a specific term or time period. • License type: License duration. This can be: SUBSCRIPTION or PERPETUAL. • Standby: The standby product instance UDI, followed by the status of the authorization code installation for this UDI. • Member: The member product instance UDI, followed by the status of the authorization code installation for this UDI. For more information about the duration or term of a license's validity, see License Duration, on page 3.
Purchased Licenses	Header for license purchase information.	
	Active:	The active product instance and its the UDI.
	Count:	License count.
	Description:	License description.
	License type:	License duration. This can be: SUBSCRIPTION or PERPETUAL.
	Standby:	The standby product instance UDI.
	Member:	The member product instance UDI.

HSECK9 on Cisco 4000 Series Integrated Services Router

The following sample output of the **show license authorization** command shows an export-controlled license (HSECK9) with SLAC installed on a Cisco 4000 Series Integrated Services Router.

```
Device# show license authorization

Overall status:
```

```
  Active: PID:ISR4331/K9,SN:FDO224917Q6
  Status: SMART AUTHORIZATION INSTALLED on Sep 23 17:41:10 2020 UTC
      Last Confirmation code: 5fd33d79

Authorizations:
  ISR_4331_Hsec (ISR_4331_Hsec):
    Description: U.S. Export Restriction Compliance license for 4330 series
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:ISR4331/K9,SN:FDO224917Q6
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

HSECK9 PAK on Cisco 1000 Series Integrated Services Router

The following sample output of the **show license authorization** command shows an HSECK9 PAK license on a Cisco 4000 Series Integrated Services Router.

In the output, fields `Status: NOT INSTALLED` and `Status:PAK` show that SLAC is not installed, and that the product instance has been migrated from an earlier Cisco Software Licensing (CSL) licensing model with PAK licences, to Smart Licensing Using Policy. The `Legacy License Info` section also shows this.

An HSECK9 PAK license is honored after migration and does not require SLAC installation. See: How Upgrade Affects Enforcement Types for Existing Licenses, on page 54.

The accompanying **show license usage** command output for the same product instance helps confirm that the necessary authorization is present (`Export status: RESTRICTED - ALLOWED` and `License type: Perpetual`).

```
Device# show license authorization

Overall status:

  Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
      Status: NOT INSTALLED
      Status:PAK

Legacy License Info:
  regid.2017-04.com.cisco.ISR_1100_8P_Application,1.0_c4cf42aa-2d60-4f4e-83dd-c5c9672132c9:

    DisplayName: appxk9
    Description: appxk9
    Total available count: 1
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
        License type: PERPETUAL
          Term Count: 1

  regid.2017-04.com.cisco.ISR_1100_8P_Security,1.0_6b61b693-0daa-42d4-8cee-930de5c1b37c:
    DisplayName: securityk9
    Description: securityk9
    Total available count: 1
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
        License type: PERPETUAL
```

```
          Term Count: 1

  regid.2017-08.com.cisco.ISR_1100_8P_Hsec,1.0_34a5e7e7-722a-41ab-bdad-d53d5a3cac14:
    DisplayName: hseck9
    Description: hseck9
    Total available count: 1
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391J3
        License type: PERPETUAL
          Term Count: 1

Device# show license usage

License Authorization:
  Status: Not Applicable

hseck9 (ISR_1100_8P_Hsec):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Perpetual

appxk9 (ISR_1100_8P_Application):
  Description: appxk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: appxk9
  Feature Description: appxk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

securityk9 (ISR_1100_8P_Security):
  Description: securityk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: securityk9
  Feature Description: securityk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual
```

HSECK9 SLR on Cisco 1000 Series Integrated Services Router

The following sample output of the **show license authorization** command on a Cisco 1000 Series Integrated Services Router shows a Specific License Reservation (SLR) authorization code that includes an HSECK9 license.

In the output, fields `Status: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC` and `Last Confirmation code: 0708eeec` show that an SLR authorization code has been installed. The `Specified license reservations` section shows that and HSECK9 license (ISR_1100_8P_Hsec) is included. This shows that the product instance has been migrated from the earlier Smart Licensing

environment with reserved licenses (or SLR licenses), to Smart Licensing Using Policy, and includes an HSECK9 license.

A SLAC does not have to be installed again in this scenario. See: How Upgrade Affects Enforcement Types for Existing Licenses, on page 54.

The accompanying **show license usage** command output for the same product instance helps confirm that the necessary authorization is present (`Export status: RESTRICTED - ALLOWED`).

```
Device# show license authorization
Overall status:
  Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
      Status: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
      Last Confirmation code: 0708eeec

Specified license reservations:
  Cisco 1100 Series with 8 LAN Ports, Cisco One Foundation Suite
(ISR_1100_8P_FoundationSuite):
    Description: Cisco 1100 Series with 8 LAN Ports, Cisco One Foundation Suite
    Total reserved count: 1
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
        Authorization type: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
        License type: PERPETUAL
          Term Count: 1
  ISR_1100_8P_Hsec (ISR_1100_8P_Hsec):
    Description: Cisco 1100 Series with 8 LAN Ports, U.S. Export Restriction Compliance
license
    Total reserved count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C1111-8PLTEEAWB,SN:FGL214391JK
        Authorization type: SPECIFIC INSTALLED on Jan 19 05:59:54 2021 UTC
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available


Derived Licenses:
  Entitlement Tag:
regid.2017-08.com.cisco.ISR_1100_8P_Hsec,1.0_34a5e7e7-722a-41ab-bdad-d53d5a3cac14
  Entitlement Tag:
regid.2018-12.com.cisco.ISR_1100_8P_UnifiedCommunication,1.0_55775cb5-538d-482e-b57f-fc8af02f93a3

  Entitlement Tag:
regid.2017-04.com.cisco.ISR_1100_8P_FoundationSuite,1.0_6f4a1f6f-b607-45cb-8bd0-d672ac06a314
```

```
Device# show license usage

License Authorization:
  Status: Not Applicable

hseck9 (ISR_1100_8P_Hsec):
  Description: hseck9
  Count: 1
  Vecsion: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
```

```
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC EXPORT AUTHORIZATION KEY INSTALLED
    Total reserved count: UNLIMITED

uck9 (ISR_1100_8P_UnifiedCommunication):
  Description: uck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: uck9
  Feature Description: uck9
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: NOT INSTALLED

FoundationSuiteK9 (ISR_1100_8P_FoundationSuite):
  Description: FoundationSuiteK9
  count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: FoundationSuiteK9
  Feature Description: FoundationSuiteK9
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 1
```

No HSEC, SLAC on Cisco 4000 Series Integrated Services Router

The following sample output of the **show license authorization** command a Cisco 4000 Series Integrated Services Router that is not using export-controlled functionality or throughput greater than 250 Mbps.

In the output, field `Status: NOT INSTALLED` shows that SLAC is not installed.

The accompanying **show license usage** command output for the same product instance helps verify that all the licenses being used on this product instance are unenforced (all of them have `Enforcement type: NOT ENFORCED`), therefore not requiring SLAC installation.

```
Device# show license authorization
Overall status:
  Active: PID:ISR4351/K9,SN:FDO21512BJB
      Status: NOT INSTALLED

Purchased Licenses:
  No Purchase Information Available

Derived Licenses:
  Entitlement Tag:
regid.2015-01.com.cisco.ISR_4351_400M_Performance,1.0_79a9ccb4-d7c3-46fd-9980-7efe247c90e5
  Entitlement Tag:
regid.2015-01.com.cisco.ISR_4351_Application,1.0_601ccfff-5601-4293-98d2-2f653d864ce0
  Entitlement Tag:
regid.2014-12.com.cisco.ISR_4351_UnifiedCommunication,1.0_a04fec0e-e944-4096-bcf8-05d6e9a0a6d3

  Entitlement Tag:
regid.2014-12.com.cisco.ISR_4351_Security,1.0_df7d8d7f-b71a-4d3d-a9ab-aec7828a37a7
```

```
Device# show license usage
License Authorization:
  Status: Not Applicable

throughput (ISR_4351_400M_Performance):
  Description: throughput
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: throughput
  Feature Description: throughput
  Enforcement type: NOT ENFORCED
  License type: Perpetual

appxk9 (ISR_4351_Application):
  Description: appxk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: appxk9
  Feature Description: appxk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

uck9 (ISR_4351_UnifiedCommunication):
  Description: uck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: uck9
  Feature Description: uck9
  Enforcement type: NOT ENFORCED
  License type: Perpetual

securityk9 (ISR_4351_Security):
  Description: securityk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: securityk9
  Feature Description: securityk9
  Enforcement type: NOT ENFORCED
  License type: Perpetual
```

show license data

To display license data conversion information, enter the **show license data** command in privileged EXEC mode.

show license data conversion

Syntax Description

conversion	Displays information about the license conversion.

Command Modes Privileged EXEC (Device#)

Command History

Release	Modification
This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2	This command was introduced.

show license data conversion

The following is sample output from the **show license data conversion** command.

```
Device# show license data conversion
Smart Licensing Data - Conversion
================================
```

show license eventlog

To display event logs relating to Smart Licensing Using Policy, enter the **show license eventlog** command in privileged EXEC mode.

show license eventlog [*days*]

Syntax Description

days	Enter the number of days for which you want to display event logs. The valid value range is from 0 to 2147483647.

Command Modes Privileged EXEC (Device#)

Command History

Release	Modification
This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2.	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2	Additional events were added with the introduction of Smart Licensing Using Policy: • Installation and removal of a policy • Request, installation and removal of an authorization code. • Installation and removal of a trust code. • Addition of authorization source information for license usage.

Examples

• Example: Event log for one day, on page 288

• Example: All event logs , on page 288

Example: Event log for one day

The following is sample output from the **show license eventlog** command. The command is configured to display events for one day.

```
Device# show license eventlog 1

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
No time source, 12:50:20.640 EDT Fri Sep 11 2020

**** Event Log ****

2020-09-11 00:50:17.693 EDT SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_ERM_RESET" MSG="ERM-Reset: Client 0, AP-GROUP group, 2 features
air-network-advantage,air-dna-advantage"
2020-09-11 00:50:17.695 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896"
2020-09-11 00:50:17.695 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790"
2020-09-11 00:50:50.175 EDT SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
2020-09-11 08:50:17.694 EDT SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_ERM_RESET" MSG="ERM-Reset: Client 0, AP-GROUP group, 2 features
air-network-advantage,air-dna-advantage"
2020-09-11 08:50:17.696 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896"
2020-09-11 08:50:17.696 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790"
2020-09-11 08:50:52.804 EDT SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
```

Example: All event logs

The following is sample output from the **show license eventlog** command. The command is configured to display all events.

```
Device# show license eventlog
**** Event Log ****

2020-09-22 20:23:27.699 UTC SAEVT_INIT_START version="4.13.23_rel/62"
2020-09-22 20:23:27.701 UTC SAEVT_INIT_CRYPTO success="False" error="Crypto Initialization
 has not been completed"
2020-09-22 20:23:27.702 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmfRegister"
2020-09-22 20:23:32.840 UTC SAEVT_READY
2020-09-22 20:23:32.841 UTC SAEVT_ENABLED
2020-09-22 20:23:33.455 UTC SAEVT_EXPORT_FLAG exportAllowed="False"
2020-09-22 20:23:35.806 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmfInitialize"
2020-09-22 20:23:35.815 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6"
2020-09-22 20:23:35.816 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHAchkptRegister"
2020-09-22 20:23:49.682 UTC SAEVT_HA_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6" haRole="Active"
2020-09-22 20:23:49.735 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6"
haRole="Active"
2020-09-22 20:23:49.737 UTC SAEVT_HA_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6" haRole="Active"
2020-09-22 20:23:50.043 UTC SAEVT_INIT_CONFIG_READ_BEGIN
2020-09-22 20:23:54.353 UTC SAEVT_INIT_CONFIG_READ_DONE
2020-09-22 20:23:55.112 UTC SAEVT_INIT_SYSTEM_INIT
2020-09-22 20:23:56.114 UTC SAEVT_INIT_CRYPTO success="False" error="Crypto Initialization
 has not been completed"
2020-09-22 20:24:26.120 UTC SAEVT_INIT_CRYPTO success="True"
```

```
2020-09-22 20:24:26.133 UTC SAEVT_COMM_RESTORED
2020-09-22 20:24:26.402 UTC SAEVT_INIT_COMPLETE
2020-09-22 20:25:26.132 UTC SAEVT_PRIVACY_CHANGED enabled="True"
2020-09-22 20:31:34.912 UTC SAEVT_HOSTNAME_CHANGE
2020-09-22 20:35:30.873 UTC SAEVT_CONFIG_PERSISTED
2020-09-22 20:39:27.795 UTC SAEVT_INIT_START version="4.13.23_rel/62"
2020-09-22 20:39:27.798 UTC SAEVT_INIT_CRYPTO success="False" error="Crypto Initialization
 has not been completed"
2020-09-22 20:39:27.798 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmfRegister"
2020-09-22 20:39:33.333 UTC SAEVT_READY
2020-09-22 20:39:33.334 UTC SAEVT_ENABLED
2020-09-22 20:39:33.914 UTC SAEVT_EXPORT_FLAG exportAllowed="False"
2020-09-22 20:39:36.300 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmfInitialize"
2020-09-22 20:39:36.311 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6"
2020-09-22 20:39:36.312 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHAchkptRegister"
2020-09-22 20:39:52.391 UTC SAEVT_TAG_EXPORT exportAllowed="False" count="0"
entitlementTag="regid.2015-02.com.cisco.ISR_4331_Hsec,1.0_7998f136-248d-4ee9-94be-2b561c04a51e"
2020-09-22 20:39:53.058 UTC SAEVT_HA_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6" haRole="Active"
2020-09-22 20:39:53.300 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6"
haRole="Active"
2020-09-22 20:39:53.300 UTC SAEVT_HA_ROLE udi="PID:ISR4331/K9,SN:FDO224917Q6" haRole="Active"
2020-09-22 20:39:55.146 UTC SAEVT_INIT_CONFIG_READ_BEGIN
2020-09-22 20:40:01.700 UTC SAEVT_TAG_AUTHORIZED count="1"
entitlementTag="regid.2017-05.com.cisco.ISR_4331_BOOST,1.0_d5ca3d93-a3a9-480d-98f7-c7b06ddcc973"
2020-09-22 20:40:01.704 UTC SAEVT_HOSTNAME_CHANGE
2020-09-22 20:40:02.140 UTC SAEVT_TAG_AUTHORIZED count="1"
entitlementTag="regid.2015-01.com.cisco.ISR_4331_Application,1.0_4dd5e243-4754-4fed-b8aa-cdd9ff0e82c0"
2020-09-22 20:40:02.142 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_LICENSE_REQUEST" MSG="License appxk9, dev ISR4331, count 1, reslt
 0, alt 0"
2020-09-22 20:40:02.374 UTC SAEVT_TAG_AUTHORIZED count="1"
entitlementTag="regid.2014-12.com.cisco.ISR_4331_UnifiedCommunication,1.0_fc59e79d-8a80-469b-b1fb-0307e6e76108"
2020-09-22 20:40:02.376 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_LICENSE_REQUEST" MSG="License uck9, dev ISR4331, count 1, reslt
0, alt 0"
2020-09-22 20:40:02.608 UTC SAEVT_TAG_AUTHORIZED count="1"
entitlementTag="regid.2014-12.com.cisco.ISR_4331_Security,1.0_dba7c7eb-f2b3-4824-9690-10e46d998fa5"
2020-09-22 20:40:02.610 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_LICENSE_REQUEST" MSG="License securityk9, dev ISR4331, count 1,
reslt 0, alt 0"
2020-09-22 20:40:02.651 UTC SAEVT_INIT_CONFIG_READ_DONE
2020-09-22 20:40:03.445 UTC SAEVT_INIT_SYSTEM_INIT
2020-09-22 20:40:04.456 UTC SAEVT_INIT_CRYPTO success="False" error="Crypto Initialization
 has not been completed"
2020-09-22 20:40:34.458 UTC SAEVT_INIT_CRYPTO success="True"
2020-09-22 20:40:34.461 UTC SAEVT_COMM_RESTORED
2020-09-22 20:40:34.739 UTC SAEVT_INIT_COMPLETE
2020-09-22 20:41:34.459 UTC SAEVT_PRIVACY_CHANGED enabled="True"
2020-09-22 20:41:39.216 UTC SAEVT_INIT_CRYPTO success="True"
2020-09-22 20:42:35.750 UTC SAEVT_UTILITY_REPORT_START
2020-09-22 20:42:36.725 UTC SAEVT_UTILITY_RUM_FAIL error="[CSSM_ACCOUNT_ACCESS_DENIED] Smart
 Account access denied, user has no permission."
2020-09-22 21:33:20.102 UTC SAEVT_UTILITY_RUM_FAIL error="[ERROR_CSSMCONN_PING_ERR] CSLU
could not connect to the Cisco network. Please check your network settings."
2020-09-22 21:36:21.869 UTC SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
2020-09-23 00:07:15.577 UTC SAEVT_UTILITY_RUM_FAIL error="[ERROR_CSSMCONN_API] CSSM connector
 API failed"
2020-09-23 06:25:36.828 UTC SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
2020-09-23 16:23:05.822 UTC SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
2020-09-23 16:31:11.018 UTC SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
2020-09-23 17:41:10.921 UTC SAEVT_RESERVE_INSTALL_START udi="PID:ISR4331/K9,SN:FDO224917Q6"

[redacted]
 Export Restriction Compliance license for 4330
```

[illegible]
2020-09-23 17:41:10.937 UTC SAEVT_TAG_EXPORT exportAllowed="False" count="0"
entitlementTag="regid.2015-02.com.cisco.ISR_4331_Hsec,1.0_7998f136-248d-4ee9-94be-2b561c04a51e"
2020-09-23 17:41:10.965 UTC SAEVT_TAG_EXPORT exportAllowed="True" count="0"
entitlementTag="regid.2015-02.com.cisco.ISR_4331_Hsec,1.0_7998f136-248d-4ee9-94be-2b561c04a51e"
2020-09-23 17:41:11.965 UTC SAEVT_STATE_RESERVE_AUTHORIZED
2020-09-23 17:46:12.269 UTC SAEVT_RESERVE_RETURN_START udi="PID:ISR4331/K9,SN:FDO224917Q6"

[illegible]
 Export Restriction Compliance license for 4330
[illegible]
2020-09-23 17:46:12.283 UTC SAEVT_TAG_EXPORT exportAllowed="False" count="0"
entitlementTag="regid.2015-02.com.cisco.ISR_4331_Hsec,1.0_7998f136-248d-4ee9-94be-2b561c04a51e"

show license history message

To display communication history between the product instance and CSSM or CSLU (as the case may be), enter the **show license history message** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting.

show license history message

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2	This command was introduced.

Usage Guidelines

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra** privileged EXEC commands.

show license reservation

To display license reservation information, enter the **show license reservation** command in privileged EXEC mode.

show license reservation

This command has no arguments or keywords.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2.	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2	The command continues to be available, but with the introduction of Smart Licensing Using Policy, it is not longer applicable to SLR and PLR licenses. Use the **show license authorization** command in privileged EXEC mode instead.
Cisco IOS XE Dublin 17.10.1	With the introduction of support for PLR in this release, this command was restored.

Examples

show license reservation: PLR Installed in the Smart Licensing Using Policy Environment (Cisco Cloud Services Router 1000v)

The following is sample output of the **show license reservation** command on a product instance where PLR is activated.

```
Devide# show license reservation
Overall status:
  Active: PID:CSR1000V,SN:9QLBLATKXM4
      Status: UNIVERSAL INSTALLED on Nov 09 00:12:18 2022 UTC
```

show license rum

To display information about Resource Utilization Measurement reports (RUM report) available on the product instance, including report IDs, the current processing state of a report, error information (if any), and to save the detailed or summarized view that is displayed, enter the **show license rum** command in privileged EXEC mode.

show license rum { **feature** { *license_name* | **all** } | **id** { *rum_id* | **all** } } [**detail**] [**save** *path*]

Syntax Description

feature { *license_name* | **all** }	Displays RUM report information based on the license name. Specify a particular license name to display all RUM reports for that license, or use the **all** keyword to display all RUM reports available on the product instance.
id { *rum_id* | **all** }	Displays RUM report information based on the RUM report ID. Specify a report ID to display information for a single report, or use the **all** keyword to display all RUM reports available on the product instance.

detail	Displays detailed RUM report information. You can use this to display detailed information by license name and detailed information by RUM report ID.
save *path*	Saves the information that is displayed. This can be the simplified or detailed version and depends on the preceeding keywords you have entered. Information about 200 RUM reports can be displayed. If there are more 200 RUM reports on the product instance, you can view information about all the RUM reports by saving it to a text (.txt) file. **Note** This option saves the information *about* RUM reports and is not for reporting purposes. It does not save the RUM report, which is an XML file containing usage information.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1a	This command was introduced.

Usage Guidelines

A RUM report is a license usage report, which the product instance generates, to fulfil reporting requirements as specified by the policy. An acknowledgement (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. You can use the **show license rum** command to:

- Display information about the available RUM reports on the product instance - filtered by ID or license name.
- Display a short summary of the information or display a detailed view of the information.
- Track a RUM report throughout its lifecycle (from the time it is first generated until its acknowledgement from CSSM). By displaying the current processing state and condition of a report you can ascertain if and when there is a problem in the reporting workflow.
- Save the displayed information. The CLI displays information about up to 200 reports. If there are more than 200 reports on the product instance and you want to view information about all of them, save the displayed info in a .txt file and export to the desired location to view.

To display a statistical view of RUM report information (the total number of reports on the product instance, the number of reports that have a corresponding ACK, the number of reports waiting for an ACK etc.) refer to the `Usage Report Summary:` section of the **show license all** and **show license tech** privileged EXEC commands.

The **show license tech** command also provides RUM report related information that the Cisco technical support team can use to troubleshoot, if there are problems with RUM reporting.

Examples

For information about fields shown in the display, see Table 11: show license rum (simplified view) Field Descriptions, on page 293 and Table 12: show license rum (detailed view) Field Descriptions, on page 294

For examples of the **show license rum** command, see:

- show license rum feature: Simplified and Detailed View, on page 296
- Saving RUM Report View, on page 298

Table 11: show license rum (simplified view) Field Descriptions

Field Name	Description
Report Id	A numeric field that identifies a RUM report. The product instance automatically assigns an ID to every RUM report it generates. An ID may be up to 20 characters long.
State	This field displays the current processing state of a RUM report, and can be only one of the following: • OPEN: This means new measurements are being added to the report. • CLOSED: This means no further measurements can be added to this report, and the report is ready for communication to CSSM. • PENDING: This is a transitional status that you may see if you display a report while it is being transmitted. • UNACK: This means the report was transmitted and is waiting for confirmation from CSSM, that it is processed. • ACK: This means the report was processed or acknowledged by CSSM and is eligible for deletion.

Field Name	Description

Flag	Indicates the condition of the RUM report, and is displayed in the form of a character. Each character represents a specific condition, and can be only one of the following values:
	• N: Normal; This means no errors have been detected and the report is going through normal operation.
	• P: Purged; This means the report was removed due to system resource limitation, and can refer to a shortage of disk space or insufficient memory. If this flag is displayed, refer to the `State Change Reason` field in the detailed view for more information.
	• E: Error; This means an error was detected in the RUM report. If this flag is displayed, refer to the detailed view for more information. Possible workflow issues include and are not limited to the following:
	  • RUM report was dropped by CSSM. If this is the issue, the `State` field displays value `ACK`, but the `State Change Reason` does not change to `ACKED`.
	  • RUM Report data is missing. If this is the issue, the `Storage State` field displays value `MISSING` .
	  • Tracking information is missing. If this is the case the `State` field displays value `UNACK` and the `Transaction ID` field has no information.
	Note
	Occasional errors in RUM reports do not require any action from you and are not an indication of a problem. It is only if you see a large number of reports (greater than 10) with errors that you must contact the Cisco technical support team.

Feature Name	The name of the license that the RUM report applies to.

Table 12: show license rum (detailed view) Field Descriptions

Field Name	Description
Report Id	A numeric field that identifies a RUM report. The product instance automatically assigns an ID to every RUM report it generates. An ID may be up to 20 characters long.
Metric Name:	Shows the type of data that is recorded. For a RUM report, the only possible value is ENTITLEMENT, and refers to measurement of license usage.
Feature Name:	The name of the license that the RUM report applies to.
Metric Value	A unique identifier for the data that is recorded. This is the same as the “Entitlement Tag” in the output of the **show license tech** commad and it displays information about the license being tracked.

Field Name	Description
UDI	Composed of the Product ID (PID) and serial number of the product instance.
Previous Report Id:	ID of the previous RUM report that the product instance generated for a license.
Next Report Id:	The ID that the product instance will use for the next RUM report it generates for a llicense.
State:	Displays the current processing state of a RUM report. The value displayed here is always the same as the value displayed in the simplified view. For the list of possible values see Table 11: show license rum (simplified view) Field Descriptions, on page 293above.
State Change Reason:	Displays the reason for a RUM report state change. Not all state changes provide a reason. • NONE: This means the RUM report is going through its normal lifecycle (for instance, from OPEN → CLOSED → ACK). This state change reason is usually accompanied by an `N` flag (meaning Normal) in the simplified view and requires no action from you. • ACKED: RUM report was processed normally by CSSM. • REMOVED: RUM report was received and requested to be removed by CSSM. • RELOAD: RUM report state was changed due to some type of device reload. • DECONFIG: License was removed from configuration.
Start Time: End Time:	Timestamps for measurement start and measurement end for a RUM report. Together, the start time and end time provide the time duration that the measurements cover.
Storage State:	Displays current storage state of the RUM report and can be one of the following values: • EXIST: This means the data for the RUM report is located in storage. • DELETED: This means the data was intentionally deleted. Refer to the `Storage State Change Reason` in the output of the **show license tech** command for more information about this storage state. • PURGED: This means the data was deleted due to a system resource limitation. Refer to the `Storage State Change Reason` in the output of the **show license tech** command for more information about this storage state. • MISSING: This means data is missing from storage. If reports are identified as missing, there is no recovery process.

Field Name	Description
Transaction ID:	Contains tracking information for the RUM report. This information can be either polling information or ACK import information. The Transaction Message contains the error message, if the product instance receives one when importing an ACK. The information in these fields is used by the Cisco technical support team when troubleshooting problems with RUM reports.
Transaction Message:	

show license rum feature: Simplified and Detailed View

The following is sample output of the **show license rum feature all** and **show license rum feature alldetail** commands on a Cisco Catalyst 8300 router (C8300-1N1S-4T2X).

The output is filtered to display a simplified view of all the RUM reports for all the licenses on the product instance, followed by a detailed view of all the RUM reports for all the licenses:

```
Router# show license rum feature all

Smart Licensing Usage Report:
=====================================
Report Id,          State,    Flag, Feature Name
1638518477          UNACK     N     network-advantage_10M
1638518478          UNACK     N     dna-advantage_10M
1638518479          ACK       E     network-advantage_10M
1638518480          ACK       E     dna-advantage_10M
1638518482          ACK       N     network-advantage_T2
1638518483          ACK       N     dna-advantage_T2
1638518484          ACK       N     hseck9
1638518485          OPEN      N     network-advantage_T2
1638518486          OPEN      N     dna-advantage_T2
1638518487          OPEN      N     hseck9


Router# show license rum feature all detail

Smart Licensing Usage Report Detail:
=====================================
Report Id: 1638518477
  Metric Name: ENTITLEMENT
  Feature Name: network-advantage_10M
  Metric Value: regid.2018-12.com.cisco.ESR_P_10M_A,1.0_8946a476-b904-4d0a-9d0b-2b1e5de891a3

  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 0,    Next Report Id: 1638518479
  State: UNACK,      State Change Reason: REPORTING
  Start Time: Dec 03 08:12:05 2021 UTC,      End Time: Dec 03 08:12:06 2021 UTC
  Storage State: EXIST
  Transaction ID: 715896687973761034
  Transaction Message: <none>

Report Id: 1638518478
  Metric Name: ENTITLEMENT
  Feature Name: dna-advantage_10M
  Metric Value: regid.2018-12.com.cisco.DNA_P_10M_A,1.0_7f2e8a7a-e74d-4d71-af46-1ae7b3faf320

  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 0,    Next Report Id: 1638518480
  State: UNACK,      State Change Reason: REPORTING
```

```
  Start Time: Dec 03 08:12:05 2021 UTC,      End Time: Dec 03 08:12:06 2021 UTC
  Storage State: EXIST
  Transaction ID: 715896687973761034
  Transaction Message: <none>

Report Id: 1638518479
  Metric Name: ENTITLEMENT
  Feature Name: network-advantage_10M
  Metric Value: regid.2018-12.com.cisco.ESR_P_10M_A,1.0_8946a476-b904-4d0a-9d0b-2b1e5de891a3

  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 1638518477,    Next Report Id: 0
  State: ACK,      State Change Reason: DROPPED
  Start Time: Dec 03 08:12:06 2021 UTC,      End Time: Dec 03 08:24:19 2021 UTC
  Storage State: EXIST
  Transaction ID: 0
  Transaction Message: Report already received.

Report Id: 1638518480
  Metric Name: ENTITLEMENT
  Feature Name: dna-advantage_10M
  Metric Value: regid.2018-12.com.cisco.DNA_P_10M_A,1.0_7f2e8a7a-e74d-4d71-af46-1ae7b3faf320

  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 1638518478,    Next Report Id: 0
  State: ACK,      State Change Reason: DROPPED
  Start Time: Dec 03 08:12:06 2021 UTC,      End Time: Dec 03 08:24:19 2021 UTC
  Storage State: EXIST
  Transaction ID: 0
  Transaction Message: Report already received.

Report Id: 1638518482
  Metric Name: ENTITLEMENT
  Feature Name: network-advantage_T2
  Metric Value: regid.2020-10.com.cisco.NWSTACK_T2_A,1.0_83edc508-0ee4-468e-8962-0a4fde995e80

  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 0,    Next Report Id: 1638518485
  State: ACK,      State Change Reason: ACKED
  Start Time: Dec 03 08:29:31 2021 UTC,      End Time: Dec 03 08:29:32 2021 UTC
  Storage State: DELETED
  Transaction ID: 0
  Transaction Message: Report already received.

Report Id: 1638518483
  Metric Name: ENTITLEMENT
  Feature Name: dna-advantage_T2
  Metric Value: regid.2020-10.com.cisco.DSTACK_T2_A,1.0_b072e613-aa2c-4ed0-ab46-ae91ddc7dfb5

  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 0,    Next Report Id: 1638518486
  State: ACK,      State Change Reason: ACKED
  Start Time: Dec 03 08:29:31 2021 UTC,      End Time: Dec 03 08:29:32 2021 UTC
  Storage State: DELETED
  Transaction ID: 0
  Transaction Message: Report already received.

Report Id: 1638518484
  Metric Name: ENTITLEMENT
  Feature Name: hseck9
  Metric Value: regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844
  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 0,    Next Report Id: 1638518487
  State: ACK,      State Change Reason: ACKED
```

```
  Start Time: Dec 03 08:29:31 2021 UTC,      End Time: Dec 03 08:29:32 2021 UTC
  Storage State: DELETED
  Transaction ID: 0
  Transaction Message: Report already received.

Report Id: 1638518485
  Metric Name: ENTITLEMENT
  Feature Name: network-advantage_T2
  Metric Value: regid.2020-10.com.cisco.NWSTACK_T2_A,1.0_83edc508-0ee4-468e-8962-0a4fde995e80

  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 1638518482,    Next Report Id: 0
  State: OPEN,      State Change Reason: None
  Start Time: Dec 03 08:29:32 2021 UTC,      End Time: Dec 07 01:45:57 2021 UTC
  Storage State: EXIST
  Transaction ID: 0
  Transaction Message: <none>

Report Id: 1638518486
  Metric Name: ENTITLEMENT
  Feature Name: dna-advantage_T2
  Metric Value: regid.2020-10.com.cisco.DSTACK_T2_A,1.0_b072e613-aa2c-4ed0-ab46-ae91ddc7dfb5

  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 1638518483,    Next Report Id: 0
  State: OPEN,      State Change Reason: None
  Start Time: Dec 03 08:29:32 2021 UTC,      End Time: Dec 07 01:45:57 2021 UTC
  Storage State: EXIST
  Transaction ID: 0
  Transaction Message: <none>

Report Id: 1638518487
  Metric Name: ENTITLEMENT
  Feature Name: hseck9
  Metric Value: regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844
  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 1638518484,    Next Report Id: 0
  State: OPEN,      State Change Reason: None
  Start Time: Dec 03 08:29:32 2021 UTC,      End Time: Dec 07 01:45:57 2021 UTC
  Storage State: EXIST
  Transaction ID: 0
  Transaction Message: <none>
```

Saving RUM Report View

The following example shows you how to save a simplified view of the **show license rum feature all** command.

By using the **feature** and **all** keywords, the output is filtered to display all RUM reports for all licenses being used on the product instance. You can then transfer it to a location from where you can open the text file and view the information.

```
Device# show license rum feature all save bootflash:all-rum-stats.txt
Device# copy bootflash:all-rum-stats.txt tftp://10.8.0.6/user01/
```

show license status

To display license status information, enter the **show license status** command in privileged EXEC mode.

show license status

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes `Trust code installed:`, `Policy in use`, `Policy name:` , reporting requirements as in the policy (`Attributes:`), and fields related to usage reporting. Command output no longer displays Smart Account and Virtual account information.
Cisco IOS XE Cupertino 17.7.1a	Command output was updated to display Smart Account and Virtual account information.

Usage Guidelines

Account Information in the output

Starting with Cisco IOS XE Cupertino 17.7.1a, every ACK includes the Smart Account and Virtual Account that was reported to, in CSSM. When it receives the ACK, the product instance securely stores only the latest version of this information - as determined by the timestamp in the ACK. The Smart Account and Virtual Account information that is displayed in the `Account Information` section of this command's output is therefore always as per the latest available ACK on the product instance.

If a product instance is moved from one Smart Account and Virtual Account to another, the next ACK after the move will have this updated information. The output of this command is updated once this ACK is available on the product instance.

The ACK may be received directly (where the product instance is connected to CSSM), or indirectly (where the product instance is connect to CSSM through CSLU, Cisco DNA Center, or SSM On-Prem), or by manually importing the ACK (where a product instance is in an air-gapped network).

Note Account information is not displayed if the product instance is managed by Cisco vManage. In this case, account information is maintained and displayed in the **License Management** page of the Cisco vManage menu.

Examples

For information about fields shown in the display, see Table 13: show license status Field Descriptions, on page 300

For sample output, see:

- Example: show license status (Cisco Catalyst 8300 Series Edge Platforms), on page 305
- Example: show license status (Cisco 4000 Series Integrated Services Routers), on page 306.

Table 13: show license status Field Descriptions

Field		Description
Utility	Header for utility settings that are configured on the product instance.	
	Status:	Status
	Utility report:	Last attempt:
	Customer Information:	The following fields are displayed: • Id: • Name: • Street • City: • State: • Country: • Postal Code:
Smart Licensing Using Policy:	Header for policy settings on the product instance.	
	Status:	Indicates if Smart Licensing Using Policy is enabled. Smart Licensing Using Policy is supported starting from Cisco IOS XE Amsterdam 17.3.2 and is always enabled on supported software images.
Account Information:	Header for account information that the product instance belongs to, in CSSM. This section is displayed only if the software version on the product instance is Cisco IOS XE Cupertino 17.7.1a or a later release. If an ACK is not installed on the product instance, these fields display `<none>`.	
	Smart Account:	The Smart Account that the product instance is part of. This information is always as per the latest available ACK on the product instance.
	Virtual Account:	The Virtual Account that the product instance is part of. This information is always as per the latest available ACK on the product instance.

Field		Description
Data Privacy:	Header for privacy settings that are configured on the product instance.	
	Sending Hostname:	A *yes* or *no* value which shows if the hostname is sent in usage reports.
	Callhome hostname privacy:	Indicates if the Call Home feature is configured as the mode of transport for reporting. If configured, one of these values is displayed: • ENABLED • DISABLED
	Smart Licensing hostname privacy:	One of these values is displayed: • ENABLED • DISABLED
	Version privacy:	One of these values is displayed: • ENABLED • DISABLED
Transport:	Header for transport settings that are configured on the product instance.	
	Type:	Mode of transport that is in use. Additional fields are displayed for certain transport modes. For example, if transport type is set to CSLU, the CSLU address is also displayed.

Field		Description
Policy:	Header for policy information that is applicable to the product instance.	
	Policy in use:	Policy that is applied This can be one of the following: Cisco default, Product default, Permanent License Reservation, Specific License Reservation, PAK license, Installed on <date>, Controller.
	Policy name:	Name of the policy
	Reporting ACK required:	A *yes* or *no* value which specifies if the report for this product instance requires CSSM acknowledgement (ACK) or not. The default policy is always set to "yes".
	Perpetual Attributes	Policy values for perpetual licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name
	Subscription Attributes:	Policy values for subscription licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name
	Enforced License Attributes:	

Field		Description
		Policy values for subscription licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name
	Export License Attributes:	Policy values for subscription licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name
Miscellaneous	Header for custom ID.	
	Custom Id:	ID

Field		Description
Usage Reporting:	Header for usage reporting (RUM reports) information.	
	Last ACK received:	Date and time of last ACK received, in the local time zone.
	Next ACK deadline:	Date and time for next ACK. If the policy states that an ACK is not requires then this field displays `none`. **Note** If an ACK is required and is not received by this deadline, a syslog is displayed.
	Reporting Interval:	Reporting interval in days The value displayed here depends on you configure the **license smart usage interval***interval_in_days* and the policy value. For more information, see the corresponding Syntax Description: license smart (global config), on page 249.
	Next ACK push check:	Date and time when the product instance will submit the next polling request for an ACK. Date and time are in the local time zone. This applies only to product instance- initiated communication to CSSM or CSLU. If the reporting interval is zero, or if no ACK polling is pending, then this field displays `none`.
	Next report push:	Date and time when the product instance will send the next RUM report. Date and time are in the local time zone. If the reporting interval is zero, or if there are no pending RUM reports, then this field displays `none`.
	Last report push:	Date and time for when the product instance sent the last RUM report. Date and time are in the local time zone.
	Last report file write:	Date and time for when the product instance last saved an offline RUM report. Date and time are in the local time zone.
	Last report pull:	Date and time for when usage reporting information was retrieved using data models. Date and time are in the local time zone.

Field		Description
Trust Code Installed:	Header for trust code-related information. Displays date and time if trust code is installed. Date and time are in the local time zone. If a trust code is not installed, then this field displays `none`.	
	Active:	Active product instance. In a High Availability set-up, the the UDIs of all product instances in the set-up, along with corresponding trust code installation dates and times are displayed.
	Standby:	Standby product instance.
	Member:	Member product instance

Example: show license status (Cisco Catalyst 8300 Series Edge Platforms)

The following is sample output of the **show license status** command, on a product instance where the software version is Cisco IOS XE Cupertino 17.7.1a. The account information as in the last installed ACK is displayed (Last ACK received: Dec 03 08:34:58 2021 UTC):

```
Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: Eg-SA As of Dec 03 15:26:02 2021 UTC
  Virtual Account: Eg-VA

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

Policy:
  Policy in use: Installed On Dec 03 08:23:45 2021 UTC
  Policy name: SLE Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
```

```
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 111 (Customer Policy)
    Report on change (days): 111 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: Dec 03 08:34:58 2021 UTC
  Next ACK deadline: Jan 02 08:34:58 2022 UTC
  Reporting push interval: 30  days
  Next ACK push check: Dec 07 08:31:32 2021 UTC
  Next report push: Jan 02 08:30:57 2022 UTC
  Last report push: Dec 03 08:30:57 2021 UTC
  Last report file write: <none>

Trust Code Installed: Dec 03 08:23:45 2021 UTC
```

Example: show license status (Cisco 4000 Series Integrated Services Routers)

The following is sample output of the **show license status** command on a Cisco 4000 Series Integrated Services Router.

```
Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Policy:
  Policy in use: Installed On Oct 29 21:43:33 2020 UTC
  Policy name: SLP Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 60 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 30 (Customer Policy)
```

```
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: Oct 23 23:36:38 2020 UTC
  Next ACK deadline: Dec 22 23:36:38 2020 UTC
  Reporting push interval: 30  days
  Next ACK push check: Oct 30 05:45:45 2020 UTC
  Next report push: Nov 22 23:32:38 2020 UTC
  Last report push: Oct 23 23:32:38 2020 UTC
  Last report file write: <none>

Trust Code Installed: Oct 09 17:56:19 2020 UTC
```

show license summary

To display a brief summary of license usage, which includes information about licenses being used, the count, and status, enter the **show license summary** command in Privileged EXEC mode.

show license summary

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2	Command output was updated to reflect valid license status for Smart Licensing Using Policy. Valid license statuses include: `IN USE`, `NOT IN USE`, `NOT AUTHORIZED`. Command output was also updated to remove registration and authorization information. Command output no longer displays Smart Account and Virtual account information.
Cisco IOS XE Cupertino 17.7.1a	Command output was updated to display Smart Account and Virtual account information.

Usage Guidelines

Account Information in the output

Starting with Cisco IOS XE Cupertino 17.7.1a, every ACK includes the Smart Account and Virtual Account that was reported to, in CSSM. When it receives the ACK, the product instance securely stores only the latest version of this information - as determined by the timestamp in the ACK. The Smart Account and Virtual Account information that is displayed in the `Account Information` section of this command's output is therefore always as per the latest available ACK on the product instance.

If a product instance is moved from one Smart Account and Virtual Account to another, the next ACK after the move will have this updated information. The output of this command is updated once this ACK is available on the product instance.

The ACK may be received directly (where the product instance is connected to CSSM), or indirectly (where the product instance is connect to CSSM through CSLU, Cisco DNA Center, or SSM On-Prem), or by manually importing the ACK (where a product instance is in an air-gapped network).

Note Account information is not displayed if the product instance is managed by Cisco vManage. In this case, account information is maintained and displayed in the **License Management** page of the Cisco vManage menu.

Examples

For information about fields shown in the display, see Table 14: show license summary Field Descriptions, on page 308

For sample outputs, see:

- Example: show license summary: Displaying Account Information (Catalyst 8200 Series Edge Platform), on page 309
- Example: show license summary: All IN USE (Cisco 4000 Series Integrated Services Routers), on page 309

Table 14: show license summary Field Descriptions

Field	Description
Account Information: Smart Account: Virtual Account:	The Smart Account and Virtual Account that the product instance is part of is always as per the latest available ACK on the product instance. This field is displayed only if the software version on the product instance Cupertino 17.7.1a or a later release. If an ACK is not installed on the product instance, these fields display <n
License	Name of the licenses in use
Entitlement Tag	Short name for license
Count	License count

Field	Description
Status	License status can be one of the following • In-Use: Valid license, and in-use. • Not In-Use • Not Authorized: Means that the license requires installation of S more information, see Authorization Code, on page 4

Example: show license summary: Displaying Account Information (Catalyst 8200 Series Edge Platform)

The following is sample output of the **show license summary** command, on a product instance where the software version is Cisco IOS XE Cupertino 17.7.1a.

```
Device# show license summary

Account Information:
  Smart Account: Eg-SA As of Dec 03 15:26:02 2021 UTC
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage_T2    (NWSTACK_T2_A)                    1 IN USE
  dna-advantage_T2        (DSTACK_T2_A)                     1 IN USE
  Router US Export Lic... (DNA_HSEC)                        1 IN USE
```

Example: show license summary: All IN USE (Cisco 4000 Series Integrated Services Routers)

The following is sample output of the **show license summary** command where all licenses are in-use.

```
Devide# show license summary
License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  hseck9                  (ISR_4331_Hsec)                   1 IN USE
  booster_performance     (ISR_4331_BOOST)                  1 IN USE
  appxk9                  (ISR_4331_Application)            1 IN USE
  uck9                    (ISR_4331_UnifiedCommun...)       1 IN USE
  securityk9              (ISR_4331_Security)               1 IN USE
```

show license tech

To display licensing information to help the technical support team, enter the **show license tech** command in privileged EXEC mode. The output for this command includes outputs of several other **show license** commands and more.

show license tech { **message** | **rum** { **feature** { *license_name* | **all** } | **id** { *rum_id* | **all** } } [**detail**] [**save** *path*] | **support** }

Syntax Description

message	Displays messages concerning trust establishment, usage reporting, result polling, authorization code requests and returns, and trust synchronization. This is the same information as displayed in the output of the **show license history message** command.
rum { **feature** { *license_name* | **all** } | **id** { *rum_id* | **all** } } [**detail**] [**save** *path*]	Displays information about Resource Utilization Measurement reports (RUM reports) on the product instance, including report IDs, the current processing state of a report, error information (if any), and an option save the displayed RUM report information. **Note** This option saves the information *about* RUM reports and is not for reporting purposes. It does not save the RUM report, which is an XML file containing usage information.
support	Displays licensing information that helps the technical support team to debug a problem.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2.	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2.	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy.
Cisco IOS XE Cupertino 17.7.1a	The **rum** keyword and additional options under this keyword were added: { **feature** { *license_name* | **all** } | **id** { *rum_id* | **all** } } The output of the **show license tech support** command was enhanced to display the following information: • RUM report information, in section `License Usage` and `Usage Report Summary`. • Smart Account and Virtual account information, in section `Account Information:`. The **data conversion**, **eventlog** and **reservation** keywords were removed from this command. They continue to be available as separate show commands, that is, **show license data**, **show license eventlog**, and **show license reservation** respectively.

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing (whether smart licensing is enabled, all associated licensing certificates, compliance status, and so on).

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2 or a later release, command output displays fields pertinent to Smart Licensing Using Policy. Note the following guidelines:

- Troubleshooting with a Support Representative

  When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

- RUM Report Information in the output

  - The output of the **show license tech support** command displays the following sections pertaining to RUM reports:

    Table 15: show license tech support: Field Descriptions for Header "License Usage", on page 311

```
<output truncated>
License Usage
=============
 Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 1
      Current Report: 1638518487       Previous: 1638518484
<output truncated>
```

Table 15: show license tech support: Field Descriptions for Header "License Usage"

Field Name	Description
Interval:	This is a fixed measurement duration and is always 15 minutes.
Current Value:	Information about the current license count.
Current Report:	ID of the currently OPEN report for the license.
Previous:	ID of the last OPEN report for the license. This report will have state CLOSED now.

  - Table 16: show license tech support: Field Descriptions for Header "Usage Report Summary", on page 312

```
<output truncated>
Usage Report Summary:
=====================
Total: 10,  Purged: 0(0)
Total Acknowledged Received: 3,  Waiting for Ack: 2(7)
Available to Report: 3  Collecting Data: 3
Maximum Display: 10  In Storage: 7,  MIA: 0(0)
Report Module Status: Ready
<output truncated>
```

Table 16: show license tech support: Field Descriptions for Header "Usage Report Summary"

Field Name	Description
Total:	Total number of reports that the product instance has ever generated. **Note** This total does not refer to the total number of reports *currently available* on and being tracked by the product instance. For this you must sum up the `Total Acknowledged Received:` and `Available to Report` fields.
Purged:	The number of reports deleted due to a system resource limitation. This number includes RUM reports where the product instance no longer has tracking information.
Total Acknowledged Received:	The number of RUM reports acknowledged on this product instance.
Waiting for Ack:	The number of RUM reports waiting for an ACK. This is the total number of reports in an `UNACK` state, where the product instance still has tracking information.
Available to Report:	The number of RUM reports that are available to send to CSSM. This is the total number of reports in an `OPEN` or `CLOSED` state, where the product instance still has tracking information.
Collecting Data:	Number of reports where the product instance is currently collecting measurements.
Maximum Display:	Number of reports available for display in a **show** command's output.
In Storage:	Number of reports currently stored on the disk
MIA:	The number of reports missing.

- The output of the **show license tech rum** command with the **detail** option, displays the following fields pertaining to RUM reports: Table 17: show license tech rum: Field Descriptions for Header "Smart Licensing Usage Report Detail", on page 313

```
<output truncated>
Smart Licensing Usage Report Detail:
====================================
Report Id: 1638518477
  Metric Name: ENTITLEMENT
  Feature Name: network-advantage_10M
  Metric Value:
regid.2018-12.com.cisco.ESR_P_10M_A,1.0_8946a476-b904-4d0a-9d0b-2b1e5de891a3
  UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
  Previous Report Id: 0,    Next Report Id: 1638518479
  Version: 2.0
  State: UNACK,      State Change Reason: REPORTING
  Start Time: Dec 03 08:12:05 2021 UTC,      End Time: Dec 03 08:12:06 2021 UTC
  Storage State: EXIST,  Storage State Change Reason: None
```

```
  Transaction ID: 715896687973761034
  Transaction Message: <none>
  Report Size: 1129(947)
<output truncated>
```

The options available under the **show license tech rum** keyword are the same as the options available with the **show license rum** privileged EXEC command. The sample output that is displayed in the *simplified view* is also the same. But if you use the **detail** keyword (for example if you enter **show license tech rum feature** *license_name* **detail**), the detailed view is displayed and this has a few *additional* fields when compared to **show license rum**.

Table 17: show license tech rum: Field Descriptions for Header "Smart Licensing Usage Report Detail"

Field Name	Description
Version:	Displays the format of the report during transmission. Starting with Cisco IOS XE Cupertino 17.7.1a, RUM reports are stored in a new format that reduces processing time. This field indicates if the product instance is using the old format or the new format.
Storage State:	Indicates if a given report is currently in storage. In addition to the displaying the current storage state of the RUM report, with these possible values: EXIST, DELETED, PURGED, MISSING, if a "(1)" is displayed next to the label (`Storage State (1)`), this means the RUM report is in the older (pre-17.7.1a format) and will be processed accordingly. If the RUM report is in the new format, the field is displayed as `Storage State` - without any extra information.
Storage State Change Reason:	Displays the reason for the change in the storage state change. Not all state changes provide a reason. • NONE: This means no reason was recorded for the the storage state change. • PROCESSED: This means the RUM report was deleted after CISCO has processed the data. • LIMIT_STORAGE: This means the RUM report was deleted because the product instance reached it's storage limit. • LIMIT_TIME: This means the RUM report was deleted because the report reached the persisted time limit.
Transaction ID: Transaction Message:	If the transaction ID displays a correlation ID and an error status is displayed, the product instance displays the error code field in this section. If there are no errors, no data is displayed here.

Field Name	Description
Report Size	This field displays two numbers. The first number is the size of raw report for communication, in bytes. The second number is the disk space used for saving the report, also in bytes. The second number is displayed only if report is stored in the new format.

Examples

show license tech support on Catalyst 8300 Series Edge Platforms, on page 314

show license tech support on Catalyst 8300 Series Edge Platforms

The following is sample output of the **show license tech support** command on a Catalyst 8300 Series Edge router running Cisco IOS XE Cupertino 17.7.1a.

```
Device# show license tech support

Smart Licensing Tech Support info

Smart Licensing Status
======================

Smart Licensing is ENABLED

License Conversion:
  Automatic Conversion Enabled: True
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: Eg-SA As of Dec 03 15:26:02 2021 UTC
  Virtual Account: Eg-VA

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Address: <empty>
    Port: <empty>
    Username: <empty>
    Password: <empty>
  Server Identity Check: True
```

```
  VRF: <empty>

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Installed On Dec 03 08:23:45 2021 UTC
  Policy name: SLE Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 111 (Customer Policy)
    Report on change (days): 111 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)

Usage Reporting:
  Last ACK received: Dec 03 08:34:58 2021 UTC
  Next ACK deadline: Jan 02 08:34:58 2022 UTC
  Reporting push interval: 30  days State(4) InPolicy(30)
  Next ACK push check: Dec 07 08:31:32 2021 UTC
  Next report push: Jan 02 08:30:57 2022 UTC
  Last report push: Dec 03 08:30:57 2021 UTC
  Last report file write: <none>

License Usage
=============
Handle: 1
  License: network-advantage_T2
  Entitlement Tag:
regid.2020-10.com.cisco.NWSTACK_T2_A,1.0_83edc508-0ee4-468e-8962-0a4fde995e80
  Description: network-advantage_T2
  Count: 1
  Version: 1.0
  Status: IN USE(15)
  Status time: Dec 03 08:28:54 2021 UTC
  Request Time: Dec 03 08:28:54 2021 UTC
  Export status: NOT RESTRICTED
  Feature Name: network-advantage_T2
  Feature Description: network-advantage_T2
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 1
      Current Report: 1638518485       Previous: 1638518482
  Soft Enforced: True

Handle: 2
  License: dna-advantage_T2
  Entitlement Tag:
regid.2020-10.com.cisco.DSTACK_T2_A,1.0_b072e613-aa2c-4ed0-ab46-ae91ddc7dfb5
  Description: dna-advantage_T2
```

```
  Count: 1
  Version: 1.0
  Status: IN USE(15)
  Status time: Dec 03 08:28:54 2021 UTC
  Request Time: Dec 03 08:28:54 2021 UTC
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage_T2
  Feature Description: dna-advantage_T2
  Enforcement type: NOT ENFORCED
  License type: Subscription
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 1
      Current Report: 1638518486       Previous: 1638518483
  Soft Enforced: True

Handle: 3
  License: Router US Export Lic. for DNA
  Entitlement Tag: regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844

  Description: U.S. Export Restriction Compliance license for DNA based Routers
  Count: 1
  Version: 1.0
  Status: IN USE(15)
  Status time: Dec 03 08:28:57 2021 UTC
  Request Time: Dec 03 08:28:57 2021 UTC
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Export
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 1
      Current Report: 1638518487       Previous: 1638518484

Product Information
===================
UDI: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5

Agent Version
=============
Smart Agent for Licensing: 5.3.16_rel/55

Upcoming Scheduled Jobs
=======================
Current time: Dec 07 02:12:02 2021 UTC
Daily: Dec 07 08:28:52 2021 UTC (6 hours, 16 minutes, 50 seconds remaining)
Authorization Renewal: Expired Not Rescheduled
Init Flag Check: Expired Not Rescheduled
Reservation configuration mismatch between nodes in HA mode: Expired Not Rescheduled
Retrieve data processing result: Dec 07 08:31:32 2021 UTC (6 hours, 19 minutes, 30 seconds
 remaining)
Start Utility Measurements: Dec 07 02:15:57 2021 UTC (3 minutes, 55 seconds remaining)
Send Utility RUM reports: Jan 02 08:30:56 2022 UTC (26 days, 6 hours, 18 minutes, 54 seconds
 remaining)
Save unreported RUM Reports: Dec 07 03:01:07 2021 UTC (49 minutes, 5 seconds remaining)
Process Utility RUM reports: Dec 07 08:39:57 2021 UTC (6 hours, 27 minutes, 55 seconds
remaining)
External Event: Jan 02 08:34:57 2022 UTC (26 days, 6 hours, 22 minutes, 55 seconds remaining)
Operational Model: Expired Not Rescheduled
```

```
Communication Statistics:
=========================
Communication Level Allowed: DIRECT
Overall State: <empty>
Trust Establishment:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Acknowledgement:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Usage Reporting:
  Attempts: Total=1, Success=1, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: OK_POLL on Dec 03 08:30:56 2021 UTC
    Failure Reason: <none>
  Last Success Time: Dec 03 08:30:56 2021 UTC
  Last Failure Time: <none>
Result Polling:
  Attempts: Total=5, Success=1, Fail=4  Ongoing Failure: Overall=3 Communication=0
  Last Response: INVALID STATUS CODE on Dec 06 08:31:32 2021 UTC
    Failure Reason: Invalid Polling Id 4294967295 provided in the polling request
  Last Success Time: Dec 03 08:34:58 2021 UTC
  Last Failure Time: Dec 06 08:31:32 2021 UTC
Authorization Request:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Confirmation:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Return:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Sync:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Hello Message:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>

License Certificates
====================
Production Cert: True
Not registered. No certificates installed
```

```
HA Info
==========
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: True

Reservation Info
================
License reservation: DISABLED

Overall status:
  Active: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
      Reservation status: SMART AUTHORIZATION INSTALLED on Dec 03 08:24:35 2021 UTC
      Request code: <none>
      Last return code: <none>
      Last Confirmation code: 418b11b3
      Reservation authorization code:
<smartLicenseAuthorization><udi>P:C8300-1N1S-4T2X,S:FDO2250A0J5</udi><authorizationCode><customerInfo><smartAccount>BU
 Production
[redacted]
 US Export Lic. for DNA</displayName><tagDescription>U.S. Export Restriction Compliance
license for DNA based
[redacted]


Authorizations:
  Router US Export Lic. for DNA (DNA_HSEC):
    Description: U.S. Export Restriction Compliance license for DNA based Routers
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Start Date: <none>
          End Date: <none>
          Term Count: 1
          Subscription ID: <none>

Purchased Licenses:
  No Purchase Information Available

Usage Report Summary:
=====================
Total: 10,  Purged: 0(0)
Total Acknowledged Received: 3,  Waiting for Ack: 2(7)
Available to Report: 3  Collecting Data: 3
Maximum Display: 10  In Storage: 7,  MIA: 0(0)
Report Module Status: Ready

Other Info
==========
Software ID: regid.2020-05.com.cisco.C8300BE,1.0_5b66594f-27ab-4615-9d15-4aad4969497f
Agent State: authorized
TS enable: True
Transport: Smart
  Default URL: https://smartreceiver.cisco.com/licservice/license
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
```

```
Privacy Send IP: True
Build type:: Production
sizeof(char)  : 1
sizeof(int)   : 4
sizeof(long)  : 4
sizeof(char *): 8
sizeof(time_t): 4
sizeof(size_t): 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: True
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN, POLICY_USAGE
Check Point Interface: True
Config Management Interface: False
License Map Interface: True
HA Interface: True
Trusted Store Interface: True
Platform Data Interface: True
Crypto Version 2 Interface: False
SAPluginMgmtInterfaceMutex: True
SAPluginMgmtIPDomainName: True
SmartTransportVRFSupport: True
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartTransportServerIdCheck: True
SmartTransportProxySupport: True
SmartAgentPolicyDisplayFormat: 0
SmartAgentReportOnUpgrade: False
SmartAgentIndividualRUMEncrypt: 2
SmartAgentMaxRumMemory: 50
SmartAgentConcurrentThreadMax: 10
SmartAgentPolicyControllerModel: False
SmartAgentPolicyModel: True
SmartAgentFederalLicense: True
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: True
conversionAllowed: True
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
HighAvailabilityOverrideEvent: UnknownPlatformEvent
platformIndependentOverrideEvent: UnknownPlatformEvent
platformOverrideEvent: UnknownPlatformEvent
```

```
WaitForHaRole: False
standbyIsHot: False
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 11 KB
Local Device: P:C8300-1N1S-4T2X,S:FDO2250A0J5, state[2], Trust Data INSTALLED  TrustId:256
Overall Trust: INSTALLED (2)
Clock sync-ed with NTP: False

Platform Provided Mapping Table
===============================
  C8300-1N1S-4T2X: Total licenses found: 2595
Enforced Licenses:
  P:C8300-1N1S-4T2X,S:FDO2250A0J5:
    hseck9: regid.2019-03.com.cisco.DNA_HSEC,1.0_509c41ab-05a8-431f-95fe-ec28086e8844 (3)
    hseck9:  (3)
```

show license udi

To display UDI information for a product instance, enter the **show license udi** command in Privileged EXEC mode. In a High Availability set-up, the output displays UDI information for all connected product instances.

show license UDI

This command has no arguments or keywords.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2	This command was introduced.

Examples

The following are sample outputs of the **show license summary** command, on various Cisco product instances, and various set-ups.

- Example: show license udi with standalone (Cisco 4000 Series Integrated Services Router), on page 320
- Example: show license udi with active and standby (Cisco Catalyst 8000 Edge Platforms Family), on page 321

Example: show license udi with standalone (Cisco 4000 Series Integrated Services Router)

The following is sample output from the **show license udi** command on a product instance with a single RP.

```
Device# show license udi
```

```
UDI: PID:ISR4331/K9,SN:FDO224917Q6
```

Example: show license udi with active and standby (Cisco Catalyst 8000 Edge Platforms Family)

The following is sample output from the **show license udi** command in a High Availability set-up where an active and a standby product instances exist. UDI information is displayed for both.

```
Device# show license udi

UDI: PID:C8500L-8S4X,SN:JAD2331191E
HA UDI List:
    Active:PID:C8500L-8S4X,SN:JAD2331191E
    Standby:PID:C8500L-8S4X,SN:JAD2331191E
```

show license usage

To display license information for all licenses on a product instance, enter the **show license usage** command in privileged EXEC mode.

show license usage

This command has no arguments or keywords.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes the `Status`, `Enforcement type` fields. Command output was also updated to remove reservation related information, authorization status information, and export status information.

Examples

The following are sample outputs of the **show license usage** command on various product instances. See Table 18: show license usage Field Descriptions, on page 322 for information about fields shown in the display.

- Example: show license usage with unenforced and export-controlled licenses (Cisco 4000 Series Integrated Services Routers), on page 323
- Example: show license usage with unenforced licenses (Cisco Catalyst 9500 Series Switches), on page 324

Table 18: show license usage Field Descriptions

Field	Description
License Authorization: Status:	Displays overall authorization status.
():	Name of the license as in CSSM. If this license is one that requires an authorization code, the name of the li the code.
Description	Description of the license as in CSSM.
Count	License count. If the license is not in-use, the count is reflected as zero.
Version	Version.
Status	License status can be one of the following • In-Use: Valid license, and in-use. • Not In-Use • Not Authorized: Means that the license requires installation of SLA more information, see Authorization Code, on page 4
Export Status:	Indicates if this license is export-controlled or not. Accordingly, one of the is displayed: • RESTRICTED - ALLOWED • RESTRICTED - NOT ALLOWED • NOT RESTRICTED
Feature name	Name of the feature that uses this license.
Feature Description:	Description of the feature that uses this license.
Enforcement type	Enforcement type status for the license. This may be one of the followin • ENFORCED • NOT ENFORCED • EXPORT RESTRICTED - ALLOWED • EXPORT RESTRICTED - NOT ALLOWED For more information about enforcement types, see License Enforcemen 3

Example: show license usage with unenforced and export-controlled licenses (Cisco 4000 Series Integrated Services Routers)

The following is sample output of the **show license usage** command. Unenforced and export-controlled licenses are in-use here.

```
Device# show license usage

License Authorization:
  Status: Not Applicable

hseck9 (ISR_4331_Hsec):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED

booster_performance (ISR_4331_BOOST):
  Description: booster_performance
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: booster_performance
  Feature Description: booster_performance
  Enforcement type: NOT ENFORCED

appxk9 (ISR_4331_Application):
  Description: appxk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: appxk9
  Feature Description: appxk9
  Enforcement type: NOT ENFORCED

uck9 (ISR_4331_UnifiedCommunication):
  Description: uck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: uck9
  Feature Description: uck9
  Enforcement type: NOT ENFORCED

securityk9 (ISR_4331_Security):
  Description: securityk9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: securityk9
  Feature Description: securityk9
  Enforcement type: NOT ENFORCED
```

Example: show license usage with unenforced licenses (Cisco Catalyst 9500 Series Switches)

The following is sample output of the **show license usage** command. Only unenforced licenses are in-use here.

```
Device# show license usage
Load for five secs: 1%/0%; one minute: 0%; five minutes: 0%
No time source, 12:59:18.941 EDT Fri Sep 11 2020

License Authorization:
  Status: Not Applicable
network-advantage (C9500 Network Advantage):
  Description: C9500 Network Advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: C9500 Network Advantage
  Enforcement type: NOT ENFORCED
dna-essentials (C9500 24Y4C DNA Essentials):
  Description: C9500-24Y4C DNA Essentials
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-essentials
  Feature Description: C9500-24Y4C DNA Essentials
  Enforcement type: NOT ENFORCED
```

show platform software sl-infra

To display troubleshooting information and for debugging, enter the **show platform software sl-infra** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting and debugging.

show platform software sl-infra { **all** | **current** | **debug** | **stored** }

Syntax Description

all	Displays current, debugging, and stored information.
current	Displays current license-related information.
debug	Enables debugging
stored	Displays information that is stored on the product instance.

Command Modes

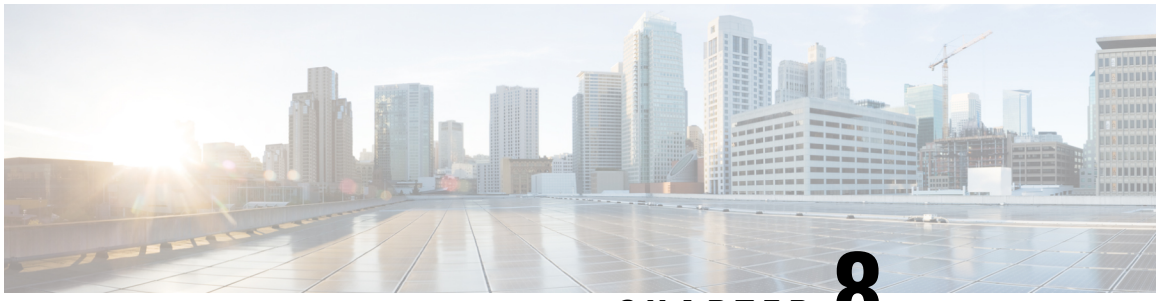
Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2	This command was introduced.

Usage Guidelines

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.



CHAPTER 8

Troubleshooting Smart Licensing Using Policy

- System Message Overview, on page 327
- Smart Licensing Using Policy System Messages, on page 328

System Message Overview

This section describes Smart Licensing Using Policy specific system messages. The system software sends these messages to the console (and, optionally, to a logging server on another system). Not all system messages mean problems with your system. Some messages are informational, and others can help diagnose problems with communications lines, internal hardware, or the system software.

How to Read System Messages

System log messages can contain up to 80 characters. Each system message begins with a percent sign (%) and is structured as follows:

```
%FACILITY-SEVERITY-MNEMONIC: Message-text
```

%FACILITY

Two or more uppercase letters that show the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software

SEVERITY

A single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation.

Table 19: Message Severity Levels

Severity Level	Description
0 - emergency	System is unusable.
1 - alert	Immediate action required.
2 - critical	Critical condition.
3 - error	Error condition.

Severity Level	Description
4 - warning	Warning condition.
5 - notification	Normal but significant condition.
6 - informational	Informational message only.
7 - debugging	Message that appears during debugging only.

MNEMONIC

A code that uniquely identifies the message.

Message-text

Message-text is a text string describing the condition. This portion of the message sometimes contains detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because the information in these variable fields changes from message to message, it is represented here by short strings enclosed in square brackets ([ ]). A decimal number, for example, is represented as [dec].

Table 20: Variable Fields in Messages

Severity Level	Description
[char]	Single character
[chars]	Character string
[dec]	Decimal number
[enet]	Ethernet address (for example, 0000.FEED.00C0)
[hex]	Hexadecimal number
[inet]	Internet address (for example, 10.0.2.16)
[int]	Integer
[node]	Address or node name
[t-line]	Terminal line number in octal (or in decimal if the decimal-TTY service is enabled)
[clock]	Clock (for example, 01:20:08 UTC Tue Mar 2 1993

Smart Licensing Using Policy System Messages

This section provides the list of Smart Licensing Using Policy related system messages you may encounter, possible reasons (incase it is a failure message), and recommended action (if action is required).

- %SMART_LIC-3-POLICY_INSTALL_FAILED
- %SMART_LIC-3-AUTHORIZATION_INSTALL_FAILED

- %SMART_LIC-3-COMM_FAILED
- %SMART_LIC-3-COMM_RESTORED
- %SMART_LIC-3-POLICY_REMOVED
- %SMART_LIC-3-TRUST_CODE_INSTALL_FAILED
- %SMART_LIC-4-REPORTING_NOT_SUPPORTED
- %SMART_LIC-6-POLICY_INSTALL_SUCCESS
- %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS
- %SMART_LIC-6-AUTHORIZATION_REMOVED
- %SMART_LIC-6-REPORTING_REQUIRED
- %SMART_LIC-6-TRUST_CODE_INSTALL_SUCCESS
- %SMART_LIC-4- UTILITY_TRUST_CODE
- %SMART_LIC-4-UTILITY_SUBSCRIPTION_LICENSE
- %SMART_LIC-4-UTILITY_NO_ACK
- %SMART_LIC-4-UTILITY_TRANSPORT_NOT_CONFIG
- %SMART_LIC-3-UTILITY_REPORT_FAILED
- %SMART_LIC-3-UTILITY_STARTED
- %SMART_LIC-6-UTILITY_STOPPED

```
Error Message %SMART_LIC-3-POLICY_INSTALL_FAILED: The installation of a new
licensing policy has failed: [chars].
```

Explanation: A policy was installed, but an error was detected while parsing the policy code, and installation failed. [chars] is the error string with details of the failure.

Possible reasons for failure include:

- A signature mismatch: This means that the system clock is not accurate.
- A timestamp mismatch: This means the system clock on the product instance is not synchronized with CSSM.

Recommended Action:

For both possible failure reasons, ensure that the system clock is accurate and synchronized with CSSM. Configure the **ntp server** command in global configuration mode. For example:

```
Device(config)# ntp server 198.51.100.100 version 2 prefer
```

If the above does not work and policy installation still fails, contact your Cisco technical support representative.


```
Error Message %SMART_LIC-3-AUTHORIZATION_INSTALL_FAILED: The install of a new
licensing authorization code has failed on [chars]: [chars].
```

Explanation: An authorization code was installed, but installation failed. The first [chars] is the UDI for which the authorization code installation failed, and the second [chars] is the error string with details of the failure.

Possible reasons for failure include:

- Not enough licenses with authorization for currently configured features: This means that you have not generated the requisite authorizations for all the required licenses.
- UDI mismatch: One or more UDIs in the authorization code file do not match with the product instance where you are installing the authorization code file. If you have generated authorization codes for multiple UDIs, for a High Availability set-up, all the UDIs listed in the authorization code file must match with all the UDIs in the High Availability set-up. If this is not the case, installation fails.

  Cross-check all UDIs in the authorizatin code file against the UDIs of the product instance (standalone or High Availability) as follows:

  Sample authorization code file with UDI information:

  ```
  <smartLicenseAuthorization>
  <udi>P:CSR1000V,S:9D1YXJM3LKC</udi>

  <output truncated>
  </smartLicenseAuthorization>
  ```

  Sample output of UDI information on a product instance:

  ```
  Device# show license udi
  UDI: PID:CSR1000V,SN:9D1YXJM3LKC
  ```

- A signature mismatch: This means that the system clock is not accurate.

Recommended Action

- In the output of the **show license tech support** command, check the `Failure Reason:` field to understand what may have gone wrong.

  ```
  Device# show license tech support
  <output truncated>
  Authorization Confirmation:
    Attempts: Total=2, Success=2, Fail=0  Ongoing Failure: Overall=0 Communication=0
    Last Response: OK on Sep 23 17:51:52 2020 UTC
      Failure Reason: <none>
    Last Success Time: Sep 23 17:51:52 2020 UTC
    Last Failure Time: <none>
  ```

- Not enough licenses in authorization for currently configured features and UDI mismatch:

  Use the **show license udi** command to verify that you have the correct and complete list of UDIs. This command displays all product instances in case of High Availability set-up. Then complete these tasks again: Generating and Downloading SLAC from CSSM to a File, on page 199 and Installing a File on the Product Instance, on page 215.

- Signature mismatch:

  Ensure that the system clock is accurate and synchronized with CSSM. To do this, configure the **ntp server** command in global configuration mode. For example:

  ```
  Device(config)# ntp server 198.51.100.100 version 2 prefer
  ```

If the above does not work and policy installation still fails, contact your Cisco technical support representative.

```
Error Message %SMART_LIC-3-COMM_FAILED: Communications failure with the [chars] :
[chars]
```

Explanation: Smart Licensing communication either with CSSM, or CSLU, or SSM On-Prem failed. The first [chars] is the currently configured transport type, and the second [chars] is the error string with details of the failure. This message appears for every communication attempt that fails.

Possible reasons for failure include:

- CSSM, CSLU, SSM On-Prem is not reachable: This means that there is a network reachability problem.
- 404 host not found: This means the CSSM server is down.
- A TLS or SSL handshake failure caused by a missing client certificate. The certificate is required for TLS authentication of the two communicating sides. A recent server upgrade may have cause the certificate to be removed. This reason applies only to a topology where the product instance is directly connected to CSSM.

Note If the error message is displayed for this reason, there is no actual configuration error or disruption in the communication with CSSM.

For topologies where the product instance initiates the sending of RUM reports (Connected to CSSM Through CSLU: Product Instance-Initiated Communication, Connected Directly to CSSM, CSLU Disconnected from CSSM: Product Instance-Initiated Communication, and SSM On-Prem Deployment: Product Instance-Initiated Communication) if this communication failure message coincides with scheduled reporting (**license smart usage interval** *interval_in_days* global configuration command), the product instance attempts to send out the RUM report for up to four hours after the scheduled time has expired. If it is still unable to send out the report (because the communication failure persists), the system resets the interval to 15 minutes. Once the communication failure is resolved, the system reverts the reporting interval to last configured value.

Recommended Action:

Troubleshooting steps are provided for when CSSM is not reachable or there is a missing client certificate, when CSLU is not reachable, and when SSM On-Prem is not reachable.

- If a client certificate is missing and there is no actual configuration error or disruption in the communication with CSSM:

  Configure the **ip http client secure-trustpoint** *trustpoint-name* command in global configuration mode. For *trustpoint-name*, enter only `SLA-TrustPoint`. This command specifies that the secure HTTP client should use the certificate associated with the trustpoint indicated by the trustpoint-name argument.

- If CSSM is not reachable and the configured transport type is **smart**:

  1. Check if the smart URL is configured correctly. Use the **show license status** command in privileged EXEC mode, to check if the URL is exactly as follows: https://smartreceiver.cisco.com/licservice/license. If it is not, reconfigure the **license smart url smart** *smar_URL* command in global configuration mode.
  2. Check DNS resolution. Verify that the product instance can ping `smartreceiver.cisco.com` or the nslookup translated IP. The following example shows how to ping the translated IP

```
Device# ping 171.70.168.183
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 171.70.168.183, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

- If CSSM is not reachable and the configured transport type is **callhome**:

  1. Check if the URL is entered correctly. Use the **show license status** command in privileged EXEC mode, to check if the URL is exactly as follows: https://tools.cisco.com/its/service/oddce/services/DDCEService.
  2. Check if Call Home profile `CiscoTAC-1` is active and destination URL is correct. Use the **show call-home profile all** command in privileged EXEC mode:

     ```
     Current smart-licensing transport settings:
      Smart-license messages: enabled
      Profile: CiscoTAC-1 (status: ACTIVE)
      Destination  URL(s):  https://tools.cisco.com/its/service/oddce/services/DDCEService
     ```

  3. Check DNS Resolution. Verify that the product instance can ping `tools.cisco.com`, or the nslookup translated IP.

     ```
     Device# ping tools.cisco.com
     Type escape sequence to abort.
     Sending 5, 100-byte ICMP Echos to 173.37.145.8, timeout is 2 seconds:
     !!!!!
     Success rate is 100 percent (5/5), round-trip min/avg/max = 41/41/42 ms
     ```

     If the above does not work check the following: If the product instance IP network is up. To ensure that the network is up, configure the **no shutdown** command in interface configuration mode.

     Check if the device is subnet masked with a subnet IP, and if the DNS IP is confgured.

  4. Verify that the HTTPs client source interface is correct.

     Use the **show ip http client** command in privileged EXEC mode to display current configuration. Use **ip http client source-interface** command in global configuration mode to reconfigure it.

     In case the above does not work, double-check your routing rules, and firewall settings.

- If CSLU is not reachable:

  1. Check if CSLU discovery works.

     - Zero-touch DNS discovery of `cslu-local` or DNS discovery of your domain..

       In the **show license all** command output, check if the `Last ACK received:` field. If this has a recent timestamp it means that the product instance has connectivity with CSLU. If it is not, proceed with the following checks:

       Check if the product instance is able to ping `cslu-local`. A successful ping confirms that the product instance is reachable.

       If the above does not work, configure the name server with an entry where hostname `cslu-local` is mapped to the CSLU IP address (the windows host where you installed CSLU). Configure the **ip domain name** *domain-name* and **ip name-server** *server-address* commands in global configuration mode. Here the CSLU IP is 192.168.0.1 and name-server creates entry `cslu-local.example.com`:

```
Device(config)# ip domain name example.com
Device(config)# ip name-server 192.168.0.1
```

- CSLU URL is configured.

  In the **show license all** command output, under the `Transport:` header check the following: The `Type:` must be `cslu`and `Cslu address:` must have the hostname or the IP address of the windows host where you have installed CSLU. Check if the rest of the address is configured as shown below and check if the port number is 8182.

  ```
  Transport:
    Type: cslu
    Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  ```

  If it is not, configure the **license smart transport cslu** and **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* commands in global configuration mode

2. For CSLU-initiated communication, in addition to the CSLU discovery checks listed above, check the following:

   Verify HTTP connectivity. Use the **show ip http server session-module** command in privileged EXEC mode. In the output, under header `HTTP server current connections:`, check that `SL_HTTP` is active. If it is not re-configure the **ip http** commands as mentioned in Ensuring Network Reachability for CSLU-Initiated Communication, on page 171.

   From a Web browser on the device where CSLU is installed, verify `https://<product-instance-ip>/`. This ensures that the REST API from CSLU to the product instance works as expected.

- If SSM On-Prem is not reachable:

1. For product instance-initiated communication, check if the SSM On-Prem transport type and URL are configured correctly.

   In the **show license all** command output, under the `Transport:` header check the following: The `Type:` must be `cslu`and `Cslu address:` must have the hostname or the IP address of the server where you have installed SSM On-Prem and <tenantID> of the *default* local virtual account. See the example below:

   ```
   Transport:
     Type: cslu
     Cslu address: https://192.168.0.1/cslu/v1/pi/on-prem-default
   ```

   Check if you have the correct URL from SSM On-Prem (See Retrieving the Transport URL (SSM On-Prem UI), on page 189) and then configure **license smart transport cslu** and **license smart url cslu** *http://<ip>/cslu/v1/pi/<tenant ID>* commands in global configuration mode.

   Check that you have configured any other required commands for your network, as mentioned in Ensuring Network Reachability for Product Instance-Initiated Communication, on page 186

2. For SSM On-Prem-initiated communication, check HTTPs connectivity.

   Use the **show ip http server session-module** command in privileged EXEC mode. In the output, under header `HTTP server current connections:`, check that `SL_HTTP` is active. If it is not re-configure the **ip http** commands as mentioned in Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 194.

3. Check trustpoint and that certificates are accepted.

For both forms of communication in an SSM On-Prem Deployment, ensure that the correct trustpoint is used and that the necessary certificates are accepted:

```
Device(config)# crypto pki trustpoint SLA-TrustPoint
Device(ca-trustpoint)#
Device(ca-trustpoint)# enrollment terminal
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# end
Device# copy running-config startup-config
```

If the above does not work and the communication failure persists, contact your Cisco technical support representative.

```
Error Message  %SMART_LIC-3-COMM_RESTORED: Communications with the [chars] restored.
[chars] - depends on the transport type
        - Cisco Smart Software Manager (CSSM)
        - Cisco Smart License utility (CSLU)
Smart Agent communication with either the Cisco Smart Software Manager (CSSM) or the Cisco
 Smart License
utility (CSLU) has been restored. No action required.
```

Explanation: Product instance communication with either the CSSM, CSLU, or SSM On-Prem is restored.

Recommended Action: No action required.

```
Error Message %SMART_LIC-3-POLICY_REMOVED: The licensing policy has been removed.
```

Explanation: A previously installed *custom* licensing policy has been removed. The `Cisco default` policy is then automatically effective. This may cause a change in the behavior of smart licensing.

Possible reasons for failure include:

If you have entered the **license smart factory reset** command in privileged EXEC mode all licensing information including the policy is removed.

Recommended Action:

If the policy was removed intentionally, then no further action is required.

If the policy was removed inadvertantly, you can reapply the policy. Depending on the topology you have implemented, follow the corresponding method to retrieve the policy:

- Connected Directly to CSSM:

  Enter **show license status**, and check field `Trust Code Installed:`. If trust is established, then CSSM will automatically return the policy again. The policy is automatically re-installed on product instances of the corresponding Virtual Account.

  If trust has not been established, complete these tasks: Generating a New Token for a Trust Code from CSSM, on page 211 and Establishing Trust with an ID Token, on page 212. When you have completed these tasks, CSSM will automatically return the policy again. The policy is then automatically installed on all product instances of that Virtual Account.

- Connected to CSSM Through CSLU:
  - For product instance-initiatied communication), enter the **license smart sync** command in privileged EXEC mode. The synchronization request causes CSLU to push the missing information (a policy or authurization code) to the product instance.
  - For CSLU-initiated communication, complete this task:Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 170. This causes CSLU to detect and re-furnish the missing policy in an ACK response.
- CSLU Disconnected from CSSM:
  - For product instance-initiatied communication), enter the **license smart sync** command in privileged EXEC mode. The synchronization request causes CSLU to push the missing information (a policy or authurization code) to the product instance. Then complete these tasks in the given order: Export to CSSM (CSLU Interface), on page 175 > Uploading Data or Requests to CSSM and Downloading a File, on page 214 > Import from CSSM (CSLU Interface), on page 176.
  - For CSLU-initiated communication, complete this task:Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 170 . This causes CSLU to detect and re-furnish the missing policy in an ACK response. Then complete these tasks in the given order: Export to CSSM (CSLU Interface), on page 175 > Uploading Data or Requests to CSSM and Downloading a File, on page 214 >Import from CSSM (CSLU Interface), on page 176 .
- No Connectivity to CSSM and No CSLU

  If you are in an entirely air-gapped network, from a workstation that has connectivity to the internet and CSSM complete this task: Downloading a Policy File from CSSM, on page 213.

  Then complete this task on the product instance: Installing a File on the Product Instance, on page 215.
- SSM On-Prem Deployment
  - For product instance-initiatied communication), enter the **license smart sync** command in privileged EXEC mode. The causes the product instance to synchronize with SSM On-Prem and restore any required or missing information. Then synchronize SSM On-Prem with CSSM if required:
  - For SSM On-Prem-initiated communication: In the SSM On-Prem UI, navigate to **Reports** > **Synchronisation pull schedule with the devices** > **Synchronise now with the device**.

  For both forms of communication in an SSM On-Prem Deployment, synchronize with CSSM using either option:
  - SSM On-Prem is connected to CSSM: In the SSM On-Prem UI, Smart Licensing workspace, nagivate to **Reports** > **Usage Schedules** > **Synchronize now with Cisco**.
  - SSM On-Prem is not connected to CSSM: See Exporting and Importing Usage Data (SSM On-Prem UI), on page 192.

If the above does not work and the custom policy is not restored, contact your Cisco technical support representative.

```
Error Message %SMART_LIC-3-TRUST_CODE_INSTALL_FAILED: The install of a new licensing
trust code has failed on [chars]: [chars].
```

Explanation: Trust code installation has failed. The first [chars] is the UDI where trust code installation was attempted. The second [chars] is the error string with details of the failure.

Possible reasons for failure include:

- A trust code is already installed: Trust codes are node-locked to the UDI of the product instance. If the UDI is already registered, and you try to install another one, installation fails.
- Smart Account-Virtual Account mismatch: This means the Smart Account or Virtual Account (for which the token ID was generated) does not include the product instance on which you installed the trust code. The token generated in CSSM, applies at the Smart Account or Virtual Account level and applies only to all product instances in that account.
- A signature mismatch: This means that the system clock is not accurate.
- Timestamp mismatch: This means the product instance time is not synchronized with CSSM, and can cause installation to fail.

Recommended Action:

- A trust code is already installed: If you want to install a trust code inspite of an existing trust code on the product instance, re-configure the **license smart trust idtoken** *id_token_value* {**local** | **all**} [**force**] command in privileged EXEC mode, and be sure to include the **force** keyword this time. Entering the **force** keyword sets a force flag in the message sent to CSSM to create a new trust code even if one already exists.
- Smart Account-Virtual Account mismatch:

  Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**>**Inventory** > **Product Instances**.

  Check if the product instance on which you want to generate the token is listed in the selected Virtual Account. If it is, proceed to the next step. If not, check and select the correct Smart Account and Virtual Account. Then complete these tasks again: Generating a New Token for a Trust Code from CSSM, on page 211 and Installing a File on the Product Instance, on page 215 again.
- Timestamp mismatch and signature mismatch: Configure the **ntp server** command in global configuration mode. For example:

  ```
  Device(config)# ntp server 198.51.100.100 version 2 prefer
  ```

```
Error Message    %SMART_LIC-4-REPORTING_NOT_SUPPORTED: The CSSM OnPrem that this
product instance is connected to is down rev and does not support the enhanced policy and
usage
reporting mode.
```

Explanation: Cisco Smart Software Manager On-Prem (formerly known as Cisco Smart Software Manager satellite) is supported in the Smart Licensing Using Policy environment starting with Cisco IOS XE Amsterdam 17.3.3 only (See Cisco Smart Software Manager On-Prem (SSM On-Prem), on page 14). In *unsupported* releases, the product instance will behave as follows:

- Stop sending registration renewals and authorization renewals.

- Start recording usage and saving RUM reports locally.

Recommended Action:

You have the following options:

- Refer to and implement one of the supported topologies instead. See: Supported Topologies, on page 15.
- Upgrade to a release where SSM On-Prem is supported with Smart Licensing Using Policy. See Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy, on page 147.

```
Error Message %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy
was successfully installed.
```

Explanation: A policy was installed in one of the following ways:

- Using Cisco IOS commands.
- CSLU-initiated communication.
- As part of an ACK response.

Recommended Action: No action is required. If you want to know which policy is applied (the policy in-use) and its reporting requirements, enter the **show license all** command in privileged EXEC mode.

```
Error Message %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing
authorization code was successfully installed on: [chars].
```

Explanation: [chars] is the UDI where the authorization code was installed successfully.

Recommended Action: No action is required. If you want to know the details of the authorization code that was installed, enter the **show license authorization** command in privileged EXEC mode.

You can also use the **show license all** and **show license tech support** commands in privileged EXEC mode, to see the kind of authorization installed, and the type of entitlement the product instance can use.

```
Error Message %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code has
 been removed from [chars]
```

Explanation: [chars] is the UDI where the authorization code was installed. The authorization code has been removed. This removes the licenses from the product instance and may cause a change in the behavior of smart licensing and the features using licenses.

Recommended Action: No action is required. If you want to see the current state of the license, enter the **show license all** command in privileged EXEC mode.

```
Error Message %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement
will be required in [dec] days.
```

Explanation: This is an alert which means that RUM reporting to Cisco is required. [dec] is the amount of time (in days) left to meet this reporting requirements.

Recommended Action: Ensure that RUM reports are sent within the requested time. The topology you have implemented determines the reporting method.

- Connected to CSSM Through CSLU
  - For product instance-initiatied communication: Enter the **license smart sync** command in privileged EXEC mode. If CSLU is currently logged into CSSM the reports will be automatically sent to the associated Smart Account and Virtual Account in CSSM.
  - For CSLU-initiated communication, complete this task:Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 170.
- Connected Directly to CSSM: Enter the **license smart sync** command in privileged EXEC mode.
- Connected to CSSM Through a Controller: If the product instance is managed by a controller, the controller will send the RUM report at the scheduled time.

  If you are using Cisco DNA Center as the controller, you have the option of ad-hoc reporting. See the *Cisco DNA Center Administrator Guide* of the required release (Release 2.2.2 onwards) > *Manage Licenses* > *Upload Resource Utilization Details to CSSM*.
- CSLU Disconnected from CSSM: If the product instance is connected to CSLU, synchronize with the product instance as shown for "Connected to CSSM Through CSLU"above, then complete these tasks: Export to CSSM (CSLU Interface), on page 175, Uploading Data or Requests to CSSM and Downloading a File, on page 214, and Import from CSSM (CSLU Interface), on page 176.
- No Connectivity to CSSM and No CSLU: Enter the **license smart save usage** command in privileged EXEC mode, to save the required usage information in a file. Then, from a workstation where you have connectivity to CSSM, complete this task: Uploading Data or Requests to CSSM and Downloading a File, on page 214.
- SSM On-Prem Deployment:

  Synchronize the product instance with SSM On-Prem:
  - For product instance-initiatied communication: Enter the **license smart sync** command in privileged EXEC mode. If CSLU is currently logged into CSSM the reports will be automatically sent to the associated Smart Account and Virtual Account in CSSM.
  - For SSM On-Prem-initiated communication, complete this task: In the SSM On-Prem UI, navigate to **Reports** > **Synchronisation pull schedule with the devices** > **Synchronise now with the device**.

  Synchronize usage information with CSSM (*choose one*)
  - SSM On-Prem is connected to CSSM: In the SSM On-Prem UI, Smart Licensing workspace, nagivate to **Reports** > **Usage Schedules** > **Synchronize now with Cisco**.
  - SSM On-Prem is not connected to CSSM: See Exporting and Importing Usage Data (SSM On-Prem UI), on page 192.

```
Error Message %SMART_LIC-6-TRUST_CODE_INSTALL_SUCCESS: A new licensing trust code
 was successfully installed on [chars].
```

Explanation:[chars] is the UDI where the trust code was successfully installed.

Recommended Action: No action is required. If you want to verify that the trust code is installed, enter the **show license status** command in privileged EXEC mode. Look for the updated timestamp under header `Trust Code Installed:` in the output.

```
Error Message %SMART_LIC-4-UTILITY_TRUST_CODE: Trust establishment with an ID TOKEN
 is required before utility usage reporting can start.
```

Explanation:

The utility mode is enabled, and the product instance is directly connected to CSSM using Smart transport, but a trust code is *not* installed. This message is displayed once a week until a trust code is installed or the utility mode is disabled.

If the error condition is detected during normal operation, the message is displayed immediately. It can also be detected at boot time after the system processes the configuration, if the error exists.

Recommended Action:

Complete these tasks: Generating a New Token for a Trust Code from CSSM, on page 211 and Establishing Trust with an ID Token, on page 212.

```
Error Message %SMART_LIC-4-UTILITY_SUBSCRIPTION_LICENSE: Utility mode is in use with
a license that does not have a subscription id: [chars]
```

Explanation: The utility mode is enabled and a license without a subscription ID is in use. [chars] is the license that is in use. This message is generated only once for each license.

Possible reasons for this include:

- If a license with a subscription ID was in use and then new subscription information is returned in a RUM ACK that does not include an ID for this license.
- If the utility mode is enabled and the license is in-use some time after that, this system message is generated 30 days later, if a subscription ID is not available.
- Delayed communication. There may be a lag between the time that you enabled the utility mode and when the subscription ID and other utility information in the RUM ACK is available on the product instance. For example, if you use CSLU or SSM On-Prem, when the product instance receives information will depend on when CSLU or SSM On-Prem is scheduled to synchronize with the product instance.

Note Note that this system message is not generated if an authorization code is installed for the entitlement tag.

Recommended Action:

If the licenses that you are using do not have subscription IDs, you can order them in CCW. The licenses and corresponding subscription IDs, are deposited in the Smart Account and Virtual Account in CSSM.

If the licenses that you are using already have subscription IDs, and you are still seeing this message because of delayed communication, you can initiate an on-demand synchronization based on the topology you have implemented:

- If you have implemented a topology where the product-instance initiates communication, that is, *Connected Directly to CSSM* or topology, or *Connected to CSSM Through CSLU* (product-instance initiated mode), or *CSLU Disconnected from CSSM* (product-instance initiated mode), or*SSM On-Prem Deployment* (product-instance initiated mode), enter the **license smart sync** command in privileged EXEC mode.
- If you have implemented a topology where CSLU or SSM On-Prem initiate communiation, that is, *Connected to CSSM Through CSLU* (CSLU-initiated mode), or *CSLU Disconnected from CSSM* (CSLU-initiated mode), or *SSM On-Prem Deployment* (CSLU-initiated mode), then from the CSLU or SSM On-Prem UI, initiate an on-demand synchronization with the product instance.
- If using the *No Connectivity to CSSM and No CSLU* topology, install the ACK on the product instance: Installing a File on the Product Instance, on page 215.

```
Error Message %SMART_LIC-4-UTILITY_NO_ACK: A Usage report acknowledgement has not
been received in the last [dec] days. An Acknowledgement is required every 30 days.
```

Explanation: A RUM ACK message has not been received within the last 30 days. [dec] is the number of days.

In the utility mode, a RUM ACK is required every 30 days. This message will be generated every 30 days until the a RUM ACK is received.

Possible reasons for this include:

- Connectivity problems. Depending on thetopology you have implemented, this can mean a connectivity problem with CSSM, or CSLU, or SSM On-Prem
- Delayed communication. There may be a lag between the time that a RUM Report is sent and the RUM ACK is available on the product instance. For example, if you use CSLU or SSM On-Prem, when the product instance receives information will depend on when CSLU or SSM On-Prem is scheduled to synchronize with the product instance.

Recommended Action:

In case of connectivity problems, refer to the troubleshooting steps that apply to your topology: %SMART_LIC-3-COMM_FAILED.

If RUM reports have been sent, the output of the **show license all** command, field `Next report push` will reflect this informaiton. But if an ACK is not available in case of delayed communication, initiate an on-demand synchronization based on the topology you have implemented:

- If you have implemented a topology where the product-instance initiates communication, that is, *Connected Directly to CSSM* or topology, or *Connected to CSSM Through CSLU* (product-instance initiated mode), or *CSLU Disconnected from CSSM* (product-instance initiated mode), or*SSM On-Prem Deployment* (product-instance initiated mode), enter the **license smart sync** command in privileged EXEC mode.
- If you have implemented a topology where CSLU or SSM On-Prem initiate communiation, that is, *Connected to CSSM Through CSLU* (CSLU-initiated mode), or *CSLU Disconnected from CSSM* (CSLU-initiated mode), or *SSM On-Prem Deployment* (CSLU-initiated mode), then from the CSLU or SSM On-Prem UI, initiate an on-demand synchronization with the product instance.
- If using the *No Connectivity to CSSM and No CSLU* topology, install the ACK on the product instance: Installing a File on the Product Instance, on page 215.

If an ACK is still not successfully received, contact your Cisco technical support representative.

```
Error Message %SMART_LIC-4-UTILITY_TRANSPORT_NOT_CONFIG: To support utility mode
the transport must be set to 'smart transport' or 'cslu'.
```

Explanation: The utility mode is enabled, but the transport type is not set correctly. This system message is generated once-a-week until the correct transport setting is configured, or the utility mode is disabled.

If the error condition is detected during normal operation, the message is displayed immediately. It can also be detected at boot time after the system processes the configuration, or if you change the transport mode or utility mode.

Recommended Action:

In the utility mode, the transport type must be **smart**, or **cslu**, or **off**. Configure the transport mode depending on the topology you have implemented: Setting the Transport Type, URL, and Reporting Interval, on page 216.

```
Error Message %SMART_LIC-3-UTILITY_REPORT_FAILED: Smart Agent for Licensing Utility
 has failed to send usage Report.
```

Explanation: Because of a communications failure, the product instance failed to send the RUM report.

Recommended Action:

Check if the RUM report is due any time soon. If not, and the problem is with a server or link that is down, you can try again after some time.

If the communication failure persists, check if the transport type and URL have been set as required by the topology.

Also see %SMART_LIC-3-COMM_FAILED.

If the communication failure persists, contact your Cisco technical support representative.

```
Error Message %SMART_LIC-6-UTILITY_STARTED: Smart Agent for Licensing Utility has
started sending usage reports
```

Explanation: Product instance communication with either the CSSM, CSLU, or SSM On-Prem is restored.

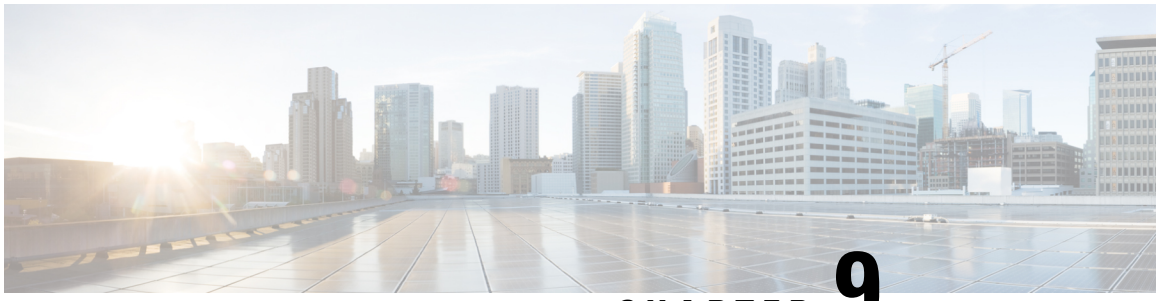
Recommended Action: No action required.

```
Error Message %SMART_LIC-6-UTILITY_STOPPED: Smart Agent for Licensing Utility has
stopped sending usage reports
```

Explanation: The utility mode is disabled.

Recommended Action: No action required.

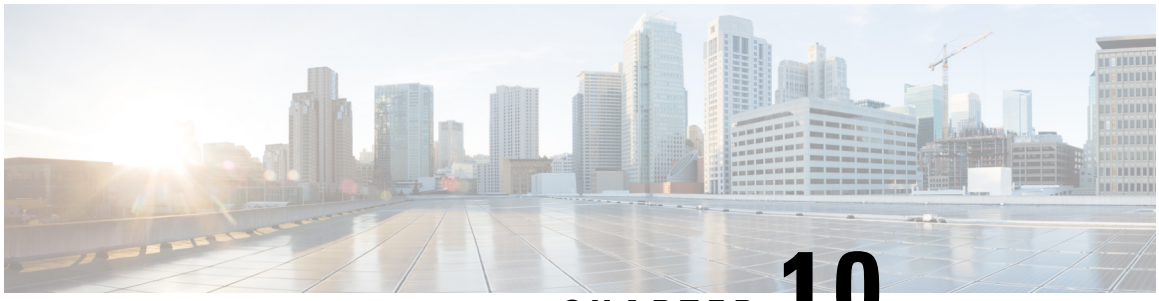
RUM reports continue to be sent, but they are not flagged as being in the utility mode.



CHAPTER 9

Additional References for Smart Licensing Using Policy

Related Topic	Document Title
Cisco Smart Software Manager (CSSM) Help	Smart Software Manager Help
Cisco Smart License Utility (CSLU) Installation and User guides. We recommend that you always use the latest version of CSLU that is available.	Click *Smart Licensing Utility* on the Software Download page.
SSM On-Prem Release Notes, and Console, Installation, Quick Start, and User Guides We recommend that you always use the latest version of SSM On-Prem that is available.	Click *Smart Software Manager On-Prem* on the Software Download page.
System Message Guides (Applicable to all products running Cisco IOS-XE software). Search for `SMART_LIC` to locate licensing related system messages.	Error and System Messages.
Information about the licenses that are available on Cisco Catalyst 8000 Edge Platforms Family, supported throughput options, and how to configure the available licenses and throughput.	Licenses and Licensing Models in Cisco Catalyst 8300 and Catalyst 8200 Series Edge Platforms Software Configuration Guide. Licenses and Licensing Models in Cisco Catalyst 8500 and 8500L Series Edge Platforms Software Configuration Guide. Licenses and Licensing Models in Cisco Catalyst 8000V Edge Software Installation And Configuration Guide.
Syntax information for commands related to throughput configuration on physical and virtual platforms.	Cisco IOS Interface and Hardware Component Command Reference
Syntax information for commands related to configuration of boot level licenses on routing platforms.	Cisco IOS Software Activation Command Reference



CHAPTER 10

Feature History for Smart Licensing Using Policy

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Table 21: Feature History for Smart Licensing Using Policy

Feature Name	Releases	Feature Information
Smart Licensing Using Policy	Cisco IOS XE Amsterdam 17.3.2	An enhanced version of Smart Licensing, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use. Starting with this release, Smart Licensing Using Policy is automatically enabled on the device. This is also the case when you upgrade to this release. By default, your Smart Account and Virtual Account in CSSM is enabled for Smart Licensing Using Policy.
Cisco DNA Center Support for Smart Licensing Using Policy	Cisco IOS XE Amsterdam 17.3.2	Cisco DNA Center supports Smart Licensing Using Policy functionality starting with Cisco DNA Center Release 2.2.2. When you use Cisco DNA Center to manage a product instance, Cisco DNA Center connects to CSSM, and is the interface for all communication to and from CSSM. For information about the comptabile controller and product instance versions, see: Support Information for Controller: Cisco DNA Center. For information about this topology, see the Cisco DNA Center as a Controller, on page 21 and Using Cisco DNA Center as a Controller, on page 38.

Feature Name	Releases	Feature Information
Smart Software Manager On-Prem (SSM On-Prem) Support for Smart Licensing Using Policy	Cisco IOS XE Amsterdam 17.3.3	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. For information about the comptabile SSM On-Prem and product instance versions, see: Cisco Smart Software Manager On-Prem (SSM On-Prem), on page 14. For an overview of this topology, and to know how to implement it, see SSM On-Prem Deployment, on page 26 and Workflow for Topology: SSM On-Prem Deployment, on page 46. For information about migrating from an exisiting version of SSM On-Prem, to one that supports Smart Licensing Using Policy, see Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy, on page 147.
Smart Licensing Using Policy	Cisco IOS XE Bengaluru 17.4.1	Starting with this release, Smart Licensing Using Policy is supported on these platforms: • Catalyst 8000V Edge Software • Catalyst 8200 Series Edge Platforms • Cisco 1100 Terminal Services Gateway • Cisco Cloud Services Router 1000v. (To support Smart Licensing Using Policy, this platform requires upgrade from a CSRv .bin image to a Catalyst 8000V software image.) • Cisco Integrated Services Virtual Router. (To support Smart Licensing Using Policy, this platform requires upgrade from an ISRv .bin image to a Catalyst 8000V software image.) See Supported Products, on page 2 for the complete list of products that support the feature.

Feature Name	Releases	Feature Information
License Management for Smart Licensing Using Policy, Using Cisco vManage	Cisco IOS XE Bengaluru 17.5.1a	Cisco SD-WAN operates together with Cisco SSM to provide license management through Cisco vManage for devices operating with Cisco SD-WAN. For this you have to implement a topology where Cisco vManage is connected to CSSM. For information about the comptabile controller and product instance versions, see: Support Information for Controller: Cisco vManage. For information about this topology, see the Connected to CSSM Through a Controller, on page 20 and Workflow for Topology: Connected to CSSM Through a Controller, on page 38 sections of this document. More information about Cisco vManage is also available in the License Management for Smart Licensing Using Policy section of the *Cisco SD-WAN Getting Start Guide*.
Phasing Out of device-specific HSECK9 licenses.	Cisco IOS XE Bengaluru 17.6.1a	With the introduction of Cisco Digital Network Architecture (Cisco DNA), 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 this release, 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 have unused device-specific HSECK9 licenses, mutiple options are available to you. See Phasing Out of Device-Specific HSECK9 Licenses, on page 153.
Snapshots for PAK licenses	Cisco IOS XE Bengaluru 17.6.2	The library that manages PAK licenses is being deprecated from the software image. In order to continue supporting and honouring any existing PAK licenses you may have, the system automatically takes a snapshot of the PAK license and triggers a Device-Led Conversion process, to convert the PAK license to a Smart License. See: Snapshots for PAK Licenses , on page 159.

Feature Name	Releases	Feature Information
Factory-installed trust code	Cisco IOS XE Cupertino 17.7.1a	For new hardware orders, a trust code is now installed at the time of manufacturing. You cannot use a factory-installed trust code to communicate with CSSM. See Benefits of Smart Licensing Using Policy, on page 1 and Trust Code, on page 8.
Support for trust code in additional topologies		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. See: • Trust Code, on page 8 • Connected to CSSM Through CSLU, on page 16 and Tasks for Product Instance-Initiated Communication, on page 33. • CSLU Disconnected from CSSM, on page 23 and Tasks for Product Instance-Initiated Communication, on page 41. • No Connectivity to CSSM and No CSLU, on page 24 and Workflow for Topology: No Connectivity to CSSM and No CSLU, on page 45.
Ability to save authorization code request and return in a file and simpler upload in the CSSM Web UI		If your product instance is in an air-gapped network, you can now save a SLAC request in a file on the product instance. The SLAC request file must be uploaded to the CSSM Web UI. You can then download the file containing the SLAC code and install it on the product instance. You can also upload a return request file in a similar manner. With this new method you do not have to gather and enter the required details on the CSSM Web UI to generate a SLAC. You also do not have to locate the product instance in the CSSM Web UI to return an authorization code. In the CSSM Web UI, the request or return file is uploaded in the same location and in the same way as you upload a RUM report. See Generating and Saving a SLAC Request on the Product Instance, on page 203, Removing and Returning an Authorization Code, on page 204, and Uploading Data or Requests to CSSM and Downloading a File, on page 214.

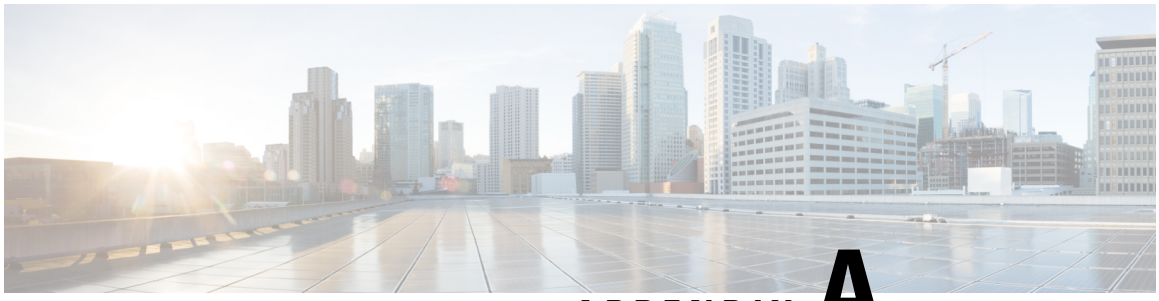
Feature Name	Releases	Feature Information
Support to collect software version in a RUM report		If version privacy is disabled (**no license smart privacy version** global configuration command), the Cisco IOS-XE software version running on the product instance and Smart Agent version information is *included* in the RUM report. See license smart (global config), on page 249.
RUM Report optimization and availability of statistics		RUM report generation and related processes have been optimized. This includes a reduction in the time it takes to process RUM reports, better memory and disk space utilization, and visibility into the RUM reports on the product instance (how many there are, the processing state each one is in, if there are errors in any of them, and so on). See show license rum, on page 291, show license tech, on page 309, and show license all, on page 272.
Account information included in **show** command outputs		A RUM acknowledgement (ACK) includes the Smart Account and Virtual Account that was reported to, in CSSM. Account information is displayed in the output of various **show** commands and is always as per the latest available ACK on the product instance. See show license summary, on page 307, show license status, on page 298, show license all, on page 272, and show license tech, on page 309.
CSLU support for Linux		Support for CSLU deployment on a machine (laptop or desktop) running Linux. CSLU is compatible with Linux in the following formats. See Cisco Smart License Utility (CSLU), on page 12.

Feature Name	Releases	Feature Information
Managed Service License Agreement (MSLA) Support with Smart Licensing Using Policy.	Cisco IOS XE Cupertino 17.9.1a	For Catalyst 8000V Edge Software running in the autonomous mode, you can implement a post-paid model for licenses, where you pay for the actual usage of a license instead of pre-paying for the licenses you may require. See: Managed Service License Agreement (MSLA), on page 15 and Utility Mode, on page 29.
New mechanism to send data privacy related information		A new mechanism to send all data privacy related information was introduced. This information is no longer included in a RUM report.If data privacy is disabled (**no license smart privacy** {**all** | **hostname** | **version**}} global configuration command), data privacy related information is sent in a separate sync message or offline file. Depending on the topology you have implemented, the product instance initiates the sending of this information in a separate message, or CSLU and SSM On-Prem initiates the retrieval of this information from the product instance, or this information is saved in the offline file that is generated when you enter the license smart save usage privileged EXEC command See license smart (global config), on page 249.
Hostname support		If you configure a hostname on the product instance and disable the corresponding privacy setting (**no license smart privacy hostname** global configuration command), hostname information is sent from the product instance. Depending on the topology you have implemented, the hostname information is received by CSSM, and CSLU or SSM On-Prem. It is then displayed on the corresponding user interface. See license smart (global config), on page 249.
Support for trust code in additional topologies		A trust code is automatically obtained in topologies where CSLU initiates the retrieval of data from the product instance. See: Trust Code, on page 8, Connected to CSSM Through CSLU, on page 16, CSLU Disconnected from CSSM, on page 23.
VRF support		

Feature Name	Releases	Feature Information
		On a product instance where VRF is supported, you can configure a VRF to send all licensing data to CSSM, or CSLU, or SSM On-Prem. To configure a VRF, enter the **license smart vrf** *vrf_string* command in global configuration mode. See license smart (global config), on page 249.
RUM report throttling		For all topologies where the product instance initiates communication, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. The affected topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated communication), *CSLU Disconnected from CSSM* (product instance-initiated communication), and *SSM On-Prem Deployment* (product instance-initiated communication). You can override the reporting frequency throttling, by entering the **license smart sync** command in privileged EXEC mode. This triggers an on-demand synchronization with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. 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 Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to *all* subsequent releases. See: Connected Directly to CSSM, on page 18, Connected to CSSM Through CSLU, on page 16, CSLU Disconnected from CSSM, on page 23, SSM On-Prem Deployment, on page 26.
Permanent License Reservation (PLR) in Smart Licensing Using Policy	Cisco IOS XE Dublin 17.10.1a	A PLR enables you to use an unlimited count of any license on the product instance. It is suited to a high-security deployment or entirely air-gapped networks where a product instance cannot communicate online, with anything outside its network. See: Permanent License Reservation in the Smart Licensing Using Policy Environment, on page 161

Feature Name	Releases	Feature Information
Snapshots for PAK licenses	Cisco IOS XE Dublin 17.11.1a	The PAK-managing library is discontinued and the provision to ***take*** a snapshot is no longer available. 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 releases where the system can take a snapshot of the PAK license and complete DLC, and then again upgrade to the required, later release. See: Snapshots for PAK Licenses , on page 159.
Forced return option for an HSECK9 license that is in-use	Cisco IOS XE Dublin 17.15.1	The **force-reload** [**no-prompt**] keywords were introduced. See: Returning SLAC for an HSECK9 License That Is In-Use, on page 209.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/



APPENDIX A

Appendix: License Ordering Information

• Ordering Information for HSECK9 Licenses, on page 353

Ordering Information for HSECK9 Licenses

The following tables provide information that you can use to order HSECK9 licenses.

PIDS Mapping To CSSM Entitlement (Cisco IOS XE Bengaluru 17.6.1 and Later Releases)

User Type	Platform	Product ID or SKU (SKUs appended with "=" are spares)	License type	Entitlement deposited in CSSM
DNA a la carte (new deployments)	ISR 1100-6G & 1100X-6G	DNA-HSEC-K9	DNA-HSEC	Router US Export Lic for DNA
DNA a la carte (existing deployments)	ISR 1100-6G & 1100X-6G	DNA-HSEC-L	DNA-HSEC	Router US Export Lic for DNA
DNA a la carte (Spare)	ISR 1100-6G & 1100X-6G	C8000-HSEC=	DNA-HSEC	Router US Export Lic for DNA
DNA Enterprise Agreement (EA)	All ISR 1K & 4K	DNA-HSEC-L	DNA-HSEC	Router US Export Lic for DNA
Existing device-specific HSECK9 users	ISR 1K & ISR 4K Routers	DNA-HSEC-UPGD=	DNA-HSEC	Router US Export Lic for DNA
DNA a la carte (existing deployments)	ISR 1K & ISR 4K Routers	DNA-HSEC-UPGD	DNA-HSEC	Router US Export Lic for DNA

User Type	Platform	Product ID or SKU (SKUs appended with "=" are spares)	License type	Entitlement deposited in CSSM
DNA a la carte (new deployments) & Non-DNA	ISR4K	ISR4K-HSECK9	DNA-HSEC	Router US Export Lic for DNA
	ISR4K	ISR4K-HSECK9=	DNA-HSEC	Router US Export Lic for DNA
	ISR1K 2P and ISR1K 4P	ISR1K2P4P-HSECK9	DNA-HSEC	Router US Export Lic for DNA
	ISR1K 2P and ISR1K 4P	ISR1K2P4P-HSECK9=	DNA-HSEC	Router US Export Lic for DNA
	ISR1K 8P	ISR1K8P-HSECK9	DNA-HSEC	Router US Export Lic for DNA
	ISR1K 8P	ISR1K8P-HSECK9=	DNA-HSEC	Router US Export Lic for DNA

PIDS Mapping To CSSM Entitlement (Cisco IOS XE Bengaluru 17.5.x and Earlier Releases)

User Type	Platform	Product ID or SKU SKUs appended with "=" are spares	License type	Entitlement Deposited in CSSM
DNA EA, DNA a la carte & Non-DNA	ISR 1K 2P	FL-1100-2P-HSEC=	Device-Specific HSEC	ISR_1100_2P_HSEC
	ISR 1K 2P	FL-1100-2P-HSEC	Device-Specific HSEC	ISR_1100_2P_HSEC
	ISR 112X 4P, ISR 113X 4P	FL-1K-4P-HSEC-SV	Device-Specific HSEC	ISR_1100_4P_Hsec
	ISR 116X 8P	FL-P1K-8P-HSEC-SV=	Device-Specific HSEC	ISR_1100_8P_Hsec
	SR 112X 8P, ISR 113X 8P	FL-1K-8P-HSEC-SV	Device-Specific HSEC	ISR_1100_8P_Hsec
	ISR 116X 8P	FL-P1K-8P-HSEC-SV	Device-Specific HSEC	ISR_1100_8P_Hsec
	ISR 110X 4P, ISR 111X 4P	FL-1100-4P-HSEC=	Device-Specific HSEC	ISR_1100_4P_Hsec
	ISR 110X 8P, ISR 111X 8P	FL-1100-8P-HSEC=	Device-Specific HSEC	ISR_1100_8P_Hsec
	ISR 110X 4P, ISR 111X 4P	FL-1100-4P-HSEC	Device-Specific HSEC	ISR_1100_4P_Hsec
	ISR 110X 8P, ISR 111X 8P	FL-1100-8P-HSEC	Device-Specific HSEC	ISR_1100_8P_Hsec
	ISR 4350	FL-4350-HSEC-K9=	Device-Specific HSEC	ISR_4351_Hsec
	ISR 4320	FL-4320-HSEC-K9=	Device-Specific HSEC	ISR_4321_Hsec
	ISR 4350	FL-4350-HSEC-K9	Device-Specific HSEC	ISR_4351_Hsec
	ISR 4320	FL-4320-HSEC-K9	Device-Specific HSEC	ISR_4321_Hsec
	ISR 4330	FL-4330-HSEC-K9=	Device-Specific HSEC	ISR_4331_Hsec
	ISR 4400	FL-44-HSEC-K9=	Device-Specific HSEC	ISR_4400_Hsec
	ISR 4330	FL-4330-HSEC-K9	Device-Specific HSEC	ISR_4331_Hsec
	ISR 4400	FL-44-HSEC-K9	Device-Specific HSEC	ISR_4400_Hsec

Appendix: License Ordering Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020–2023 Cisco Systems, Inc. All rights reserved.