Preface

This Preface chapter describes the organization of this document, the document conventions that have been used, and explains how to find additional information on related products and services.

Note

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

• Navigating Through the Content, on page ii
• Document Conventions, on page iii

Navigating Through the Content

This document is grouped into these major sections:

• Information About Smart Licensing Using Policy: Provides an overview of how one operates in the Smart Licensing Using Policy environment.

  Architecture: Covers the components that may be part of your implementation. One or more components make a supported topology - you have to implement one of the topologies to operate in the Smart Licensing Using Policy environment.

  Concepts: Covers the key concepts that help you understand how the feature works.

Supported Topologies: Describes the various ways in which you can implement Smart Licensing Using Policy.

Supported Products: Covers the list of products that this guide is applicable to.

Interaction with Other Features: Covers considerations that apply to a High Availability configuration, and how upgrading or downgrading software affects the way Smart Licensing Using Policy works.

• How to Configure Smart Licensing Using Policy: Workflows by Topology: Provides configuration information to implement supported topologies for new deployments only.
• Task Library for Smart Licensing Using Policy: A grouping of all tasks. Includes tasks performed on a product instance, on the CSLU interface, and in the CSSM Web UI.

• Command Reference for Smart Licensing Using Policy: Provides detailed command syntax information. It includes only Smart Licensing commands.

• Troubleshooting for Smart Licensing Using Policy: Provides the list of Smart Licensing Using Policy-related system messages you may encounter, possible reasons for failure, and recommended action.

• Additional References for Smart Licensing Using Policy: Provides links to related documentation.

• Feature History for Smart Licensing Using Policy: Provides information about when new features or enhancements for Smart Licensing Using Policy are introduced.

This document does not cover the detailed steps involved in ordering and billing, although there are references to these aspects in this document where applicable.

### Document Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^ or Ctrl</td>
<td>Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)</td>
</tr>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><em>Italic</em> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic</em> font.</td>
</tr>
<tr>
<td><strong>Courier</strong> font</td>
<td>Terminal sessions and information the system displays appear in <strong>courier</strong> font.</td>
</tr>
<tr>
<td><strong>Bold Courier</strong> font</td>
<td><strong>Bold Courier</strong> font indicates text that the user must enter.</td>
</tr>
<tr>
<td>[x]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>...</td>
<td>An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.</td>
</tr>
<tr>
<td></td>
<td>A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.</td>
</tr>
<tr>
<td>[x</td>
<td>y]</td>
</tr>
<tr>
<td>{x</td>
<td>y}</td>
</tr>
</tbody>
</table>
**Convention** | **Description**
--- | ---
[x {y | z}] | Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.

string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

<> | Nonprinting characters such as passwords are in angle brackets.

[] | Default responses to system prompts are in square brackets.

! # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

**Reader Alert Conventions**

This document may use the following conventions for reader alerts:

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Tip**

Means *the following information will help you solve a problem*.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Timesaver**

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

**Warning**

**IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS
CHAPTER 1

Introduction to Smart Licensing Using Policy

Smart Licensing Using Policy is 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.

The primary benefits of this enhanced licensing model are:

• Seamless day-0 operations
  After a license is ordered, no preliminary steps, such as registration or generation of keys etc., are required unless you use an export-controlled or enforced license. These licenses require authorization before use. For all other licenses, product features can be configured on the device right-away.

• Consistency in Cisco IOS XE
  Campus and industrial ethernet switching, routing, and wireless devices that run Cisco IOS XE software, have a uniform licensing experience.

• Visibility and manageability
  Tools, telemetry and product tagging, to know what is in-use.

• Flexible, time series reporting to remain compliant
  Easy reporting options are available, whether you are directly or indirectly connected to Cisco Smart Software Manager (CSSM), or in an air-gapped network.

This document provides conceptual, configuration, and troubleshooting information for Smart Licensing Using Policy on Cisco Aggregation, Integrated, and Cloud Service Routers, Cisco Catalyst 8000 Edge Platforms Family, and Cisco Terminal Services Gateways.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.
Overview

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

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

  **Note**

  To simplify your implementation of Smart Licensing Using Policy, provide your Smart Account and Virtual Account information when placing an order for new hardware or software. This allows Cisco to install applicable policies and authorization codes (terms explained in the Concepts, on page 7 section below), at the time of manufacturing.

- Use: Most licenses are unenforced. This means that you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. Only export-controlled and enforced licenses require Cisco authorization before use. License usage is recorded on your device with timestamps and the required workflows can be completed at a later date.

- Report license usage to CSSM: Multiple options are available for license usage reporting. You can use the Cisco Smart Licensing Utility (CSLU) or report usage information directly to CSSM. A provision for offline reporting for closed networks, where you download usage information and upload to CSSM, is also available. The usage report is in plain text XML format. See: Sample Resource Utilization Measurement Report, on page 69.

- Reconcile: For situations where delta billing applies (purchased versus consumed).
Architecture

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

Product Instance

A product instance is a single instance of a Cisco product, identified by a Unique Device Identifier (UDI). A product instance records and reports license usage (RUM reports), and provides alerts and system messages about overdue reports, communication failures, etc. RUM reports and usage data are securely stored in the product instance.

Throughout this document, the term product instance refers to all supported physical and virtual product instances - unless noted otherwise. For information about the product instances that are within the scope of this document, see Supported Products, on page 18.

CSSM

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

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

See the Supported Topologies, on page 11 section to know about the different ways in which you can connect to CSSM

In CSSM you can:

- Create, manage, or view virtual accounts.
- Create and manage Product Instance Registration Tokens.
- Transfer licenses between virtual accounts or view licenses.
- Transfer, remove, or view product instances.
- Run reports against your virtual accounts.
- Modify your email notification settings.
- View overall account information.

CSLU

Cisco Smart License Utility (CSLU) is a Windows-based reporting utility that provides aggregate licensing workflows while being connected to CSSM or in a disconnected mode. This utility performs the following key functions:

- Provides options relating to how workflows are triggered. The workflows can be triggered by CSLU or by the product instance.
- Collects usage reports from the product instance and uploads these usage reports to the corresponding Smart Account or Virtual Account – online, or offline, using files. Similarly, the RUM report ACK is collected online, or offline, and sent back to the product instance.

- Sends authorization code requests to CSSM and receives authorization codes\(^1\) from CSSM.

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

- Install the windows application, to use CSLU as a standalone tool that is connected to CSSM.

- Install the windows application, to use CSLU as a standalone tool that is disconnected from CSSM. With this option, the required usage information is downloaded to a file and then uploaded to CSSM. This is suited to air-gapped networks.

---

**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**
- **Support Information for Controller: Cisco vManage**

---

\(^1\) You can use CSLU to forward authorization code requests for Cisco routers that operate in controller mode (for Cisco SD-WAN features).
Table 1: Support Information for Controller: Cisco DNA Center

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

² The minimum required version for this controller. This means support continues on all subsequent releases - unless noted otherwise.
³ The minimum required Cisco IOS-XE version on the product instance. This means support continues on all subsequent releases - unless noted otherwise.


Table 2: Support Information for Controller: Cisco vManage

<table>
<thead>
<tr>
<th>Minimum Required Cisco vManage Version for Smart Licensing Using Policy ⁴</th>
<th>Minimum Required Cisco IOS XE Version ⁵</th>
<th>Supported Product Instances</th>
</tr>
</thead>
</table>

⁴ The minimum required version for this controller. This means support continues on all subsequent releases - unless noted otherwise.
⁵ The minimum required Cisco IOS-XE version on the product instance. This means support continues on all subsequent releases - unless noted otherwise.
For more information about Cisco vManage, see the support page at: https://www.cisco.com/c/en/us/support/routers/sd-wan/series.html.

For information about how to implement a topology with a supported controller, see Connected to CSSM Through a Controller, on page 14.

SSM On-Prem

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

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

<table>
<thead>
<tr>
<th>Minimum Required SSM On-Prem Version for Smart Licensing Using Policy⁶</th>
<th>Minimum Required Cisco IOS XE Version⁷</th>
<th>Supported Product Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 8, Release 202102</td>
<td>Cisco IOS XE Amsterdam 17.3.3</td>
<td>All Supported Products, on page 18</td>
</tr>
</tbody>
</table>

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

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

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.

Concepts

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

License Enforcement Types

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

• Unenforced or Not Enforced

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

• Enforced

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

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

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

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

Authorization Code

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

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

<table>
<thead>
<tr>
<th>Enforcement Type</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export-controlled</td>
<td>HSECK9</td>
</tr>
<tr>
<td>Enforced</td>
<td>MRP Client</td>
</tr>
<tr>
<td></td>
<td>MRP Manager</td>
</tr>
</tbody>
</table>

In addition to the above licenses, throughput configuration greater than 250 Mbps requires a SLAC. But if the product instance already has one of the following: a SLAC for an HSECK9 license, or an HSECK9 PAK license, or an SLR authorization code included as part of an HSECK9 license - then you do not have to install SLAC again for throughput greater 250 Mbps.
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 Authorization Keys (PAK). The authorization code for these existing licenses is supported after upgrade to Smart Licensing Using Policy.

**Policy**

A policy provides the product instance with these reporting instructions:

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

- First report requirement (days): The first report must be sent within the duration specified here. If the value here is zero, no first report is required.

- Reporting frequency (days): The next RUM report must be sent within the duration specified here. If the value here is zero, it means no further reporting is required unless there is a usage change.

- Report on change (days): In case of a change in license usage, a report must be sent within the duration specified here. If the value here is zero, no report is required on usage change. If the value here is not zero, reporting is required after the change is made. All the scenarios listed below count as changes in license usage on the product instance:
  - Changing licenses consumed (includes changing to a different license, and, adding or removing a license).
  - Going from consuming zero licenses to consuming one or more licenses.
  - Going from consuming one or more licenses to consuming zero licenses.

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).

**Note**

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 10) 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.

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

<table>
<thead>
<tr>
<th>Policy: Cisco default</th>
<th>Default Policy Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export (Perpetual/Subscription)</td>
<td>Reporting ACK required: Yes</td>
</tr>
<tr>
<td>Note</td>
<td>First report requirement (days): 0</td>
</tr>
<tr>
<td></td>
<td>Reporting frequency (days): 0</td>
</tr>
<tr>
<td></td>
<td>Report on change (days): 0</td>
</tr>
<tr>
<td>Enforced (Perpetual/Subscription)</td>
<td>Reporting ACK required: Yes</td>
</tr>
<tr>
<td>Note</td>
<td>First report requirement (days): 0</td>
</tr>
<tr>
<td></td>
<td>Reporting frequency (days): 0</td>
</tr>
<tr>
<td></td>
<td>Report on change (days): 0</td>
</tr>
<tr>
<td>Unenforced/Non-Export Perpetual</td>
<td>Reporting ACK required: Yes</td>
</tr>
<tr>
<td></td>
<td>First report requirement (days): 365</td>
</tr>
<tr>
<td></td>
<td>Reporting frequency (days): 0</td>
</tr>
<tr>
<td></td>
<td>Report on change (days): 90</td>
</tr>
<tr>
<td>Unenforced/Non-Export Subscription</td>
<td>Reporting ACK required: Yes</td>
</tr>
<tr>
<td></td>
<td>First report requirement (days): 90</td>
</tr>
<tr>
<td></td>
<td>Reporting frequency (days): 90</td>
</tr>
<tr>
<td></td>
<td>Report on change (days): 90</td>
</tr>
</tbody>
</table>

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

RUM Report and Report Acknowledgement

A Resource Utilization Measurement report (RUM report) is a license usage report, which 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.

The policy that is applied to a product instance determines the following reporting requirements:

- 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.

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 as well.

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

**Trust Code**

A UDI-tied public key with which the product instance signs every RUM report. This prevents tampering and ensures data authenticity.

**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 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 provides 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, 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 receiving RUM reports from the product instance and sending the same to CSSM, authorization code installation, 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.

**Where to Go Next:**
To implement this topology, see *Workflow for Topology: Connected to CSSM Through CSLU*, on page 27.

**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 a token from the corresponding Smart Account and Virtual Account in CSSM, and installation on the product instance.

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.

**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.
- 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 29 > Product Instance Configuration > Configure a connection method and transport type > Option 1.*
Where to Go Next:

To implement this topology, see Workflow for Topology: Connected Directly to CSSM, on page 29.

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

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

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.

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 6: Product Instances that Support SLAC Generation for HSECK9 license on the Cisco DNA Center GUI, on page 32.

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 30 > Using Cisco DNA Center as a Controller, on page 31.

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 licenses to edge devices, view information about the licenses that are being used and the licenses that are available for assignment.
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 30 > 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.
Considerations or Recommendations:
None.

Where to Go Next:
To implement this topology, see Workflow for Topology: CSLU Disconnected from CSSM, on page 34.

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

Where to Go Next:
To implement this topology, see Workflow for Topology: No Connectivity to CSSM and No CSLU, on page 37.

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 5: Smart Licensing Using Policy: Supported Products

<table>
<thead>
<tr>
<th>Product Category</th>
<th>Product Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Aggregation, Integrated, and Cloud Service Routers</td>
<td></td>
</tr>
<tr>
<td>Product Category</td>
<td>Product Series</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>Cisco 1000 Series Integrated Services Routers</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco 4000 Series Integrated Services Routers</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco ASR 1000 Series Aggregation Services Routers</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cisco Cloud Services Router 1000v</strong> (Requires upgrade from a CSRv .bin image to a Catalyst 8000V software image.)</td>
</tr>
<tr>
<td></td>
<td><strong>Cisco Integrated Services Virtual Router</strong> (Requires upgrade from an ISRv .bin image to a Catalyst 8000V software image.)</td>
</tr>
<tr>
<td><strong>Cisco Catalyst 8000 Edge Platforms Family</strong></td>
<td><strong>Catalyst 8200 Series Edge Platforms</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Catalyst 8300 Series Edge Platforms</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Catalyst 8500 Series Edge Platforms</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Catalyst 8000V Edge Software</strong></td>
</tr>
<tr>
<td><strong>Cisco Terminal Services Gateways</strong></td>
<td><strong>Cisco 1100 Terminal Services Gateway</strong></td>
</tr>
</tbody>
</table>

**Interactions with Other Features**

**High Availability**

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

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

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

**Authorization Code Requirements in a High Availability Set-Up**

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

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

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

**Trust Code Requirements in a High Availability Set-Up**

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

**Policy Requirements in a High Availability Set-Up**

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

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

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

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

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

---

9 The Cisco StackWise Virtual feature, which is available on Cisco Catalyst switches, is an example of such a set-up.

10 The Quad-Supervisor with Route Processor Redundancy, which is available on Cisco Catalyst switches, is an example of such a set-up.
For reporting: Only the active product instance reports usage. The active reports usage information for all devices (standbys or members – as applicable) in the High Availability set-up. In addition to scheduled reporting, the following events trigger reporting:

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

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

For a new member or standby addition:

- A product instance that is connected to CSLU, does not take any further action.
- A product instance that is directly connected to CSSM, performs trust synchronization. Trust synchronization involves the following:
  
  Installation of trust code on the standby or member if not installed already.

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

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

  Sending of a RUM report with current usage information.

### Upgrades

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.

### 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.

#### CSL RTU License Data: Before Upgrage

This example displays the output before the upgrade for the CSL RTU license.

```
Device#show license all
License Store: Primary License Storage
License Store: Built-In License Storage
```
Identifying the Current Licensing Model Before Upgrade

Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
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.

- 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 59.

- 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: If a license used on a product instance was registered to a Smart Account and had the export-control flag enabled in CSSM to enable a throughput greater than 250 Mbps, you must install a SLAC after upgrading to Smart Licensing Using Policy. This is the case with Cisco Cloud Services Routers 1000v and Cisco Integrated Services Virtual Routers. An HSECK9 license is not available for these platforms, but a throughput configuration that is greater than 250 Mbps would have required an export-control flag in the earlier licensing environments. Further, for both these product instances, to support Smart Licensing Using Policy, you must upgrade to a Catalyst 8000V software image, where HSECK9 licenses (requiring SLAC) are available. SLAC installation is therefore required after migration, to authorize a throughput greater than 250 Mbps.

---

**Note**

If a Cisco Cloud Services Router 1000v or a Cisco Integrated Services Virtual Router have a throughput greater than 250 Mbps before upgrade, the system displays the throughput as set 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.
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.

- If a product instance had an HSECK9 PAK license before upgrade, you do not have to install a SLAC again after upgrade.

- 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.

### How Upgrade Affects Reporting for Existing Licenses

<table>
<thead>
<tr>
<th>Existing License</th>
<th>Reporting Requirements After Migration to Smart Licensing Using Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right-to-Use (RTU)</td>
<td>Depends on the license being used.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Smart Licensing (Registered and Authorized license)</td>
<td>Depends on the policy.</td>
</tr>
<tr>
<td>Specific License Reservation (SLR)</td>
<td>Required only if there is a change in license consumption.</td>
</tr>
<tr>
<td></td>
<td>An existing SLR authorization code authorizes existing license consumption after upgrade to Smart Licensing Using Policy.</td>
</tr>
<tr>
<td>Product Authorization Keys (PAK)</td>
<td>Required only if there is a change in license consumption.</td>
</tr>
<tr>
<td></td>
<td>PAK licenses have perpetual validity, but reporting is required if there is a change in license consumption.</td>
</tr>
<tr>
<td>Permanent License Reservation (PLR)</td>
<td>Not required.</td>
</tr>
<tr>
<td></td>
<td>PLR licenses have perpetual validity, and reporting is not required even if there is a change in license consumption.</td>
</tr>
<tr>
<td>Cisco Software Licensing (CSL)</td>
<td>Not required.</td>
</tr>
<tr>
<td></td>
<td>CSL licenses have perpetual validity, and reporting is not required even if there is a change in license consumption.</td>
</tr>
<tr>
<td>Evaluation or expired licenses</td>
<td>Based on the reporting requirements of the Cisco default policy.</td>
</tr>
</tbody>
</table>

### 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:

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

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, for applicable topologies.

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.

Downgrades

To downgrade, you must downgrade the software version on the product instance. This section provides information about downgrades for new deployments only.

New Deployment Downgrade

If you had a newly purchased product instance with a software version where Smart Licensing Using Policy was already enabled by default and you want to downgrade to a software version where Smart Licensing Using Policy is not supported, then the outcome of the downgrade depends on whether a Trust Code, on page 11 was installed while you were still operating in the Smart Licensing Using Policy environment.

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 as applicable in the Smart Licensing environment.

- 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.
CHAPTER 3

How to Configure Smart Licensing Using Policy: Workflows by Topology

This section provides sequential configuration information to implement Supported Topologies, in the simplest and fastest way.

- Workflow for Topology: Connected to CSSM Through CSLU, on page 27
- Workflow for Topology: Connected Directly to CSSM, on page 29
- Workflow for Topology: Connected to CSSM Through a Controller, on page 30
- Workflow for Topology: CSLU Disconnected from CSSM, on page 34
- Workflow for Topology: No Connectivity to CSSM and No CSLU, on page 37

Workflow for Topology: Connected to CSSM Through CSLU

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

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

Tasks for Product Instance-Initiated Communication

CSLU Installation → CSLU Preference Settings → Product Instance Configuration

1. **CSLU Installation**
   
   Where task is performed: A Windows host (laptop, desktop, or a Virtual Machine (VM))
   
   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.

2. **CSLU Preference Settings**
   
   Where tasks are performed: CSLU
   
   a. Logging into Cisco (CSLU Interface), on page 40
   
   b. Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 40
   
   c. Adding a Product-Initiated Product Instance in CSLU (CSLU Interface), on page 40
3. Product Instance Configuration

Where tasks are performed: Product Instance

a. Ensuring Network Reachability for Product Instance-Initiated Communication, on page 41

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
```

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 and if required, it sends a trust code request. To know when the product instance will be sending this information, enter the `show license all` command in privileged EXEC mode and in the output, check the date for field `Next report push:`.

CSLU forwards the information to CSSM and the returning ACK to the product instance, for installation. It gets the ACK from CSSM and sends this back to the product instance for installation.

Tasks for CSLU-Initiated Communication

CSLU Installation → CSLU Preference Settings → Product Instance Configuration

1. CSLU Installation
Where task is performed: A Windows host (laptop, desktop, or a Virtual Machine (VM)
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.

2. CSLU Preference Settings
Where tasks is performed: Product Instance
a. Logging into Cisco (CSLU Interface), on page 40
b. Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 40
c. Adding a CSLU-Initiated Product Instance in CSLU (CSLU Interface), on page 43
d. Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 43

3. Product Instance Configuration
Where tasks is performed: Product Instance
Ensuring Network Reachability for CSLU-Initiated Communication, on page 44

Result:
You can now collect and send a RUM report to CSSM, in CSLU, by navigating to the Actions for Selected… menu, and selecting Collect Usage. The RUM report is sent to CSSM. Along with this first report, if applicable and if required, CSLU sends a trust code request and an authorization code request to CSSM. It gets the ACK from CSSM and sends this back to the product instance for installation.

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.

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 49
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

- Option 2:
  Smart transport through an HTTPs proxy: See the Configuring Smart Transport Through an HTTPs Proxy, on page 52 section.

- Option 3:
  Configure Call Home service for direct cloud access. See the Configuring the Call Home Service for Direct Cloud Access, on page 53 section.

- 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 56 section.

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 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 63

   b. Having downloaded the token, you can now install the trust code on the product instance: Installing a Trust Code, on page 63

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 MB (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 59

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.

If you want to change your reporting interval to report more frequently: on the product instance, configure the license smart usage interval command. For more information, see license smart (global config), on page 77

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

<table>
<thead>
<tr>
<th>Product Instance</th>
<th>Minimum Required Cisco DNA Center Release</th>
<th>Minimum Required Cisco IOS XE Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 1000 Series Integrated Services Routers</td>
<td>Cisco DNA Center Release 2.2.2</td>
<td>Cisco IOS XE Amsterdam 17.3.2</td>
</tr>
<tr>
<td>Cisco 4000 Series Integrated Services Routers</td>
<td></td>
<td>Cisco IOS XE Amsterdam 17.3.2</td>
</tr>
<tr>
<td>Catalyst 8300 Series Edge Platforms</td>
<td></td>
<td>Cisco IOS XE Amsterdam 17.3.2</td>
</tr>
<tr>
<td>Catalyst 8500 Series Edge Platforms</td>
<td></td>
<td>Cisco IOS XE Amsterdam 17.3.2</td>
</tr>
<tr>
<td>Catalyst 8200 Series Edge Platforms</td>
<td></td>
<td>Cisco IOS XE Bengaluru 17.4.1</td>
</tr>
</tbody>
</table>

**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:

1. **Smart Account Set-Up**
   - Where tasks are performed: CSSM Web UI, [https://software.cisco.com/](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 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 Account 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 58
  
  b. Installing a File on the Product Instance, on page 66

- **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(config)# copy running-config startup-config

h. 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 63

Having downloaded the token, you can now install the trust code on the product instance: Installing a Trust Code, on page 63.

Device# license smart trust idtoken NGMwMjk5mYtNZaxMS00NzMZmtgWm all force
c. Request and install SLAC: Manually Requesting and Auto-Installing a SLAC, on page 59

Device# license smart authorization request add 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

CSLU Installation → CSLU Preference Settings → Product Instance Configuration → Download All for Cisco and Upload From Cisco

1. **CSLU Installation**

   Where task is performed: A Windows host (laptop, desktop, or a Virtual Machine (VM)

   Go to *Cisco Smart License Utility Quick Start Setup Guide*

2. **CSLU Preference Settings**

   Where tasks are performed: CSLU

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

   b. Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 40

   c. Adding a Product-Initiated Product Instance in CSLU (CSLU Interface), on page 40
3. **Product Instance Configuration**

   Where tasks are performed: Product Instance

   a. **Ensuring Network Reachability for Product Instance-Initiated Communication**, on page 41

   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
         ```

4. **Download All for Cisco and Upload From Cisco**

   Where tasks are performed: CSLU and CSSM

   a. **Download All For Cisco (CSLU Interface)**, on page 48

   b. **Uploading Usage Data to CSSM and Downloading an ACK**, on page 65

   c. **Upload From Cisco (CSLU Interface)**, on page 49

**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 and if required, it sends a trust code request. To know when the product instance will be sending this information, enter the `show license all` command in privileged EXEC mode and in the output, check the date for field `Next report push:`.

Since CSLU is disconnected from CSSM, you must save usage data which CSLU has collected from the product instance to a file. 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.

**Tasks for CSLU-Initiated Communication**

1. **CSLU Installation**
   - Where task is performed: A Windows host (laptop, desktop, or a Virtual Machine (VM))
   - Go to *Cisco Smart License Utility Quick Start Setup Guide*

2. **CSLU Preference Settings**
   - Where tasks is performed: Product Instance
   - In the CSLU Preferences tab, click the **Cisco Connectivity** toggle switch to off. The field switches to “Cisco Is Not Available”.
   - Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 40
   - Adding a CSLU-Initiated Product Instance in CSLU (CSLU Interface), on page 43
   - Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 43

3. **Product Instance Configuration**
   - Where tasks is performed: Product Instance
   - Ensuring Network Reachability for CSLU-Initiated Communication, on page 44

4. **Download All for Cisco and Upload From Cisco**
   - Where tasks are performed: CSLU and CSSM
   - Download All For Cisco (CSLU Interface), on page 48
   - Uploading Usage Data to CSSM and Downloading an ACK, on page 65
   - Upload From Cisco (CSLU Interface), on page 49

**Result:**

You can now collect and send a RUM report to CSSM, in CSLU, by navigating to the Actions for Selected… menu, and selecting Collect Usage. If applicable the report also includes a trust code request and authorization code request.

Since CSLU is disconnected from CSSM, you must save usage data which CSLU has collected from the product instance to a file. 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.

Workflow for Topology: No Connectivity to CSSM and No CSLU

Since you do not have to configure connectivity to any other component, the list of tasks required to set-up the topology is a small one. See, the **Results** section at the end of the workflow to know how you can complete requisite usage reporting after you have implemented this topology.

**Product Instance Configuration → Authorization Code Installation (Only if Applicable)**

1. **Product Instance Configuration**
   
   Where task is performed: Product Instance
   
   Set transport type to **off**.
   
   Enter the `license smart transport off` command in global configuration mode. Remember to save any changes to the configuration file.
   
   ```
   Device(config)# license smart transport off
   Device(config)# exit
   Device# copy running-config startup-config
   ```

2. **Authorization Code Installation (Only if Applicable)**
   
   Where tasks is performed: CSSM and then the Product Instance
   
   a. If you want to use a license that requires authorization before use (enforcement type: enforced or export-controlled): Generating and Downloading SLAC from CSSM to a File
   
   b. Install the downloaded SLAC file: Installing a File on the Product Instance, on page 66

**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 priviledged EXEC mode. In the example below, all RUM reports are saved to the flash memory of the product instance, in file `all_rum.txt`. See the `license smart (privileged EXEC), on page 82 command for command syntax details. In the example, 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
   ```

2. Upload usage data to CSSM: Uploading Usage Data to CSSM and Downloading an ACK, on page 65
3. Install the ACK on the product instance: Installing a File on the Product Instance, on page 66
Workflow for Topology: No Connectivity to CSSM and No CSLU
CHAPTER 4

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 40
- Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 40
- Adding a Product-Initiated Product Instance in CSLU (CSLU Interface), on page 40
- Ensuring Network Reachability for Product Instance-Initiated Communication, on page 41
- Adding a CSLU-Initiated Product Instance in CSLU (CSLU Interface), on page 43
- Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 43
- Ensuring Network Reachability for CSLU-Initiated Communication, on page 44
- Download All For Cisco (CSLU Interface), on page 48
- Upload From Cisco (CSLU Interface), on page 49
- Setting Up a Connection to CSSM , on page 49
- Configuring Smart Transport Through an HTTPs Proxy, on page 52
- Configuring the Call Home Service for Direct Cloud Access, on page 53
- Configuring the Call Home Service for Direct Cloud Access through an HTTPs Proxy Server, on page 56
- Requesting SLACs for Multiple Product Instances (CSLU Interface), on page 57
- Generating and Downloading SLAC from CSSM to a File, on page 58
- Manually Requesting and Auto-Installing a SLAC , on page 59
- Removing and Returning an Authorization Code, on page 61
- Removing the Product Instance from CSSM, on page 62
- Generating a New Token for a Trust Code from CSSM, on page 63
- Installing a Trust Code, on page 63
- Downloading a Policy File from CSSM, on page 65
- Uploading Usage Data to CSSM and Downloading an ACK, on page 65
- Installing a File on the Product Instance, on page 66
- Setting the Transport Type and URL, on page 67
- Sample Resource Utilization Measurement Report, on page 69
- HSECK9 License Mapping Table for Routing Product Instances, on page 69
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.

**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.

**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.

**Step 1**  Select the **Preferences tab**.
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 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 (product instance-initiated communication).

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-type-number`
4. `vrf forwarding vrf-name`
5. `ip address ip-address mask`
6. `negotiation auto`
7. `end`
8. `ip http client source-interface interface-type-number`
9. `ip route ip-address ip-mask subnet mask`
10. `{ip | ipv6} name-server server-address 1 ... server-address 6`
11. `ip domain lookup source-interface interface-type-number`
12. `ip domain name domain-name`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td>Example: <code>Device&gt;</code> <code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Device&gt;</code> <code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface <code>interface-type-number</code></td>
<td>Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.</td>
</tr>
<tr>
<td>Example: <code>Device (config)</code> <code>interface gigabitethernet0/0</code></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>4</td>
<td>vrf forwarding vrf-name</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# vrf forwarding Mgmt-vrf</td>
</tr>
<tr>
<td>5</td>
<td>ip address ip-address mask</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# ip address 192.168.0.1 255.255.0.0</td>
</tr>
<tr>
<td>6</td>
<td>negotiation auto</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# negotiation auto</td>
</tr>
<tr>
<td>7</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config-if)# end</td>
</tr>
<tr>
<td>8</td>
<td>ip http client source-interface interface-type-number</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip http client source-interface gigabitethernet0/0</td>
</tr>
<tr>
<td>9</td>
<td>ip route ip-address ip-mask subnet mask</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1</td>
</tr>
<tr>
<td>10</td>
<td>[ip</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# Device(config)# ip name-server vrf mgmt-vrf 173.37.137.85</td>
</tr>
<tr>
<td>11</td>
<td>ip domain lookup source-interface interface-type-number</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip domain lookup source-interface gigabitethernet0/0</td>
</tr>
<tr>
<td>12</td>
<td>ip domain name domain-name</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Device(config)# ip domain name example.com</td>
</tr>
</tbody>
</table>
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

Step 1
Go to the Inventory tab and from the Product Instances table, select Available Actions → Add Single Product Instance.

Step 2
Enter the Host (IP Address) of the Host.

Step 3
Select the Connect Method and select an appropriate CSLU Initiated connect method.

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.
If you click General, the detailed Add Product modal opens.

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 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 Instance, filling in the Host name and selecting a CSLU Initiated connect method), select Actions for Selected > Collect Usage. CSLU connects to the selected Product Instance(s) 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 Product Instances > Download for Cisco.

If you are working in CSLU-initiated mode, complete these steps to configure CSLU to collect RUM reports from Product Instances.

Step 1
Select the Preference tab and enter a valid Smart Account and Virtual Account, and then select an appropriate CSLU Initiated collect method. (If there have been any changes in Preferences, make sure you click Save.)

Step 2
Open the Inventory tab and select one or more Product Instances.

Step 3
From the CSLU main screen, select Available actions > 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 to Cisco, select Download for Cisco from the Product Instances Menu.

Step 4

From the Download for Cisco 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 Usage Data to CSSM and Downloading an ACK, on page 65.

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).

**SUMMARY STEPS**

1. enable
2. configure terminal
3. aaa new model
4. aaa authentication login default local
5. aaa authorization exec default local
6. ip routing
7. 
   | ip | ipv6 | name-server server-address 1 ...server-address 6 |
8. ip domain lookup source-interface interface-type-number
9. ip domain name name
10. no username name
11. username name privilege level password password
12. `interface interface-type-number`
13. `vrf forwarding vrf-name`
14. `ip address ip-address mask`
15. `negotiation auto`
16. `no shutdown`
17. `end`
18. `ip http server`
19. `ip http authentication local`
20. `ip http secure-server`
21. `ip http max-connections`
22. `ip tftp source-interface interface-type-number`
23. `ip route ip-address ip-mask subnet mask`
24. `logging host`
25. `end`
26. `show ip http server session-module`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>aaa new model</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa new model</td>
</tr>
<tr>
<td></td>
<td>(Required) Enable the authentication, authorization, and accounting (AAA) access control model.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>aaa authentication login default local</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa authentication login default local</td>
</tr>
<tr>
<td></td>
<td>(Required) Sets AAA authentication to use the local username database for authentication.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>aaa authorization exec default local</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa authorization exec default local</td>
</tr>
<tr>
<td></td>
<td>Sets the parameters that restrict user access to a network. The user is allowed to run an EXEC shell.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>ip routing</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ip routing</td>
</tr>
<tr>
<td></td>
<td>Enables IP routing.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>(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.</td>
</tr>
<tr>
<td>{ip</td>
<td>ipv6} name-server server-address 1 ... server-address 6</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>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).</td>
</tr>
<tr>
<td>ip domainlookup source-interface interface-type-number</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ip domainlookup source-interface gigabitethernet0/0</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).</td>
</tr>
<tr>
<td>ip domain name name</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ip domain name vrf Mgmt-vrf cisco.com</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>(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 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.</td>
</tr>
<tr>
<td>no username name</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# no username admin</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>(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.</td>
</tr>
<tr>
<td>username name privilege level password password</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# username admin privilege 15 password 0 lab</td>
</tr>
</tbody>
</table>

### Note
Enter this username and password in CSLU (Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 43 → Step 4. f. CSLU can then collect RUM reports from the product instance.)
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td><code>interface interface-type-number</code></td>
<td>Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device (config)# interface gigabitethernet0/0</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td><code>vrf forwarding vrf-name</code></td>
<td>Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-if)# vrf forwarding Mgmt-vrf</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td><code>ip address ip-address mask</code></td>
<td>Defines the IP address for the VRF.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-if)# ip address 192.168.0.1 255.255.0.0</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td><code>negotiation auto</code></td>
<td>Enables auto-negotiation operation for the speed and duplex parameters of an interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-if)# negotiation auto</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td><code>no shutdown</code></td>
<td>Restarts a disabled interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-if)# no shutdown</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td><code>end</code></td>
<td>Exits the interface configuration mode and enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-if)# end</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td><code>ip http server</code></td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# ip http server</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td><code>ip http authentication local</code></td>
<td>(Required) Specifies a particular authentication method for HTTP server users. The <code>local</code> keyword means that the login user name, password and privilege level access combination specified in the local system configuration (by the <code>username</code> global configuration command) should be used for authentication and authorization.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# ip http authentication local</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td><code>ip http secure-server</code></td>
<td>(Required) Enables a secure HTTP (HTTPS) server. The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# ip http server</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td><code>ip http max-connections</code></td>
<td>(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.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config)# ip http max-connections 16</td>
<td></td>
</tr>
<tr>
<td><strong>Step</strong></td>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>---------</td>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Step 22</td>
<td><code>ip tftp source-interface interface-type-number</code></td>
<td>Specifies the IP address of an interface as the source address for TFTP connections. <strong>Example:</strong> Device(config)# <code>ip tftp source-interface GigabitEthernet0/0</code></td>
</tr>
<tr>
<td>Step 23</td>
<td><code>ip route ip-address ip-mask subnet mask</code></td>
<td>Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route. <strong>Example:</strong> Device(config)# <code>ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1</code></td>
</tr>
<tr>
<td>Step 24</td>
<td><code>logging host</code></td>
<td>Logs system messages and debug output to a remote host. <strong>Example:</strong> Device(config)# <code>logging host 172.25.33.20 vrf Mgmt-vrf</code></td>
</tr>
<tr>
<td>Step 25</td>
<td><code>end</code></td>
<td>Exits the global configuration mode and enters privileged EXEC mode. <strong>Example:</strong> Device(config)# <code>end</code></td>
</tr>
<tr>
<td>Step 26</td>
<td><code>show ip http server session-module</code></td>
<td>(Required) Verifies HTTP connectivity. In the output, check that <code>SL_HTTP</code> 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 <code>https://&lt;product-instance-ip&gt;/</code>. This ensures that the REST API from CSLU to the product instance works as expected. <strong>Example:</strong> Device# <code>show ip http server session-module</code></td>
</tr>
</tbody>
</table>

**Download All For Cisco (CSLU Interface)**

The Download All for Cisco menu option is a manual process used for offline purposes. Complete these steps to use the Download For Cisco menu option.

**Step 1** From the CSLU Preferences Tab screen, click the **Cisco Connectivity** toggle switch to **off**. The field switches to “Cisco Is Not Available”.

**Step 2** Navigate to **Product Instances > Download All For Cisco**

**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  Go to a station that has connectivity to Cisco, and complete the following: Uploading Usage Data to CSSM and Downloading an ACK, on page 65
Once the file is downloaded, you can transfer to CSLU.

Step 5  Click Upload From Cisco. See: Upload From Cisco (CSLU Interface), on page 49.

Upload From Cisco (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.

Step 1  Make sure you have downloaded the ACK file for the device. See: Download All For Cisco (CSLU Interface), on page 48

Step 2  From the CSLU main screen, select Product Instance > Upload from Cisco.

Step 3  A Cisco File Upload modal opens 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 ACK 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.

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:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. (ip | ipv6) name-server server-address 1 ...server-address 6
4. ip name-server vrf Mgmt-vrf server-address 1...server-address 6
5. ip domain lookup source-interface interface-type interface-number
6. ip domain name domain-name
7. ip host tools.cisco.com ip-address
8. interface interface-type-number
9. ntp server ip-address [version number] [key key-id] [prefer]
10. switchport access vlan vlan_id
### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>`{ip</td>
<td>ipv6} name-server server-address 1 ... server-address 6`</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config)# ip name-server 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>ip name-server vrf Mgmt-vrf server-address 1 ... server-address 6</code></td>
<td>(Optional) Configures DNS on the VRF interface. You can specify up to six name servers. Separate each server address with a space. <strong>Note</strong> This command is an alternative to the <code>ip name-server</code> command.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config)# ip name-server vrf Mgmt-vrf 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>ip domain lookup source-interface interface-type interface-number</code></td>
<td>Configures the source interface for the DNS domain lookup.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config)# ip domain lookup source-interface Vlan100</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>ip domain name domain-name</code></td>
<td>Configures the domain name.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config)# ip domain name example.com</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>ip host tools.cisco.com ip-address</code></td>
<td>Configures static hostname-to-address mappings in the DNS hostname cache if automatic DNS mapping is not available.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Device(config)# ip host tools.cisco.com 209.165.201.30</code></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>8</td>
<td>interface interface-type-number</td>
<td>Configures a Layer 3 interface. Enter an interface type and number or a VLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface Vlan100</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ip address 192.0.2.10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>ntp server ip-address [version number] [key key-id] [prefer]</td>
<td>(Required) Activates the NTP service (if it has not already been activated) and enables the system to synchronize the system software 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.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ntp server 198.51.100.100 version 2 prefer</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>switchport access vlan vlan_id</td>
<td>Enables the VLAN for which this access port carries traffic and sets the interface as a nontrunking nontagged single-VLAN Ethernet interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface GigabitEthernet1/0/1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switchport access vlan 100</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switchport mode access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config-if)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)#</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>ip route ip-address ip-mask subnet mask</td>
<td>Configures a route on the device. You can configure either a static route or a dynamic route.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ip route 192.0.2.0 255.255.255.255</td>
<td></td>
</tr>
<tr>
<td></td>
<td>192.0.2.1</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>ip http client source-interface interface-type-number</td>
<td>(Required) Configures a source interface for the HTTP client. Enter an interface type and number or a VLAN.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ip http client source-interface Vlan100</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>exit</td>
<td>Exits global configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device(config)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>copy running-config startup-config</td>
<td>Saves your entries in the configuration file.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>
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.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `license smart transport smart`
4. `license smart url default`
5. `license smart proxy {address address_hostname | port port_num}`
6. `exit`
7. `copy running-config startup-config`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>license smart transport smart</code></td>
<td>Enables Smart transport mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# license smart transport smart</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>license smart url default</code></td>
<td>Automatically configures the Smart URL (<a href="https://smartreceiver.cisco.com/licservice/license">https://smartreceiver.cisco.com/licservice/license</a>). For this option to work as expected, the transport mode in the previous step must be configured as <code>smart</code>.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# license smart transport default</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>`license smart proxy {address address_hostname</td>
<td>port port_num}`</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Device(config)# license smart proxy 198.51.100.10 port 3128</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>• <em>address address_hostname</em>: Specifies the proxy address. Enter the IP address or hostname of the proxy server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <em>port port_num</em>: Specifies the proxy port. Enter the proxy port number.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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)”.

---

**SUMMARY STEPS**

1. enable
2. configure terminal
3. license smart transport callhome
4. license smart url url
5. service call-home
6. call-home
7. contact-email-address email-address
8. profile name
9. active
10. destination transport-method http {email | http}
11. destination address { email email_address | http url}
12. exit
13. exit
14. copy running-config startup-config
15. show call-home profile {name | all}
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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**
| *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-address 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
  ```
### Command or Action

| Step 9 | `active` |
| Example: | Device(config-call-home-profile)# `active` |

| 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` |

| Step 11 | `destination address { email email_address | http url}` |

| Step 12 | `exit` |
| Example: | Device(config-call-home-profile)# `exit` |

| Step 13 | `exit` |
| Example: | Device(config-call-home)# `end` |

| Step 14 | `copy running-config startup-config` |
| Example: | Device# `copy running-config startup-config` |

| Step 15 | `show call-home profile {name | all}` |

### Purpose

- **anonymous-reporting-only.** When this is set, only crash, inventory, and test messages will be sent.
  
  Use the `show call-home profile all` command to check the profile status.

  Enables the destination profile.

  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.

  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://`.

  Exits Call Home destination profile configuration mode and returns to Call Home configuration mode.

  Exits Call Home configuration mode and returns to privileged EXEC mode.

  Saves your entries in the configuration file.

  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:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. license smart transport callhome
4. service call-home
5. call-home
6. http-proxy *proxy-address* *proxy-port* *port-number*
7. exit
8. exit
9. copy running-config startup-config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> license smart transport callhome</td>
<td>Enables Call Home as the transport mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# license smart transport callhome</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> service call-home</td>
<td>Enables the Call Home feature.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Device(config)# service call-home</td>
<td>Enters Call Home configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> call-home</td>
<td>Configures the proxy server information to the Call Home service.</td>
</tr>
<tr>
<td>Example: Device(config)# call-home</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> http-proxy proxy-address proxy-port port-number</td>
<td>Exits Call Home configuration mode and enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device(config-call-home)# http-proxy 198.51.100.10 port 5000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits global configuration mode and enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device(config-call-home)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td></td>
</tr>
<tr>
<td>Example: Device(config)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> copy running-config startup-config</td>
<td>Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Example: Device# copy running-config startup-config</td>
<td></td>
</tr>
</tbody>
</table>

### 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

**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.

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

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.

Step 1
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.

Step 2
Click the Inventory tab.

Step 3
Click the Product Instances tab

Step 4
Click the Authorize License Enforced Features tab.

Step 5
Enter the PID and Serial Number.

**Note**
Do not populate any of the other fields.
Step 6  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 69 for reference.

Step 7  Click Next
Step 8  Click Generate Authorization Code
Step 9  Download the authorization code and save as a .csv file.
Step 10 Install the file on the product instance. See Installing a File on the Product Instance, on page 66.

Manually Requesting and Auto-Installing a SLAC

To request CSSM 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

Before you proceed, check the following as well:

- The product instance on which you are requesting the SLAC is connected CSSM or CSLU.
- 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:
- A trust code is installed, if you are directly connected to CSSM. Enter the show license all command in privileged EXEC mode. In the output check field Trust Code Installed:

SUMMARY STEPS

1. enable
2. license smart authorization request { add | replace } feature_name { all | local }
3. show license authorization

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>
| Step 2 license smart authorization request { add | replace } feature_name { all | local } | The license smart authorization request command requests a SLAC from CSSM or CSLU (CSSLU in-turn}
Manually Requesting and Auto-Installing a SLAC

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# license smart authorization request add hseck9 local</td>
<td>fetches it from CSSM). A SLAC is returned and automatically installed on the product instance. Specify if you want to add to or replace an existing SLAC:</td>
</tr>
<tr>
<td></td>
<td>• <strong>add</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>replace</strong>: 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.</td>
</tr>
<tr>
<td></td>
<td>For <strong>feature_name</strong>, 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:</td>
</tr>
<tr>
<td></td>
<td>• <strong>all</strong>: Gets the authorization code for <strong>all</strong> devices in a High Availability set-up</td>
</tr>
<tr>
<td></td>
<td>• <strong>local</strong>: Gets the authorization code for the <strong>active</strong> 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:</td>
</tr>
<tr>
<td></td>
<td>• Only on Cisco 1000, 4000 Series Integrated Services Routers, and Catalyst 8300 Edge Platforms:</td>
</tr>
<tr>
<td></td>
<td><strong>license feature feature_name</strong>: Enables the feature to automatically request the code.</td>
</tr>
<tr>
<td></td>
<td>Device# license feature hseck9</td>
</tr>
<tr>
<td></td>
<td>• Only on Catalyst 8000V Edge Software, Cisco Cloud Services Router 1000v, Cisco Integrated Services Virtual Routers:</td>
</tr>
<tr>
<td></td>
<td>**platform hardware throughput level MB {500</td>
</tr>
<tr>
<td></td>
<td>Device(config)# platform hardware throughput level MB 5000</td>
</tr>
</tbody>
</table>

**Step 3**

<table>
<thead>
<tr>
<th>Example: show license authorization</th>
<th>Displays the authorization code installed on the product instance.</th>
</tr>
</thead>
</table>

Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
Removing and Returning an Authorization Code

To remove an authorization code for a license and to return it to your license pool in CSSM, complete the following steps. You can use this procedure for all authorization codes (SLAC, SLR, PLR, etc.).

Before you begin

Supported topologies: all

SUMMARY STEPS

1. enable
2. show license summary
3. license smart authorization return {all | local} {offline [path] | online}
4. show license all

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>show license summary</td>
<td>Ensure that the license that you want to remove and return is not in-use. If it is in-use, you must first disable the feature.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# show license summary</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>license smart authorization return {all</td>
<td>local} {offline [path]</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# license smart authorization return local online</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# license smart authorization return local offline</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter this return code in Cisco Smart Software Manager portal: UDI: PID:CSR1000V, SN: 9NOG5XBLCO7 Return code: Cr9JHx-L1x5Rj-ftwzg1-h9QZAU-L5DT1-babWol-FABPf9-Wk1Dn7-Rp7</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>show license all</td>
<td></td>
</tr>
</tbody>
</table>

Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
Removing the Product Instance from CSSM

If you return an authorization code using the `offline` keyword, that is, you have configured `license smart authorization return {all | local} offline [path]`, you must manually enter the return code in CSSM. To complete the return process for `offline` option, complete the following task:

**Before you begin**

Supported topologies: No Connectivity to CSSM and No CSLU

**Step 1**
Log in to the CSSM Web UI at [https://software.cisco.com](https://software.cisco.com) and click **Smart Software Licensing**.

Log in using the username and password provided by Cisco.

**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**
Click the required product instance to expand the same.
The Overview window is displayed.

**Step 7**
From the Actions drop-down list, choose Remove.
The Remove Product Instance window is displayed.

**Step 8**
In the Reservation Return Code field, enter the return code.
**Step 9**
Click Remove Product Instance.
The license is returned to the license pool.

---

### 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

**Step 1**
Log in to the CSSM Web UI at [https://software.cisco.com](https://software.cisco.com) and click Smart Software Licensing.
Log in using the username and password provided by Cisco.

**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.

**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.

---

### Installing a Trust Code

To manually install a trust code, complete the following steps

**Before you begin**
Supported topologies:
SUMMARY STEPS

1. Generating a New Token for a Trust Code from CSSM, on page 63
2. `enable`
3. `license smart trust idtoken id_token_value {local | all} [force]`
4. `show license status`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Generating a New Token for a Trust Code from CSSM, on page 63</td>
<td>In case you have not completed this already, generate and download a trust code file from CSSM.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode. Enter your password, if prompted</td>
</tr>
<tr>
<td>Example: <code>Device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> `license smart trust idtoken id_token_value {local</td>
<td>all} [force]`</td>
</tr>
<tr>
<td>Example: <code>Device# license smart trust idtoken NGMwMjk5mYtnZaxM500NzMzmtgMm all force</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>show license status</code></td>
<td>Displays date and time if trust code is installed. Date and time are in the local time zone.</td>
</tr>
</tbody>
</table>
**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

---

**Step 1**
Log in to the CSSM Web UI at [https://software.cisco.com](https://software.cisco.com) and click **Smart Software Licensing**.

Log in using the username and password provided by Cisco.

**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 66

---

**Uploading Usage Data to CSSM and Downloading an ACK**

To upload a RUM report to CSSM and download an ACK when the product instance is not connected to CSSM or CSLU, complete the following task:

**Before you begin**

Supported topologies: No Connectivity to CSSM and No CSLU

---

**Step 1**
Log in to the CSSM Web UI at [https://software.cisco.com](https://software.cisco.com).

Log in using the username and password provided by Cisco.

**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**.

You cannot delete a usage report in CSSM, after it has been uploaded.

**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 it 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 .txt ACK file for the report you uploaded.
Wait for the ACK to appear in the Acknowledgement column. If there many RUM reports to process, CSSM may take a few minutes.
You can now install the file on the product instance or you can transfer it to CSLU.

## Installing a File on the Product Instance

To install a SLAC, or policy, or ACK, or token on the product instance when the product instance is not connected to CSSM or CSLU, 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 58
- For a policy, see Downloading a Policy File from CSSM, on page 65
- For an ACK, see Uploading Usage Data to CSSM and Downloading an ACK, on page 65

### SUMMARY STEPS

1. enable
2. copy source bootflash:file-name
3. license smart import bootflash:file-name
4. show license all

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> copy source bootflash:file-name</td>
<td>Copies the file from its source location or directory to the flash memory of the product instance.</td>
</tr>
<tr>
<td>Example: Device# copy tftp://10.8.0.6/example.txt bootflash:</td>
<td></td>
</tr>
</tbody>
</table>

### Notes

- **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.
Setting the Transport Type and URL

To configure the mode of transport for a product instance, complete the following task:

**Before you begin**

Supported topologies: all

**SUMMARY STEPS**

1. enable
2. ```configure terminal```
3. ```license smart transport { automatic | callhome | cslu | off | smart }```  
4. ```license smart url { url | cslu | cslu_url | default | smart | smart_url | utility | smart_url }```  
5. ```license smart usage interval interval_in_days```  

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode. Enter your password, if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 license smart transport</td>
<td>Selects the type of message transport the product instance will use. Choose from the following options:</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# license smart transport cslu</td>
<td></td>
</tr>
</tbody>
</table>

- **automatic**: Sets the transport mode to default, which is CSLU.
- **callhome**: Enables Call Home as the transport mode.
## Setting the Transport Type and URL

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>cslu</strong>: Enables CSLU as the transport mode. This is the default transport mode.</td>
<td></td>
</tr>
<tr>
<td>• <strong>off</strong>: Disables all communication from the product instance.</td>
<td></td>
</tr>
<tr>
<td>• <strong>smart</strong>: Enables Smart transport.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 4

**license smart url**

- `url` | `cslu cslu_url` | `default` | `smart smart_url` | `utility smart_url`

_sets URL that is used for the configured transport mode. Depending on the transport mode you've chosen in the previous step, configure the corresponding URL here:*

**Example:**

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

- **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`

- **cslu cslu_url**: If you have configured the transport mode as `cslu`, configure this option. Enter the CSLU 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.

- **default**: Configure this option to use the default connection to CSSM. The default URL is as follows:

  `http://cslu-local:8182/cslu/v1/pi`

- **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. No further action is required for this duplicate entry.

- **utility smart_url**: Although visible on the CLE, this option is not supported.

### Step 5

**license smart usage interval**

_sets the reporting interval in days. By default the RUM report is sent every 30 days. The valid value range is 1 to 3650.*

**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 do not configure an interval, the reporting interval is determined entirely by the policy.
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
<?xml version="1.0" encoding="UTF-8"?
 <smartLicense>

 </smartLicense>

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 58), 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.
<table>
<thead>
<tr>
<th>Product Family</th>
<th>PID</th>
<th>License Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISR1K-8P</td>
<td>C1111-8P</td>
<td>ISR_1100_8P_Hsec</td>
</tr>
<tr>
<td></td>
<td>C1111-8PLTEEA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PLTELA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PWB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PWA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PWZ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PWQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PWC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PWR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PWK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PWS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PLTEEAWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PLTEEAWB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PLTEEAWA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PLTEEAWR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PLTELAWZ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PLTELAWN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PLTELAWQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PLTELAWC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PLTELAWK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PLTELAWD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PLTELAWA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-8PLTELAWS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1116-8P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1116-8PLTEEA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-8P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-8PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-8PLTEEA</td>
<td></td>
</tr>
<tr>
<td>Product Family</td>
<td>PID</td>
<td>License Name</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------</td>
<td>----------------------</td>
</tr>
<tr>
<td></td>
<td>C1117-8PLTELA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-8PMLTEEA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-8PWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-8PWA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-8PWZ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-8PMWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-8PLTEEAW</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-8PLTELAWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-8PLTELAWZ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111X-8P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1112-8P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1112-8PLTEEAA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1113-8P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1113-8PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1113-8PLTEEAA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1113-8PLTELA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1113-8PMLTEEA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1113-8PWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1113-8PWZ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1113-8PMWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1113-8PLTEEAW</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1113-8PLTE LAWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1113-8PLTELAWZ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1114-8P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1114-8PLTEEAA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1115-8P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1115-8PLTEEAA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1115-8PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1115-8PMLTEEA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1118-8P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1121-8PLTEPWE</td>
<td></td>
</tr>
<tr>
<td>Product Family</td>
<td>PID</td>
<td>License Name</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------</td>
<td>--------------</td>
</tr>
<tr>
<td></td>
<td>C1121-8PLTEPWB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1121-8PLTEPWZ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1121-8PLTEPWQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1121-8PLTEP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1121X-8PLTEP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1121-8P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1121X-8P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1161-8P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1161X-8P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1161-8PLTEP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1161X-8PLTEP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1126-8PLTEP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1127-8PLTEP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1127-8PMLTEP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1126X-8PLTEP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1127X-8PLTEP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1127X-8PMLTEP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1128-8PLTEP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1121X-8PLTEPWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1121X-8PLTEPWB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1121X-8PLTEPWZ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1121X-8PLTEPWA</td>
<td></td>
</tr>
<tr>
<td>Product Family</td>
<td>PID</td>
<td>License Name</td>
</tr>
<tr>
<td>---------------</td>
<td>-----</td>
<td>-----------------------</td>
</tr>
<tr>
<td>ISR1K - 4P</td>
<td>C1111-4P</td>
<td>ISR_1100_4P_Hsec</td>
</tr>
<tr>
<td></td>
<td>C1111-4PLTEEA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-4PLTELA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-4PWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-4PWB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-4PWA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-4PWZ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-4PWN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-4PWQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-4PWC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-4PWR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-4PWK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111-4PWD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1111X-4P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1116-4P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1116-4PLTEEA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1116-4PLTEEAWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1116-4PWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-4P</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-4PLTEEA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-4PLTELA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-4PLTEEAWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-4PLTEEAWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-4PLTEEAWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-4PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-4PMLTEEA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-4PMLTEEAWE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C1117-4PMWE</td>
<td></td>
</tr>
<tr>
<td>Product Family</td>
<td>PID</td>
<td>License Name</td>
</tr>
<tr>
<td>----------------</td>
<td>-----</td>
<td>--------------</td>
</tr>
<tr>
<td>C1101-4P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1101-4PLTEPC1101-4PLTEPWE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1101-4PLTEPWB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1101-4PLTEPWD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1101-4PLTEPWZ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1101-4PLTEPWA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1101-4PLTEPWH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1101-4PLTEPWQ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1101-4PLTEPWR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1101-4PLTEPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1101-4PLTEPWF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-4PLTE2P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-4PLTE2PWB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-4PLTE2PWD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-4PLTE2PWE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-4PLTE2PWZ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-4PLTE2PWA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-4PLTE2PWH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-4PLTE2PWQ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-4PLTE2PWR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-4PLTE2PWN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-4PLTE2PWF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1118-4P</td>
<td></td>
<td>ISR_1100_2P_Hsec</td>
</tr>
<tr>
<td>C1121-4P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1121-4PLTEP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISR1K-2P</td>
<td>C1109-2PLTEGB</td>
<td></td>
</tr>
<tr>
<td>C1109-2PLTEUS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-2PLTEVZ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-2PLTEJN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-2PLTEAU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C1109-2PLTEIN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product Family</td>
<td>PID</td>
<td>License Name</td>
</tr>
<tr>
<td>---------------</td>
<td>-----</td>
<td>--------------</td>
</tr>
<tr>
<td>ISR4200</td>
<td>ISR4221/K9</td>
<td>ISR4220_HSEC</td>
</tr>
<tr>
<td></td>
<td>ISR4221X/K9</td>
<td></td>
</tr>
<tr>
<td>ISR4300</td>
<td>ISR4321/K9</td>
<td>ISR_4321_Hsec</td>
</tr>
<tr>
<td></td>
<td>ISR4331/K9</td>
<td>ISR_4331_Hsec</td>
</tr>
<tr>
<td></td>
<td>ISR4351/K9</td>
<td>ISR_4531_Hsec</td>
</tr>
<tr>
<td>ISR4400</td>
<td>ISR4431/K9</td>
<td>ISR_4400_Hsec</td>
</tr>
<tr>
<td></td>
<td>ISR4451/K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISR4451-X/K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISR4461/K9</td>
<td></td>
</tr>
<tr>
<td>C8300</td>
<td>C8300-1N1S-4T2X</td>
<td>Router US Export Lic for DNA</td>
</tr>
<tr>
<td></td>
<td>C8300-1N1S-6T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C8300-2N2S-4T2X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C8300-2N2S-6T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C8300-1N1S-4G2X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C8300-1N1S-6G</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C8300-2N2S-4G2X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C8300-2N2S-6G</td>
<td></td>
</tr>
<tr>
<td>C8200</td>
<td>C8200-1N-4T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C8200-1N-1G</td>
<td></td>
</tr>
<tr>
<td>ISR1100</td>
<td>ISR1100-6G</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISR1100-4G</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISR1100-4GLTENA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISR1100-4GLTEGB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISR1100X-4G</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISR1100X-6G</td>
<td></td>
</tr>
<tr>
<td>C8500</td>
<td>C8500-12X4QC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C8500-12X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C8500L-8S4X</td>
<td></td>
</tr>
<tr>
<td>C8000V</td>
<td>not applicable</td>
<td></td>
</tr>
<tr>
<td>CSR1000V</td>
<td>not applicable</td>
<td></td>
</tr>
<tr>
<td>ISRV</td>
<td>not applicable</td>
<td></td>
</tr>
</tbody>
</table>
HSECK9 License Mapping Table for Routing Product Instances
CHAPTER 5

Command Reference for Smart Licensing Using Policy

This section provides complete command syntax information for Smart Licensing commands.

- license smart (global config), on page 77
- license smart (privileged EXEC), on page 82
- show license all, on page 86
- show license authorization, on page 89
- show license data, on page 98
- show license eventlog, on page 98
- show license history message, on page 101
- show license reservation, on page 102
- show license status, on page 102
- show license summary, on page 110
- show license tech, on page 112
- show license udi, on page 118
- show license usage, on page 119
- show platform software sl-infra, on page 123

license smart (global config)

To configure licensing-related settings such as the mode of transport and the URL that the product instance uses to communicate with Cisco Smart Software Manager (CSSM), to configure the usage reporting interval, to configure the information that must be excluded or included in a usage report, 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_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 | postalcode postalcode | state state | street street } } }

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_url | default | smart smart_url | utility secondary_url } | usage { customer-tags { tag1 | tag2 | tag3 | tag4 } | tag_value } | interval interval_in_days | utility }

Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>custom_id ID</strong></td>
<td>Although visible on the CLI, this option is not supported.</td>
</tr>
<tr>
<td><strong>enable</strong></td>
<td>Although visible on the CLI, configuring this keyword has no effect. Smart licensing is always enabled.</td>
</tr>
<tr>
<td>**privacy all</td>
<td>hostname</td>
</tr>
<tr>
<td></td>
<td>• <strong>all</strong>: Sends only the minimal licensing information in any communication.</td>
</tr>
<tr>
<td></td>
<td>• <strong>hostname</strong>: Excludes the hostname from any communication.</td>
</tr>
<tr>
<td></td>
<td>• <strong>version</strong>: Excludes Smart Agent version information from any communication. The Smart Agent resides on every product instance.</td>
</tr>
<tr>
<td>**proxy address address_hostname</td>
<td>port port**</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Configure the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>address address_hostname</strong>: Configures the proxy address.</td>
</tr>
<tr>
<td></td>
<td>For <strong>address_hostname</strong>, enter the IP address or hostname of the proxy.</td>
</tr>
<tr>
<td></td>
<td>• <strong>port port</strong>: Configures the proxy port.</td>
</tr>
<tr>
<td></td>
<td>For <strong>port</strong>, enter the proxy port number.</td>
</tr>
<tr>
<td><strong>reservation</strong></td>
<td>Enables or disables a license reservation feature.</td>
</tr>
<tr>
<td><strong>server-identity-check</strong></td>
<td>Enables or disables the HTTP secure server identity check.</td>
</tr>
</tbody>
</table>

**Note**: Although visible on the CLI, this option is not applicable in the Smart Licensing Using Policy environment, because license reservation is no longer required. To request and install an authorization code, use the license smart authorization request command in privileged exec mode instead. See license smart (privileged EXEC), on page 82.
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.
- **off**: Disables all communication from the product instance.
- **smart**: Enables Smart transport.
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:

```plaintext
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

The `no license smart url` command reverts to the default URL.

- **cslu cslu_url**: If you have configured the transport mode as `cslu`, configure this option. Enter the CSLU URL as follows:

```plaintext
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` 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:

```plaintext
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_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 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.

utility [ customer_info \{ city city \| country country \| postalcode postalcode \| state state \| street street \} ]

Although visible on the CLI, this option is not supported.

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2</td>
</tr>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
The following keywords and variables were introduced with Smart Licensing Using Policy:

- Under the `url` keyword, these options were introduced:

  ```
  { cslu | 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`.

### Usage Guidelines

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 communication 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.

### license smart (privileged EXEC)

To configure licensing functions such as requesting or returning authorization codes, saving Resource Utilization Measurement reports (RUM reports), importing files 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), 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 } feature_name { all | local } | return { all | local } } | offline { path | online } } | clear eventlog | export return { all | local } feature_name | factory reset | 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 }]
```

### Syntax Description

- **smart**
  Provides options for Smart Licensing.

- **authorization**
  Provides the option to request for, or return, authorization codes.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request</td>
<td>Requests an authorization code from CSSM or CSLU (CSLU in-turn fetches it from CSSM) and installs it on the product instance.</td>
</tr>
<tr>
<td>add</td>
<td>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.</td>
</tr>
<tr>
<td>replace</td>
<td>Replaces the existing authorization code. The new authorization code will contain only the requested license. All licenses in the current authorization code are returned. 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>feature_name</td>
<td>Name of the license for which you are requesting an authorization code.</td>
</tr>
<tr>
<td>all</td>
<td>Performs the action for all product instances in a High Availability configuration.</td>
</tr>
<tr>
<td>local</td>
<td>Performs the action for the active product instance. This is the default option.</td>
</tr>
<tr>
<td>return</td>
<td>Returns an authorization code back to the license pool in CSSM.</td>
</tr>
<tr>
<td>offline file_path</td>
<td>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.</td>
</tr>
<tr>
<td>online</td>
<td>Means that the product instance is in a connected mode. The authorization code is returned to CSLU or CSSM directly.</td>
</tr>
<tr>
<td>clear eventlog</td>
<td>Clears all event log files from the product instance.</td>
</tr>
<tr>
<td>export return</td>
<td>Returns the authorization key for an export-controlled license.</td>
</tr>
<tr>
<td>factory reset</td>
<td>Clears all saved Smart Licensing information from the product instance.</td>
</tr>
<tr>
<td>import filepath_filename</td>
<td>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.</td>
</tr>
<tr>
<td>save</td>
<td>Provides options to save RUM reports or trust code requests.</td>
</tr>
<tr>
<td>trust-request filepath_filename</td>
<td>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.</td>
</tr>
</tbody>
</table>
usage \{ all | days \textit{days} | rum-id \textit{rum-ID} | unreported \} \{ file \textit{file_path} \}

Saves RUM reports (license usage information) in the specified location. You must specify one of these options:

- **all**: Saves all RUM reports.
- **days \textit{days}**: Saves RUM report for the last \textit{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 \textit{rum-ID}**: Saves a specified RUM ID. The valid value range is 0 to 18446744073709551615.
- **unreported**: Saves all unreported RUM reports.

**file \textit{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 CSLU or CSSM, 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 \textit{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 \textit{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 \texttt{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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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 }

### Usage Guidelines

Smart Licensing Using Policy is enabled by default. A no form of **license smart** command in privileged EXEC mode is not available.

Entering the **licence smart factory reset** removes all Smart licensing information 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 Authorization, or RMA), or being decommissioned permanently. We also recommend that you send a RUM report to CSSM, before licensing information is removed from the product instance, to ensure that CSSM has up-to-date usage information.

### Examples

- Example: SLAC installed on Cisco 4000 Series Integrated Services Routers, on page 85

- Example: SLAC returned for Cisco 4000 Series Integrated Services Routers, on page 86

### Example: SLAC installed on Cisco 4000 Series Integrated Services Routers

The following sample output of the **license smart authorization request add** command shows how a SLAC is requested and automatically installed, for a Cisco 4000 Series Integrated Services Router. The **show license authorization** shows sample output after installation.

Device# license smart authorization request add 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
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

Example: SLAC returned for Cisco 4000 Series Integrated Services Routers

The following sample output of the license smart authorization return command shows how a SLAC is returned online, for a Cisco 4000 Series Integrated Services Router. (If it were returned offline, the return code displayed here would have to be returned, by manually entering the return code in 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: CPo1Sz-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.

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced in a release earlier than Cisco IOS XE Amsterdam</td>
</tr>
<tr>
<td>17.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Modification

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.

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

Miscellaneous:
  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):
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Amsterdam 17.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following are sample outputs of the show license authorization command, on various Cisco product instances. See Table 7: show license authorization Field Descriptions, on page 90 for information about fields shown in the display.
For information about when SLAC is required, see Authorization Code, on page 8.

**Table 7: show license authorization Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Status</td>
<td>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.</td>
</tr>
<tr>
<td>Active: Status:</td>
<td>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.</td>
</tr>
<tr>
<td>Standby: Status:</td>
<td>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.</td>
</tr>
<tr>
<td>Member: Status:</td>
<td>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.</td>
</tr>
<tr>
<td>ERROR:</td>
<td>Configuration errors or discrepancies in the High Availability set-up, if any.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authorizations</td>
<td>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.</td>
</tr>
<tr>
<td>():</td>
<td>License name and a shortened form of the license name.</td>
</tr>
<tr>
<td>Description</td>
<td>License description.</td>
</tr>
<tr>
<td>Total available count:</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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 7.                                                  |
<p>| Term information:     |                                                                                                                                                                                                           |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Header providing license duration information. The following fields maybe included under this header:</td>
</tr>
<tr>
<td></td>
<td>• Active: The active product instance UDI, followed by the status of the authorization code installation for this UDI.</td>
</tr>
<tr>
<td></td>
<td>• Authorization type: Type of authorization code installed and date of installation. The type can be: SLAC, UNIVERSAL, SPECIFIED, PAK, RTU.</td>
</tr>
<tr>
<td></td>
<td>• Start Date: Displays validity start date if the license is for a specific term or time period.</td>
</tr>
<tr>
<td></td>
<td>• Start Date: Displays validity end date if the license is for a specific term or time period.</td>
</tr>
<tr>
<td></td>
<td>• Term Count: License count.</td>
</tr>
<tr>
<td></td>
<td>• Subscription ID: Displays ID if the license is for a specific term or time period.</td>
</tr>
<tr>
<td></td>
<td>• License type: License duration. This can be: SUBSCRIPTION or PERPETUAL.</td>
</tr>
<tr>
<td></td>
<td>• Standby: The standby product instance UDI, followed by the status of the authorization code installation for this UDI.</td>
</tr>
<tr>
<td></td>
<td>• Member: The member product instance UDI, followed by the status of the authorization code installation for this UDI.</td>
</tr>
<tr>
<td></td>
<td>For more information about the duration or term of a license's validity, see License Duration, on page 8.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Purchased Licenses</td>
<td>Header for license purchase information.</td>
</tr>
<tr>
<td></td>
<td>Active: The active product instance and its the UDI.</td>
</tr>
<tr>
<td></td>
<td>Count: License count.</td>
</tr>
<tr>
<td></td>
<td>Description: License description.</td>
</tr>
<tr>
<td></td>
<td>License type: License duration. This can be: SUBSCRIPTION or PERPETUAL.</td>
</tr>
<tr>
<td></td>
<td>Standby: The standby product instance UDI.</td>
</tr>
<tr>
<td></td>
<td>Member: The member product instance UDI.</td>
</tr>
</tbody>
</table>

**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.

```
Device# show license authorization

Overall status:
Active: PID:ISR4331/K9,SN:FDO224917Q6
Status: NOT INSTALLED

Authorization:
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
```

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 23.
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 23.

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_3a45e72-722a41ab-d53d5a3cac14
Entitlement Tag:
regid.2018-12.com.cisco.ISR_1100_8P_UnifiedCommunication,1.0_55775cb5-538d482e-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
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
No HSEC, SLAC on Cisco 4000 Series Integrated Services Router

The following sample output of the `show license authorization` command on 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_79a9cbb4-d7c3-46fd-9980-7efe247c90e5
  Entitlement Tag: regid.2015-01.com.cisco.ISR_4351_Application,1.0_601ccfff-5601-4293-98d2-2f653db64ce0
  Entitlement Tag: regid.2014-12.com.cisco.ISR_4351_UnifiedCommunication,1.0_a04fec0e-e944-4096-bcf8-05d6e9a06ad3

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Amsterdam 17.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

```
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 ]
```

Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Amsterdam 17.3.2</td>
<td>Additional events were added with the introduction of Smart Licensing Using Policy:</td>
</tr>
<tr>
<td></td>
<td>• Installation and removal of a policy</td>
</tr>
<tr>
<td></td>
<td>• Request, installation and removal of an authorization code.</td>
</tr>
<tr>
<td></td>
<td>• Installation and removal of a trust code.</td>
</tr>
<tr>
<td></td>
<td>• Addition of authorization source information for license usage.</td>
</tr>
</tbody>
</table>

**Examples**

- Example: Event log for one day, on page 99
- Example: All event logs, on page 100

**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"
```

Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
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 20:23:7.702 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmfRegister"
2020-09-22 20:23:32.840 UTC SAEVTREADY
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 20:23:49.735 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 20:23:53.353 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_HA_EVENT eventType="SmartAgentEvtHArmfRegister"
2020-09-22 20:39:33.333 UTC SAEVTREADY
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"
```

Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
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 reservation

Syntax Description
This command has no arguments or keywords.

Command Modes
Privileged EXEC (Device#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Amsterdam 17.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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.

Note
Starting from Cisco IOS XE Amsterdam 17.3.2, use the show license authorization command instead of show license reservation to display information for licenses that require authorization before use.

show license reservation

This command has no arguments or keywords.

Command Modes
Privileged EXEC (Device#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2.</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Amsterdam 17.3.2</td>
<td>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.</td>
</tr>
</tbody>
</table>

show license status

To display license status information, enter the show license status command in privileged EXEC mode.

show license status
show license status

Command Modes

Privileged EXEC (Device#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command was introduced in</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>a release earlier than Cisco IOS</td>
<td></td>
</tr>
<tr>
<td>XE Amsterdam 17.3.2</td>
<td></td>
</tr>
<tr>
<td>Cisco IOS XE Amsterdam 17.3.2</td>
<td>Command output was updated to reflect new fields that are applicable to</td>
</tr>
<tr>
<td></td>
<td>Smart Licensing Using Policy. This includes Trust code installed:, Policy in</td>
</tr>
<tr>
<td></td>
<td>use, Policy name: , reporting requirements as in the policy (Attributes:),</td>
</tr>
<tr>
<td></td>
<td>and fields related to usage reporting.</td>
</tr>
<tr>
<td></td>
<td>Command output no longer displays Smart Account and Virtual account</td>
</tr>
<tr>
<td></td>
<td>information.</td>
</tr>
</tbody>
</table>

Examples

show license status on Cisco 4000 Series Integrated Services Routers, on page 109.

See Table 8: show license status Field Descriptions, on page 103 for information about fields shown in the display.

Table 8: show license status Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utility</td>
<td>Header for utility settings that are configured on the product instance.</td>
</tr>
<tr>
<td></td>
<td>Status: Status</td>
</tr>
<tr>
<td></td>
<td>Utility report: Last attempt:</td>
</tr>
<tr>
<td></td>
<td>Customer Information: The following fields are displayed:</td>
</tr>
<tr>
<td></td>
<td>• Id:</td>
</tr>
<tr>
<td></td>
<td>• Name:</td>
</tr>
<tr>
<td></td>
<td>• Street</td>
</tr>
<tr>
<td></td>
<td>• City:</td>
</tr>
<tr>
<td></td>
<td>• State:</td>
</tr>
<tr>
<td></td>
<td>• Country:</td>
</tr>
<tr>
<td></td>
<td>• Postal Code:</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Smart Licensing Using Policy:</td>
<td>Header for policy settings on the product instance.</td>
</tr>
<tr>
<td>Status:</td>
<td>Indicates if Smart Licensing Using Policy is enabled.</td>
</tr>
<tr>
<td></td>
<td>Smart Licensing Using Policy is supported starting from Cisco IOS XE Amsterdam 17.3.2 and is always enabled on supported software images.</td>
</tr>
<tr>
<td>Data Privacy:</td>
<td>Header for privacy settings that are configured on the product instance.</td>
</tr>
<tr>
<td>Sending Hostname:</td>
<td>A yes or no value which shows if the hostname is sent in usage reports.</td>
</tr>
<tr>
<td>Callhome hostname privacy:</td>
<td>Indicates if the Call Home feature is configured as the mode of transport for reporting. If configured, one of these values is displayed:</td>
</tr>
<tr>
<td></td>
<td>• ENABLED</td>
</tr>
<tr>
<td></td>
<td>• DISABLED</td>
</tr>
<tr>
<td>Smart Licensing hostname privacy:</td>
<td>One of these values is displayed:</td>
</tr>
<tr>
<td></td>
<td>• ENABLED</td>
</tr>
<tr>
<td></td>
<td>• DISABLED</td>
</tr>
<tr>
<td>Version privacy:</td>
<td>One of these values is displayed:</td>
</tr>
<tr>
<td></td>
<td>• ENABLED</td>
</tr>
<tr>
<td></td>
<td>• DISABLED</td>
</tr>
<tr>
<td>Transport:</td>
<td>Header for transport settings that are configured on the product instance.</td>
</tr>
<tr>
<td>Type:</td>
<td>Mode of transport that is in use.</td>
</tr>
<tr>
<td></td>
<td>Additional fields are displayed for certain transport modes. For example, if transport type is set to CSLU, the CSLU address is also displayed.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Policy:</td>
<td>Header for policy information that is applicable to the product instance.</td>
</tr>
<tr>
<td>Policy in use:</td>
<td>Policy that is applied</td>
</tr>
<tr>
<td></td>
<td>This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>- Cisco default, Product default,</td>
</tr>
<tr>
<td></td>
<td>- Permanent License Reservation,</td>
</tr>
<tr>
<td></td>
<td>- Specific License Reservation,</td>
</tr>
<tr>
<td></td>
<td>- PAK license, Installed on &lt;date&gt;, Controller.</td>
</tr>
<tr>
<td>Policy name:</td>
<td>Name of the policy</td>
</tr>
<tr>
<td>Reporting ACK required:</td>
<td>A yes or no value which specifies if the report for this product instance</td>
</tr>
<tr>
<td></td>
<td>requires CSSM acknowledgement (ACK) or not. The default policy is always set</td>
</tr>
<tr>
<td></td>
<td>to “yes”.</td>
</tr>
<tr>
<td>Perpetual Attributes:</td>
<td>Policy values for perpetual licenses.</td>
</tr>
<tr>
<td></td>
<td>• First report requirement (days): The maximum amount of time available</td>
</tr>
<tr>
<td></td>
<td>before the first report must be sent, followed by policy name.</td>
</tr>
<tr>
<td></td>
<td>• Reporting frequency (days): The maximum amount of time available before</td>
</tr>
<tr>
<td></td>
<td>the subsequent report must be sent, followed by policy name.</td>
</tr>
<tr>
<td></td>
<td>• Report on change (days): The maximum amount of time available to send a</td>
</tr>
<tr>
<td></td>
<td>report in case of a change in license usage, followed by policy name.</td>
</tr>
<tr>
<td>Subscription Attributes:</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Policy values for subscription licenses.</td>
</tr>
<tr>
<td></td>
<td>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.</td>
</tr>
<tr>
<td></td>
<td>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>Enforced License Attributes: Policy values for subscription licenses.</td>
</tr>
<tr>
<td></td>
<td>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.</td>
</tr>
<tr>
<td></td>
<td>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>Export License Attributes:</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Policy values for subscription licenses.</td>
</tr>
<tr>
<td></td>
<td>• First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name.</td>
</tr>
<tr>
<td></td>
<td>• Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name.</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
</tbody>
</table>

<p>| Miscellaneous        | Header for custom ID.                                                        |
|                      | Custom Id: ID                                                               |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage Reporting:</td>
<td>Header for usage reporting (RUM reports) information.</td>
</tr>
<tr>
<td>Last ACK received:</td>
<td>Date and time of last ACK received, in the local time zone.</td>
</tr>
<tr>
<td>Next ACK deadline:</td>
<td>Date and time for next ACK. If the policy states that an ACK is not required then this field displays none.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If an ACK is required and is not received by this deadline, a syslog is displayed.</td>
</tr>
<tr>
<td>Reporting Interval:</td>
<td>Reporting interval in days</td>
</tr>
<tr>
<td></td>
<td>The value displayed here depends on you configure the <code>license smart usage interval interval_in_days</code> and the policy value. For more information, see the corresponding Syntax Description: <code>license smart (global config), on page 77</code>.</td>
</tr>
<tr>
<td>Next ACK push check:</td>
<td>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.</td>
</tr>
<tr>
<td>Next report push:</td>
<td>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.</td>
</tr>
<tr>
<td>Last report push:</td>
<td>Date and time for when the product instance sent the last RUM report. Date and time are in the local time zone.</td>
</tr>
<tr>
<td>Last report file write:</td>
<td>Date and time of last RUM report. Date and time are in the local time zone.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Date and time for when the product instance last saved an offline RUM report. Date and time are in the local time zone.</td>
<td></td>
</tr>
<tr>
<td>Last report pull</td>
<td>Date and time for when usage reporting information was retrieved using data models. Date and time are in the local time zone.</td>
</tr>
</tbody>
</table>
| 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                                                    |

**show license status on 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:
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

This command has no arguments or keywords.

Command Modes

Privileged EXEC (Device#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Modification

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.

Examples

The following are sample outputs of the show license summary command, on various Cisco product instances. See Table 9: show license summary Field Descriptions, on page 111 for information about fields shown in the display.

- Example: show license summary: All IN USE (Cisco 4000 Series Integrated Services Routers), on page 111

Table 9: show license summary Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>Name of the licenses in use</td>
</tr>
<tr>
<td>Entitlement Tag</td>
<td>Short name for license</td>
</tr>
<tr>
<td>Count</td>
<td>License count</td>
</tr>
<tr>
<td>Status</td>
<td>License status can be one of the following</td>
</tr>
<tr>
<td></td>
<td>• In-Use: Valid license, and in-use.</td>
</tr>
<tr>
<td></td>
<td>• Not In-Use</td>
</tr>
<tr>
<td></td>
<td>• Not Authorized: Means that the license requires installation of SLAC before use. For more information, see Authorization Code, on page 8</td>
</tr>
</tbody>
</table>

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

Sword#show license summary

License Usage:

<table>
<thead>
<tr>
<th>License</th>
<th>Entitlement Tag</th>
<th>Count</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>hseck9 (ISR_4331_Hsec)</td>
<td>1 IN USE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>booster_performance (ISR_4331_BOOST)</td>
<td>1 IN USE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>appxk9 (ISR_4331_Application)</td>
<td>1 IN USE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 { data { conversion } | eventlog [{ days }] | reservation | support }
```

**Syntax Description**
- `data { conversion }` Displays license data conversion information.
- `eventlog [{ days }]` Displays event logs related to Smart Licensing Using Policy. For `days`, enter the number of days for which you want to display event logs. The valid value range is from 0 to 2147483647.
- `reservation` Displays license reservation information.
- `support` Displays licensing information that helps the technical support team to debug a problem.

**Command Modes**
Privileged EXEC (Device#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2.</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Amsterdam 17.3.2.</td>
<td>Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy.</td>
</tr>
</tbody>
</table>

**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.

**Examples**

show license tech support on Cisco 4000 Series Integrated Services Routers, on page 112

**show license tech support on Cisco 4000 Series Integrated Services Routers**
The following is sample output from the `show license tech support` command on a Cisco 4000 Series Integrated Services Router.

```
Device# show license tech support
Smart Licensing Tech Support info
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:
    Address: <empty>
    Port: <empty>
    Username: <empty>
    Password: <empty>
  Server Identity Check: True

Miscellaneous:
  Custom Id: <empty>

Policy:
  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)

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 State(4) InPolicy(60)
  Next report push: Oct 30 05:45:45 2020 UTC
  Next report push: Nov 22 23:32:38 2020 UTC
License Usage
-------------
Handle: 1
License: hseck9
Entitlement Tag:
regid.2015-02.com.cisco.ISR_4400_Hsec,1.0_2a5a1571-f3bc-4a0c-8c00-a047b8ad6ca8
Description: hseck9
Count: 1
Version: 1.0
Status: IN USE(15)
Status time: Oct 23 23:31:42 2020 UTC
Request Time: Oct 23 23:31:42 2020 UTC
Export status: RESTRICTED - ALLOWED
Feature Name: hseck9
Feature Description: hseck9
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 1

Handle: 2
License: booster_performance
Entitlement Tag:
regid.2017-05.com.cisco.ISR_4431_BOOST,1.0_4cdbfebf-5af9-424c-a42d-a2ce9579cfb1
Description: booster_performance
Count: 1
Version: 1.0
Status: IN USE(15)
Status time: Oct 23 23:31:42 2020 UTC
Request Time: Oct 23 23:31:42 2020 UTC
Export status: NOT RESTRICTED
Feature Name: booster_performance
Feature Description: booster_performance
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 1
    Soft Enforced: True

Handle: 3
License: appxk9
Entitlement Tag:
regid.2015-01.com.cisco.ISR_4400_Application,1.0_da87444e-68bb-4821-8aab-63f8531a0430
Description: appxk9
Count: 1
Version: 1.0
Status: IN USE(15)
Status time: Oct 23 23:32:04 2020 UTC
Request Time: Oct 23 23:32:04 2020 UTC
Export status: NOT RESTRICTED
Feature Name: appxk9
Feature Description: appxk9
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 1
    Soft Enforced: True

Handle: 4
License: securityk9
Entitlement Tag:
Description: securityk9
Count: 1
Version: 1.0
Status: IN USE(15)
Status time: Oct 23 23:32:04 2020 UTC
Request Time: Oct 23 23:32:04 2020 UTC
Export status: NOT RESTRICTED
Feature Name: securityk9
Feature Description: securityk9
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 1
    Soft Enforced: True

Product Information
---------------------
UDI: PID:ISR4431/K9,SN:FOC22446T0U

Agent Version
--------------
Smart Agent for Licensing: 5.1.3_rel/8

Upcoming Scheduled Jobs
------------------------
Current time: Oct 30 04:59:15 2020 UTC
Daily: Oct 30 23:31:13 2020 UTC (18 hours, 31 minutes, 58 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: Oct 30 05:45:44 2020 UTC (46 minutes, 29 seconds remaining)
Start Utility Measurements: Oct 30 05:02:38 2020 UTC (3 minutes, 23 seconds remaining)
Send Utility RUM reports: Nov 22 23:32:37 2020 UTC (23 days, 18 hours, 33 minutes, 22 seconds remaining)
Save unreported RUM Reports: Oct 30 05:47:48 2020 UTC (48 minutes, 33 seconds remaining)
Process Utility RUM reports: Oct 30 23:32:26 2020 UTC (18 hours, 33 minutes, 11 seconds remaining)
Data Synchronization: Expired Not Rescheduled
External Event: Dec 22 23:36:37 2020 UTC (53 days, 18 hours, 37 minutes, 22 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 Oct 23 23:32:37 2020 UTC
  Failure Reason: <none>
  Last Success Time: Oct 23 23:32:37 2020 UTC
  Last Failure Time: <none>
Result Polling:
Attempts: Total=164, Success=2, Fail=162  Ongoing Failure: Overall=161 Communication=0
Last Response: INVALID STATUS CODE on Oct 30 04:45:45 2020 UTC
Failure Reason: Invalid Polling Id 4294967295 provided in the polling request
Last Success Time: Oct 23 23:36:39 2020 UTC
Last Failure Time: Oct 30 04:45:45 2020 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=1, Success=1, Fail=0  Ongoing Failure: Overall=0 Communication=0
Last Response: OK on Oct 29 21:43:33 2020 UTC
Failure Reason: <none>
Last Success Time: Oct 29 21:43:33 2020 UTC
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:ISR4431/K9,SN:FOC22446T0U
Reservation status: SMART AUTHORIZATION INSTALLED on Oct 09 17:56:21 2020 UTC
Request code: <none>
Last return code: <none>
Last Confirmation code: 910fc7b7
Reservation authorization code:
<smartlicenseAuthorization><udi>P:ISR4431/K9,S:FOC22446T0U</udi><authorizationCode><customerInfo><smartAccount>BU
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:ISR4431/K9, SN:FOC22446T0U
    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

Other Info
----------
Software ID: regid.2014-12.com.cisco.ISR_4400,1.0_e633c5f0-fde6-47b3-a4cf-34110373fef2
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
XDS version: 0.12.0.0
Config Persist Received: False
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
License Map Interface: True
HA Interface: True
Trusted Store Interface: True
Platform Data Interface: True
Crypto Version 2 Interface: False
SAPluginMgmtInterfaceMutex: True
SAPluginMgmtIPDomainName: True
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
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.
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 Reference for Smart Licensing Using Policy

show license usage

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command was introduced.</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Amsterdam 17.3.2</td>
<td>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.</td>
</tr>
</tbody>
</table>

Examples

The following are sample outputs of the show license usage command on various product instances. See Table 10: show license usage Field Descriptions, on page 120 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 121
- Example: show license usage with unenforced licenses (Cisco Catalyst 9500 Series Switches), on page 122

Table 10: show license usage Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Authorization:</td>
<td>Displays overall authorization status.</td>
</tr>
<tr>
<td>Status:</td>
<td></td>
</tr>
<tr>
<td>():</td>
<td>Name of the license as in CSSM.</td>
</tr>
<tr>
<td></td>
<td>If this license is one that requires an authorization code, the name of the license comes from the code.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the license as in CSSM.</td>
</tr>
<tr>
<td>Count</td>
<td>License count. If the license is not in-use, the count is reflected as zero.</td>
</tr>
<tr>
<td>Version</td>
<td>Version.</td>
</tr>
<tr>
<td>Status</td>
<td>License status can be one of the following</td>
</tr>
<tr>
<td></td>
<td>• In-Use: Valid license, and in-use.</td>
</tr>
<tr>
<td></td>
<td>• Not In-Use</td>
</tr>
<tr>
<td></td>
<td>• Not Authorized: Means that the license requires installation of SLAC before use. For more information, see Authorization Code, on page 8</td>
</tr>
</tbody>
</table>
### Field Description

**Export Status:** Indicates if this license is export-controlled or not. Accordingly, one of the following statuses 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 following:

- **ENFORCED**
- **NOT ENFORCED**
- **EXPORT RESTRICTED - ALLOWED**
- **EXPORT RESTRICTED - NOT ALLOWED**

For more information about enforcement types, see [License Enforcement Types, on page 7](#).

---

**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
```

---

For more information about enforcement types, see [License Enforcement Types, on page 7](#).
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: 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: 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.

```
license call-home { 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Amsterdam 17.3.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.
show platform software sl-infra
CHAPTER 6

Troubleshooting Smart Licensing Using Policy

- System Message Overview, on page 125
- Smart Licensing Using Policy System Messages, on page 126

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 11: Message Severity Levels

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - emergency</td>
<td>System is unusable.</td>
</tr>
<tr>
<td>1 - alert</td>
<td>Immediate action required.</td>
</tr>
<tr>
<td>2 - critical</td>
<td>Critical condition.</td>
</tr>
<tr>
<td>3 - error</td>
<td>Error condition.</td>
</tr>
</tbody>
</table>
### 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 Licensing Using Policy-related system messages:

- `%SMART_LIC-3-POLICY_INSTALL_FAILED`
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 authorization 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 58 and Installing a File on the Product Instance, on page 66.

- 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 with CSLU 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 or CSLU is not reachable: This means that there is a network reachability problem.
- 404 host not found: This means the CSSM server is down.

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, and CSLU Disconnected from CSSM: 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 the value that you last configured.

**Recommended Action:**

Troubleshooting steps are provided for when CSSM is not reachable and when CSLU is not reachable.

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 configured.

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 44.
   
   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 the above does not work and policy installation still fails, 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)
Explanation: Product instance communication with either the CSSM or CSLU is restored.

Recommended Action: No action required.

Error Message %SMART_LIC-3-POLICY_REMOVED: The licensing policy has been removed.

Explanation: A previously installed 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 inadvertently, 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 63 and Installing a Trust Code, on page 63. 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-initiated communication), enter the license smart sync command in privileged EXEC mode. The synchronization request causes CSLU to push the missing information (a policy or authorization code) to the product instance.

  - For CSLU-initiated communication, complete this task: Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 43. This causes CSLU to detect and re-furnish the missing policy in an ACK response.

- CSLU Disconnected from CSSM:

  - For product instance-initiated communication), enter the license smart sync command in privileged EXEC mode. The synchronization request causes CSLU to push the missing information (a policy or authorization code) to the product instance. Then complete these tasks in the given order: Download All For Cisco (CSLU Interface), on page 48 > Uploading Usage Data to CSSM and Downloading an ACK, on page 65 > Upload From Cisco (CSLU Interface), on page 49.
For CSLU-initiated communication, complete this task: Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 43. This causes CSLU to detect and re-furnish the missing policy in an ACK response. Then complete these tasks in the given order: Download All For Cisco (CSLU Interface), on page 48 > Uploading Usage Data to CSSM and Downloading an ACK, on page 65 > Upload From Cisco (CSLU Interface), on page 49.

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 65.

Then complete this task on the product instance: Installing a File on the Product Instance, on page 66.

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 63 and Installing a File on the Product Instance, on page 66 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 SSM On-Prem, on page 7). 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: Refer to and implement one of the supported topologies instead (See: Supported Topologies, on page 11), or upgrade to a release where SSM On-Prem is supported with Smart Licensing Using Policy.

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.

• If the product instance is directly connected to CSSM, or to CSLU and the product instance is configured to initiate communication complete this step on the product instance, the product instance will automatically send usage information at the scheduled time. If it is not sent at the scheduled time, because of technical difficulties, you can license smart sync command in privileged EXEC mode. For syntax details, see license smart (privileged EXEC), on page 82.

• If the product instance is connected to CSLU and CSLU is configured to initiate communication, complete: Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 43.

• If the product instance is connected to CSLU, but CSLU is disconnected from CSSM, complete these tasks: Download All For Cisco (CSLU Interface), on page 48, Uploading Usage Data to CSSM and Downloading an ACK, on page 65, and Upload From Cisco (CSLU Interface), on page 49.

• If the product instance is disconnected from CSSM and you are not using CSLU either, 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 Usage Data to CSSM and Downloading an ACK, on page 65.

• If the product instance is managed by a controller, the controller will send the RUM report at the scheduled time. If you want to trigger an ad-hoc report, you can do so in the Cisco DNA Center GUI.

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.
### Additional References for Smart Licensing Using Policy

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Smart Software Manager (CSSM) Help</td>
<td>Smart Software Manager Help</td>
</tr>
<tr>
<td>Cisco Smart License Utility (CSLU) installation and user guides</td>
<td>Cisco Smart License Utility Quick Start Setup Guide</td>
</tr>
<tr>
<td></td>
<td>Cisco Smart License Utility User Guide</td>
</tr>
</tbody>
</table>

Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
## 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 13: Feature History for Smart Licensing Using Policy

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Licensing Using Policy</td>
<td>Cisco IOS XE Amsterdam 17.3.2</td>
<td>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.</td>
</tr>
<tr>
<td>Cisco DNA Center Support for Smart Licensing Using Policy</td>
<td>Cisco IOS XE Amsterdam 17.3.2</td>
<td>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 compatible 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 14 and Using Cisco DNA Center as a Controller, on page 31.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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 18 for the complete list of products that support the feature.                                                                 |
| 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 this topology, see the Connected to CSSM Through a Controller, on page 14 and Workflow for Topology: Connected to CSSM Through a Controller, on page 30 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.                                                                 |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnmg.cisco.com/