Smart Licensing Using Policy for Cisco Wireless Controllers

First Published: 2020-10-30

Last Modified: 2024-09-02

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

CHAPTER 1

Information About Smart Licensing Using Policy

Smart Licensing Using Policy is an enhanced version of Smart Licensing, with the 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.

This document focuses on conceptual, configuration, and troubleshooting information for Smart Licensing Using Policy on Cisco Catalyst 9800 Series Wireless Controllers and Cisco Embedded Wireless Controller on Cisco Catalyst 9100 Access Points.

Information About 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.

This document focuses on conceptual, configuration, and troubleshooting information for Smart Licensing Using Policy on Cisco Catalyst 9800 Series Wireless Controllers and Cisco Embedded Wireless Controller on Cisco Catalyst 9100 Access Points.

Benefits of Smart Licensing Using Policy

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

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

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

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

Supported Products

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

Table 1: Supported Product Instances: Cisco Catalyst Wireless Controllers

Cisco Catalyst Wireless Controllers	When Support for Smart Licensing Using Policy was Introduced
Cisco Catalyst 9800-40 Wireless Controller	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9800-L Wireless Controller	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9800-CL Wireless Controller	Cisco IOS XE Amsterdam 17.3.2a
Cisco Catalyst 9800 embedded Wireless Controller	Cisco IOS XE Amsterdam 17.3.2a
Cisco Embedded Wireless Controller on Cisco Catalyst 9100 Access Points (EWC-AP)	Cisco IOS XE Amsterdam 17.3.2a

Key Concepts of Smart Licensing Using Policy

This section explains the important concepts that help with understanding how the Smart Licensing Using Policy solution is designed to work.

License Enforcement Types

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

- 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. Enforced licenses are not applicable to Cisco wireless controllers.

- Export-Controlled

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

An example of an export-controlled license is the High Speed Encryption (HSECK9) license, which is available on certain Cisco Routers. Export-controlled licenses are not applicable to Cisco wireless controllers.

Unenforced or Not Enforced

Unenforced licenses do not require authorization before use in air-gapped networks, or registration, in connected networks. The terms of use for such licenses are as per the general terms.

All licenses available on Cisco wireless controllers are examples of unenforced licenses.

Enforced

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

None of the licenses available on Cisco Catalyst 9800 Series Wireless Controllers and Cisco Embedded Wireless Controller on Cisco Catalyst 9100 Access Points belong to this enforcement type.

Export Controlled

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

An example of an export-controlled license is the High Security (HSECK9) key, which is available on *certain* Cisco devices. Export-controlled licenses are not applicable to Cisco wireless controllers.

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.

  AIR Network Essentials and AIR Network Advantage licenses are examples of unenforced, perpetual licenses that are available on Cisco wireless controllers.

- Subscription: The license is valid only until a certain date.

  AIR Digital Network Architecture (DNA) Essentials and AIR DNA Advantage licenses are examples of unenforced subscription licenses that are available on Cisco wireless controllers.

Authorization Code

An authorization code is not required for any of the licenses available on Cisco wireless controllers, but if you are upgrading from an earlier licensing model to Smart Licensing Using Policy, you may have a Specific License Reservation (SLR) with its own authorization code. The SLR authorization code is supported after upgrade to Smart Licensing Using Policy.

Note While existing SLRs are carried over after upgrade, you cannot request a new SLR in the Smart Licensing Using Policy environment, because the notion of "reservation" does not apply. For an air-gapped network, the No Connectivity to CSSM and No CSLU topology applies instead.

For more information about how the SLR authorization code is handled, see Example: SLR to Smart Licensing Using Policy, on page 56. If you want to return an SLR authorization code, see Removing and Returning an Authorization Code, on page 103.

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 subsequent report must be sent within the duration specified here.

  If the value here is zero, it means no further reporting is required *unless* there is a usage change.
- Report on change (days): In case of a change in license usage, a report must be sent within the duration specified here.

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

  If the value here is not zero, reporting *is* required after the change is made. All the scenarios listed below count as changes in license usage on the product instance:
  - Changing licenses consumed (includes changing to a different license, and, adding or removing a license).
  - Going from consuming zero licenses to consuming one or more licenses.
  - Going from consuming one or more licenses to consuming zero licenses.

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

Understanding Policy Selection

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

`Cisco default` is the default policy that is always available in the product instance. If no other policy is applied, the product instance applies this default policy. The Table 2: Policy: Cisco default shows the `Cisco default` policy values.

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

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

Table 2: Policy: Cisco default

Policy: `Cisco default`	**Default Policy Values**
Export (Perpetual/Subscription) **Note** Applied only to licenses with enforcement type "Export-Controlled".	Reporting ACK required: Yes First report requirement (days): 0 Reporting frequency (days): 0 Report on change (days): 0
Enforced (Perpetual/Subscription) **Note** Applied only to licenses with enforcement type "Enforced".	Reporting ACK required: Yes First report requirement (days): 0 Reporting frequency (days): 0 Report on change (days): 0
Unenforced/Non-Export Perpetual[1]	Reporting ACK required: Yes First report requirement (days): 365 Reporting frequency (days): 0 Report on change (days): 90
Unenforced/Non-Export Subscription	Reporting ACK required: Yes First report requirement (days): 90 Reporting frequency (days): 90 Report on change (days): 90

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

RUM Report and Report Acknowledgement

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

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

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

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

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

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

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

If the product instance you are using is a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the conditions for a mandatory ACK starting with Cisco IOS XE Cupertino 17.7.1. For more information, see RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72.

RUM report generation, storage, and management

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

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

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

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

Trust Code

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

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

There are multiple ways to obtain a trust code.

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

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

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

  Here you generate an *ID token* in the CSSM Web UI to obtain a trust code and install it on the product instance. You must overwrite the factory-installed trust code if there is one. If a product instance is directly connected to CSSM, use this method to enable the product instance to communicate with CSSM in a secure manner. This method of obtaining a trust code is applicable to all the options of directly connecting to CSSM. For more information, see Connected Directly to CSSM, on page 15.

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

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

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

If a trust code is installed on the product instance, the output of the **show license status** command displays a timestamp in the `Trust Code Installed:` field.

CHAPTER 2

How Smart Licensing Using Policy Works

This section lists the components that may be involved in an implementation of Smart Licensing Using Policy, followed by the sequential stages of managing licenses for Cisco Catalyst 9800 Series Wireless Controllers and Cisco Embedded Wireless Controller on Cisco Catalyst 9100 Access Points.

Components Involved

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

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

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

Product Instance

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

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

Cisco Smart Software Manager (Cisco SSM)

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

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

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

Cisco Smart License Utility (CSLU)

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

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

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

Controller

A management application or service that manages multiple product instances.

Note Throughout this chapter, and in the context of Smart Licensing Using Policy, the term "controller" or "Controller" always means a management application or service that manages a product instance. The term is not used to refer to Cisco Catalyst Wireless Controllers, which are *product instances*. On Cisco Catalyst Wireless Controllers, Cisco Catalyst Center is the supported controller.

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

Table 3: Support Information for Controller: Cisco Catalyst Center

Minimum Required Cisco Catalyst Center Version for Smart Licensing Using Policy[2]	Minimum Required Cisco IOS XE Version[3]	Supported Product Instances
Cisco Catalyst Center Release 2.2.2	Cisco IOS XE Amsterdam 17.3.2a	• Cisco Catalyst 9800-40 Wireless Controller • Cisco Catalyst 9800-80 Wireless Controller • Cisco Catalyst 9800-L Wireless Controller • Cisco Catalyst 9800-CL Wireless Controller • Cisco Catalyst 9800 embedded Wireless Controller • Cisco Embedded Wireless Controller on Cisco Catalyst 9100 Access Points (EWC-AP)

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

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

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

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

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

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

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

Minimum Required SSM On-Prem Version for Smart Licensing Using Policy[4]	Minimum Required Cisco IOS XE Version[5]	Supported Product Instances
Version 8, Release 202102	Cisco IOS XE Amsterdam 17.3.3	• Cisco Catalyst 9800-40 Wireless Controller • Cisco Catalyst 9800-80 Wireless Controller • Cisco Catalyst 9800-L Wireless Controller • Cisco Catalyst 9800-CL Wireless Controller • Cisco Catalyst 9800 embedded Wireless Controller • Cisco Embedded Wireless Controller on Cisco Catalyst 9100 Access Points (EWC-AP)

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

5 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.

Stages of License Management with the Smart Licensing Using Policy Solution

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

1. Set up a Smart Account and one or more Virtual accounts to structure your Cisco assets (licenses, devices, and general terms). You can view and manage Smart Account and Virtual Accounts in the Cisco SSM portal.

2. Purchase or order licenses through existing channels. Once purchased, assets are available in your organization's Smart Account and Virtual Accounts, and can be accessed through the Cisco SSM portal. Ensuring that the licenses are in the correct Smart Account and Virtual Account is essential to consume your licenses.

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

3. Configure and use the required licenses.

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

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

   Multiple ways of interfacing with Cisco SSM are available – each way is called a topology. An organization's network requirements and security policy are some of the factors that determine the choice of topology. For each topology, the accompanying overview describes how the set-up is designed to work, and provides considerations and recommendations, if any. To know about all the available topology options, see Connecting to Cisco SSM, on page 13.

Connecting to Cisco SSM

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

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

Based on the topology that is selected, refer to the corresponding workflow under *Implementing Smart Licensing Policy*, to know how to implement it. These workflows provide the simplest and fastest way to implement a topology. These workflows are meant for new deployments and not for upgrading or migrating from an existing licensing solution.

Connected to CSSM Through CSLU

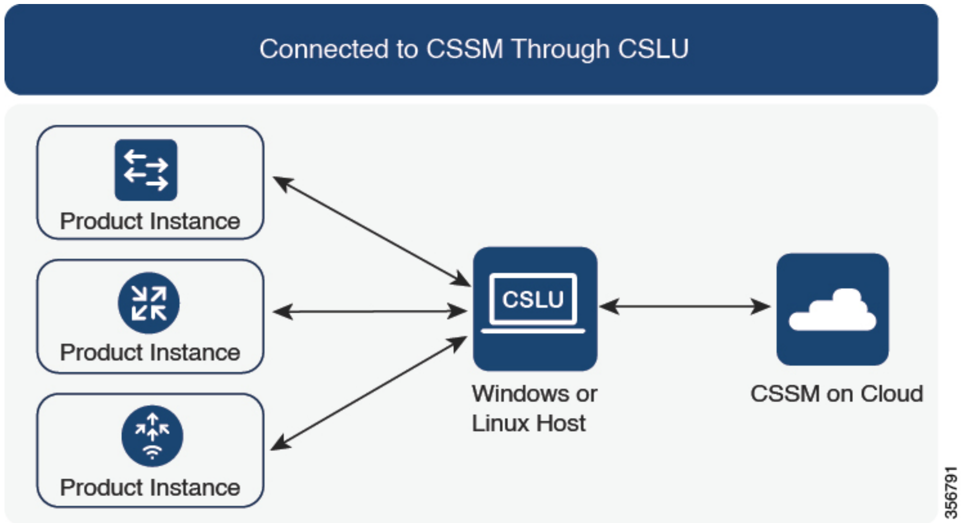
Overview:

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

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

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

Figure 1: Topology: Connected to CSSM Through CSLU



Considerations or Recommendations:

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

Release-Wise Changes and Enhancements:

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

From Cisco IOS XE Cupertino 17.7.1:

- Trust code request and installation

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

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

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

- RUM report throttling

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

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

  RUM report throttling applies to and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train.

Where to Go Next:

To implement this topology, see #unique_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.

Note A factory-installed trust code cannot be used for communication with CSSM. This means that for this topology, even if a factory-installed trust code exists, you must obtain a trust code by generating an ID token in CSSM, and you must overwrite the existing factory-installed trust code. Also see: Trust Code, on page 6.

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

- Use Smart transport to communicate with CSSM

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

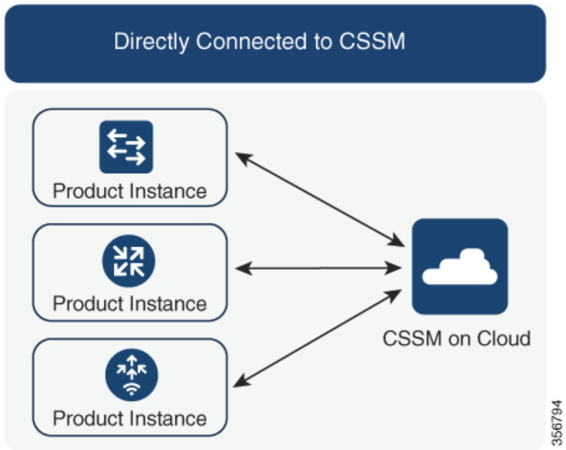
  - Smart transport: In this method, a product instance uses a specific Smart transport licensing server URL. This must be configured exactly as shown in the workflow section.
  - Smart transport through an HTTPs proxy: In this method, a product instance uses a proxy server to communicate with the licensing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

- Use Call Home to communicate with CSSM.

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

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

Figure 2: Topology: Connected Directly to CSSM



Considerations or Recommendations:

Smart transport is the recommended transport method when directly connecting to CSSM. This recommendation applies to:

- New deployments.
- Earlier licensing models. Change configuration after migration to Smart Licensing Using Policy.
- Registered licenses that currently use the Call Home transport method. Change configuration after migration to Smart Licensing Using Policy.
- Evaluation or expired licenses in an earlier licensing model. Change configuration after migration to Smart Licensing Using Policy.

To change configuration after migration, see #unique_28 > Product Instance Configuration > Configure a connection method and transport type > Option 1.

Release-Wise Changes and Enhancements:

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

- RUM report throttling

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

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

  RUM report throttling applies to and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train.

Where to Go Next:

To implement this topology, see #unique_28.

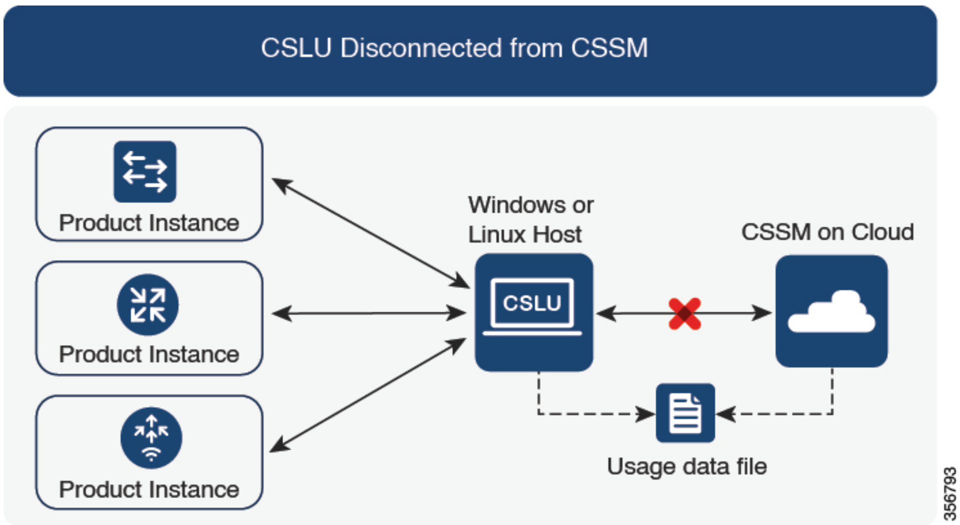
CSLU Disconnected from CSSM

Overview:

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

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

Figure 3: Topology: CSLU Disconnected from CSSM



Considerations or Recommendations:

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

Release-Wise Changes and Enhancements:

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

From Cisco IOS XE Cupertino 17.7.1:

- Trust code request and installation

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

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

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

- RUM report throttling

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

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

  RUM report throttling applies to and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train.

Where to Go Next:

To implement this topology, see #unique_30.

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. The supported controller for Cisco Catalyst Wireless Controllers is Cisco Catalyst Center

Overview:

If a product instance is managed by Cisco Catalyst Center as the controller, the product instance records license usage and saves the same, but it is the Cisco Catalyst 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 Catalyst Center must be part of its inventory and must be assigned to a site. Cisco Catalyst 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 Catalyst 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 Catalyst Center.

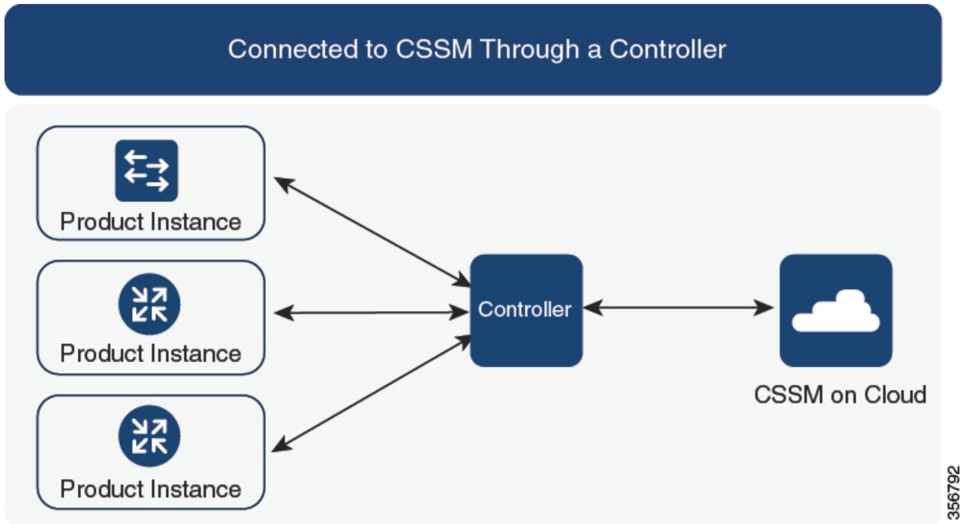
Note Ad hoc reporting must be performed at least once before a product instance is eligible for scheduled reporting.

The first ad hoc report enables Cisco Catalyst 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 Catalyst Center also enables you to install and remove SLAC for export-controlled licenses. Since all available licenses on Cisco Catalyst Wireless Controllers are unenforced licenses, SLAC installation and removal do not apply.

A trust code is *not* required.

Figure 4: Topology: Connected to CSSM Through a Controller



Considerations or Recommendations:

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

Where to Go Next:

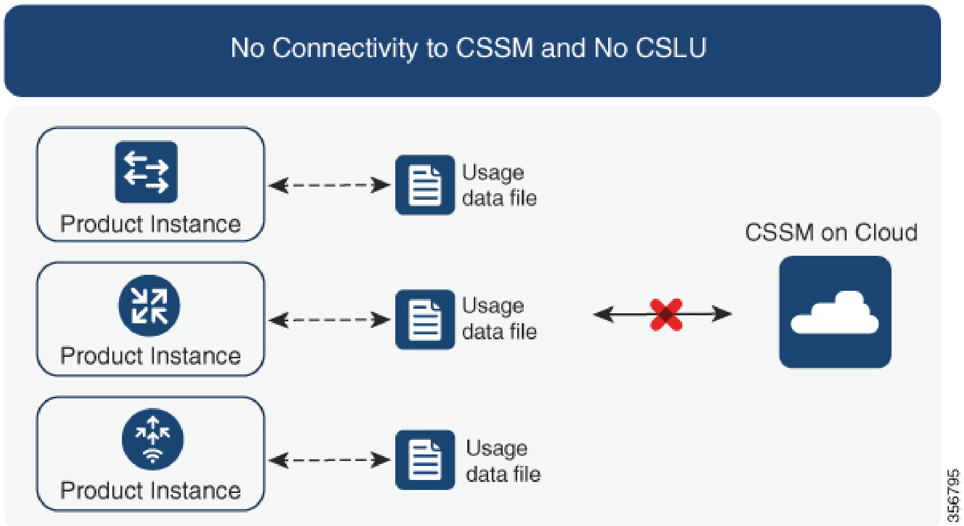
To implement this topology, see Workflow for Topology: Connected to CSSM Through a Controller, on page 31.

No Connectivity to CSSM and No CSLU

Overview:

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

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



Considerations or Recommendations:

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

Release-Wise Changes and Enhancements

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

From Cisco IOS XE Cupertino 17.7.1:

- Trust code request and installation

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

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

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

- Simpler authorization code return

  A simpler way to upload an authorization code return file is available in the CSSM Web UI. You do not have to locate the product instance in the correct Virtual Account in the CSSM Web UI any longer. You can upload the return file, as you would a RUM report.

Where to Go Next:

To implement this topology, see #unique_34.

SSM On-Prem Deployment

Overview:

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

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

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

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

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

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

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

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

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

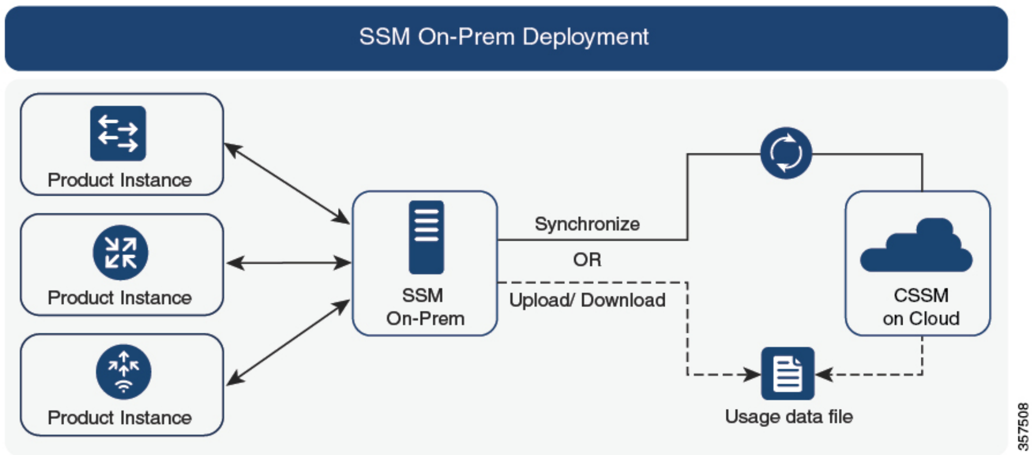
In SSM On-Prem, the reporting interval is set to the default policy on the product instance. You can change this, but only to report more frequently (a narrower interval), or you can install a custom policy if available.

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

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

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

Figure 6: Topology: SSM On-Prem Deployment



Considerations or Recommendations:

This topology is suited to the following situations:

- If you want to manage your product instances on your premises, as opposed communicating directly with CSSM for this purpose.
- If your company's policies prevent your product instances from reporting license usage directly to Cisco (CSSM).
- If your product instances are in an air-gapped network and cannot communicate online, with anything outside their network.

Apart from support for Smart Licensing Using Policy, some of the key benefits of SSM On-Prem *Version 8* include:

- Multi-tenancy: One tenant constitutes one Smart Account-Virtual Account pair. SSM On-Prem enables you to manage multiple pairs. Here you create local accounts that reside in SSM On-Prem. Multiple local accounts roll-up to a Smart Account-Virtual Account pair in CSSM. For more information, see the Cisco Smart Software Manager On-Prem User Guide > *About Accounts and Local Virtual Accounts*.

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

- Scale: Supports up to a total of 300,000 product instances

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

  High-Availability deployment is supported on the SSM On-Prem console and the required command details are available in the Cisco Smart Software On-Prem Console Guide.

- Options for online and offline connectivity to CSSM.

SSM On-Prem Limitations:

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

Release-Wise Changes and Enhancements:

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

From Cisco IOS XE Cupertino 17.9.1:

- RUM report throttling

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

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

  RUM report throttling applies to and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train.

Where to Go Next:

To implement this topology, see Workflow for Topology: SSM On-Prem Deployment, on page 36

If you are migrating from an existing version of SSM On-Prem, the sequence in which you perform the various upgrade-related activities is crucial. See Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy, on page 67

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

A wireless N+1 topology, where “n” number of wireless controllers act as primary and a “+1” wireless controller acts as the secondary or fallback wireless controller for Access Points (APs). Each Access Point is configured with a primary and a secondary wireless controller. In case of a failure on the primary, all access points that were connected to the primary now fallback to the secondary wireless controller.

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 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 secondary 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.

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

For reporting: Only the active product instance reports usage. The active reports usage information for all devices 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 the standby that was added or removed.
- A switchover.
- A reload.

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

For addition or removal of a new standby:

- 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 if not installed already.

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

For addition or removal of a secondary:

There are no product instance functions that apply exclusively to the addition or removal of a secondary product instance. Further, all the secondary product instances are in the same Smart Account and Virtual Account as the primary product instance.

CHAPTER 3

Implementing Smart Licensing Using Policy

This chapter provides the simplest and fastest way to implement Smart Licensing Using Policy for new deployments. If you are migrating from an existing licensing model, see Migrating to Smart Licensing Using Policy, on page 43.

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 laptop, desktop, or a Virtual Machine (VM) running Windows 10 or Linux.

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

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

2. ***CSLU Preference Settings***

   Where tasks are performed: CSLU

   a. Logging into Cisco (CSLU Interface), on page 75

   b. Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 75

c. Adding a Product-Initiated Product Instance in CSLU (CSLU Interface), on page 76

3. ***Product Instance Configuration***

   Where tasks are performed: Product Instance

   a. Ensuring Network Reachability for Product Instance-Initiated Communication, on page 76.

   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. 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
Device(config)# exit
Device# copy running-config startup-config
```

Result:

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

In the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train, and all subsequent releases from Cisco IOS XE Cupertino 17.9.1 onwards:

The product instance does not send more than one RUM report a day. You can override this for an on-demand synchronization between the product instance and CSSM, by entering the **license smart sync** command in privileged EXEC mode.

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

To verify trust code installation, enter the **show license status** command in privileged EXEC mode. Check for the updated timestamp in the `Trust Code Installed` field.

In case of a change in license usage, see Configuring an AIR License, on page 113 to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72.

Tasks for CSLU-Initiated Communication

CSLU Installation → CSLU Preference Settings→ Product Instance Configuration → Usage Synchronization

1. ***CSLU Installation***

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

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

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

2. ***CSLU Preference Settings***

   Where tasks is performed: CSLU

   a. Logging into Cisco (CSLU Interface), on page 75

   b. Configuring a Smart Account and a Virtual Account (CSLU Interface), on page 75

   c. Adding a CSLU-Initiated Product Instance in CSLU (CSLU Interface), on page 78

3. ***Product Instance Configuration***

   Where tasks is performed: Product Instance

   Ensuring Network Reachability for CSLU-Initiated Communication, on page 80

4. ***Usage Synchronization***

   Where tasks is performed: Product Instance

   Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 78

Result:

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

In case of a change in license usage, see Configuring an AIR License, on page 113 to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72.

Workflow for Topology: Connected Directly to CSSM

Smart Account Set-Up → Product Instance Configuration → Trust Establishment with CSSM

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 95

   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. 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:

     Configure Smart transport through an HTTPs proxy. See Configuring Smart Transport Through an HTTPs Proxy, on page 98

   - Option 3:

     Configure Call Home service for direct cloud access. See Configuring the Call Home Service for Direct Cloud Access, on page 99.

   - Option 4:

     Configure Call Home service for direct cloud access through an HTTPs proxy. See Configuring the Call Home Service for Direct Cloud Access through an HTTPs Proxy Server, on page 101.

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

   Where task is performed: CSSM Web UI and then the 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 106

b. Having downloaded the token, you can now install the trust code on the product instance: Installing a Trust Code, on page 106

Result:

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

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

To change the reporting interval, configure the **license smart usage interval** command in global configuration mode. For syntax details see the *license smart (privileged EXEC)* command in the Command Reference for the corresponding release.

In case of a change in license usage, see Configuring an AIR License, on page 113 to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72.

Workflow for Topology: Connected to CSSM Through a Controller

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

Product Instance Configuration → Cisco Catalyst Center **Configuration**

1. ***Product Instance Configuration***

   Where task is performed: Product Instance

   Enable NETCONF. Cisco Catalyst 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 Catalyst Center Configuration***

   Where tasks is performed: Cisco Catalyst 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 Catalyst 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 Catalyst Center to establish a connection with CSSM.

See the *Cisco Catalyst 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 Catalyst Center inventory and assign them to a site.

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

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

Result:

After you implement the topology, *you* must trigger the very first ad hoc report in Cisco Catalyst Center, to establish a mapping between the Smart Account and Virtual Account, and product instance. See the *Cisco Catalyst 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 Catalyst Center handles subsequent reporting based on the reporting policy.

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

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72.

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→ Usage Synchronization

1. ***CSLU Installation***

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

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

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

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 75

   c. Adding a Product-Initiated Product Instance in CSLU (CSLU Interface), on page 76

3. ***Product Instance Configuration***

   Where tasks are performed: Product Instance

   a. Ensuring Network Reachability for Product Instance-Initiated Communication, on page 76

   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. 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
Device(config)# exit
Device# copy running-config startup-config
```

4. ***Usage Synchronization***

Where tasks are performed: CSLU and CSSM

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

a. Export to CSSM (CSLU Interface), on page 79

b. Uploading Data or Requests to CSSM and Downloading a File, on page 108

c. Import from CSSM (CSLU Interface), on page 80

Result:

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

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

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

To verify trust code installation, enter the `show license status` command in privileged EXEC mode. Check for the updated timestamp in the `Trust Code Installed` field.

In case of a change in license usage, see Configuring an AIR License, on page 113 to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72.

Tasks for CSLU-Initiated Communication

CSLU Installation → CSLU Preference Settings → Product Instance Configuration → Usage Synchronization

1. ***CSLU Installation***

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

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

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

2. ***CSLU Preference Settings***

   Where tasks is 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 75

c. Adding a CSLU-Initiated Product Instance in CSLU (CSLU Interface), on page 78

d. Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 78

3. ***Product Instance Configuration***

   Where task is performed: Product Instance

   Ensuring Network Reachability for CSLU-Initiated Communication, on page 80

4. ***Usage Synchronization***

   Where tasks are performed: CSLU and CSSM

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

   a. Export to CSSM (CSLU Interface), on page 79

   b. Uploading Data or Requests to CSSM and Downloading a File, on page 108

   c. Import from CSSM (CSLU Interface), on page 80

Result:

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

In case of a change in license usage, see Configuring an AIR License, on page 113 to know how it affects reporting.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72.

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

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

Where task is performed: Product Instance

Set transport type to **off**.

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

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

Result:

All communication to and from the product instance is disabled. To report license usage you must save RUM reports to a file on the product instance. From a workstation that has connectivity to the Internet and Cisco, upload the file to CSSM:

1. Generate and save RUM reports

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

   Starting with Cisco IOS XE Cupertino 17.7.1, if a trust code does not already exist on the product instance, configuring this command automatically includes a trust code request in the RUM report. This is supported in a standalone, as well as a High Availability set-up.

   In the example below, the file is first saved 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 Data or Requests to CSSM and Downloading a File, on page 108.

3. Install the ACK on the product instance: Installing a File on the Product Instance, on page 109.

If you want to change license usage, see Configuring an AIR License, on page 113.

If you want to return an SLR authorization code, see Removing and Returning an Authorization Code, on page 103.

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72.

Workflow for Topology: SSM On-Prem Deployment

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

Tasks for Product Instance-Initiated Communication

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

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

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

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

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

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

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

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

   Where tasks are performed: SSM On-Prem UI

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

   - If you want your product instances to be added and validated in SSM On-Prem before they are reported in CSSM (for added security).
   - If you have created local virtual accounts (in addition to the default local virtual account) in SSM On-Prem. In this case you must provide SSM On-Prem with the Smart Account and Virtual Account information for the product instances in these local virtual accounts, so that SSM On-Prem can report usage to the correct license pool in CSSM.

   a. Assigning a Smart Account and Virtual Account (SSM On-Prem UI), on page 84

   b. Validating Devices (SSM On-Prem UI), on page 85

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

3. ***Product Instance Configuration***

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

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

   a. Ensuring Network Reachability for Product Instance-Initiated Communication, on page 85

   b. Retrieving the Transport URL (SSM On-Prem UI), on page 88

   c. Setting the Transport Type, URL, and Reporting Interval, on page 110

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

4. ***Initial Usage Synchronization***

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

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

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

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

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

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

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

- Option 1:

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

- Option 2:

  SSM On-Prem is not connected to CSSM: See Exporting and Importing Usage Data (SSM On-Prem UI), on page 89.

Result:

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

For subsequent reporting, you have the following options:

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

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

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

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

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

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

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

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

- Upload and download the required files for reporting: Exporting and Importing Usage Data (SSM On-Prem UI), on page 89).

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72.

Tasks for SSM On-Prem Instance-Initiated Communication

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

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

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

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

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

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

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

2. ***Product Instance Addition***

   Where task is performed: SSM On-Prem UI

   Depending on whether you want to add a single product instance or multiple product instances, follow the corresponding sub-steps: Adding One or More Product Instances (SSM On-Prem UI), on page 89.

3. ***Product Instance Configuration***

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

   Remember to save any configuration changes on the product instance, by entering the **copy running-config startup-config** command in privileged EXEC mode: Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 91.

4. ***Initial Usage Synchronization***

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

a. Retrieve usage information from the product instance.

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

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

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

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

- Option 1:

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

- Option 2:

  SSM On-Prem is not connected to CSSM. See: Exporting and Importing Usage Data (SSM On-Prem UI), on page 89.

Result:

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

For subsequent reporting, you have the following options:

- To retrieve usage information from the product instance, you can:
  - In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports** > **Usage Schedules** > **Synchronize now with Cisco**.
  - Schedule periodic retrieval of information from the product instance by configuring a frequency. In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports** > **Usage Schedules** > **Synchronization pull schedule with the devices**. Enter values in the following fields:
    - **Days**: Refers to how *often* synchronization occurs. For example, if you enter 2, synchronization occurs once every two days.
    - **Time of Day:**: Refers to the time at which synchronization occurs, in the 24-hour notation system. For example, if you enter 14 hours and 0 minutes, synchronization occurs at 2 p.m. (1400).
  - Collect usage data from the product instance without being connected to CSSM. In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Inventory** > **SL Using Policy** tab. Select one or more product instances by enabling the coresponding check box. Click **Actions for Selected...** > **Collect Usage**. On-Prem connects to the selected Product Instance(s) and collects the usage reports. These usage reports are then stored in On-Prem's local library. These reports can then be transferred to Cisco if On-Prem is connected to Cisco, or (if you are not connected to Cisco) you can manually trigger usage collection by selecting **Export/Import All..** > **Export Usage to Cisco**.

- To synchronize usage information with CSSM, you can:
  - Schedule periodic synchronization with CSSM. In the SSM On-Prem UI, navigate to **Reports** > **Usage Schedules** > **Synchronization schedule with Cisco**. Enter the following frequency information and save:
    - **Days**: Refers to how *often* synchronization occurs. For example, if you enter 2, synchronization occurs once every two days.
    - **Time of Day:**: Refers to the time at which synchronization occurs, in the 24-hour notation system. For example, if you enter 14 hours and 0 minutes, synchronization occurs at 2 p.m. (1400).
  - Upload and download the required files for reporting: Exporting and Importing Usage Data (SSM On-Prem UI), on page 89).

If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72.

CHAPTER 4

Migrating to Smart Licensing Using Policy

To upgrade to Smart Licensing Using Policy, you must upgrade the software version (image) on the product instance to a supported version.

Before you Begin

Ensure that you have read the Upgrades, on page 44 section, to understand how Smart Licensing Using Policy handles all earlier licensing models.

Smart Licensing Using Policy is introduced in Cisco IOS XE Amsterdam 17.3.2a. This is therefore the minimum required version for Smart Licensing Using Policy.

Note that all the licenses that you are using prior to migration will be available after upgrade. This means that not only registered and authorized licenses (including reserved licenses), but also evaluation licenses will be migrated. The advantage with migrating registered and authorized licenses is that you will have fewer configuration steps to complete after migration, because your configuration is retained after upgrade (transport type configuration and configuration for connection to CSSM, all authorization codes). This ensures a smoother transition to the Smart Licensing Using Policy environment.

Device-led conversion is not supported for migration to Smart Licensing Using Policy.

Upgrading the Wireless Controller Software

For information about the upgrade procedure:

- For Cisco Embedded Wireless Controller on Cisco Catalyst 9100 Access Points, see the *Software Upgrade* section in the Cisco Embedded Wireless Controller on Catalyst Access Points Online Help
- For all other supported wireless controllers, see the *System Upgrade* > *Upgrading the Cisco Catalyst 9800 Wireless Controller Software* section of the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide for the required release.

  If you are upgrading a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the conditions for a mandatory ACK starting with Cisco IOS XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72.

You can use the procedure to upgrade in install mode or ISSU (ISSU only on supported platforms and supported releases)

After Upgrading the Software Version

- Complete topology implementation.

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

No matter which licensing model you upgrade from, you can change the topology after upgrade.

- Synchronize license usage with CSSM

  No matter which licensing model you are upgrading from and no matter which topology you implement, synchronize your usage information with CSSM. For this you have to follow the reporting method that applies to the topology you implement. This initial synchronization ensures that up-to-date usage information is reflected in CSSM and a custom policy (if available), is applied. The policy that is applicable after this synchronization also indicates subsequent reporting requirements. These rules are also tabled here: How Upgrade Affects Reporting for Existing Licenses, on page 45

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

Sample Migration Scenarios

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

Note For SSM On-Prem, the sequence in which you perform the various upgrade-related activities is crucial. So only for this scenario, the migration sequence has been provided - and not an example.

- Upgrades, on page 44
- Downgrades, on page 46
- Sample Migration Scenarios, on page 49
- Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy, on page 67

Upgrades

This section explains the following aspects:

Migrating from earlier licensing models to Smart Licensing Using Policy. When migrating from earlier licensing models, also see the #unique_75 section for examples of migration scenarios that apply to Cisco Catalyst Wireless Controllers.

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

Identifying the Current Licensing Model Before Upgrade

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

How Upgrade Affects Enforcement Types for Existing Licenses

When you upgrade to a software version which supports Smart Licensing Using Policy, the way existing licenses are handled, depends primarily on the license enforcement type.

- An unenforced license that was being used before upgrade, continues to be available after the upgrade. All licenses on Cisco Catalyst Wireless Controllers are unenforced licenses. This includes licenses from all earlier licensing models:
  - Smart Licensing
  - Specific License Reservation (SLR), which has an accompanying authorization code. The authorization code continues to be valid after upgrade to Smart Licensing Using Policy and authorizes existing license consumption.
  - Evaluation or expired licenses from any of the above mentioned licensing models.
- An enforced or export-controlled license that was being used before upgrade, continues to be available after upgrade if the required authorization exists.

  There are no export-controlled or enforced licenses on any of the supported Cisco Catalyst Wireless Controllers, therefore, these enforcement types and the requisite SLAC do not apply.

How Upgrade Affects Reporting for Existing Licenses

Existing License	Reporting Requirements After Migration to Smart Licensing Using Policy
Specific License Reservation (SLR)	Required only if there is a change in license consumption. An existing SLR authorization code authorizes existing license consumption after upgrade to Smart Licensing Using Policy.
Smart Licensing (Registered and Authorized license)	Depends on the policy.
Evaluation or expired licenses	Based on the reporting requirements of the Cisco default policy.

How Upgrade Affects Transport Type for Existing Licenses

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

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

Transport type Before Upgrade	License or License State Before Upgrade	Transport Type After Upgrade
Default (callhome)	evaluation	cslu (default in Smart Licensing Using Policy)
	SLR	off
	registered	callhome
smart	evaluation	off
	SLR	off
	registered	smart

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* when a product instance is directly connected to CSSM. See Connected Directly to CSSM.

Upgrades Within the Smart Licensing Using Policy Environment

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

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

Downgrades

This section provides information about downgrades to an earlier licensing model, for new deployments and existing deployments. It also covers information relevant to downgrades within in the Smart Licensing Using Policy environment.

New Deployment Downgrade

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

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

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

Table 4: Outcome and Action for New Deployment Downgrade to Smart Licensing

In the Smart Licensing Using Policy Environment	Downgrade to..	Outcome and Further Action
Standalone product instance, connected directly to CSSM, and trust established.	Cisco IOS XE Amsterdam 17.3.1 OR Cisco IOS XE Gibraltar 16.12.4 and later releases in Cisco IOS XE Gibraltar 16.12.x	No further action is required. 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.
	Any other release (other than the ones mentioned in the row above) that supports Smart Licensing	Action is required: You must reregister the product instance. Generate an ID token in the CSSM Web UI and on the product instance, configure the **license smart register idtoken** *idtoken* command in global configuration mode.
High Availability set-up, connected directly to CSSM, and trust established.	Any release that supports Smart Licensing	Action is required: You must reregister the product instance. Generate an ID token in the CSSM Web UI and on the product instance, configure the **license smart register idtoken** *idtoken* **all** command in global configuration mode.
Any other topology. (Connected to CSSM Through CSLU, CSLU Disconnected from CSSM, No Connectivity to CSSM and No CSLU)	Any release that supports Smart Licensing	Action is required. Restore licenses to a registered and authorized state by following the procedures that are applicable in the Smart Licensing environment.

Upgrade and Then Downgrade

This section describes considerations and actions that apply if a product instance is upgraded to a software version that supports Smart Licensing Using Policy and then downgraded to an earlier licensing model.

When you downgrade such a product instance, *license consumption does not change* and any product features you have configured on the product instance are preserved – only the features and functions that are available with Smart Licensing Using Policy are not available anymore. Refer to the corresponding section below to know more about reverting to an earlier licensing model.

Upgrade to Smart Licensing Using Policy and then Downgrade to Smart Licensing

The outcome of the downgrade depends on whether a trust code was installed while you were still operating in the Smart Licensing Using Policy environment, and further action may be required depending on the release you downgrade to. See the table below.

Table 5: Outcome and Action for Upgrade to Smart Licensing Using Policy and then Downgrade to Smart Licensing

In the Smart Licensing Using Policy Environment	Downgrade to..	Outcome and Further Action
Standalone product instance, connected directly to CSSM, and trust established.	Cisco IOS XE Amsterdam 17.3.1 OR Cisco IOS XE Gibraltar 16.12.4 and later releases in Cisco IOS XE Gibraltar 16.12.x	No further action is required. The system recognizes the trust code and converts it back to a registered ID token, and this reverts the license to an AUTHORIZED and REGISTERED state.
	Any other release (other than the ones mentioned in the row above) that supports Smart Licensing	Action is required: You must reregister the product instance. Generate an ID token in the CSSM Web UI and on the product instance, configure the **license smart register idtoken***idtoken* command in global configuration mode.
High Availability set-up, connected directly to CSSM, and trust established.	Any release that supports Smart Licensing	Action is required: You must reregister the product instance. Generate an ID token in the CSSM Web UI and on the product instance, configure the **license smart register idtoken** *idtoken* **all** command in global configuration mode.
Any other topology (Connected to CSSM Through CSLU, CSLU Disconnected from CSSM, No Connectivity to CSSM and No CSLU)	Any release that supports Smart Licensing.	Action is required. Restore licenses to a registered and authorized state by following the procedures that are applicable in the Smart Licensing environment.

Note Licenses that were in an evaluation or expired state in the Smart Licensing environment, revert to that same state after downgrade.

Upgrade to Smart Licensing Using Policy and then Downgrade to SLR

To revert to SLR, all that is required is for the image to be downgraded. The license remains reserved and authorized – no further action is required.

However, if you have returned an SLR while in the Smart Licensing Using Policy environment, then you must repeat the process of procuring an SLR as required, in the supported release.

Downgrades Within the Smart Licensing Using Policy Environment

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

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

Sample Migration Scenarios

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

Note For SSM On-Prem, the sequence in which you perform the various upgrade-related activities is crucial. So only for this scenario, the migration sequence has been provided - and not an example.

Example: Smart Licensing to Smart Licensing Using Policy

The following is an example of a Cisco Catalyst 9800-CL Wireless Controller migrating from Smart Licensing to Smart Licensing Using Policy.

Table 6: Smart Licensing to Smart Licensing Using Policy: show Commands, on page 50

The CSSM Web UI After Migration, on page 53

Reporting After Migration, on page 56

The **show** command outputs below call-out key fields to check, before and after migration.

Table 6: Smart Licensing to Smart Licensing Using Policy: show Commands

<table>
<tr><th>Before Upgrade (Smart Licensing)</th><th>After Upgrade (Smart Licensing Using Policy)</th></tr>
<tr><td>

show license summary

The `Status` and `License Authorization` fields show that the license is `REGISTERED` and `AUTHORIZED`.

```
Device# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: SA-Eg-Company-02
  Virtual Account: Dept-02
  Export-Controlled Functionality: ALLOWED
  Last Renewal Attempt: None
  Next Renewal Attempt: May 01 08:19:02 2021 IST

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Dec 02 08:19:09 2020 IST

License Usage:
  License                  Entitlement tag        Count
 Status

-----------------------------------------------------------------

  AP Perpetual Network... (DNA_NWSTACK_E)           1
AUTHORIZED
  Aironet DNA Essentia... (AIR-DNA-E)               1
AUTHORIZED
```

</td><td>

show license summary

The `Status` field shows that the licenses are now `IN USE` instead of registered and authorized.

```
Device# show license summary

License Usage:
  License                 Entitlement Tag         Count
 Status

-----------------------------------------------------------------

  air-network-essentials  (DNA_NWSTACK_E)
1 IN USE
  air-dna-essentials      (AIR-DNA-E)
1 IN USE
```

</td></tr>
</table>

<table>
<tr><th>Before Upgrade (Smart Licensing)</th><th>After Upgrade (Smart Licensing Using Policy)</th></tr>
<tr><td>

show license usage

One perpetual and one subscription license are being used before upgrade.

</td><td>

show license usage

All licenses are migrated and the `Enforcement Type` field displays NOT ENFORCED.

There are no export-controlled or enforced licenses on Cisco Catalyst Wireless Controllers.

</td></tr>
</table>

Before Upgrade (Smart Licensing)	After Upgrade (Smart Licensing Using Policy)

Device# **show license usage**
 	
License Authorization:
  Status: AUTHORIZED on Nov 02 08:21:29 2020 IST
 	
AP Perpetual Networkstack Essentials (DNA_NWSTACK_E):
  Description: AP Perpetual Network Stack entitled with DNA-E
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
 	
Aironet DNA Essentials Term Licenses (AIR-DNA-E):
  Description: DNA Essentials for Wireless
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED
	Device# **show license usage**
	
	License Authorization:
	  Status: Not Applicable
	
	air-network-essentials (DNA_NWSTACK_E):
	  Description: air-network-essentials
	  Count: 1
	  Version: 1.0
	  Status: IN USE
	  Export status: NOT RESTRICTED
	  Feature Name: air-network-essentials
	  Feature Description: air-network-essentials
	  Enforcement type: NOT ENFORCED
	  License type: Perpetual
	
	air-dna-essentials (AIR-DNA-E):
	  Description: air-dna-essentials
	  Count: 1
	  Version: 1.0
	  Status: IN USE
	  Export status: NOT RESTRICTED
	  Feature Name: air-dna-essentials
	  Feature Description: air-dna-essentials
	  Enforcement type: NOT ENFORCED
	  License type: Perpetual

Before Upgrade (Smart Licensing)	After Upgrade (Smart Licensing Using Policy)
show license status	**show license status** The `Transport:` field shows that the transport type, which was configured before update, is retained after upgrade. The `Policy:` header and details show that a custom policy was available in the Smart Account or Virtual Account – this has also been automatically installed on the product instance. (After establishing trust, CSSM returns a policy. The policy is then automatically installed.) The `Usage Reporting:` header: The `Next report push:` field provides information about when the product instance will send the next RUM report to CSSM. The `Trust Code Installed:` field shows that the ID token is successfully converted and a trusted connected has been established with CSSM.

<table>
<tr><th>Before Upgrade (Smart Licensing)</th><th>After Upgrade (Smart Licensing Using Policy)</th></tr>
<tr><td><pre>
Device# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

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

Transport:
  Type: Callhome

Registration:
  Status: REGISTERED
  Smart Account: SA-Eg-Company-02
  Virtual Account: Dept-02
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Nov 02 08:19:02
2020 IST
  Last Renewal Attempt: None
  Next Renewal Attempt: May 01 08:19:01 2021 IST
  Registration Expires: Nov 02 08:14:06 2021 IST

License Authorization:
  Status: AUTHORIZED on Nov 02 08:21:29 2020 IST
  Last Communication Attempt: SUCCEEDED on Nov 02
08:21:29 2020 IST
  Next Communication Attempt: Dec 02 08:19:09 2020 IST
  Communication Deadline: Jan 31 08:14:15 2021 IST

Export Authorization Key:
  Features Authorized:
    <none>
</pre></td><td><pre>
Device# show license status
Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

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

Transport:
  Type: Callhome

Policy:
  Policy in use: Installed On Nov 02 09:09:47 2020 IST
  Policy name: SLE Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 60 (Customer
Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 30 (Customer
Policy)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:

    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: Nov 02 09:09:47 2020 IST
  Next ACK deadline: Jan 01 09:09:47 2021 IST
  Reporting push interval: 30 days
  Next ACK push check: Nov 02 09:13:54 2020 IST
  Next report push: Dec 02 09:05:45 2020 IST
  Last report push: Nov 02 09:05:45 2020 IST
  Last report file write: <none>

Trust Code Installed:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
    INSTALLED on Nov 02 08:59:26 2020 IST
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
    INSTALLED on Nov 02 09:00:45 2020 IST
</pre></td></tr>
</table>

Before Upgrade (Smart Licensing)	After Upgrade (Smart Licensing Using Policy)
show license udi	**show license udi** This is a High Availability set-up and the command displays all UDIs in the set-up. There is no change in the sample output before and after migration.

`Device# show license udi`
`UDI: PID:C9800-CL-K9,SN:93BBAH93MGS`
 	
`HA UDI List:`
`    Active:PID:C9800-CL-K9,SN:93BBAH93MGS`
`    Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN`
	`Device# show license udi`
	`UDI: PID:C9800-CL-K9,SN:93BBAH93MGS`
	
	`HA UDI List:`
	`    Active:PID:C9800-CL-K9,SN:93BBAH93MGS`
	`    Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN`

The CSSM Web UI After Migration

Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**. Under **Inventory** > **Product Instances**.

The product instance previously displayed with the host name (Catalyst 9800CL Cloud Wireless Controller in this example) is now displayed with the UDI instead. All migrated UDIs are displayed, that is, PID:C9800-CL-K9,SN:93BBAH93MGS, and PID:C9800-CL-K9,SN:9XECPSUU4XN.

Only the active product instance reports usage, therefore, PID:C9800-CL-K9,SN:93BBAH93MGS displays license consumption information under **License Usage**. The standby does not report usage and the **License Usage** for the standby displays No Records Found.

Figure 7: Smart Licensing to Smart Licensing Using Policy: Hostname of Product Instance on the CSSM Web UI Before Migration

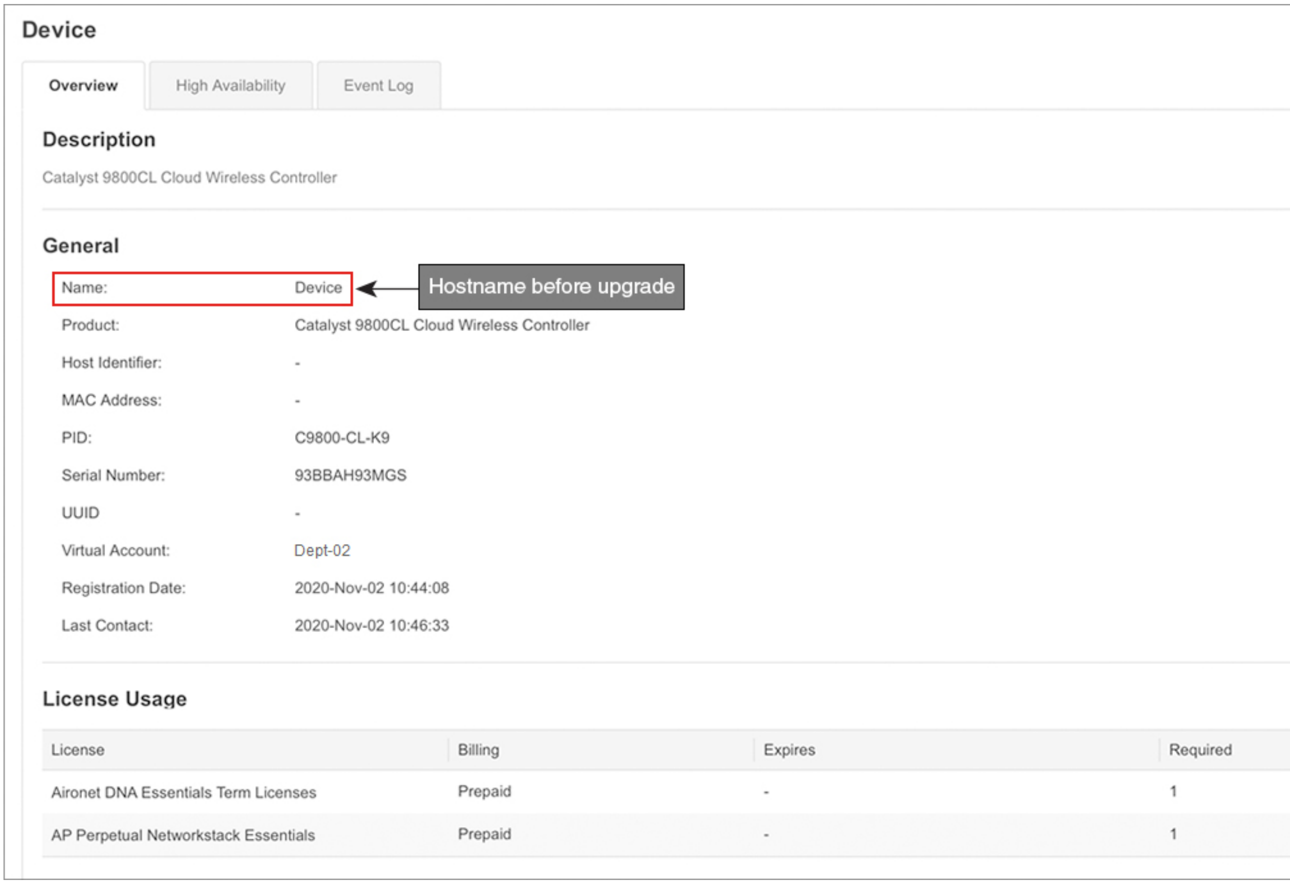


Figure 8: Smart Licensing to Smart Licensing Using Policy: UDI and License Usage Under Active Product Instance After Migration

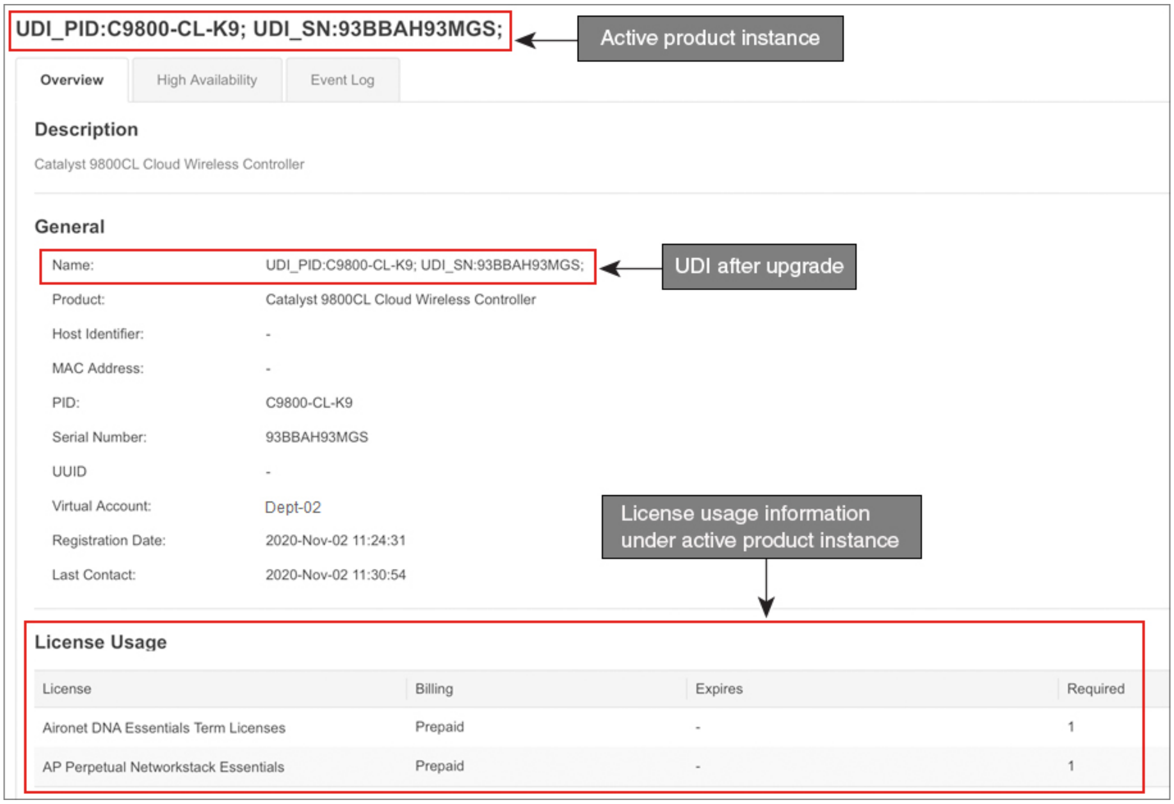
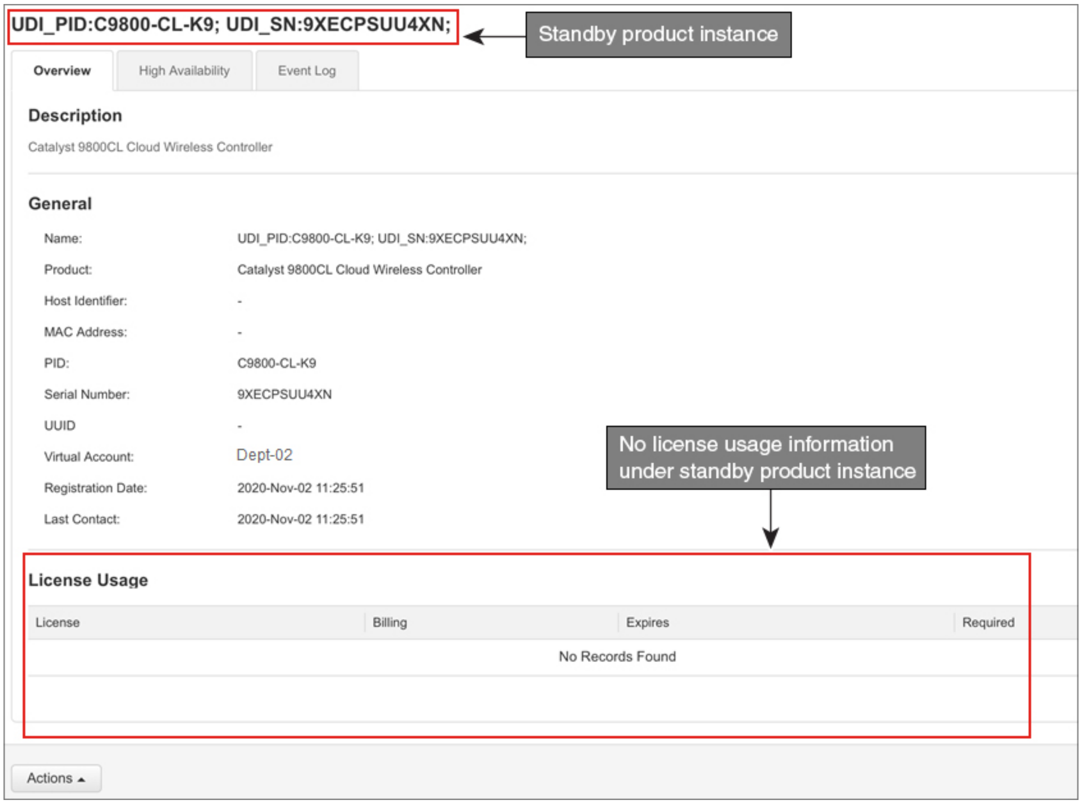


Figure 9: Smart Licensing to Smart Licensing Using Policy: Standby Product Instance After Migration



It is always the active that reports usage, so if the active in this High Availability set-up changes, the new active product instance will display license consumption information and report usage.

Reporting After Migration

The product instance sends the next RUM report to CSSM, based on the policy.

If you want to change your reporting interval to report more frequently: on the product instance, configure the **license smart usage interval** command in global configuration mode. For syntax details see the *license smart (global config)* command in the Command Reference for the corresponding release.

Example: SLR to Smart Licensing Using Policy

The following is an example of a Cisco Catalyst 9800-CL Wireless Controller migrating from Specific License Reservation (SLR) to Smart Licensing Using Policy. This is a High Availability set-up with an active and standby.

License conversion is automatic and authorization codes are migrated. No further action is required to complete migration. After migration the No Connectivity to CSSM and No CSLU, on page 19 topology is effective. For information about the SLR authorization code in the Smart Licensing Using Policy environment, see Authorization Code, on page 3.

Table 7: SLR to Smart Licensing Using Policy: show Commands, on page 57

The CSSM Web UI After Migration, on page 61

Reporting After Migration, on page 63

The **show** command outputs below call-out key fields to check, before and after migration.

Table 7: SLR to Smart Licensing Using Policy: show Commands

Before Upgrade (SLR)	After Upgrade (Smart Licensing Using Policy)

show license summary
 	
The `Registration` and `License Authorization` status fields show that the license was `REGISTERED - SPECIFIC LICENSE RESERVATION` and `AUTHORIZED - RESERVED`.
 	
`Device# `**`show license summary`**
 	
`Smart Licensing is ENABLED`
`License Reservation is ENABLED`
 	
`Registration:`
 	
`  `**`Status: REGISTERED - SPECIFIC LICENSE RESERVATION`**
`  Export-Controlled Functionality: ALLOWED`
 	
`License Authorization:`
`  Status: AUTHORIZED - RESERVED`
 	
`License Usage:`
`  License                Entitlement tag         Count`
` Status`
 	
`--------------------------------------------------------------`
 	
`  AP Perpetual Network... (DNA_NWStack)`
` 1 AUTHORIZED`
`  Aironet DNA Advantag... (AIR-DNA-A)`
` 1 AUTHORIZED`
	show license summary
	
	Licenses are migrated , but none of the APs have joined the controller, current consumption (Count) is therefore zero, and the `Status` field shows that the licenses are `NOT IN USE`.
	
	`Device# `**`show license summary`**
	`License Reservation is ENABLED`
	
	`License Usage:`
	`  License                Entitlement Tag      Count`
	`Status`
	
	`--------------------------------------------------------------`
	
	`  Aironet DNA Advantag... (AIR-DNA-A)            0 `**`NOT`**
	` `**`IN USE`**
	`  AP Perpetual Network... (DNA_NWStack)          0 `**`NOT`**
	` `**`IN USE`**

Before Upgrade (SLR)	After Upgrade (Smart Licensing Using Policy)
show license reservation	**show license authorization** The `Last Confirmation code:` field shows that the SLR authorization code is successfully migrated for the active and standby product instances in the High Availability set-up. The `Specified license reservations:` header shows that a perpetual license (AP Perpetual Networkstack Advantage) and a subscription license (Aironet DNA Advantage Term Licenses) are the migrated SLR licenses.

Before Upgrade (SLR)	After Upgrade (Smart Licensing Using Policy)

<pre>Device# **show license reservation**
License reservation: ENABLED
 	
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Reservation status: SPECIFIC INSTALLED on Nov 02
 03:16:01 2020 IST
      Export-Controlled Functionality: ALLOWED
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Reservation status: SPECIFIC INSTALLED on Nov 02
 03:15:45 2020 IST
      Export-Controlled Functionality: ALLOWED
      Last Confirmation code: ad4382fe
 	
Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled
with DNA-A
    Total reserved count: 20
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10</pre>	

Before Upgrade (SLR)	After Upgrade (Smart Licensing Using Policy)

	<pre>Device# **show license authorization**
	Overall status:
	  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
	      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020
	 IST
	      Last Confirmation code: 102fc949
	  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
	      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020
	 IST
	      Last Confirmation code: ad4382fe
	
	Specified license reservations:
	  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
	    Description: DNA Advantage for Wireless
	    Total reserved count: 20
	    Enforcement type: NOT ENFORCED
	    Term information:
	      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
	        Authorization type: SPECIFIC INSTALLED on Nov
	02 03:15:45 2020 IST
	        License type: TERM
	          Start Date: 2020-OCT-14 UTC
	          End Date: 2021-APR-12 UTC
	          Term Count: 5
	        Authorization type: SPECIFIC INSTALLED on Nov
	02 03:15:45 2020 IST
	        License type: TERM
	          Start Date: 2020-JUN-18 UTC
	          End Date: 2020-DEC-15 UTC
	          Term Count: 5
	      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
	        Authorization type: SPECIFIC INSTALLED on Nov
	02 03:15:45 2020 IST
	        License type: TERM
	          Start Date: 2020-OCT-14 UTC
	          End Date: 2021-APR-12 UTC
	          Term Count: 10
	  AP Perpetual Networkstack Advantage (DNA_NWStack):
	    Description: AP Perpetual Network Stack entitled
	with DNA-A
	    Total reserved count: 20
	    Enforcement type: NOT ENFORCED
	    Term information:
	      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
	        Authorization type: SPECIFIC INSTALLED on Nov
	02 03:15:45 2020 IST
	        License type: TERM
	          Start Date: 2020-OCT-14 UTC
	          End Date: 2021-APR-12 UTC
	          Term Count: 5
	        Authorization type: SPECIFIC INSTALLED on Nov
	02 03:15:45 2020 IST
	        License type: TERM
	          Start Date: 2020-JUN-18 UTC
	          End Date: 2020-DEC-15 UTC
	          Term Count: 5
	      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
	        Authorization type: SPECIFIC INSTALLED on Nov
	02 03:15:45 2020 IST
	        License type: TERM
	          Start Date: 2020-OCT-14 UTC
	          End Date: 2021-APR-12 UTC</pre>

Before Upgrade (SLR)	After Upgrade (Smart Licensing Using Policy)

	`Term Count: 10`
	
	`Purchased Licenses:`
	`No Purchase Information Available`

Before Upgrade (SLR)	After Upgrade (Smart Licensing Using Policy)
show license status	**show license status** Under the `Transport:` header, the `Type:` field displays that the transport type is set to off. Under the `Usage Reporting:` header, the `Next report push:` field displays if and when the next RUM report must be uploaded to CSSM.

<table>
<tr><th>Before Upgrade (SLR)</th><th>After Upgrade (Smart Licensing Using Policy)</th></tr>
<tr><td>-</td><td><pre>
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: Transport Off

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
   First report requirement (days): 365 (CISCO default)

    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
   First report requirement (days): 90 (CISCO default)

    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:

    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: Nov 01 20:31:46 2020 IST
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>
</pre></td></tr>
</table>

The CSSM Web UI After Migration

Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**. Under **Inventory** > **Product Instances**.

There are no changes in the **Product Instances** tab. The Last Contact column displays "Reserved Licenses" since there has been no usage reporting yet. After the requisite RUM report is uploaded and acknowledged "Reserved Licenses" is no longer displayed and license usage is displayed only in the active product instance.

Figure 10: SLR to Smart Licensing Using Policy: Active Product Instance Before Upgrade

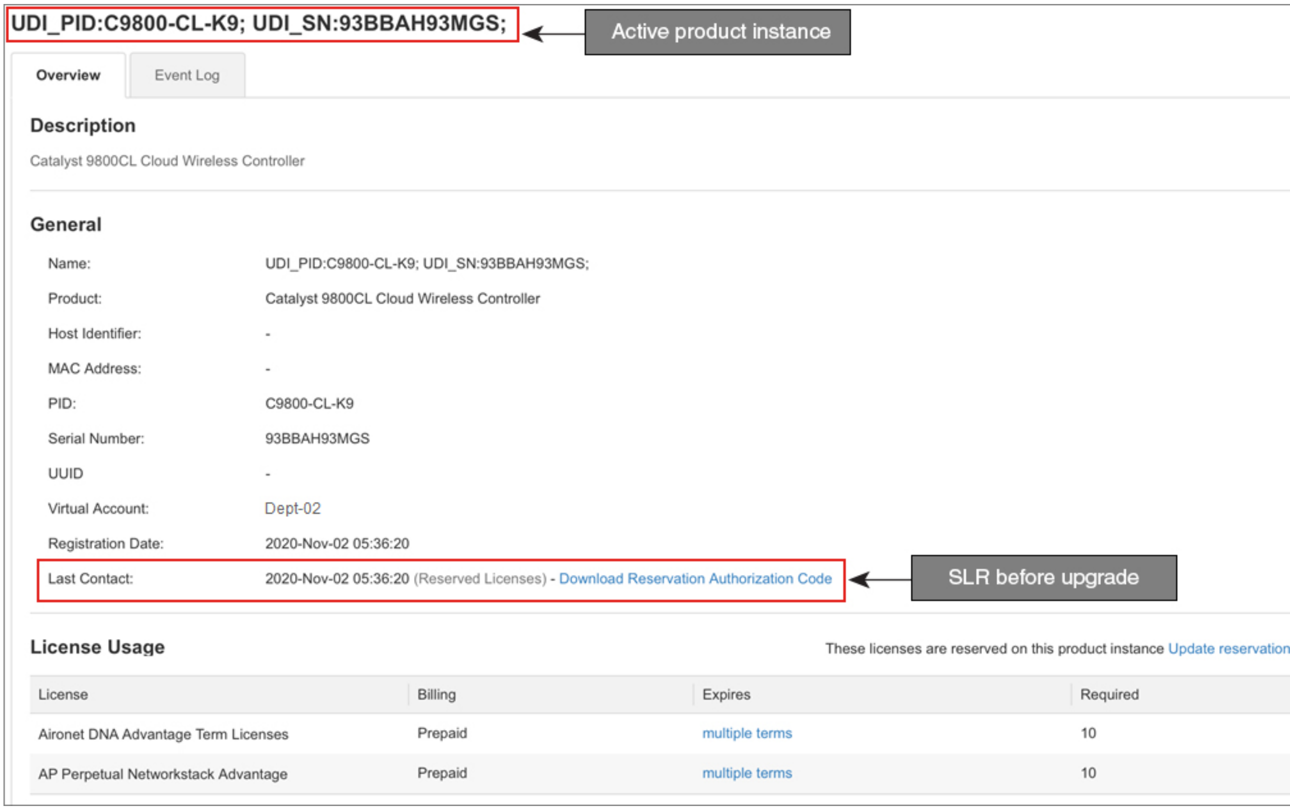
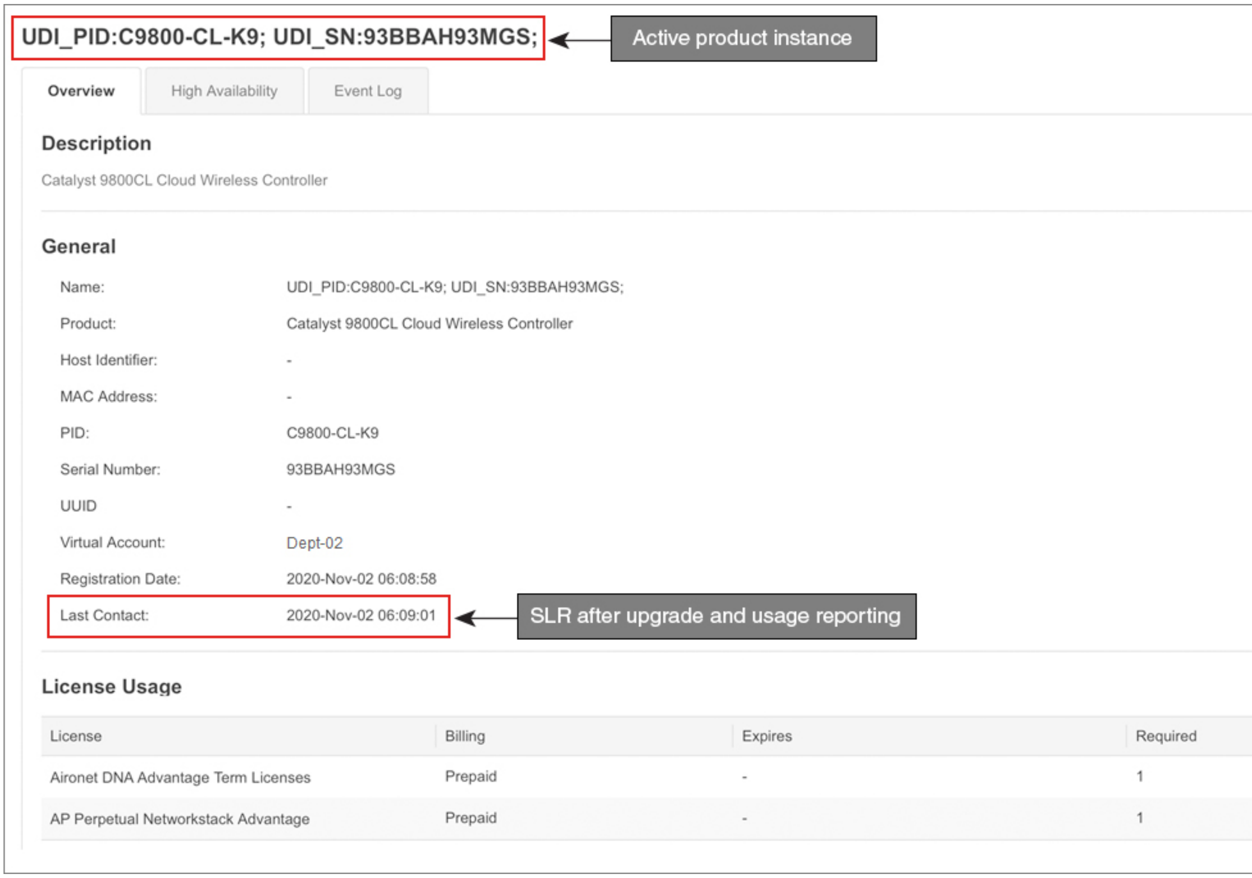


Figure 11: SLR to Smart Licensing Using Policy: Active Product Instance After Upgrade



Reporting After Migration

SLR licenses require reporting only when there is a change in license consumption (For example, when using a subscription license which is for specified term).

In an air-gapped network, use the `Next report push:` date in the **show license status** output to know when the next usage report must be sent. This ensures that the product instance and CSSM are synchronized.

Since all communication to and from the product instance is disabled, to report license usage you must save RUM reports to a file 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 privileged EXEC mode. In the example below, all RUM reports are saved to the flash memory of the product instance, in file `all_rum.txt`. For syntax details see the *license smart (privileged EXEC)* command in the Command Reference. In the example, the file is first saved to bootflash and then copied to a TFTP location:

   ```
   Device# license smart save usage all 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 Data or Requests to CSSM and Downloading a File, on page 108.

3. Install the ACK on the product instance: Installing a File on the Product Instance, on page 109.

Example: Evaluation or Expired to Smart Licensing Using Policy

The following is an example of a Cisco Catalyst 9800-CL Wireless Controller with evaluation expired licenses (Smart Licensing) that are migrated to Smart Licensing Using Policy.

The notion of evaluation licenses does not apply to Smart Licensing Using Policy. When the software version is upgraded to one that supports Smart Licensing Using Policy, all licenses are displayed as IN USE and the Cisco default policy is applied to the product instance. Since all licenses on Cisco Catalyst Wireless Controllers are unenforced (enforcement type), no functionality is lost.

Migration information is covered in these sections:

Table 8: Evaluation or Expired to Smart Licensing Using Policy: show Commands, on page 64

The CSSM Web UI After Migration, on page 67

Reporting After Migration, on page 67

The table below calls out key changes or new fields to check for in the **show** command outputs, after upgrade to Smart Licensing Using Policy

Table 8: Evaluation or Expired to Smart Licensing Using Policy: show Commands

<table>
<tr><th>Before Upgrade (Smart Licensing, Evaluation Mode)</th><th>After Upgrade (Smart Licensing Using Policy)</th></tr>
<tr><td>

show license summary

Licenses are UNREGISTERED and in `EVAL MODE`.

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

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

License Authorization:
  Status: EVAL EXPIRED

License Usage:
  License            Entitlement tag    Count Status

-------------------------------------------------------

                     (DNA_NWStack)          1 EVAL
EXPIRED
                     (AIR-DNA-A)            1 EVAL
EXPIRED
```

</td><td>

show license summary

All licenses are migrated and `IN USE`. There are no EVAL MODE licenses.

```
Device# show license summary
License Usage:
  License                 Entitlement Tag        Count
 Status

-------------------------------------------------------

  air-network-advantage   (DNA_NWStack)              1
 IN USE
  air-dna-advantage       (AIR-DNA-A)                1
 IN USE
```

</td></tr>
<tr><th>Before Upgrade (Smart Licensing, Evaluation Mode)</th><th>After Upgrade (Smart Licensing Using Policy)</th></tr>
<tr><td>

show license usage

</td><td>

show license usage

The `Enforcement Type` field displays NOT ENFORCED. (There are no export-controlled or enforced licenses on Cisco Catalyst Wireless Controllers).

</td></tr>
</table>

Before Upgrade (Smart Licensing, Evaluation Mode)	After Upgrade (Smart Licensing Using Policy)

`Device#` **`show license usage`**
`License Authorization:`
`  Status: EVAL EXPIRED on Apr 14 18:20:46 2020 UTC`
 	
`(DNA_NWStack):`
`  Description:`
`  Count: 1`
`  Version: 1.0`
`  Status: EVAL EXPIRED`
`  Export status: NOT RESTRICTED`
 	
`(AIR-DNA-A):`
`  Description:`
`  Count: 1`
`  Version: 1.0`
`  Status: EVAL EXPIRED`
`  Export status: NOT RESTRICTED`
	`Device#` **`show license usage`**
	`License Authorization:`
	`  Status: Not Applicable`
	
	`air-network-advantage (DNA_NWStack):`
	`  Description: air-network-advantage`
	`  Count: 1`
	`  Version: 1.0`
	`  Status: IN USE`
	`  Export status: NOT RESTRICTED`
	`  Feature Name: air-network-advantage`
	`  Feature Description: air-network-advantage`
	`  Enforcement type: NOT ENFORCED`
	`  License type: Perpetual`
	
	`air-dna-advantage (AIR-DNA-A):`
	`  Description: air-dna-advantage`
	`  Count: 1`
	`  Version: 1.0`
	`  Status: IN USE`
	`  Export status: NOT RESTRICTED`
	`  Feature Name: air-dna-advantage`
	`  Feature Description: air-dna-advantage`
	`  Enforcement type: NOT ENFORCED`
	`  License type: Perpetual`

Before Upgrade (Smart Licensing, Evaluation Mode)	After Upgrade (Smart Licensing Using Policy)
show license status	**show license status** The `Transport:` field displays that the default type is set, but a URL or a method for the product instance to discover CSLU is not specified. The `Trust Code Installed:` field displays that a trust code is not installed. The `Policy:` header and details show that the `Cisco default` policy is applied. Under the `Usage Reporting:` header, the `Next report push:` field provides information about when the next RUM report must be sent to CSSM.

Before Upgrade (Smart Licensing, Evaluation Mode)

```
Device# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

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

Transport:
  Type: Callhome

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

License Authorization:
  Status: EVAL EXPIRED on Apr 14 18:20:46 2020 UTC

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

After Upgrade (Smart Licensing Using Policy)

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

Smart Licensing Using Policy:
  Status: ENABLED

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

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

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
   First report requirement (days): 365 (CISCO default)

    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
   First report requirement (days): 90 (CISCO default)

    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:

    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>
```

The CSSM Web UI After Migration

Log in to the CSSM Web UI at https://software.cisco.com and click **Smart Software Licensing**. Under **Inventory** > **Product Instances**, the Last Contact field for the migrated product instances display an updated timestamp after migration.

Reporting After Migration

Implement any one of the supported topologies, and fulfil reporting requirements. See Connecting to Cisco SSM, on page 13 and Implementing Smart Licensing Using Policy, on page 27. The reporting method you can use depends on the topology you implement.

Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy

If you are using a version of SSM On-Prem that is earlier than the minimum required version (See Cisco Smart Software Manager On-Prem (SSM On-Prem), on page 11), you can use this section as an outline of the process and sequence you have to follow to migrate the SSM On-Prem version and the product instance.

1. Upgrade SSM On-Prem.

   Upgrade to the minimum required Version 8, Release 202102 or a later version.

   Refer to the Cisco Smart Software Manager On-Prem Migration Guide.

2. Upgrade the product instance.

   For information about the minimum required software version, see Cisco Smart Software Manager On-Prem (SSM On-Prem), on page 11.

   For information about the upgrade procedure, refer to the pointers provided in Migrating to Smart Licensing Using Policy, on page 43, *Upgrading the Wireless Controller Software*.

3. Re-Register a local account with CSSM

   Online and Offline options are available. Refer to the Cisco Smart Software Manager On-Prem Migration Guide > *Re-Registering a local Account (Online Mode)* or *Manually Re-Registering a Local Account (Offline Mode)* .

   Once re-registration is complete, the following events occur automatically:

   - SSM On-Prem responds with new transport URL that points to the tenant in SSM On-Prem.
   - The transport type configuration on the product instance changes from **call-home** or **smart**, to **cslu**. The transport URL is also updated automatically.

4. Save configuration changes on the product instance, by entering the **copy running-config startup-config** command in privileged EXEC mode.

5. Clear older On-Prem Smart Licensing certificates on the product instance and reload the product instance. Do not save configuration changes after this.

Note This step is required only if the software version running on the product instance is Cisco IOS XE Amsterdam 17.3.x or Cisco IOS XE Bengaluru 17.4.x.

Enter the **license smart factory reset** and then the **reload** commands in privileged EXEC mode.

```
Device# license smart factory reset
Device# reload
```

6. Perform usage synchronization

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

   ```
   Device(config)# license smart sync local
   ```

   You can verify this in the SSM On-Prem UI. Go to **Inventory** > **SL Using Policy**. In the **Alerts** column, the following message is displayed: Usage report from product instance.

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

      - Option 1:

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

      - Option 2:

        SSM On-Prem is not connected to CSSM. See Exporting and Importing Usage Data (SSM On-Prem UI), on page 89.

Result:

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

For subsequent reporting, you have the following options:

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

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

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

  - Enter the **license smart sync** privileged EXEC command, for ad hoc or on-demand synchronization between the product instance and SSM On-Prem.

- To synchronize usage information with CSSM:

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

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

- Upload and download the required files for reporting. See Exporting and Importing Usage Data (SSM On-Prem UI), on page 89.

CHAPTER 5

Task Library for Smart Licensing Using Policy

This section is a grouping of tasks that apply to Smart Licensing Using Policy. It includes tasks performed on a product instance, on the CSLU interface, and on the CSSM Web UI.

To implement a particular topology, refer to the corresponding workflow to know the sequential order of tasks that apply. See #unique_90.

To perform any additional configuration tasks, for instance, to configure a different license, or use an add-on license, or to configure a narrower reporting interval, refer to the corresponding task here. Check the "Supported Topologies" where provided, before you proceed.

RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller

About This Requirement

Beginning with Cisco IOS XE Cupertino 17.7.1, if you are using a *Cisco Catalyst 9800-CL Wireless Controller*, you must complete RUM (Resource Utilization Measurement) reporting and ensure that the Acknowledgment (ACK) is made available on the product instance - at least once. This is to ensure that correct and up-to-date usage information is reflected in CSSM.

Prior to Cisco IOS XE Cupertino 17.7.1, RUM reporting and ACK installation was not mandatory for a Cisco Catalyst *9800-CL* Wireless Controller (unlike other Cisco Catalyst Wireless Controllers).

This requirement is applicable to:

- A new Cisco Catalyst 9800-CL Wireless Controller purchased through the Cisco Commerce portal or downloaded from the Software Download page, and where the software version running on the product instance is Cisco IOS XE Cupertino 17.7.1 or a later release.

- An existing Cisco Catalyst 9800-CL Wireless Controller that is upgraded to Cisco IOS XE Cupertino 17.7.1 or later release.

Required Action to Meet This Requirement

The following procedure provides information about what you have to do to ensure compliance with this requirement and avoid any throttling restrictions on new and upgraded product instances. This procedure is followed by a flow chart which depicts the same information.

1. Check when the ACK is expected. Note system behavior if you don't meet the ACK deadline.

   Enter the **show license air entities summary** command in privileged EXEC mode and check field `License Ack expected within.....................: [n] days.`

   System behavior if you do not meet the ACK deadline:

Note If the number of AP joins is greater than 10, the system displays this system message once-a-day until an ACK is installed: %IOSXE_RP_EWLC_NOT-2-MSGDEVICENOTREG.

- *If an ACK is not installed by the ACK deadline, and the count of currently active APs is lesser than or equal to 50*, the system throttles the AP join count to 50.

- *If an ACK is not installed by the ACK deadline and the count of currently active APs is greater than 50*, these currently active APs are not disconnected, but no new AP joins are allowed.
- If there is a reload after the throttled state has come into effect, the system throttles the number of currently active APs to 50 when the system comes up after reload.
- If there is a stateful switchover (SSO) after the throttled state has come into effect, all connected APs remain joined.
- The following system message is displayed when the throttling restriction is effective and a new AP tries to join: %CAPWAPAC_TRACE_MSG-3-MAX_LICENSE_AP_LIMIT_REACHED.

The AP join restriction and the display of the system messages continues until the first ACK is made available on the product instance.

2. Implement a supported topology.

If you have not already done so, implement one of the supported topologies and complete usage reporting. The method you use to send the RUM report to CSSM and ACK installation depends on the topology you implement.

For more information, see: Connecting to Cisco SSM, on page 13 and Implementing Smart Licensing Using Policy, on page 27.

3. Ensure that the ACK is available on the product instance.

In the output of the **show license status** command in privileged EXEC mode check for an updated timestamp in the `Last ACK received:`.

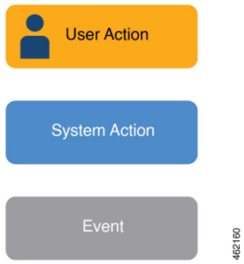
```
Device# show license status
<output truncated>
Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>
```

In the output of the **show license air entities summary** command in privileged EXEC mode, the `License Ack expected within.....................: [n] days` field is no longer displayed.

```
Device# show license air entities summary
Upcoming license report time...................: 21:05:16.092 UTC Mon Oct 25 2021
No. of APs active at last report...............: 57
No. of APs newly added with last report........: 57
No. of APs deleted with last report............: 0
```

Once the first ACK is installed, the system messages (%IOSXE_RP_EWLC_NOT-2-MSGDEVICENOTREG and %CAPWAPAC_TRACE_MSG-3-MAX_LICENSE_AP_LIMIT_REACHED) are not displayed any longer and AP join throttling restrictions are lifted.

Figure 12: Flow Chart of System Events, User Actions, and System Actions on a Cisco Catalyst 9800-CL Wireless Controller



Logging into Cisco (CSLU Interface)

Depending on your needs, when working in CSLU, you can either be in connected or disconnected mode. To work in the connected mode, complete these steps to connect with Cisco.

Procedure

Step 1 From the CSLU Main screen, click **Login to Cisco** (located at the top right corner of the screen).

Step 2 Enter: **CCO User Name** and **CCO Password**.

Step 3 In the CSLU Preferences tab, check that the Cisco connectivity toggle displays “Cisco Is Available”.

Configuring a Smart Account and a Virtual Account (CSLU Interface)

Both the Smart Account and Virtual Account are configured through the Preferences tab. Complete the following steps to configure both Smart and Virtual Accounts for connecting to Cisco.

Procedure

Step 1 Select the **Preferences Tab** from the CSLU home screen.

Step 2 Perform these steps for adding both a Smart Account and Virtual Account:

a) In the Preferences screen navigate to the **Smart Account** field and add the **Smart Account Name**.
b) Next, navigate to the **Virtual Account** field and add the **Virtual Account Name**.

If you are connected to CSSM (In the Preferences tab, **Cisco is Available**), you can select from the list of available SA/VAs.

If you are not connected to CSSM (In the Preferences tab, **Cisco Is Not Available**), enter the SA/VAs manually.

Note SA/VA names are case sensitive.

Step 3 Click **Save**. The SA/VA accounts are saved to the system

Only one SA/VA pair can reside on CSLU at a time. You cannot add multiple accounts. To change to another SA/VA pair, repeat Steps 2a and 2b then Save. A new SA/VA account pair replaces the previous saved pair

Adding a Product-Initiated Product Instance in CSLU (CSLU Interface)

Complete these steps to add a device-created Product Instance using the Preferences tab.

Procedure

Step 1 Select the **Preferences** tab.

Step 2 In the Preferences screen, de-select the **Validate Device** check box.

Step 3 Set the **Default Connect Method** to **Product Instance Initiated** and then click **Save**.

Ensuring Network Reachability for Product Instance-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for product instance-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps my be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Before you begin

Supported topologies: Connected to CSSM Through CSLU (product instance-initiated communication).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.

	Command or Action	Purpose
Step 4	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding Mgmt-vrf`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 5	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 6	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables auto-negotiation operation for the speed and duplex parameters of an interface. **Note** Cisco Catalyst 9800-L-F Wireless Controller 10G Ports do not support in an auto-negotiation operation.
Step 7	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.
Step 8	**ip http client source-interface** *interface-type-number* **Example:** `Device(config)# ip http client source-interface gigabitethernet0/0`	Configures a source interface for the HTTP client.
Step 9	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	(Required) Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.
Step 10	{**ip** | **ipv6**}**name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# Device(config)# ip name-server vrf mgmt-vrf 173.37.137.85`	Configures Domain Name System (DNS) on the VRF interface.
Step 11	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Configures the source interface for the DNS domain lookup.

	Command or Action	Purpose
Step 12	**ip domain name** *domain-name* **Example:** `Device(config)# ip domain name example.com`	Configure DNS discovery of your domain. In accompanying example, the name-server creates entry `cslu-local.example.com`.

Adding a CSLU-Initiated Product Instance in CSLU (CSLU Interface)

Using the CSLU interface, you can configure the connect method to be CSLU Initiated. This connect method (mode) enables CSLU to retrieve Product Instance information from the Product Instance.

Note The default Connect Method is set in the **Preferences** tab.

Complete these steps to add a Product Instance from the Inventory tab

Procedure

Step 1 Go to the **Inventory** tab and from the Product Instances table, select **Add Single Product**.

Step 2 Enter the **Host** (IP address of the Host).

Step 3 Select the **Connect Method** and select one of the CSLU Initiated connect methods.

Step 4 In the right panel, click **Product Instance Login Credentials**. The left panel of the screen changes to show the User Name and Password fields.

Step 5 Enter the product instance **User Name** and **Password**.

Step 6 Click **Save**.

The information is saved to the system and the device is listed in the Product Instances table with the Last Contact listed as never.

Collecting Usage Reports: CSLU Initiated (CSLU Interface)

CSLU also allows you to manually trigger the gathering of usage reports from devices.

After configuring and selecting a product instance (selecting **Add Single Product**, filling in the **Host** name and selecting a CSLU-initiated connect method), click **Actions for Selected** > **Collect Usage**. CSLU connects to the selected product instances and collects the usage reports. These usage reports are stored in CSLU's local library. These reports can then be transferred to Cisco if CSLU is connected to Cisco, or (if you are not connected to Cisco) you can manually trigger usage collection by selecting **Data** > **Export to CSSM**.

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

Procedure

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

Step 2 Click the **Inventory** tab and select one or more product instances.

Step 3 Click **Actions for Selected** > **Collect Usage**.

RUM reports are retrieved from each selected device and stored in the CSLU local library. The Last Contacted column is updated to show the time the report was received, and the Alerts column shows the status.

If CSLU is currently logged into Cisco the reports will be automatically sent to the associated Smart Account and Virtual Account in Cisco and Cisco will send an acknowledgement to CSLU as well as to the product instance. The acknowledgement will be listed in the alerts column of the Product Instance table. To manually transfer usage reports Cisco, from the CSLU main screen select **Data** > **Export to CSSM**.

Step 4 From the **Export to CSSM** modal, select the local directory where the reports are to be stored. (<CSLU_WORKING_Directory>/data/default/rum/unsent)

At this point, the usage reports are saved in your local directory (library). To upload these usage reports to Cisco, follow the steps described in #unique_92.

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`.

Export to CSSM (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

Procedure

Step 1 Go to the **Preferences** tab, and turn off the **Cisco Connectivity** toggle switch.

The field switches to “Cisco Is Not Available”.

Step 2 From the main menu in the CSLU home screen navigate to **Data** > **Export to CSSM**.

Step 3 Select the file from the modal that opens and click **Save**. You now have the file saved.

Note At this point you have a DLC file, RUM file, or both.

Step 4 Go to a station that has connectivity to Cisco, and complete the following: #unique_92

Once the file is downloaded, you can import it into CSLU, see #unique_93.

Import from CSSM (CSLU Interface)

Once you have received the ACK or other file (such as an authorization code) from Cisco, you are ready to Upload that file to your system. This procedure can be used for workstations that are offline. Complete these steps to select and upload files from Cisco.

Procedure

Step 1 Ensure that you have downloaded the file to a location that is accessible to CSLU.

Step 2 From the main menu in the CSLU home screen, navigate to **Data** > **Import from CSSM**.

Step 3 An Import from CSSM modal open for you to either:

- Drag and Drop a file that resides on your local drive, or
- Browse for the appropriate *.xml file, select the file and click **Open**.

If the upload is successful, you will get message indicating that the file was successfully sent to the server. If the upload is not successful, you will get an import error.

Step 4 When you have finished uploading, click the **x** at the top right corner of the modal to close it.

Ensuring Network Reachability for CSLU-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for CSLU-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps may be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Before you begin

Supported topologies: Connected to CSSM Through CSLU (CSLU-initiated communication).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new model** **Example:** `Device(config)# aaa new model`	(Required) Enable the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa authentication login default local** **Example:** `Device(config)# aaa authentication login default local`	(Required) Sets AAA authentication to use the local username database for authentication.
Step 5	**aaa authorization exec default local** **Example:** `Device(config)# aaa authorization exec default local`	Sets the parameters that restrict user access to a network. The user is allowed to run an EXEC shell.
Step 6	ip routing **Example:** `Device(config)# ip routing`	Enables IP routing.
Step 7	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300`	(Optional) Specifies the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The device sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 8	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Enables DNS-based hostname-to-address translation on your device. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).
Step 9	**ip domain name** *name* **Example:** `Device(config)# ip domain name vrf Mgmt-vrf cisco.com`	Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).

	Command or Action	Purpose
Step 10	**no username** *name* **Example:** `Device(config)# no username admin`	(Required) Clears the specified username, if it exists. For *name* , enter the same username you will create in the next step. This ensures that a duplicate of the username you are going to create in the next step does not exist. If you plan to use REST APIs for CSLU-initiated retrieval of RUM reports, you have to log in to CSLU. Duplicate usernames may cause the feature to work incorrectly if there are duplicate usernames in the system.
Step 11	**username** *name* **privilege** *level* **password** *password* **Example:** `Device(config)# username admin privilege 15 password 0 lab`	(Required) Establishes a username-based authentication system. The **privilege** keyword sets the privilege level for the user. A number between 0 and 15 that specifies the privilege level for the user. The password allows access to the name argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command. This enables CSLU to use the product instance native REST. **Note** Enter this username and password in CSLU (#unique_94 → *Step 4. f.* CSLU can then collect RUM reports from the product instance.
Step 12	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.
Step 13	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding Mgmt-vrf`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 14	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 15	**negotiation auto** **Example:**	Enables auto-negotiation operation for the speed and duplex parameters of an interface.

	Command or Action	Purpose
	`Device(config-if)# negotiation auto`	
Step 16	**no shutdown** **Example:** `Device(config-if)# no shutdown`	Restarts a disabled interface.
Step 17	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.
Step 18	**ip http server** **Example:** `Device(config)# ip http server`	(Required) Enables the HTTP server on your IP or IPv6 system, including a Cisco web browser user interface. The HTTP server uses the standard port 80, by default.

Step 19	**ip http authentication local**
	Example:
	`ip http authentication local`
	`Device(config)#`
		(Required) Specifies a particular authentication method for HTTP server users.
		The **local** keyword means that the login user name, password and privilege level access combination specified in the local system configuration (by the username global configuration command) should be used for authentication and authorization.

Step 20	**ip http secure-server** **Example:** `Device(config)# ip http server`	(Required) Enables a secure HTTP (HTTPS) server. The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.
Step 21	**ip http max-connections** **Example:** `Device(config)# ip http max-connections 16`	(Required) Configures the maximum number of concurrent connections allowed for the HTTP server. Enter an integer in the range from 1 to 16. The default is 5.
Step 22	**ip tftp source-interface** *interface-type-number* **Example:** `Device(config)# ip tftp source-interface GigabitEthernet0/0`	Specifies the IP address of an interface as the source address for TFTP connections.
Step 23	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.
Step 24	**logging host** **Example:**	Logs system messages and debug output to a remote host.

	Command or Action	Purpose
	`Device(config)# logging host 172.25.33.20 vrf Mgmt-vrf`	
Step 25	**end** **Example:** `Device(config)# end`	Exits the global configuration mode and enters privileged EXEC mode.
Step 26	**show ip http server session-module** **Example:** `Device# show ip http server session-module`	(Required) Verifies HTTP connectivity. In the output, check that `SL_HTTP` is active. Additionally, you can also perform the following checks : • From device where CSLU is installed, verify that you can ping the product instance. A successful ping confirms that the product instance is reachable. • From a Web browser on the device where CSLU is installed verify `https://<product-instance-ip>/`. This ensures that the REST API from CSLU to the product instance works as expected.

Assigning a Smart Account and Virtual Account (SSM On-Prem UI)

You can use this procedure to import one or more product instances along with corresponding Smart Account and Virtual Account information, into the SSM On-Prem database. This enables SSM On-Prem to map product instances that are part of local virtual accounts (other than the default local virtual account), to the correct license pool in CSSM:

Before you begin

Supported topologies: SSM On-Prem Deployment (product instance-initiated communication).

Procedure

Step 1 Log into the SSM On-Prem and select the **Smart Licensing** workspace.

Step 2 Navigate to **Inventory** > **SL Using Policy** > **Export/Import All** > **Import Product Instances List**

The **Upload Product Instances** window is displayed.

Step 3 Click **Download** to download the .csv template file and enter the required information for all the product instances in the template.

Step 4 Once you have filled-out the template, click **Inventory** > **SL Using Policy** > **Export/Import All** > **Import Product Instances List**.

The **Upload Product Instances** window is displayed.

Step 5 Now, click **Browse** and upload the filled-out .csv template.

Smart Account and Virtual Account information for all uploaded product instances is now available in SSM On-Prem.

Validating Devices (SSM On-Prem UI)

When device validation is enabled, RUM reports from an unknown product instance (not in the SSM On-Prem database) are rejected.

By default, devices are not validated. Complete the following steps to enable it:

Before you begin

Supported topologies: SSM On-Prem Deployment (product instance-initiated communication).

Procedure

Step 1 In the **On-Prem License Workspace** window, click **Admin Workspace** and log in, if prompted.

The **On-Prem Admin Workspace** window is displayed.

Step 2 Click the **Settings** widget.

The **Settings** window is displayed.

Step 3 Navigate to the **CSLU** tab and turn-on the **Validate Device** toggle switch.

RUM reports from an unknown product instance will now be rejected. If you haven't already, you must now add the required product instances to the SSM On-Prem database before sending RUM reports. See Assigning a Smart Account and Virtual Account (SSM On-Prem UI), on page 84

Ensuring Network Reachability for Product Instance-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for product instance-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps my be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Note Ensure that you configure steps 13, 14, and 15 exactly as shown below. These commands must be configured to ensure that the correct trustpoint is used and that the necessary certificates are accepted for network reachability.

Before you begin

Supported topologies: SSM On-Prem Deployment(product instance-initiated communication).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.
Step 4	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding Mgmt-vrf`	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 5	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.0.1 255.255.0.0`	Defines the IP address for the VRF.
Step 6	**negotiation auto** **Example:** `Device(config-if)# negotiation auto`	Enables auto-negotiation operation for the speed and duplex parameters of an interface.
Step 7	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters global configuration mode.

	Command or Action	Purpose
Step 8	**ip http client source-interface** *interface-type-number* **Example:** `Device(config)# ip http client source-interface gigabitethernet0/0`	Configures a source interface for the HTTP client.
Step 9	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	(Required) Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.
Step 10	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# Device(config)# ip name-server vrf mgmt-vrf 198.51.100.1`	Configures Domain Name System (DNS) on the VRF interface.
Step 11	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Configures the source interface for the DNS domain lookup.
Step 12	**ip domain name** *domain-name* **Example:** `Device(config)# ip domain name example.com`	Configure DNS discovery of your domain. In the accompanying example, the name-server creates entry `cslu-local.example.com`.

Step 13	**crypto pki trustpoint SLA-TrustPoint**
	Example:
	`Device(config)# crypto pki trustpoint SLA-TrustPoint`
	`Device(ca-trustpoint)#`
		(Required) Declares that the product instance should use trustpoint "SLA-TrustPoint" and enters the ca-trustpoint configuration mode. The product instance does not recognize any trustpoints until you declare a trustpoint using this command.

Step 14	enrollment terminal **Example:** `Device(ca-trustpoint)# enrollment terminal`	Required) Specifies the certificate enrollment method.
Step 15	**revocation-check none** **Example:** `Device(ca-trustpoint)# revocation-check none`	(Required) Specifies a method that is to be used to ensure that the certificate of a peer is not revoked. For the SSM On-Prem Deployment topology, enter the **none** keyword. This means that a revocation check will not be performed and the certificate will always be accepted.

	Command or Action	Purpose

Step 16	**exit**
	Example:
	`Device(ca-trustpoint)# exit`
	`Device(config)# exit`
		Exits the ca-trustpoint configuration mode and then the global configuration mode and returns to privileged EXEC mode.

Step 17	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Retrieving the Transport URL (SSM On-Prem UI)

You must configure the transport URL on the product instance when you deploy the product instance-initiated communication with SSM On-Prem deployment. This task show you how to easily copy the complete URL including the tenant ID from SSM On-Prem.

Before you begin

Supported topologies: SSM On-Prem Deployment (product instance-initiated communication).

Procedure

Step 1 Log into SSM On-Prem and select the **Smart Licensing** workspace.

Step 2 Navigate to the **Inventory** tab and from the dropdown list of local virtual accounts (top right corner), select the *default local virtual account*. When you do, the area under the **Inventory** tab displays **Local Virtual Account: Default**.

Step 3 Navigate to the **General** tab.

The **Product Instance Registration Tokens** area is displayed.

Step 4 In the **Product Instance Registration Tokens** area click **CSLU Transport URL**.

The **Product Registration URL** pop-window is displayed.

Step 5 Copy the entire URL and save it in an accessible place.

You will require the URL when you configure the transport type and URL on the product instance.

Step 6 Configure the transport type and URL. See: Setting the Transport Type, URL, and Reporting Interval, on page 110.

Exporting and Importing Usage Data (SSM On-Prem UI)

You can use this procedure to complete usage synchronization between SSM On-Prem and CSSM when SSM On-Prem is disconnected from CSSM.

Before you begin

Supported topologies:

- SSM On-Prem Deployment (SSM On-Prem-initiated communication)
- SSM On-Prem Deployment (product instance-initiated communication).

Reporting data must be available in SSM On-Prem. You must have either pushed the necessary reporting data from the product instance to SSM On-Prem (product instance-initiated communication) or retrieved the necessary reporting data from the product instance (SSM On-Prem-initiated communication).

Procedure

Step 1 Log into SSM On-Prem and select **Smart Licensing**.

Step 2 Navigate to **Inventory** > **SL Using Policy** tab.

Step 3 In the **SL Using Policy** tab area, click **Export/Import All...** > **Export Usage to Cisco**.

This generates one .tar file with *all* the usage reports available in the SSM On-Prem server.

Step 4 Complete this task in CSSM: #unique_92.

At the end of this task you will have an ACK file to import into SSM On-Prem.

Step 5 Again navigate to the **Inventory** > **SL Using Policy** tab.

Step 6 In the **SL Using Policy** tab area, click **Export/Import All...** > **Import From Cisco** . Upload the .tar ACK file.

To verify ACK import, in the **SL Using Policy** tab area check the **Alerts** column of the corresponding product instance. The following message is displayed: Acknowledgement received from CSSM.

Adding One or More Product Instances (SSM On-Prem UI)

You can use this procedure to add one product instance or to import and add multiple product instances. It enables SSM On-Prem to retrieve information from the product instance.

Before you begin

Supported topologies: SSM On-Prem Deployment (SSM On-Prem-initiated communication).

Procedure

Step 1 Log into the SSM On-Prem UI and click **Smart Licensing**.

Step 2 Navigate to **Inventory** tab. Select a local virtual account from the drop-down list in the top right corner.

Step 3 Navigate to the **SL Using Policy** tab.

Step 4 Add a single product or import multiple product instances (*choose one*).

- **To add a single product instance**:
  - **a.** In the **SL Using Policy** tab area, click **Add Single Product**.
  - **b.** In the **Host** field, enter the IP address of the host (product instance).
  - **c.** From the **Connect Method** dropdown list, select an appropriate SSM On-Prem-initiated connect method.

    The available connect methods for SSM On-Prem-initiated communication are: NETCONF, RESTCONF, and REST API.
  - **d.** In the right panel, click **Product Instance Login Credentials**.

    The **Product Instance Login Credentials** window is displayed

    Note You need the login credentials only if a product instance requires a SLAC.
  - **e.** Enter the **User ID** and **Password**, and click **Save**.

    This is the same user ID and password that you configured as part of commands required to establish network reachability (Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 91).

    Once validated, the product instance is displayed in the listing in the **SL Using Policy** tab area.

- **To import multiple product instances:**
  - **a.** In **SL Using Policy** tab, click **Export/Import All...** > **Import Product Instances List**.

    The **Upload Product Instances** window is displayed.
  - **b.** Click **Download** to download the predefined .csv template.
  - **c.** Enter the required information for all the product instances in the .csv template.

    In the template, ensure that you provide **Host**, **Connect Method** and **Login Credentials** for all product instances.

    The available connect methods for SSM On-Prem-initiated communication are: NETCONF, RESTCONF, and REST API.

    Login credentials refer to the user ID and password that you configured as part of commands required to establish network reachability (Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 91).
  - **d.** Again navigate to **Inventory** > **SL Using Policy** tab. Click **Export/Import All....** > **Import Product Instances List**.

    The **Upload Product Instances** window is displayed.

e. Now upload the filled-out .csv template.

Once validated, the product instances are displayed in the listing in the **SL Using Policy** tab.

Ensuring Network Reachability for SSM On-Prem-Initiated Communication

This task provides *possible* configurations that may be required to ensure network reachability for SSM On-Prem-initiated communication. Steps marked as "(Required)" are required for all product instances, all other steps may be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Note Ensure that you configure steps 25, 26, and 27 exactly as shown below. These commands must be configured to ensure that the correct trustpoint is used and that the necessary certificates are accepted for network reachability.

Before you begin

Supported topologies: SSM On-Prem Deployment (SSM On-Prem-initiated communication).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new model** **Example:** `Device(config)# aaa new model`	(Required) Enable the authentication, authorization, and accounting (AAA) access control model.
Step 4	**aaa authentication login default local** **Example:** `Device(config)# aaa authentication login default local`	(Required) Sets AAA authentication to use the local username database for authentication.

	Command or Action	Purpose
Step 5	**aaa authorization exec default local** **Example:** `Device(config)# aaa authorization exec default local`	Sets the parameters that restrict user access to a network. The user is allowed to run an EXEC shell.
Step 6	ip routing **Example:** `Device(config)# ip routing`	Enables IP routing.
Step 7	{**ip** | **ipv6**}**name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# ip name-server vrf Mgmt-vrf 192.168.1.100 192.168.1.200 192.168.1.300`	(Optional) Specifies the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The device sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 8	**ip domain lookup source-interface** *interface-type-number* **Example:** `Device(config)# ip domain lookup source-interface gigabitethernet0/0`	Enables DNS-based hostname-to-address translation on your device. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).
Step 9	**ip domain name** *name* **Example:** `Device(config)# ip domain name vrf Mgmt-vrf cisco.com`	Defines a default domain name that the software uses to complete unqualified hostnames (names without a dotted-decimal domain name).
Step 10	**no username** *name* **Example:** `Device(config)# no username admin`	(Required) Clears the specified username, if it exists. For *name* , enter the same username you will create in the next step. This ensures that a duplicate of the username you are going to create in the next step does not exist. If you plan to use REST APIs for SSM On-Prem-initiated retrieval of RUM reports, you have to log in to SSM On-Prem. Duplicate usernames may cause the feature to work incorrectly if there are present in the system.
Step 11	**username** *name* **privilege** *level* **password** *password*	(Required) Establishes a username-based authentication system.

	Command or Action	Purpose

	Example:
	`Device(config)# username admin privilege 15`
	`password 0 lab`
		The **privilege** keyword sets the privilege level for the user. A number between 0 and 15 that specifies the privilege level for the user.
		The password allows access to the name argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.
		This enables SSM On-Prem to use the product instance native REST.
		Note Enter this username and password in SSM On-Prem (Adding One or More Product Instances (SSM On-Prem UI), on page 89). This enables SSM On-Prem to collect RUM reports from the product instance.

Step 12	**interface** *interface-type-number* **Example:** `Device (config)# interface gigabitethernet0/0`	Enters interface configuration mode and specifies the Ethernet interface, subinterface, or VLAN to be associated with the VRF.
Step 13	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)#` **`vrf forwarding Mgmt-vrf`**	Associates the VRF with the Layer 3 interface. This command activates multiprotocol VRF on an interface
Step 14	**ip address** *ip-address mask* **Example:** `Device(config-if)#` **`ip address 192.168.0.1 255.255.0.0`**	Defines the IP address for the VRF.
Step 15	**negotiation auto** **Example:** `Device(config-if)#` **`negotiation auto`**	Enables auto-negotiation operation for the speed and duplex parameters of an interface.
Step 16	**no shutdown** **Example:** `Device(config-if)#` **`no shutdown`**	Restarts a disabled interface.
Step 17	**end** **Example:** `Device(config-if)#` **`end`**	Exits the interface configuration mode and enters global configuration mode.

	Command or Action	Purpose
Step 18	**ip http server** **Example:** `Device(config)# ip http server`	(Required) Enables the HTTP server on your IP or IPv6 system, including a Cisco web browser user interface. The HTTP server uses the standard port 80, by default.

Step 19	**ip http authentication local**
	Example:
	`ip http authentication local`
	`Device(config)#`
		(Required) Specifies a particular authentication method for HTTP server users.
		The **local** keyword means that the login user name, password and privilege level access combination specified in the local system configuration (by the username global configuration command) should be used for authentication and authorization.

Step 20	**ip http secure-server** **Example:** `Device(config)# ip http server`	(Required) Enables a secure HTTP (HTTPS) server. The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.
Step 21	**ip http max-connections** **Example:** `Device(config)# ip http max-connections 16`	(Required) Configures the maximum number of concurrent connections allowed for the HTTP server. Enter an integer in the range from 1 to 16. The default is 5.

Step 22	**ip tftp source-interface** *interface-type-number*
	Example:
	`Device(config)# ip tftp source-interface`
	
	`GigabitEthernet0/0`
		Specifies the IP address of an interface as the source address for TFTP connections.

Step 23	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route vrf mgmt-vrf 192.168.0.1 255.255.0.0 192.168.255.1`	Configures a route and gateway on the product instance. You can configure either a static route or a dynamic route.

Step 24	**logging host**
	Example:
	`Device(config)# logging host`
	`172.25.33.20`
	`vrf Mgmt-vrf`
		Logs system messages and debug output to a remote host.

Step 25	**crypto pki trustpoint SLA-TrustPoint**
	Example:
	`Device(config)# crypto pki trustpoint SLA-TrustPoint`
	`Device(ca-trustpoint)#`
		(Required) Declares that the product instance should use trustpoint “SLA-TrustPoint” and enters the ca-trustpoint configuration mode. The product instance does not recognize any trustpoints until you declare a trustpoint using this command.

	Command or Action	Purpose
Step 26	enrollment terminal **Example:** `Device(ca-trustpoint)# enrollment terminal`	Required) Specifies the certificate enrollment method.
Step 27	**revocation-check none** **Example:** `Device(ca-trustpoint)# revocation-check none`	(Required) Specifies a method that is to be used to ensure that the certificate of a peer is not revoked. For the SSM On-Prem Deployment topology, enter the **none** keyword. This means that a revocation check will not be performed and the certificate will always be accepted.

Step 28	**end**
	Example:
	`Device(ca-trustpoint)# exit`
	`Device(config)# end`
		Exits the ca-trustpoint configuration mode and then the global configuration mode and returns to privileged EXEC mode.

Step 29	**show ip http server session-module** **Example:** `Device# show ip http server session-module`	(Required) Verifies HTTP connectivity. In the output, check that `SL_HTTP` is active. Additionally, you can also perform the following checks : • From device where SSM On-Prem is installed, verify that you can ping the product instance. A successful ping confirms that the product instance is reachable. • From a Web browser on the device where SSM On-Prem is installed verify `https://<product-instance-ip>/`. This ensures that the REST API from SSM On-Prem to the product instance works as expected.
Step 30	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

Setting Up a Connection to CSSM

The following steps show how to set up a Layer 3 connection to CSSM to verify network reachability. Steps marked as "(Required)" are required for all product instances, all other steps may be required or optional, depending the kind of product instance and network requirements. Configure the applicable commands:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	{**ip** | **ipv6**} **name-server** *server-address 1 ...server-address 6*] **Example:** `Device(config)# ip name-server 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230`	Specifies the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The device sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 4	**ip name-server vrf Mgmt-vrf** *server-address 1...server-address 6* **Example:** `Device(config)# ip name-server vrf Mgmt-vrf 209.165.201.1 209.165.200.225 209.165.201.14 209.165.200.230`	(Optional) Configures DNS on the VRF interface. You can specify up to six name servers. Separate each server address with a space. **Note** This command is an alternative to the **ip name-server** command.
Step 5	**ip domain lookup source-interface** *interface-type interface-number* **Example:** `Device(config)# ip domain lookup source-interface Vlan100`	Configures the source interface for the DNS domain lookup.
Step 6	**ip domain name** *domain-name* **Example:** `Device(config)# ip domain name example.com`	Configures the domain name.
Step 7	**ip host tools.cisco.com** *ip-address* **Example:** `Device(config)# ip host tools.cisco.com 209.165.201.30`	Configures static hostname-to-address mappings in the DNS hostname cache if automatic DNS mapping is not available.

Step 8	**interface** *interface-type-number*
	Example:
	`Device(config)# interface Vlan100`
	`Device(config-if)# ip address 192.0.2.10`
		Configures a Layer 3 interface. Enter an interface type and number or a VLAN.

	Command or Action	Purpose
	`255.255.255.0` `Device(config-if)# exit`	
Step 9	**ntp server** *ip-address* [**version** *number*] [**key** *key-id*] [**prefer**] **Example:** `Device(config)# ntp server 198.51.100.100 version 2 prefer`	(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.

Step 10	**switchport access vlan** *vlan_id*
	Example:
	`Device(config)# interface GigabitEthernet1/0/1`
	`Device(config-if)# switchport access vlan 100`
	`Device(config-if)# switchport mode access`
	`Device(config-if)# exit`
	`OR`
	`Device(config)#`
		Enables the VLAN for which this access port carries traffic and sets the interface as a nontrunking nontagged single-VLAN Ethernet interface.
		Note This step is to be configured only if the switchport access mode is required. The **switchport access vlan** command may apply to Catalyst switching product instances, for example, and for routing product instances you may want to configure the **ip address** *ip-address mask* command instead.

Step 11	**ip route** *ip-address ip-mask subnet mask* **Example:** `Device(config)# ip route 192.0.2.0 255.255.255.255 192.0.2.1`	Configures a route on the device. You can configure either a static route or a dynamic route.
Step 12	**ip http client source-interface** *interface-type-number* **Example:** `Device(config)# ip http client source-interface Vlan100`	(Required) Configures a source interface for the HTTP client. Enter an interface type and number or a VLAN.
Step 13	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 14	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves your entries in the configuration file.

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:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device>` **`enable`**	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device#` **`configure terminal`**	Enters global configuration mode.
Step 3	**license smart transport smart** **Example:** `Device(config)#` **`license smart transport smart`**	Enables Smart transport mode.
Step 4	**license smart url default** **Example:** `Device(config)#` **`license smart transport default`**	Automatically configures the Smart URL (https://smartreceiver.cisco.com/licservice/license). For this option to work as expected, the transport mode in the previous step must be configured as **smart**.

Step 5	**license smart proxy** {**address** *address_hostname* | **port** *port_num*}
	Example:
	`Device(config)# license smart proxy address 192.168.0.1`
	`Device(config)# license smart proxy port 3128`
		Configures a proxy for the Smart transport mode. When a proxy is configured, licensing messages are sent to the proxy along with the final destination URL (CSSM). The proxy sends the message on to CSSM. Configure the proxy address and port number separately:
		• **address** *address_hostname*: Specifies the proxy address. Enter the IP address or hostname of the proxy server.
		• **port** *port_num*: Specifies the proxy port. Enter the proxy port number.
		
		Note the change in the criteria for the acceptance of proxy servers, starting with Cisco IOS XE Bengaluru 17.6.1: only the status code of the proxy server response is verified by the system and not the reason phrase. The RFC format is `status-line = HTTP-version SP status-code SP reason-phrase CRLF`. For

	Command or Action	Purpose
		more information about the status line, see section 3.1.2 of RFC 7230.

Configuring the Call Home Service for Direct Cloud Access

The Call Home service provides email-based and web-based notification of critical system events to CSSM. To configure the transport mode, enable the Call Home service, and configure a destination profile (A destination profile contains the required delivery information for an alert notification. At least one destination profile is required.), complete the following steps:

Note All steps are required unless specifically called-out as "(Optional)".

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `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.

	Command or Action	Purpose
Step 7	**no http secure server-identity-check** **Example:** `Device(config-call-home)#` **`no http secure server-identity-check`**	Disables server identity check when HTTP connection is established.
Step 8	**contact-email-address** *email-address* **Example:** `Device(config-call-home)#` **`contact-email-addr username@example.com`**	Assigns customer's email address and enables Smart Call Home service full reporting capability and sends a full inventory message from Call-Home TAC profile to Smart Call Home server to start full registration process. You can enter up to 200 characters in email address format with no spaces.
Step 9	**profile** *name* **Example:** `Device(config-call-home)#` **`profile CiscoTAC-1`** `Device(config-call-home-profile)#`	Enters the Call Home destination profile configuration submode for the specified destination profile. By default: • The CiscoTAC-1 profile is inactive. To use this profile with the Call Home service, you must enable the profile. • The CiscoTAC-1 profile sends a full report of all types of events subscribed in the profile. The alternative is to additionally configure `Device(cfg-call-home-profile)# anonymous-reporting-only` anonymous-reporting-only. When this is set, only crash, inventory, and test messages will be sent. Use the **show call-home profile all** command to check the profile status.
Step 10	**active** **Example:** `Device(config-call-home-profile)#` **`active`**	Enables the destination profile.
Step 11	**destination transport-method http**{**email** |**http**} **Example:** `Device(config-call-home-profile)#` **`destination transport-method http`** `AND` `Device(config-call-home-profile)#` **`no destination transport-method email`**	Enables the message transport method. In the example, Call Home service is enabled via HTTP and transport via email is disabled. The **no** form of the command disables the method.

	Command or Action	Purpose
Step 12	**destination address** { **email** *email_address* |**http** *url*} **Example:** `Device(config-call-home-profile)#` **`destination address http`** **`https://tools.cisco.com/its/service/oddce/services/DDCEService`** `AND` `Device(config-call-home-profile)#` **`no destination address http`** **`https://tools.cisco.com/its/service/oddce/services/DDCEService`**	Configures the destination e-mail address or URL to which Call Home messages are sent. When entering a destination URL, include either **http://** (default) or **https://**, depending on whether the server is a secure server. In the example provided here, a **http://** destination URL is configured; and the **no** form of the command is configured for **https://**.
Step 13	**exit** **Example:** `Device(config-call-home-profile)#` **`exit`**	Exits Call Home destination profile configuration mode and returns to Call Home configuration mode.
Step 14	**exit** **Example:** `Device(config-call-home)#` **`end`**	Exits Call Home configuration mode and returns to privileged EXEC mode.
Step 15	**copy running-config startup-config** **Example:** `Device#` **`copy running-config startup-config`**	Saves your entries in the configuration file.
Step 16	**show call-home profile** {*name* |**all**}	Displays the destination profile configuration for the specified profile or all configured profiles.

Configuring the Call Home Service for Direct Cloud Access through an HTTPs Proxy Server

The Call Home service can be configured through an HTTPs proxy server. This configuration requires no user authentication to connect to CSSM.

Note Authenticated HTTPs proxy configurations are not supported.

To configure and enable the Call Home service through an HTTPs proxy, complete the following steps:

Note All steps are required unless specifically called-out as “(Optional)”.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**license smart transport callhome** **Example:** `Device(config)# license smart transport callhome`	Enables Call Home as the transport mode.
Step 4	**service call-home** **Example:** `Device(config)# service call-home`	Enables the Call Home feature.
Step 5	**call-home** **Example:** `Device(config)# call-home`	Enters Call Home configuration mode.
Step 6	**http-proxy** *proxy-address* **proxy-port** *port-number* **Example:** `Device(config-call-home)# http-proxy 198.51.100.10 port 5000`	Configures the proxy server information to the Call Home service. Note the change in the criteria for the acceptance of proxy servers, starting with Cisco IOS XE Bengaluru 17.6.1: only the status code of the proxy server response is verified by the system and not the reason phrase. The RFC format is `status-line = HTTP-version SP status-code SP reason-phrase CRLF`. For more information about the status line, see section 3.1.2 of RFC 7230.
Step 7	**exit** **Example:** `Device(config-call-home)# exit`	Exits Call Home configuration mode and enters global configuration mode.
Step 8	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.
Step 9	**copy running-config startup-config** **Example:**	Saves your entries in the configuration file.

	Command or Action	Purpose
	`Device# copy running-config startup-config`	

Removing and Returning an Authorization Code

To remove and return an SLR authorization code, complete the following steps.

Before you begin

Supported topologies: all

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**show license summary** **Example:** `Device# show license summary`	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.

Step 3	**license smart authorization return** { **all** | **local** } { **offline** [*path*] | **online** }
	Example:
	`Device# license smart authorization return all online`
	
	`Enter this return code in Cisco Smart Software Manager portal:`
	`UDI: PID:C9800-CL-K9,SN:93BBAH93MGS`
	`    Return code:`
	`CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h`
	`UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN`
	`    Return code:`
	`CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA`
	
	`OR`
	
	`Device# license smart authorization return local offline`
	`Enter this return code in Cisco Smart Software Manager`
	`portal:`
	`UDI: PID:C9800-CL-K9,SN:93BBAH93MGS`
	`    Return code:`
	`CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h`
	`UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN`
		Returns an authorization code back to the license pool in CSSM. A return code is displayed after you enter this command.
		
		Specify the product instance:
		• **all**: Performs the action for all connected product instances in a High Availability set-up.
		• **local**: Performs the action for the active product instance. This is the default option.
		
		Specify if you are connected to CSSM or not:
		• If connected to CSSM, enter **online**. The code is automatically returned to CSSM and a confirmation is returned and installed on the product instance. If you choose this option, the return code is automatically submitted to CSSM.
		• If not connected to CSSM, enter **offline**[*path*].
		If you enter only the **offline** keyword, you must copy the return code that is displayed on the CLI and enter it in CSSM.

	Command or Action	Purpose

	`Return code:`
	`CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA`
	
	`OR`
	
	`Device# license smart authorization return local offline bootflash:return-code.txt`
		If you specify a file name and path, the return code is saved in the specified location. The file format can be any readable format. For example: `Device#` **`license smart authorization return local offline bootflash:return-code.txt`**.
		
		For software versions Cisco IOS XE Cupertino 17.7.1 and later only: After you save the return request in a file, you can upload the file to CSSM in the same location and in the same way as you upload a RUM report: #unique_92.
		
		To enter the return code in CSSM, complete this task: Removing the Product Instance from CSSM, on page 105. Proceed with the next step only after you complete this step.

Step 4	**configure terminal** **Example:** `Device#` **`configure terminal`**	Enters the global configuration mode.
Step 5	**no license smart reservation** **Example:** `Device(config)#` **`no license smart reservation`**	Disables SLR configuration on the product instance. You must complete the authorization code return process in Step 3 above - whether online or offline, before you enter the no license smart reservation command in this step. Otherwise, the return may not be reflected in CSSM or in the show command, and you will have to contact your Cisco technical support representative to rectify the problem.
Step 6	**exit** **Example:** `Device(config)#` **`exit`**	Returns to privileged EXEC mode.

Step 7	**show license all**
	
	Example:
	
	`Device#` **`show license all`**
	`<output truncated>`
	`License Authorizations`
	`======================`
	`Overall status:`
	`  Active: PID:C9800-CL-K9,SN:93BBAH93MGS`
	
	`      Status: NOT INSTALLED`
		Displays licensing information. Check the `License Authorizations` header in the output. If the return process is completed correctly, the `Last return code:` field displays the return code.

	Command or Action	Purpose
	Last return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN Status: NOT INSTALLED Last return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA <output truncated>	

Removing the Product Instance from CSSM

To remove a product instance and return all licenses to the license pool, complete the following task:

Before you begin

Supported topologies: No Connectivity to CSSM and No CSLU

If you are removing a product instance that is using reserved licenses (SLR) ensure that you have generated a return code as shown in Removing and Returning an Authorization Code, on page 103. (Enter it in Step 7 in this task).

Procedure

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 From the **Virtual Account** drop-down list, choose your Virtual Account.

Step 4 Click the **Product Instances** tab.

The list of product instances that are available is displayed.

Step 5 Locate the required product instance from the product instances list. Optionally, you can enter a name or product type string in the search tab to locate the product instance.

Step 6 In the **Actions** column of the product instance you want to remove, click the **Remove** link.

- If the product instance is *not* using a license with an SLR authorization code then the **Confirm Remove Product Instance** window is displayed.
- If the product instance *is* using a license with an SLR authorization code, then the **Remove Product Instance** window, with a field for return code entry is displayed.

Step 7 In the **Reservation Return Code** field, enter the return code you generated.

Note This step applies only if the product instance is using a license with an SLR authorization code.

Step 8 Click **Remove Product Instance**.

The license is returned to the license pool and the product instance is removed.

Generating a New Token for a Trust Code from CSSM

To generate a token to request a trust code, complete the following steps.

Generate one token for each *Virtual Account* you have. You can use same token for all the product instances that are part of one Virtual Account.

Before you begin

Supported topologies: Connected Directly to CSSM

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com and click **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**.

Note If you enter a value here, ensure that you stagger the installation of the trust code on the product instances, which is the next part of the process. If you want to simultaneously install the trust code on a large number of product instances, we recommend that you leave this field blank. Entering a limit here and simultaneously installing it on a large number of devices causes a bottleneck in the processing of these requests in CSSM and installation on some devices may fail, with the following error: `Failure Reason: Server error occurred: LS_LICENGINE_FAIL_TO_CONNECT.`

Step 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:

- Connected Directly to CSSM

Procedure

	Command or Action	Purpose
Step 1	#unique_96	In case you have not completed this already, generate and download a trust code file from CSSM.
Step 2	**enable** **Example:** `Device> `**`enable`**	Enables privileged EXEC mode. Enter your password, if prompted
Step 3	**license smart trust idtoken** *id_token_value* { **local** | **all** } [**force**] **Example:** `Device# `**`license smart trust idtoken NGMwMjk5mYtNZaxMS00NzMZmtgWm all force`**	Enables you to establish a trusted connection with CSSM. For *id_token_value*, enter the token you generated in CSSM. Enter one of following options: • **local**: Submits the trust request only for the active device in a High Availability set-up. This is the default option. • **all**: Submits the trust request for all devices in a High Availability set-up. Enter the **force** keyword to submit the trust code request in spite of an existing trust code on the product instance. Trust codes are node-locked to the UDI of the product instance. If a UDI is already registered, CSSM does not allow a new registration for the same UDI. Entering the **force** keyword sets a force flag in the message sent to CSSM to create a new trust code even if one already exists.

Step 4	**show license status**
	Example:
	`<output truncated>`
	`Trust Code Installed:`
	`  Active: PID:C9800-CL-K9,SN:93BBAH93MGS`
	
	`    INSTALLED on Nov 02 08:59:26 2020 IST`
	`  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN`
	
	`    INSTALLED on Nov 02 09:00:45 2020 IST`
		Displays date and time if trust code is installed. Date and time are in the local time zone. See field `Trust Code Installed:`.

Downloading a Policy File from CSSM

If you have requested a custom policy or if you want to apply a policy that is different from the default that is applied to the product instance, complete the following task:

Before you begin

Supported topologies:

- No Connectivity to CSSM and No CSLU
- CSLU Disconnected from CSSM

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com and click **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 109

Uploading Data or Requests to CSSM and Downloading a File

You can use this task to:

- To upload a RUM report to CSSM and download an ACK.
- To upload a SLAC or SLR authorization code return request.

  This applies only to the *No Connectivity to CSSM and No CSLU* topology and is supported starting with Cisco IOS XE Cupertino 17.7.1.

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
- CSLU Disconnected from CSSM
- SSM On-Prem Deployment (Product instance-initiated communication and SSM On-Prem-initiated communication)

Procedure

Step 1 Log in to the CSSM Web UI at https://software.cisco.com.

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**.

Upload a RUM report (`.tar` format), or a SLAC return request file (`.txt` format).

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 is was Reported, which Virtual Account it was uploaded to, the Reporting Status, Number of Product Instances reported, and the Acknowledgement status.

Step 6 In the Acknowledgement column, click **Download** to save the `.txt` ACK file for the report you uploaded.

Wait for the ACK to appear in the Acknowledgement column. If there many RUM reports or requests to process, CSSM may take a few minutes.

Depending on the topology you have implemented, you can now install the file on the product instance, or transfer it to CSLU, or import it into SSM On-Prem.

Installing a File on the Product Instance

To install a SLAC, or policy, or ACK, 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 policy, see Downloading a Policy File from CSSM, on page 108
- For an ACK, see Uploading Data or Requests to CSSM and Downloading a File, on page 108

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted

	Command or Action	Purpose
Step 2	**copy** *source* **bootflash:***file-name* **Example:** `Device# copy tftp://10.8.0.6/example.txt bootflash:`	Copies the file from its source location or directory to the flash memory of the product instance. • *source*: This is the location of the source file or directory to be copied. The source can be either local or remote • **bootflash:**: This is the destination for boot flash memory.
Step 3	**license smart import bootflash:** *file-name* **Example:** `Device# license smart import bootflash:example.txt`	Imports and installs the file on the product instance. After installation, a system message displays the type of file you just installed.
Step 4	**show license all** **Example:** `Device# show license all`	Displays license authorization, policy and reporting information for the product instance.

Setting the Transport Type, URL, and Reporting Interval

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

Before you begin

Supported topologies: all

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	
Step 3	**license smart transport** { **automatic** | **callhome** | **cslu** | **off** | **smart** } **Example:** `Device(config)# license smart transport cslu`	Configures a mode of transport for the product instance to use. Choose from the following options: • **automatic**: Sets the transport mode **cslu**. • **callhome**: Enables Call Home as the transport mode.

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td></td><td></td><td>

• **cslu**: This is the default transport mode. Enter this keyword if you are using CSLU *or* SSM On-Prem, with product instance-initiated communication.

While the transport mode keyword is the same for CSLU and SSM On-Prem, the transport URLs are different. See **license smart url cslu** *cslu_or_on-prem_url* in the next step.

• **off**: Disables all communication from the product instance.

• **smart**: Enables Smart transport.

</td></tr>
<tr><td>Step 4</td><td>

license smart url { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *smart_url* }

Example:

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

</td><td>

Sets a URL for the configured transport mode. Depending on the transport mode you've chosen in the previous step, configure the corresponding URL here:

• *url*: If you have configured the transport mode as **callhome**, configure this option. Enter the CSSM URL exactly as follows:

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

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

• **cslu** *cslu_or_on-prem_url*: If you have configured the transport mode as **cslu**, configure this option with the URL for CSLU or SSM On-Prem, as applicable.

  • If you are using CSLU, enter the URL as follows:

  http://<cslu_ip_or_host>:8182/cslu/v1/pi

  For <cslu_ip_or_host>, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

  The **no license smart url cslu** *cslu_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`

  • If you are using SSM On-Prem, enter the URL as follows:

</td></tr>
</table>

	Command or Action	Purpose

		`http://<ip>/cslu/v1/pi/<tenant ID>`
		
		For <ip>, enter the hostname or the IP address of the server where you have installed SSM On-Prem. The <tenantID> must be the default local virtual account ID.
		
		Tip You can retrieve the entire URL from SSM On-Prem. See Retrieving the Transport URL (SSM On-Prem UI), on page 88
		
		The **no license smart url cslu** *cslu_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`
		
		• **default**: Depends on the configured transport mode. Only the **smart** and **cslu** transport modes are supported with this option.
		
		If the transport mode is set to **cslu**, and you configure **license smart url default**, the CSLU URL is configured automatically (`https://cslu-local:8182/cslu/v1/pi`).
		
		If the transport mode is set to **smart**, and you configure **license smart url default**, the Smart URL is configured automatically (`https://smartreceiver.cisco.com/licservice/license`).
		
		• **smart** *smart_url*: If you have configured the transport type as **smart**, configure this option. Enter the URL exactly as follows:
		
		`https://smartreceiver.cisco.com/licservice/license`
		
		When you configure this option, the system automatically creates a duplicate of the URL in **license smart url** *url*. You can ignore the duplicate entry, no further action is required.
		
		The **no license smart url smart***smart_url* command reverts to the default URL.
		
		• **utility** *smart_url*: Although available on the CLI, this option is not supported.

	Command or Action	Purpose
Step 5	**license smart usage interval** *interval_in_days* **Example:** `Device(config)# license smart usage interval 40`	(Optional) Sets the reporting interval in days. By default the RUM report is sent every 30 days. The valid value range is 1 to 3650. If you do not configure an interval, the reporting interval is determined entirely by the policy value.
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 an AIR License

In the Smart Licensing Using Policy environment, you can use this task to configure a license, or change the license being used on the product instance, or configure an add-on license on the product instance. For example, if you are currently using AIR Network Advantage and you also want to use features available with a corresponding Digital Networking Architecture (DNA) Advantage license, you can configure the same using this task. Or for example, if you do not want to use an add-on license any more, reconfigure this command to use only the AIR Network Advantage license.

Information about available licenses can be found Smart Account or Virtual Account. The available licenses may be one of the following:

- AIR Network Essential
- AIR Network Advantage
- AIR DNA Essential
- AIR DNA Advantage

Starting with Cisco IOS XE Bengaluru 17.4.1, *only for EWC-APs*, you can opt-out of purchasing an AIR DNA license. The option to opt-out of AIR DNA licenses is available only through the Cisco Commerce portal. When you opt-out, Smart Licensing Using Policy functionality is disabled.

For a new product instance, this means:

Condition	Required Action	Outcome or Result
You opt-out of AIR DNA licenses	None.	Use only AIR Network Essentials. Smart Licensing Using Policy functionality is disabled on the product instance and for your Smart Account and Virtual Account in CSSM. License usage is not recorded, and no reporting requirements apply.
You purchase AIR DNA licenses	Enter the **license air level** command in global configuration mode and configure the corresponding AIR DNA license. Reload to use the corresponding license. Implement one of the supported topologies and fulfill reporting requirements. For information about implementing a topology, see the Supported Topologies section in this document.	Use the purchased AIR DNA and AIR Network license. Smart Licensing Using Policy functionality is enabled on the product instance and for your Smart Account and Virtual Account in CSSM.

For an existing product instance, this means:

Condition	Required Action	Outcome or Result
You are using an AIR DNA license	None.	No change. You are already in the Smart Licensing Using Policy environment.
You do not want to renew the DNA license on term expiry	On term expiry, enter the **license air level** command in global configuration mode and configure AIR Network Essentials or AIR Network Advantage. Reload to use the corresponding license.	If you had AIR DNA Essentials, you now use AIR Network Essentials. If you had AIR DNA Advantage, you now use AIR Network Advantage. Smart Licensing Using Policy functionality is disabled on the product instance and for your Smart Account and Virtual Account in CSSM. License usage is not recorded, and no reporting requirements apply.

To configure or change the license in-use, follow this procedure:

Before you begin

Supported topologies: all

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables the privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters the global configuration mode.
Step 3	**license air level** {**air-network-advantage** [**addon air-dna-advantage**] | **air-network-essentials** [**addon air-dna-essentials**] } **Example:** `Device(config)# license air level air-network-essentials addon air-dna-essentials`	Activates the configured license on the product instance. In the accompanying example, the product instance activates the AIR DNA Essentials (along with the AIR Network Essential) license after reload. **Note** Prior to Cisco IOS XE Bengaluru 17.4.1, the default for EWC-APs was AIR DNA Essentials. Starting with 17.4.1, the default is AIR Network Essentials.
Step 4	**exit** **Example:** `Device(config)# exit`	Returns to the privileged EXEC mode.
Step 5	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	Saves configuration changes.
Step 6	**reload** **Example:** `Device# reload`	Reloads the device.
Step 7	**show version** **Example:** Device# show version Cisco IOS XE Software, Version 17.03.02 Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2, RELEASE SOFTWARE <output truncated> AIR License Level: **AIR DNA Essentials** Next reload AIR license Level: **AIR DNA Essentials** Smart Licensing Status: Registration Not Applicable/Not Applicable <output truncated>	Displays currently used license and the license that is effective at the next reload information.

What to do next

After you configure a license level, the change is effective after a reload. To know if reporting is required, refer to the output of the **show license status** privileged EXEC command and check the `Next ACK deadline:` and `Next report push:` fields.

Note The change in license usage is recorded on the product instance. The next steps relating to reporting - if required - depend on your current topology.

- Connected to CSSM Through CSLU
  - Product Instance-initiated communication: The product instance triggers reporting and installs the returning ACK. CSLU sends the RUM report to CSSM and collects the ACK from CSSM.
  - CSLU-initiated communication: You have to collect usage from the CSLU interface: #unique_94. CSLU sends the RUM report to CSSM and collects the ACK from CSSM.
- Connected Directly to CSSM: The product instance triggers reporting and installs the returning ACK.
- CSLU Disconnected from CSSM:
  - Product Instance-initiated communication: The product instance triggers reporting. You then have to report usage in the disconnected mode: #unique_99 > #unique_92 > #unique_93.
  - CSLU-initiated communication: You have to collect usage from the CSLU interface and report usage in the disconnected mode: #unique_94> #unique_99 > #unique_92 > #unique_93.
- No Connectivity to CSSM and No CSLU: License usage is recorded on the product instance. You must save RUM reports to a file on the product instance, and from a workstation that has connectivity to the internet, and Cisco, upload it to CSSM: Enter **license smart save usage** privileged EXEC command to save usage > #unique_92 > #unique_100.

Sample Resource Utilization Measurement Report

The following is a sample Resource Utilization Measurement (RUM) report, in XML format (See #unique_12). Several such reports may be concatenated to form one report.


```
<?xml version="1.0" encoding="UTF-8"?>
  <smartLicense>

[illegible]

  </smartLicense>
```

CHAPTER 6

Command Reference for Smart Licensing Using Policy

license air level

To configure AIR licenses on a wireless controller, enter the **license air level** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

license air level { **air-network-advantage** [**addon air-dna-advantage**] | **air-network-essentials** [**addon air-dna-essentials**] }

no license air level

Syntax Description

air-network-advantage	Configures the AIR Network Advantage license level.

addon air-dna-advantage	(Optional) Configures the add-on AIR DNA Advantage license level. This add-on option is available with the AIR Network Advantage license.
air-network-essentials	Configures the AIR Network Essentials license level.
addon air-dna-essentials	(Optional) Configures the add-on AIR DNA Essentials license level. This add-on option is available with the AIR Network Essential license.

Command Default

For all Cisco Catalyst 9800 Wireless controllers the default license is AIR DNA Advantage.

For EWC-APs:

- Prior to Cisco IOS XE Bengaluru 17.4.1, the default license is AIR DNA Essentials.
- Starting with Cisco IOS XE Bengaluru 17.4.1, the default license is AIR Network Essentials

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available and applicable with the introduction of Smart Licensing Using Policy.
Cisco IOS XE Bengaluru 17.4.1	Only for EWC-APs, the default license was changed from AIR DNA Essentials to AIR Network Essentials.

Usage Guidelines

In the Smart Licensing Using Policy environment, you can use the **license air level** command to change the license level being used on the product instance, or to additionally configure an add-on license on the product instance. The change is effective after a reload.

The licenses that can be configured are:

- AIR Network Essential
- AIR Network Advantage
- AIR DNA Essential
- AIR DNA Advantage

You can configure AIR DNA Essential or AIR DNA Advantage license level and on term expiry, you can move to the Network Advantage or Network Essentials license level, if you do not want to renew the DNA license.

Every connecting AP requires a Cisco DNA Center License to leverage the unique value properties of the controller.

Specifics for EWC-APs

Starting with Cisco IOS XE Bengaluru 17.4.1, *only for EWC-APs*, you can opt-out of purchasing an AIR DNA license. The option to opt-out of AIR DNA licenses is available only through the Cisco Commerce portal. When you opt-out, Smart Licensing Using Policy functionality is disabled.

For a new product instance, this means:

Condition	Required Action	Outcome or Result
You opt-out of AIR DNA licenses	None.	Use only AIR Network Essentials. Smart Licensing Using Policy functionality is disabled on the product instance and for your Smart Account and Virtual Account in CSSM. License usage is not recorded, and no reporting requirements apply.
You purchase AIR DNA licenses	Enter the **license air level** command in global configuration mode and configure the corresponding AIR DNA license. Reload to use the corresponding license. Implement one of the supported topologies and fulfill reporting requirements. For information about implementing a topology, For information about implementing a topology, see the Supported Topologies section in the software configuration guide of the required release.	Use the purchased AIR DNA and AIR Network license. Smart Licensing Using Policy functionality is enabled on the product instance and for your Smart Account and Virtual Account in CSSM.

For an existing product instance, this means:

Condition	Required Action	Outcome or Result
You are using an AIR DNA license	None.	No change. You are already in the Smart Licensing Using Policy environment.
You do not want to renew the DNA license on term expiry	On term expiry, enter the **license air level** command in global configuration mode and configure AIR Network Essentials or AIR Network Advantage. Reload to use the corresponding license.	If you had AIR DNA Essentials, you now use AIR Network Essentials. If you had AIR DNA Advantage, you now use AIR Network Advantage. Smart Licensing Using Policy functionality is disabled on the product instance and for your Smart Account and Virtual Account in CSSM. License usage is not recorded, and no reporting requirements apply.

Examples

The following example show how to configure the AIR DNA Essential license level:

```
Device# configure terminal
Device(config)# license air level network-essentials addon air-dna-essentials
```

The following example shows how the AIR DNA Advantage license level is configured to begin with and then changed to AIR DNA Essentials:

Current configuration as AIR DNA Advantage:

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Advantage

Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

Configuration of AIR DNA Essentials :

```
Device# configure terminal
Device(config)# license air level air-network-essentials addon air-dna-essentials

Device# exit
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Essentials
Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>

Device# write memory
Device# reload
```

After reload:

```
Device# show version
Cisco IOS XE Software, Version 17.03.02
Cisco IOS Software [Amsterdam], C9800-CL Software (C9800-CL-K9_IOSXE), Version 17.3.2,
RELEASE SOFTWARE
<output truncated>
AIR License Level: AIR DNA Essentials
Next reload AIR license Level: AIR DNA Essentials

Smart Licensing Status: Registration Not Applicable/Not Applicable
<output truncated>
```

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), or Cisco Smart Licensing Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), to configure the usage reporting interval, to configure the information that must be exluded or included in a license usage report (RUM 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_or_on-prem_url* | **default** | **smart** *smart_url* | **utility**

secondary_url } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **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_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] }

Syntax Description

custom_id *ID*	Although available on the CLI, this option is not supported.
enable	Although visible on the CLI, configuring this keyword has no effect. Smart licensing is always enabled.
privacy { **all** | **hostname** | **version** }	Sets a privacy flag to prevent the sending of the specified data privacy related information. When the flag is disabled, the corresponding information is sent in a message or offline file created by the product instance. Depending on the topology this is sent to one or more components, including CSSM, CSLU, and SSM On-Prem. *All data privacy settings are disabled by default*. You must configure the option you want to exclude from all communication:
proxy { **address** *address_hostname* | **port** *port* }	Configures a proxy for license usage synchronization with CSLU or CSSM. This means that you can use this option to configure a proxy only if the transport mode is **license smart transport smart** (CSSM), or **license smart transport cslu** (CSLU). However, you cannot configure a proxy for license usage synchronization in an SSM On-Prem deployment, which also uses **license smart transport cslu** as the transport mode. Configure the following options: • **address** *address_hostname*: Configures the proxy address. For *address_hostname*, enter the enter the IP address or hostname of the proxy. • **port***port*: Configures the proxy port. For *port*, enter the proxy port number.

reservation	Enables or disables a license reservation feature. **Note** Although available on the CLI, this option is not applicable because license *reservation* is not applicable in the Smart Licensing Using Policy environment.
server-identity-check	Enables or disables the HTTP secure server identity check.
transport { **automatic** | **callhome** | **cslu** | **off** | **smart** }	Configures the mode of transport the product instance uses to communicate with CSSM. Choose from the following options: • **automatic**: Sets the transport mode **cslu**. **Note** The **automatic** keyword is not supported on Cisco Catalyst Wireless Controllers. • **callhome**: Enables Call Home as the transport mode. • **cslu**: Enables CSLU as the transport mode. This is the default transport mode. The same keyword applies to both CSLU *and* SSM On-Prem, but the URLs are different. See **cslu***cslu_or_on-prem_url* in the following row. • **off**: Disables all communication from the product instance. • **smart**: Enables Smart transport.

url { *url* | **cslu** *cslu_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* }

Sets URL that is used for the configured transport mode. Choose from the following options:

- *url*: If you have configured the transport mode as **callhome**, configure this option. Enter the CSSM URL exactly as follows:

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

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

- **cslu** *cslu_or_on-prem_url*: If you have configured the transport mode as **cslu**, configure this option, with the URL for CSLU or SSM On-Prem, as applicable:

  - If you are using CSLU, enter the URL as follows:

    `http://<cslu_ip_or_host>:8182/cslu/v1/pi`

    For `<cslu_ip_or_host>`, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

    The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`

  - If you are using SSM On-Prem, enter the URL as follows:

    `http://<ip>/cslu/v1/pi/<tenant ID>`

    For <ip>, enter the hostname or the IP address of the server where you have installed SSM On-Prem. The <tenantID> must be the default local virtual account ID.

    Tip You can retrieve the entire URL from SSM On-Prem. In the software configuration guide (17.3.x and later), see Smart Licensing Using Policy > Task Library for Smart Licensing Using Policy > Retrieving the Transport URL (SSM On-Prem UI).

    The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`

- **default**: Depends on the configured transport mode. Only the **smart** and **cslu** transport modes are supported with this option.

  If the transport mode is set to **cslu**, and you configure **license smart url default**, the CSLU URL is configured automatically (`https://cslu-local:8182/cslu/v1/pi`).

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

- **smart** *smart_url*: If you have configured the transport type as **smart**, configure this option. Enter the URL exactly as follows:

  `https://smartreceiver.cisco.com/licservice/license`

  When you configure this option, the system automatically creates a duplicate of the URL in **license smart url** *url*. You can ignore the duplicate entry, no further action is required.

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

- **utility** *smart_url*: Although available on the CLI, this option is not supported.

usage { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* }	Configures 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 in 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 specifies - this applies to topologies where CSLU or CSSM may be on the receiving end. If you set a value that is greater than zero and the transport type is set to **off**, then, between the *interval_in_days* and the policy value for `Ongoing reporting frequency(days):`, the lower of the two values is applied. For example, if *interval_in_days* is set to 100, and the value in the in the policy says `Ongoing reporting frequency (days):90`, RUM reports are sent every 90 days. If you do not set an interval, and the default is effective, the reporting interval is determined entirely by the policy value. For example, if the default value is effective and only unenforced licenses are in use, if the policy states that reporting is not required, then RUM reports are not sent.
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

Cisco IOS XE Amsterdam 17.3.1 or earlier: Smart Licensing is enabled by default.

Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy is enabled by default.

Command Modes

Global config (config)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	The following keywords and variables were introduced with Smart Licensing Using Policy: • Under the **url**keyword, these options were introduced: { **cslu** *cslu_url* | **smart** *smart_url* } • Under the **transport** keyword, these options were introduced: { **cslu** | **off** } Further, the default transport type was changed from **callhome**, to **cslu**. • **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } The following keywords and variables under the **license smart** command are deprecated and no longer available on the CLI: **enable**and **conversion automatic**.
Cisco IOS XE Amsterdam 17.3.3	SSM On-Prem support was introduced. For product instance-initiated communication in an SSM On-Prem deployment, the existing [**no**]**license smart url cslu***cslu_or_on-prem_url* command supports the configuration of a URL for SSM On-Prem as well. But the required URL format for SSM On-Prem is: `http://<ip>/cslu/v1/pi/<tenant ID>`. The corresponding transport mode that must be configured is also an existing command (**license smart transport cslu**).
Cisco IOS XE Cupertino 17.7.1	If version privacy is disabled (**no license smart privacy version** global configuration command), the Cisco IOS-XE software version running on the product instance and the Smart Agent version is *included* in the RUM report. To exclude version information from the RUM report, version privacy must be enabled (**license smart privacy version**).

Usage Guidelines

Communication failures and reporting

The reporting interval that you configure (**license smart usage interval** *interval_in_days* command), determines the date and time at which the product instance sends out the RUM report. If the scheduled interval coincides with a communication failure, the product instance attempts to send out the RUM report for up to four hours after the scheduled time has expired. If it is still unable to send out the report (because the communication failure persists), the system resets the interval to 15 minutes. Once the communication failure is resolved, the system reverts the reporting interval to the value that you last configured.

The system message you may see in case of a communicatin failure is %SMART_LIC-3-COMM_FAILED. For information about resolving this error and restoring the reporting interval value, in the software configuration guide of the required release (17.3.x onwards), see *System Configuration* > *Smart Licensing Using Policy* > *Troubleshooting Smart Licensing Using Policy*.

Proxy server acceptance

When configuring the **license smart proxy** {**address** *address_hostname* | **port***port*} command, note the change in the criteria for the acceptance of proxy servers, starting with Cisco IOS XE Bengaluru 17.6.1: only the status code of the proxy server response is verified by the system and not the reason phrase. The RFC format is `status-line = HTTP-version SP status-code SP reason-phrase CRLF`, where the status code is a three-digit numeric code. For more information about the status line, see section 3.1.2 of RFC 7230.

Examples

- Examples for Data Privacy, on page 128
- Examples for Transport Type and URL, on page 129
- Examples for Usage Reporting Options, on page 129

Examples for Data Privacy

The following examples show how to configure data privacy related information using **license smart privacy** command in global configuration mode. The accompanying **show license status** output displays configured information.

> **Note** The output of the **show** command only tells you if a particular option is enabled or disabled.

Here, no data privacy related information information is sent:

```
Device# configure terminal
Device(config)# license smart privacy all
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: ENABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

Here, the software version running on the product instance is Cisco IOS XE Cupertino 17.9.1. Version privacy is disabled, and the Cisco IOS-XE software version running on the product instance and the Smart Agent version is included in the RUM report:

```
Device# configure terminal
Device(config)# license smart privacy hostname
Device(config)# no license smart privacy version
Device(config)# exit

Device# show license all
<output truncated>

Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
```

```
  Proxy:
    Not Configured
  VRF:
    Not Configured

<output truncated>
```

Examples for Transport Type and URL

The following examples show how to configure some of the transport types using the **license smart transport** and the **license smart url** commands in global configuration mode. The accompanying **show license all** output displays configured information.

Transport **cslu**:

```
Device# configure terminal
Device(config)# license smart transport cslu
Device(config)# license smart url default
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  Proxy:
    Not Configured
<output truncated>
```

Transport **smart**:

```
Device# configure terminal
Device(config)# license smart transport smart
Device(config)# license smart url smart https://smartreceiver.cisco.com/licservice/license
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured
<output truncated>
```

Examples for Usage Reporting Options

The following examples show how to configure some of the usage reporting settings using the **license smart usage** command in global configuration mode. The accompanying **show running-config** output displays configured information.

Configuring the **customer-tag** option:

```
Device# configure terminal
Device(config)# license smart usage customer-tags tag1 SA/VA:01
Device(config)# exit
Device# show running-config | include tag1
license smart usage customer-tags tag1 SA/VA:01
```

Configuring a narrower reporting interval than the currently applied policy:

```
Device# show license status
<output truncated>
```

```
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Dec 21 12:02:21 2020 PST
Reporting push interval: 30 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 22 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>

Device# configure terminal
Device(config)# license smart usage interval 20
Device(config)# exit
Device# show license status
<output truncated>

Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Nov 22 12:02:21 2020 PST
Reporting push interval: 20 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 12 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>
```

license smart (privileged EXEC)

To configure licensing functions such as requesting or returning authorization codes, saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, establishing trust with Cisco Smart Software Manager (CSSM), synchronizing the product instance with CSSM, or Cisco Smart License Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), and removing licensing information from the product instance, enter the **license smart** command in privileged EXEC mode with the corresponding keyword or argument.

license smart { **authorization** { **request** { **add** | **replace** | **save** *filepath_filename* } *feature_name* { **all** | **local** } | **return** { **all** | **local** } { **offline** [*filepath_filename*] | **online** } } | **clear eventlog** | **export return** { **all** | **local** } *feature_name* | **factory reset** | **import** *filepath_filename* | **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *filepath_filename* } } | **sync** { **all** | **local** } | **trust idtoken** *id_token_value* { **local** | **all** } [**force**] }

Syntax Description

smart	Provides options for Smart Licensing.
authorization	Provides the option to request for, or return, authorization codes. Authorization codes are required *only* if you use licenses with enforcement type: export-controlled or enfored.
request	Requests an authorization code from CSSM, CSLU (CSLU in-turn fetches it from CSSM), or SSM On-Prem and installs it on the product instance.
add	Adds the requested license to the existing authorization code. The new authorization code will contain all the licenses of the existing authorization code and the requested license.

replace	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.
save*filepath_filename*	Saves the authorization code request to a file. For *filepath_filename*, specify the absolute path to the file, including the filename.
feature_name	Name of the license for which you are requesting an authorization code.
all	Performs the action for all product instances in a High Availability configuration.
local	Performs the action for the *active* product instance. This is the default option.
return	Returns an authorization code back to the license pool in CSSM.
offline *filepath_filename*	Means the product instance is not connected to CSSM. The authorization code is returned offline. This option requires you to print the return code to a file. Optionally, you can also specify a path to save the file. The file format can be any readable format, such as `.txt` If you choose the offline option, you must complete the additional step of copying the return code from the CLI or the saved file and entering it in CSSM.
online	Means that the product instance is in a connected mode. The authorization code is returned to CSLU or CSSM directly.
clear eventlog	Clears all event log files from the product instance.
export return	Returns the authorization key for an export-controlled license.
factory reset	Clears all saved licensing information from the product instance.
import *filepath_filename*	Imports a file on to the product instance. The file may be that of an authorization code, a trust code, or, or a policy. For *filepath_filename*, specify the location, including the filename.
save	Provides options to save RUM reports or trust code requests.
trust-request *filepath_filename*	Saves the trust code request for the active product instance in the specified location. For *filepath_filename*, specify the absolute path to the file, including the filename.

usage { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *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** *days*: Saves RUM report for the last *n* number of days (excluding the current day). Enter a number. The valid range is 0 to 4294967295. For example, if you enter 3, RUM reports of the last three days are saved. • **rum-Id** *rum-ID*: Saves a specified RUM ID. The valid value range is 0 to 18446744073709551615. • **unreported**: Saves all unreported RUM reports. **file** *filepath_filename*: Saves the specified usage information to a file. Specify the absolute path to the file, including the filename.
sync { **all** | **local** }	Synchronizes with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. This includes uploading pending RUM reports, downloading the ACK response, any pending authorization codes, trust codes, and policies for the product instance. Specify the product instance by entering one of these options: • **all**: Performs synchronization for all the product instances in a High Availability set-up. If you choose this option, the product instance also sends the list of all the UDIs in the synchronization request. • **local**: Performs synchronization only for the active product instance sending the request, that is, its own UDI. This is the default option.
trust idtoken *id_token_value*	Establishes a trusted connection with CSSM. To use this option, you must first generate a token in the CSSM portal. Provide the generated token value for *id_token_value*.
force	Submits a trust code request even if a trust code already exists on the product instance. A trust code is node-locked to the UDI of a product instance. If the UDI is already registered, CSSM does not allow a new registration for the same UDI. Entering the **force** keyword overrides this behavior.

Command Default

Cisco IOS XE Amsterdam 17.3.1 or earlier: Smart Licensing is enabled by default.

Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy is enabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

<table>
<tr><th>Release</th><th>Modification</th></tr>
<tr><td>Cisco IOS XE Amsterdam 17.3.2a</td><td>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 }
reservation { cancel [all | local] | install [file] key | request { all | local | universal } | return [all | authorization { auth_code | file filename } | Local] key }
mfg reservation { request | install | install file | cancel }
conversion { start | stop }
</td></tr>
<tr><td>Cisco IOS XE Amsterdam 17.3.3</td><td>Support for SSM On-Prem was introduced. You can perform licensing-related tasks such as saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, synchronizing the product instance, returning authorization codes, and removing licensing information from the product instance in an SSM On-Prem deployment.</td></tr>
<tr><td>Cisco IOS XE Cupertino 17.7.1</td><td>The following enhancements were introduced in this release:

The save filepath_filename keyword and variable was added to the license smart authorization request string.
Although visible on the CLI, the new keywords are not applicable, because there are no export-controlled or enforced licenses on any of the Cisco Catalyst Wireless Controllers.
The existing license smart save usage command was enhanced to include a trust code request in applicable topologies.
</td></tr>
</table>

Usage Guidelines

Overwriting a Trust Code

Use case for the **force** option when configuring the **license smart trust idtoken** command: You use same token for all the product instances that are part of one Virtual Account. If the product instance has moved from one account to another (for instance, because it was added to a High Availability set-up, which is part of another Virtual Account), then there may be an existing trust code you have to overwrite.

Removing Licensing Information

Entering the **licence smart factory reset** command removes all licensing information (except the licenses in-use) from the product instance, including any authorization codes, RUM reports etc. Therefore, we recommend the use of this command only if the product instance is being returned (Return Material Authrization, or RMA), or being decommissioned permanently. We also recommend that you send a RUM report to CSSM, before you remove licensing information from the product instance - this is to ensure that CSSM has up-to-date usage information.

Authorization Codes and License Reservations:

Options relating to authorization codes and license reservations:

- Since there are no export-controlled or enforced licenses on any of the Cisco Catalyst Wireless Controllers, and the notion of reserved licenses is not applicable in the Smart Licensing Using Policy environment, the following commands are not applicable:
  - { { **license smart authorization request** { **add** | **replace** | **save** *path* } *feature_name* { **all** | **local** } *request_count* } }
  - **license smart export return**
- The following option is applicable and required for any SLR authorization codes you may want to return:

  license smart authorization return { **all** | **local** } { **offline** [*path*] | **online** }

Examples

- Example for Saving Licensing Usage Information, on page 134
- Example for Installing a Trust Code, on page 135
- Example for Returning an SLR Authorization Code, on page 135

Example for Saving Licensing Usage Information

The following example shows how you can save license usage information on the product instance. You can use this option to fulfil reporting requirements in an air-gapped network. In the example, the file is first save to flash memory and then copied to a TFTP location:

```
 Device> enable
Device# license smart save usage unreported file flash:RUM-unrep.txt
Device# dir
Directory of bootflash:/

33      -rw-             5994   Nov 2 2020 03:58:04 +05:00  RUM-unrep.txt

Device# copy flash:RUM-unrep.txt tftp://192.168.0.1//auto/tftp-user/user01/
Address or name of remote host [192.168.0.1]?
Destination filename [//auto/tftp-user/user01/RUM-unrep.txt]?
!!
15128 bytes copied in 0.161 secs (93963 bytes/sec)
```

After you save RUM reports to a file, you must upload it to CSSM (from a workstation that has connectivity to the internet, and Cisco).

Example for Installing a Trust Code

The following example shows how to install a trust code even if one is already installed on the product instance. This requires connectivity to CSSM. The accompanying **show license status** output shows sample output after successful installation:

Before you can install a trust code, you must generate a token and download the corresponding file from CSSM.

Use the **show license status** command (`Trust Code Installed:`) to verify results.

```
Device> enable
Device# license smart trust idtoken
NGMwMjk5mYtNZaxMS00NzMZmtgWm local force

Device# show license status
<output truncated>
Trust Code Installed:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
    INSTALLED on Nov 02 05:19:05 2020 IST
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
    INSTALLED on Nov 02 05:19:05 2020 IST
<output truncated>
```

Example for Returning an SLR Authorization Code

The following example shows how to remove and return an SLR authorization code. Here the code is returned offline (no connectivity to CSSM). The accompanying **show license all** output shows sample output after successful return:

```
Device> enable
Device# show license all
<output truncated>
License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Last Confirmation code: ad4382fe
<output truncated>

Device# license smart authorization return local offlline
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS
    Return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h
UDI: PID:C9800-CL-K9,SN:9XECPSUU4XN
    Return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA

Device# show license all
<output truncated>
License Authorizations
======================
Overall status:
```

```
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: NOT INSTALLED
      Last return code: CqaUPW-WSPYiq-ZNU2ci-SnWydS-hBCXHP-MuyPqy-PJ1GiG-tPTGQj-S2h
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: NOT INSTALLED
      Last return code: CNLwxR-eWiAEJ-XaTEQg-j4rrYW-dSRz9j-37VpcP-imjuLD-mNeA4k-TXA
<output truncated>
```

If you choose the **offline** option, you must complete the additional step of copying the return code from the CLI or the saved file and entering it in CSSM.

license wireless high-performance

To upgrade the scale and capacity of a Cisco Catalyst C9800-L-K9 Wireless Controller, use the **license wireless high-performance** command. To unconfigure the high-performance license, use the **no** form of this command.

license wireless high-performance

no license wireless high-performance

Syntax Description

This command has no keywords or arguments

Command Default

High-performance license is not configured

Command Modes

Global(config)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.1.1s	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2	This command continues to be available and applicable with the introduction of Smart Licensing Using Policy in this release.

Usage Guidelines

This command is synchronized with the standby controller. However, the standby controller should also have a performance license to get the upgraded capacity.

The license can be released back to the license pool by unconfiguring the high-performance license. This releases the license to the license pool so that another controller can make use of it, if needed.

In the case of RMA, the customer should call Cisco Technical Assistance Center (TAC) to remove the product instances from the customer's virtual account so that all the licenses used by the controller are returned to the license pool and can be used on the new hardware.

Reboot the device before configuring the **license wireless high-performance**command.

Example

To upgrade the scale and capacity of a controller, use the following command:

```
Device# configure terminal
Device(config#) license wireless high-performance
```

show license air entities

To display information about active APs, new APs, and deleted APs in connection with a Cisco Catalyst Wireless Controller, enter the **show license air entities** command in privileged EXEC mode.

show license air entities { **added** | **bulk** | **deleted** | **no-change** | **summary** }

Syntax Description

`added`	Displays the list of newly reported APs. A newly added AP is one that was not listed in the last RUM report that the product instance generated.
bulk	Displays the list of all currently active APs for the product instance
deleted	Displays the list of deleted APs. A delete AP is one that was listed as active APs in the last RUM report that the product instance generated but is now disconnected.
no-change	Displays the list of APs where there has been no change in the status since the last report.
summary	Displays the RUM report generation particulars and information about active APs, new APs, and deleted APs, and indicates by when an acknowledgement (ACK) must be installed on the product instance.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to display information relating to Smart Licensing Using Policy.
Cisco IOS XE Cupertino 17.7.1	The output of the **show license air entities summary** command was enhanced to display the following new field only on a Cisco Catalyst 9800-CL Wireless Controller: `License Ack expected within`

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Smart Licensing Using Policy: If the software version on the device is Cisco IOS XE Amsterdam 17.3.2 or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Examples

For information about fields shown in the display for the **show license air entities summary** command, see Table 9: show license air entities summary Field Descriptions, on page 138 .

For sample output, see

- show license air entities summary on a Cisco Catalyst 9800-CL Wireless Controller, on page 138
- show license air entities summary on a Cisco Catalyst 9800-L Wireless Controller, on page 139

Table 9: show license air entities summary Field Descriptions

Field	Description
Last license report time	When the last RUM report was generated, in the local time zone.
Upcoming license report time	When the next RUM report will be generated, in the local time zone.
No. of APs active at last report	Total number of APs listed as active APs in the last RUM report that was generated.
No. of APs newly added with last report	Number of new APs in the last RUM report that was generated. For example, if the number displayed here is 2, this means the *last but one* RUM report did not list these 2 APs, and are therefore newly added in the last RUM report that the product instance generated.
No. of APs deleted with last report	Total number of APs deleted as of the last RUM report that was generated. For example, if the number displayed here is 2, this means 2 APs were in the *last but one* RUM report, but were deleted in the *last* RUM report was generated.
License Ack expected within	**Note** This field is displayed only on a Cisco Catalyst 9800-CL Wireless Controller running Cisco IOS XE Cupertino 17.7.1 or a later release. If the field is displayed, it means you must complete RUM reporting and ensure that the ACK is made available on the product instance - at least once.

show license air entities summary on a Cisco Catalyst 9800-CL Wireless Controller

This example shows how to identify when an ACK is required on a Cisco Catalyst 9800-CL Wireless Controller

Beginning with Cisco IOS XE Cupertino 17.7.1, if you are using a Cisco Catalyst 9800-CL Wireless Controller, you must complete RUM reporting and ensure that the ACK is made available on the product instance - at least once. This is to ensure that correct and up-to-date usage information is reflected in CSSM.

Prior to 17.7.1, reporting and ACK installation was not *mandatory* for a Cisco Catalyst 9800-CL Wireless Controller.

The following is sample output on a Cisco Catalyst 9800-CL Wireless Controller, where an ACK must be made available on the product instance within 179 days. If this deadline is not met, currently active APs are not disconnected, but no new AP joins are allowed after the ACK deadline is passed. System messages are also displayed daily, until the first ACK is installed.

```
Device# show license air entities summary
Upcoming license report time....................: 21:05:16.092 UTC Mon Oct 25 2021
No. of APs active at last report................: 57
No. of APs newly added with last report.........: 57
No. of APs deleted with last report.............: 0
License Ack expected within.....................: 179 days
```

Detailed information about this requirement is available in the configuration guide. In the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, version Cisco IOS XE Cupertino 17.7.1 onwards, see the *System Configuration* → *Smart Licensing Using Policy* → *RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller*.

show license air entities summary on a Cisco Catalyst 9800-L Wireless Controller

The following is sample output on a Cisco Catalyst 9800-L Wireless Controller. Note how the output on this device does not display the `License Ack expected within` field. Reporting requirements on all Cisco Catalyst Wireless Controllers (except Cisco Catalyst 9800-CL Wireless Controller) are as per the standard guidelines in the Smart Licensing Using Policy environment: Reporting is required if the policy (**show license status**) or system messages indicate that it is.

```
Device# show license air entities summary
Upcoming license report time....................: 15:13:27.403 IST Tue Oct 26 2021
No. of APs active at last report................: 1
No. of APs newly added with last report.........: 1
No. of APs deleted with last report.............: 0
```

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

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to display information relating to Smart Licensing Using Policy. Command output no longer displays Smart Account and Virtual account information.
Cisco IOS XE Cupertino 17.7.1	The output of the command was enhanced to display the following information: • RUM report statistics, in section `Usage Report Summary`. • Smart Account and Virtual Account information, in section `Account Information`.

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2 or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

This command concatenates the output of other **show license** commands, enabling you to display different kinds of licensing information together. For field descriptions, refer to the corresponding commands in the links provided below.

The `Smart Licensing Status` and `Account Information` sections of the **show license all** command corresponds with the output of the show license status, on page 157 command.

The `License Usage` section of the **show license all** command corresponds with the output of the show license usage, on page 170 command.

The `Product Information` section of the **show license all** command corresponds with the output of the show license udi, on page 169 command.

The `Agent Version` section of the **show license all** command displays the Smart Agent version and is available only in this command.

The `License Authorizations` section of the **show license all** command corresponds with the output of the show license authorization, on page 145 command.

The `Usage Report Summary` section of the **show license all** command corresponds with the output in the show license tech, on page 174 command.

Examples

For sample output, see:

Example: show license all (Cisco Catalyst 9800-CL Wireless Controllers, 17.7.1), on page 140

Example: show license all (Cisco Catalyst 9800-CL Wireless Controllers), on page 142

Example: show license all (Cisco Catalyst 9800-CL Wireless Controllers, 17.7.1)

The following is sample output of the **show license all** command, on a product instance where the software version is Cisco IOS XE Cupertino 17.7.1. Note the addition of the two new sections in this release: `Account Information` and `Usage Report Summary`:

```
Device# show license all

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

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA
```

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

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

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

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

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

No licenses in use

Product Information
===================
UDI: PID:C9800-CL-K9,SN:9KGIXIDOXFE

HA UDI List:
    Active:PID:C9800-CL-K9,SN:9KGIXIDOXFE
    Standby:PID:C9800-CL-K9,SN:9UBKZU955E4

Agent Version
=============
```

```
Smart Agent for Licensing: 5.3.14_rel/47

License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:9KGIXIDOXFE
      Status: NOT INSTALLED
  Standby: PID:C9800-CL-K9,SN:9UBKZU955E4
      Status: NOT INSTALLED

Purchased Licenses:
  No Purchase Information Available

Usage Report Summary:
=====================
Total: 0,  Purged: 0
Total Acknowledged Received: 0,  Waiting for Ack: 0
Available to Report: 0  Collecting Data: 0
```

Example: show license all (Cisco Catalyst 9800-CL Wireless Controllers)

The following is sample output of the **show license all** command on a Cisco Catalyst 9800-CL Wireless Controller. Similar output is displayed on all supported Cisco Catalyst Wireless Controllers.

```
Device# show license all

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

Smart Licensing is ENABLED
License Reservation is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

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

Transport:
  Type: Transport Off

Miscellaneous:
  Custom Id: <empty>

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

```
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: Nov 01 20:31:46 2020 IST
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

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

air-network-advantage (DNA_NWStack):
  Description: air-network-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

air-dna-advantage (AIR-DNA-A):
  Description: air-dna-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

Product Information
===================
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS

HA UDI List:
    Active:PID:C9800-CL-K9,SN:93BBAH93MGS
    Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN

Agent Version
=============
```

```
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
======================
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Last Confirmation code: ad4382fe

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled with DNA-A
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10

Purchased Licenses:
  No Purchase Information Available
```

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

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

Usage Guidelines

Only export-controlled or enforced licenses require authorization before use.

While there are no export-controlled or enforced licenses on Cisco Catalyst Wireless Controllers, you can use this command to display migrated SLR authorization codes.

Examples

See Table 10: show license authorization Field Descriptions, on page 146 for information about fields shown in the display.

See show license authorization Displaying Migrated Authorization Code, on page 148 for sample output.

Table 10: show license authorization Field Descriptions

Field		Description
Overall Status	Header for UDI information for all product instances in the set-up, the type of authorization that is installed, and configuration errors, if any. In a High Availability set-up, all UDIs in the set-up are listed.	
	Active: Status:	The active product instance UDI, followed by the status of the authorization code installation for this UDI. If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.
	Standby: Status:	The standby product instance UDI, followed by the status of the authorization code installation for this UDI. If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.
	Member: Status:	The member product instance UDI, followed by the status of the authorization code installation for this UDI. If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.
	ERROR:	Configuration errors or discrepancies in the High Availability set-up, if any.

Field		Description
Authorizations	Header for detailed license authorization information. All licenses, their enforcement types, and validity durations are displayed. Errors are displayed for each product instance if its authorization or mode does not match what is installed on the active. This section is displayed only if the product instance is using a license with an authorization code.	
	():	License name and a shortened form of the license name.
	Description	License description.
	Total available count:	Total count of licenses that are available to consume. This includes licenses of all durations (perpetual and subscription), including expired subscription licenses, for all the product instances in a High Availability setup.
	Enforcement type	Enforcement type for the license. This may be one of the following: • Enforced • Not enforced • Export-Controlled
	Term information:	

Field		Description
		Header providing license duration information. The following fields maybe included under this header: • Active: The active product instance UDI, followed by the status of the authorization code installation for this UDI. • Authorization type: Type of authorization code installed and date of installation. The type can be: SLAC, UNIVERSAL, SPECIFIED, PAK, RTU. • Start Date: Displays validity start date if the license is for a specific term or time period. • Start Date: Displays validity end date if the license is for a specific term or time period. • Term Count: License count. • Subscription ID: Displays ID if the license is for a specific term or time period. • License type: License duration. This can be: SUBSCRIPTION or PERPETUAL. • Standby: The standby product instance UDI, followed by the status of the authorization code installation for this UDI. • Member: The member product instance UDI, followed by the status of the authorization code installation for this UDI. For more information about the duration or term of a license's validity, see <link tbd>.
Purchased Licenses	Header for license purchase information.	
	Active:	The active product instance and its the UDI.
	Count:	License count.
	Description:	License description.
	License type:	License duration. This can be: SUBSCRIPTION or PERPETUAL.
	Standby:	The standby product instance UDI.
	Member:	The member product instance UDI.

show license authorization Displaying Migrated Authorization Code

The following is sample output of the **show license authorization** command on a Cisco Catalyst 9800-CL Wireless Controller. The `Last Confirmation code:` shows that SLR authorization code is available after migration. Similar output is displayed on all supported Cisco Catalyst Wireless Controllers.

```
Device# show license authorization
Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Last Confirmation code: 102fc949
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Last Confirmation code: ad4382fe

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled with DNA-A
    Total reserved count: 20
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        Authorization type: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10

Purchased Licenses:
  No Purchase Information Available
```

show license data conversion

To display license data conversion information, enter the **show license data** command in privileged EXEC mode.

show license data conversion

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available with the introduction of Smart Licensing Using Policy.

Usage Guidelines

Although visible on the CLI, this command is not applicable to Cisco Catalyst Wireless Controllers.

show license eventlog

To display event logs relating to Smart Licensing Using Policy, enter the **show license eventlog** command in privileged EXEC mode.

show license eventlog [*days*]

Syntax Description

days	Enter the number of days for which you want to display event logs. The valid value range is from 0 to 2147483647.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Additional events were added with the introduction of Smart Licensing Using Policy: • Installation and removal of a policy • Request, installation and removal of an authorization code. • Installation and removal of a trust code. • Addition of authorization source information for license usage.

Usage Guidelines

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

show license history message

To display communication history between the product instance and CSSM or CSLU (as the case may be), enter the **show license history message** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting.

show license history message

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

Usage Guidelines

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra** privileged EXEC commands.

show license reservation

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

show license reservation

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available with the introduction of Smart Licensing Using Policy.

Usage Guidelines

The command continues to be available on the CLI and corresponding output is displayed, but with the introduction of Smart Licensing Using Policy, the notion of reservation is not longer applicable. Use the **show license all** command in privileged EXEC mode, to display *migrated* SLR licenses instead (the SLR authorization code is migrated to Smart Licensing Using Policy).

show license rum

To display information about Resource Utilization Measurement reports (RUM report) available on the product instance, including report IDs, the current processing state of a report, error information (if any), and to save the detailed or summarized view that is displayed, enter the **show license rum** command in privileged EXEC mode.

show license rum { **feature** { *license_name* | **all** } | **id** { *rum_id* | **all** } } [**detail**] [**save** *path*]

Syntax Description

feature { *license_name* | **all** }	Displays RUM report information based on the license name. Specify a particular license name to display all RUM reports for that license, or use the **all** keyword to display all RUM reports available on the product instance.
id { *rum_id* | **all** }	Displays RUM report information based on the RUM report ID. Specify a report ID to display information for a single report, or use the **all** keyword to display all RUM reports available on the product instance.
detail	Displays detailed RUM report information. You can use this to display detailed information by license name and detailed information by RUM report ID.
save *path*	Saves the information that is displayed. This can be the simplified or detailed version and depends on the preceeding keywords you have entered. Information about 200 RUM reports can be displayed. If there are more 200 RUM reports on the product instance, you can view information about all the RUM reports by saving it to a text (.txt) file. **Note** This option saves the information *about* RUM reports and is not for reporting purposes. It does not save the RUM report, which is an XML file containing usage information.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.7.1	This command was introduced.

Usage Guidelines

A RUM report is a license usage report, which the product instance generates, to fulfil reporting requirements as specified by the policy. An acknowledgement (ACK) is a response from CSSM and provides information about the status of a RUM report. Once the ACK for a report is available on the product instance, it indicates that the corresponding RUM report is no longer required and can be deleted. You can use the **show license rum** command to:

- Display information about the available RUM reports on the product instance - filtered by ID or license name.
- Display a short summary of the information or display a detailed view of the information.
- Track a RUM report throughout its lifecycle (from the time it is first generated until its acknowledgement from CSSM). By displaying the current processing state and condition of a report you can ascertain if and when there is a problem in the reporting workflow.
- Save the displayed information. The CLI displays information about up to 200 reports. If there are more than 200 reports on the product instance and you want to view information about all of them, save the displayed info in a .txt file and export to the desired location to view.

To display a statistical view of RUM report information (the total number of reports on the product instance, the number of reports that have a corresponding ACK, the number of reports waiting for an ACK etc.) refer to the `Usage Report Summary:` section of the **show license all** and **show license tech** privileged EXEC commands.

The **show license tech** command also provides RUM report related information that the Cisco technical support team can use to troubleshoot, if there are problems with RUM reporting.

Examples

For information about fields shown in the display, see #unique_119 unique_119_Connect_42_table_ytd_q4m_hrb and #unique_119 unique_119_Connect_42_table_gtn_q4m_hrb

For sample output of the **show license rum** command, see:

- #unique_119 unique_119_Connect_42_example_ugm_lsd_4rb
- #unique_119 unique_119_Connect_42_example_stg_msd_4rb

Table 11: show license rum (simplified view) Field Descriptions

Field Name	Description
Report Id	A numeric field that identifies a RUM report. The product instance automatically assigns an ID to every RUM report it generates. An ID may be up to 20 characters long.

Field Name	Description
State	This field displays the current processing state of a RUM report, and can be only one of the following: • OPEN: This means new measurements are been added into this report. • CLOSED: This means no new measurements can be added to this report, and the report is ready for communication to CSSM. • PENDING: This is a transitional status that you may see if you display a report while it is being transmitted. • UNACK: This means the report was transmitted and is waiting for confirmation from CSSM, that it is processed. • ACK: This means the report was processed or acknowledged by CSSM and is eligible for deletion.

Flag	Indicates the condition of the RUM report, and is displayed in the form of a character. Each character represents a specific condition, and can be only one of the following values:
	• N: Normal; This means no errors have been detected and the report is going through normal operation.
	• P: Purged; This means the report was removed due to system resource limitation, and can refer to a shortage of disk space or insufficient memory. If this flag is displayed, refer to the `State Change Reason` field in the detailed view for more information.
	• E: Error; This means an error was detected in the RUM report. If this flag is displayed, refer to the detailed view for more information. Possible workflow issues include and are not limited to the following:
	  • RUM report was dropped by CSSM. If this is the issue, the `State` field displays value `ACK`, but the `State Change Reason` does not change to `ACKED`.
	  • RUM Report data is missing. If this is the issue, the `Storage State` field displays value `MISSING` .
	  • Tracking information is missing. If this is the case the `State` field displays value `UNACK` and the `Transaction ID` field has no information.
	Note Occasional errors in RUM reports do not require any action from you and are not an indication of a problem. It is only if you see a large number of reports (greater than 10) with errors that you must contact the Cisco technical support team.

Feature Name	The name of the license that the RUM report applies to.

Table 12: show license rum (detailed view) Field Descriptions

Field Name	Description
Report Id	A numeric field that identifies a RUM report. The product instance automatically assigns an ID to every RUM report it generates. An ID may be up to 20 characters long.
Metric Name:	Shows the type of data that is recorded. For a RUM report, the only possible value is ENTITLEMENT, and refers to measurement of license usage.
Feature Name:	The name of the license that the RUM report applies to.
Metric Value	A unique identifier for the data that is recorded. This is the same as the "Entitlement Tag" in the output of the **show license tech** commad and it displays information about the license being tracked.
UDI	Composed of the Product ID (PID) and serial number of the product instance.
Previous Report Id:	ID of the previous RUM report that the product instance generated for a license.
Next Report Id:	The ID that the product instance will use for the next RUM report it generates for a llicense.
State:	Displays the current processing state of a RUM report. The value displayed here is always the same as the value displayed in the simplified view. For the list of possible values see #unique_119 unique_119_Connect_42_table_ytd_q4m_hrbabove.
State Change Reason:	Displays the reason for a RUM report state change. Not all state changes provide a reason. • NONE: This means the RUM report is going through its normal lifecycle (for instance, from OPEN → CLOSED → ACK). This state change reason is usually accompanied by an `N` flag (meaning Normal) in the simplified view and requires no action from you. • ACKED: RUM report was processed normally by CSSM. • REMOVED: RUM report was received and requested to be removed by CSSM. • RELOAD: RUM report state was changed due to some type of device reload.
Start Time:	Timestamps for measurement start and measurement end for a RUM report. Together, the start time and end time provide the time duration that the measurements cover.
End Time:	

Field Name	Description
Storage State:	Displays current storage state of the RUM report and can be one of the following values: • EXIST: This means the data for the RUM report is located in storage. • DELETED: This means the data was intentionally deleted. Refer to the `Storage State Change Reason` in the output of the **show license tech** command for more information about this storage state. • PURGED: This means the data was deleted due to a system resource limitation. Refer to the `Storage State Change Reason` in the output of the **show license tech** command for more information about this storage state. • MISSING: This means data is missing from storage. If reports are identified as missing, there is no recovery process.
Transaction ID:	Contains tracking information for the RUM report. This information can be either polling information or ACK import information. The Transaction Message contains the error message, if the product instance receives one when importing an ACK. The information in these fields is used by the Cisco technical support team when troubleshooting problems with RUM reports.
Transaction Message:	

Example: show license rum feature: Simplified and Detailed View

The following is sample output of the **show license rum feature***license-name* and **show license rum feature***license-name***detail** commands on a Cisco Catalyst 9500 Series Switch. Similar output is displayed on all other Catalyst switches.

The output is filtered to display all RUM reports for the DNA Advantage license, followed by a detailed view of all RUM reports for the DNA Advantage license.

```
Device# show license rum feature air-dna-advantage

Smart Licensing Usage Report:

====================================

Report Id,          State,    Flag, Feature Name

1638055644          CLOSED    N     air-dna-advantage

1638055646          OPEN      N     air-dna-advantage


Device# show license rum feature air-dna-advantage detail
Smart Licensing Usage Report Detail:
====================================
Report Id: 1638055644
  Metric Name: ENTITLEMENT
  Feature Name: air-dna-advantage
  Metric Value: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790
  UDI: PID:C9800-CL-K9,SN:93SZ7RXN93Y
  Previous Report Id: 0,    Next Report Id: 1638055646
```

```
  State: CLOSED,      State Change Reason: RELOAD
  Start Time: Nov 28 12:02:09 2021 UTC,      End Time: Nov 30 22:02:13 2021 UTC
  Storage State: EXIST
  Transaction ID: 0
  Transaction Message: <none>

Report Id: 1638055646
  Metric Name: ENTITLEMENT
  Feature Name: air-dna-advantage
  Metric Value: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790
  UDI: PID:C9800-CL-K9,SN:93SZ7RXN93Y
  Previous Report Id: 1638055644,    Next Report Id: 0
  State: OPEN,      State Change Reason: None
  Start Time: Nov 30 23:12:56 2021 UTC,      End Time: Dec 01 02:12:56 2021 UTC
  Storage State: EXIST
  Transaction ID: 0
  Transaction Message: <none>
```

Example: Saving a RUM Report View

The following example shows you how to save the information that is displayed.

By using the **feature** and **all** keywords, the output is filtered to display all RUM reports for all licenses being used on the product instance. It is then transferred it to a TFTP location, from where it can opened, to view the information.

```
Device# show license rum feature all save bootflash:all-rum-stats.txt
Device# copy tftp://10.8.0.6/bootflash:all-rum-stats.txt
```

show license status

To display information about licensing settings such as data privacy, policy, transport, usage reporting and trust codes, enter the **show license status** command in privileged EXEC mode.

show license status

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes `Trust code installed:`, `Policy in use`, `Policy name:` , reporting requirements as in the policy (`Attributes:`), and fields related to usage reporting. Command output no longer displays Smart Account and Virtual account information.
Cisco IOS XE Cupertino 17.7.1	Command output was updated to display Smart Account and Virtual account information.

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Account Information in the output

Starting with Cisco IOS XE Cupertino 17.7.1, every ACK includes the Smart Account and Virtual Account that was reported to, in CSSM. When it receives the ACK, the product instance securely stores only the latest version of this information - as determined by the timestamp in the ACK. The Smart Account and Virtual Account information that is displayed in the `Account Information` section of this command's output is therefore always as per the latest available ACK on the product instance.

If a product instance is moved from one Smart Account and Virtual Account to another, the next ACK after the move will have this updated information. The output of this command is updated once this ACK is available on the product instance.

The ACK may be received directly (where the product instance is connected to CSSM), or indirectly (where the product instance is connect to CSSM through CSLU, Cisco DNA Center, or SSM On-Prem), or by manually importing the ACK (where a product instance is in an air-gapped network).

Examples

For information about the fields shown in the display, see Table 13: show license status Field Descriptions for Smart Licensing Using Policy, on page 159 .

For sample output, see:

- show license status with Account Information (Smart Licensing Using Policy), on page 164
- show license status with Cisco Default Policy (Smart Licensing Using Policy), on page 165
- show license status with Custom Policy (Smart Licensing Using Policy), on page 166

Table 13: show license status Field Descriptions for Smart Licensing Using Policy

Field		Description
Utility	Header for utility settings that are configured on the product instance.	
	Status:	Status
	Utility report:	Last attempt:
	Customer Information:	The following fields are displayed: • Id: • Name: • Street • City: • State: • Country: • Postal Code:
Smart Licensing Using Policy:	Header for policy settings on the product instance.	
	Status:	Indicates if Smart Licensing Using Policy is enabled. Smart Licensing Using Policy is supported starting from Cisco IOS XE Amsterdam 17.3.2 and is always enabled on supported software images.
Account Information:	Header for account information that the product instance belongs to, in CSSM. This section is displayed only if the software version on the product instance is Cisco IOS XE Cupertino 17.7.1 or a later release.	
	Smart Account:	The Smart Account that the product instance is part of. This information is always as per the latest available ACK on the product instance.
	Virtual Account:	The Virtual Account that the product instance is part of. This information is always as per the latest available ACK on the product instance.

Field		Description
Data Privacy:	Header for privacy settings that are configured on the product instance.	
	Sending Hostname:	A *yes* or *no* value which shows if the hostname is sent in usage reports.
	Callhome hostname privacy:	Indicates if the Call Home feature is configured as the mode of transport for reporting. If configured, one of these values is displayed: • ENABLED • DISABLED
	Smart Licensing hostname privacy:	One of these values is displayed: • ENABLED • DISABLED
	Version privacy:	One of these values is displayed: • ENABLED • DISABLED
Transport:	Header for transport settings that are configured on the product instance.	
	Type:	Mode of transport that is in use. Additional fields are displayed for certain transport modes. For example, if transport type is set to CSLU, the CSLU address is also displayed.

Field		Description
Policy:	Header for policy information that is applicable to the product instance.	
	Policy in use:	Policy that is applied This can be one of the following: Cisco default, Product default, Permanent License Reservation, Specific License Reservation, PAK license, Installed on <date>, Controller.
	Policy name:	Name of the policy
	Reporting ACK required:	A *yes* or *no* value which specifies if the report for this product instance requires CSSM acknowledgement (ACK) or not. The default policy is always set to “yes”.
	Unenforced/Non-Export Perpetual Attributes	Displays policy values for perpetual licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name
	Unenforced/Non-Export Subscription Attributes	Displays policy values for subscription licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name
	Enforced (Perpetual/Subscription) License Attributes	

Field		Description
		Displays policy values for enforced licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name
	Export (Perpetual/Subscription) License Attributes	Displays policy values for export-controlled licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name
Miscellaneous	Header for custom ID.	
	Custom Id:	ID

Field		Description
Usage Reporting:	Header for usage reporting (RUM reports) information.	
	Last ACK received:	Date and time of last ACK received, in the local time zone.
	Next ACK deadline:	Date and time for next ACK. If the policy states that an ACK is not requires then this field displays `none`. **Note** If an ACK is required and is not received by this deadline, a syslog is displayed.
	Reporting Interval:	Reporting interval in days The value displayed here depends on what you configure in the **license smart usage interval***interval_in_days* and the policy value. For more information, see the corresponding Syntax Description: license smart (global config), on page 120.
	Next ACK push check:	Date and time when the product instance will submit the next polling request for an ACK. Date and time are in the local time zone. This applies only to product instance- initiated communication to CSSM or CSLU. If the reporting interval is zero, or if no ACK polling is pending, then this field displays `none`.
	Next report push:	Date and time when the product instance will send the next RUM report. Date and time are in the local time zone. If the reporting interval is zero, or if there are no pending RUM reports, then this field displays `none`.
	Last report push:	Date and time for when the product instance sent the last RUM report. Date and time are in the local time zone.
	Last report file write:	Date and time for when the product instance last saved an offline RUM report. Date and time are in the local time zone.
	Last report pull:	Date and time for when usage reporting information was retrieved using data models. Date and time are in the local time zone.

Field		Description
Trust Code Installed:	Header for trust code-related information. Displays date and time if trust code is installed. Date and time are in the local time zone. If a trust code is not installed, then this field displays `none`.	
	Active:	Active product instance. In a High Availability set-up, the the UDIs of all product instances in the set-up, along with corresponding trust code installation dates and times are displayed.
	Standby:	Standby product instance.
	Member:	Member product instance

show license status with Account Information (Smart Licensing Using Policy)

The following is sample output of the **show license status** command, on a product instance where the software version is Cisco IOS XE Cupertino 17.7.1:

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

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA

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

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

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

```
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>
```

show license status with Cisco Default Policy (Smart Licensing Using Policy)

The following is sample output of the **show license status** command; a default is policy applied here.

```
Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

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

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

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

```
    Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>
```

show license status with Custom Policy (Smart Licensing Using Policy)

The following is sample output of the **show license status** command; a custom policy applied here.

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

Smart Licensing Using Policy:
  Status: ENABLED

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

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured

Policy:
  Policy in use: Installed On Nov 02 05:09:31 2020 IST
  Policy name: SLE Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 60 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 30 (Customer Policy)
    Report on change (days): 30 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>
```

```
Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
    INSTALLED on Nov 02 05:09:31 2020 IST
  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
    INSTALLED on Nov 02 05:09:31 2020 IST
```

show license summary

To display a brief summary of license usage, which includes information about licenses being used, the count, and status, enter the **show license summary** command in privileged EXEC mode.

show license summary

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect valid license status for Smart Licensing Using Policy. Valid license statuses include: `IN USE`, `NOT IN USE`, `NOT AUTHORIZED`. Command output was also updated to remove registration and authorization information. Command output no longer displays Smart Account and Virtual account information.
Cisco IOS XE Cupertino 17.7.1	Command output was updated to display Smart Account and Virtual account information.

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

The licenses on Cisco Catalyst Wireless Controllers are never `NOT AUTHORIZED`, because none of the available licenses are export-controlled or enforced (Only these licenses require authorization before use).

Account Information in the output

Starting with Cisco IOS XE Cupertino 17.7.1, every ACK includes the Smart Account and Virtual Account that was reported to, in CSSM. When it receives the ACK, the product instance securely stores only the latest version of this information - as determined by the timestamp in the ACK. The Smart Account and Virtual Account information that is displayed in the `Account Information` section of this command's output is therefore always as per the latest available ACK on the product instance.

If a product instance is moved from one Smart Account and Virtual Account to another, the next ACK after the move will have this updated information. The output of this command is updated once this ACK is available on the product instance.

The ACK may be received directly (where the product instance is connected to CSSM), or indirectly (where the product instance is connect to CSSM through CSLU, Cisco DNA Center, or SSM On-Prem), or by manually importing the ACK (where a product instance is in an air-gapped network).

Examples

See Table 14: show license summary Field Descriptions, on page 168 for information about fields shown in the display.

show license summary: IN USE (Smart Licensing Using Policy), on page 168

show license summary: NOT IN USE (Smart Licensing Using Policy), on page 169

Table 14: show license summary Field Descriptions

Field	Description
Account Information: Smart Account: Virtual Account:	The Smart Account and Virtual Account that the product instance is part of. This information is always as per the latest available ACK on the product instance. This field is displayed only if the software version on the product instance is Cisco IOS XE Cupertino 17.7.1 or a later release.
License	Name of the licenses in use
Entitlement Tag	Short name for license
Count	License count
Status	License status can be one of the following • In-Use: Valid license, and in-use. • Not In-Use • Not Authorized: Means that the license requires installation of SLAC before use.

show license summary: IN USE (Smart Licensing Using Policy)

The following is sample output of the **show license summary** command, on a product instance where the software version is Cisco IOS XE Cupertino 17.7.1:

```
Devide# show license summary

Account Information:
  Smart Account: Eg-SA
```

```
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  air-network-essentials  (DNA_NWSTACK_E)                   1 IN USE
  air-dna-essentials      (AIR-DNA-E)                       1 IN USE
```

show license summary: NOT IN USE (Smart Licensing Using Policy)

The following is sample output of the **show license summary** command, where no APs have joined the controller. Current consumption (Count) is therefore zero, and the `Status` field shows that the licenses are `NOT IN USE`:

```
Device# show license summary

Device#show license summary
License Reservation is ENABLED

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  Aironet DNA Advantag... (AIR-DNA-A)                       0 NOT IN USE
  AP Perpetual Network... (DNA_NWStack)                     0 NOT IN USE
```

show license udi

To display Unique Device Identifier (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

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available with the introduction of Smart Licensing Using Policy.

Usage Guidelines

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Examples

show license udi with Standalone Product Instance, on page 170

show license udi with Active and Standby, on page 170

show license udi with Standalone Product Instance

The following is sample output from the **show license udi** command on a standalone product instance.

```
Device# show license udi

UDI: PID:C9800-L-F-K9,SN:FCW2323W016
```

show license udi with Active and Standby

The following is sample output from the **show license udi** command in a High Availability set-up where an active and a standby product instances exist. UDI information is displayed for both.

```
Device# show license udi

UDI: PID:C9800-CL-K9,SN:93BBAH93MGS

HA UDI List:
    Active:PID:C9800-CL-K9,SN:93BBAH93MGS
    Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN
```

show license usage

To display license usage information such as status, a count of licenses being used, and enforcement type, enter the **show license usage** command in privileged EXEC mode.

show license usage

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC

Command History

Release	Modification
This command was introduced in a release earlier than Cisco IOS XE Amsterdam 17.3.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	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.

Usage Guidelines

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Examples

See Table 15: show license usage Field Descriptions, on page 171 for information about fields shown in the display.

show license usage with unenforced licenses (Smart Licensing Using Policy), on page 172

show license usage with unenforced SLR licenses (Smart Licensing Using Policy), on page 172

Table 15: show license usage Field Descriptions

Field	Description
License Authorization: Status:	Displays overall authorization status.
():	Name of the license as in CSSM. If this license is one that requires an authorization code, the name of th the code.
Description	Description of the license as in CSSM.
Count	License count. If the license is not in-use, the count is reflected as ze
Version	Version.
Status	License status can be one of the following • In-Use: Valid license, and in-use. • Not In-Use • Not Authorized: Means that the license requires installation of S more information, see
Export Status:	Indicates if this license is export-controlled or not. Accordingly, one of 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.

Field	Description
Utility Subscription id:	ID Not applicable, because the corresponding confiuration option is not sup
Enforcement type	Enforcement type status for the license. This may be one of the followin • ENFORCED • NOT ENFORCED • EXPORT RESTRICTED - ALLOWED • EXPORT RESTRICTED - NOT ALLOWED For more information about enforcement types, see <link tbd>

show license usage with unenforced licenses (Smart Licensing Using Policy)

The following is sample output of the **show license usage** command. Unenforced licenses are in-use here.

```
Device# show license usage

License Authorization:
  Status: Not Applicable

air-network-essentials (DNA_NWSTACK_E):
  Description: air-network-essentials
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-network-essentials
  Feature Description: air-network-essentials
  Enforcement type: NOT ENFORCED
  License type: Perpetual

air-dna-essentials (AIR-DNA-E):
  Description: air-dna-essentials
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-essentials
  Feature Description: air-dna-essentials
  Enforcement type: NOT ENFORCED
  License type: Perpetual
```

show license usage with unenforced SLR licenses (Smart Licensing Using Policy)

The following is sample output of the **show license usage** command. Migrated SLR licenses are in-use here:

```
Device# show license usage

air-network-advantage (DNA_NWStack):
  Description: air-network-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
```

```
  Export status: NOT RESTRICTED
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20

air-dna-advantage (AIR-DNA-A):
  Description: air-dna-advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 20
```

show platform software sl-infra

To display troubleshooting information and for debugging, enter the **show platform software sl-infra** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting and debugging.

show platform software sl-infra { **all** | **current** | **debug** | **stored** }

Syntax Description

all	Displays current, debugging, and stored information.
current	Displays current license-related information.
debug	Enables debugging
stored	Displays information that is stored on the product instance.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

Usage Guidelines

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

show license tech

To display licensing information to help the technical support team to solve a problem, enter the **show license tech** command in privileged EXEC mode. The output for this command includes outputs of several other **show license** commands and more.

show license tech { **message** | **rum** { **feature** { *license_name* | **all** } | **id** { *rum_id* | **all** } } [**detail**] [**save** *path*] | **support** }

Syntax Description

message	Displays messages concerning trust establishment, usage reporting, result polling, authorization code requests and returns, and trust synchronization. This is the same information as displayed in the output of the **show license history message** command.
rum { **feature** { *license_name* | **all** } | **id** { *rum_id* | **all** } } [**detail**] [**save** *path*]	Displays information about Resource Utilization Measurement reports (RUM reports) on the product instance, including report IDs, the current processing state of a report, error information (if any), and an option save the displayed RUM report information. **Note** This option saves the information *about* RUM reports and is not for reporting purposes. It does not save the RUM report, which is an XML file containing usage information.
support	Displays licensing information that helps the technical support team to debug a problem.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy.

Release	Modification
Cisco IOS XE Cupertino 17.7.1	The **rum** keyword and additional options under this keyword were added: { **feature** { *license_name* | **all** } | **id** { *rum_id* | **all** } } The output of the **show license tech support** command was enhanced to display the following information: • RUM report information, in section `License Usage` and `Usage Report Summary`. • Smart Account and Virtual account information, in section `Account Information:`. The **data conversion**, **eventlog** and **reservation** keywords were removed from this command. They contitute to be available as separate show commands, that is, **show license data**, **show license eventlog**, and **show license reservation** respectively.

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing (whether smart licensing is enabled, all associated licensing certificates, compliance status, and so on).

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2 or a later release, command output displays fields pertinent to Smart Licensing Using Policy. Note the following guidelines:

- Troubleshooting with a Support Representative

  When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

- RUM Report Information in the output

  - The output of the **show license tech support** command displays the following sections pertaining to RUM reports:

    Table 16: show license tech support: Field Descriptions for Header "License Usage", on page 176

    ```
    <output truncated>
    License Usage
    =============
      Measurements:
        ENTITLEMENT:
          Interval: 00:15:00
          Current Value: 800
          Current Report: 1638055645       Previous: 0
     <output truncated>
    ```

    Table 17: show license tech support: Field Descriptions for Header "Usage Report Summary", on page 177

    ```
    <output truncated>
    Usage Report Summary:
    =====================
    Total: 4,  Purged: 0(0)
    ```

```
Total Acknowledged Received: 0,  Waiting for Ack: 0(4)
Available to Report: 4  Collecting Data: 2
Maximum Display: 4  In Storage: 4,  MIA: 0(0)
Report Module Status: Ready

<output truncated>
```

- The output of the **show license tech rum** command when used with the **detail** keyword, displays the following fields pertaining to RUM reports: Table 18: show license tech rum: Field Descriptions for Header "Smart Licensing Usage Report Detail", on page 177.

  The options available under the **show license tech rum** keyword are the same as the options available with the **show license rum** privileged EXEC command. The sample output that is displayed in the *simplified view* is also the same. But if you use the **detail** keyword (for example if you enter **show license tech rum feature** *license_name* **detail**), the detailed view is displayed and this has a few *additional* fields when compared to **show license rum**.

```
<output truncated>
Smart Licensing Usage Report Detail:
====================================
Report Id: 1638055644
  Metric Name: ENTITLEMENT
  Feature Name: air-dna-advantage
  Metric Value:
regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790
  UDI: PID:C9800-CL-K9,SN:93SZ7RXN93Y
  Previous Report Id: 0,    Next Report Id: 1638055646
  Version: 2.0
  State: CLOSED,      State Change Reason: RELOAD
  Start Time: Nov 28 12:02:09 2021 UTC,      End Time: Nov 30 22:02:13 2021 UTC
  Storage State: EXIST,  Storage State Change Reason: None
  Transaction ID: 0
  Transaction Message: <none>
  Report Size: 54880(54987)
<output truncated>
```

Table 16: show license tech support: Field Descriptions for Header "License Usage"

Field Name	Description
Interval:	This is a fixed measurement duration and is always 15 minutes.
Current Value:	Information about the current license count.
Current Report:	ID of the currently OPEN report for the license.
Previous:	ID of the last OPEN report for the license. This report will have state CLOSED now.

Table 17: show license tech support: Field Descriptions for Header "Usage Report Summary"

Field Name	Description
Total:	Total number of reports that the product instance has ever generated. **Note** This total does not refer to the total number of reports *currently available* on and being tracked by the product instance. For this you must sum up the `Total Acknowledged Received:` and `Available to Report` fields.
Purged:	The number of reports deleted due to a system resource limitation. This number includes RUM reports where the product instance no longer has tracking information.
Total Acknowledged Received:	The number of RUM reports acknowledged on this product instance.
Waiting for Ack:	The number of RUM reports waiting for an ACK. This is the total number of reports in an `UNACK` state, where the product instance still has tracking information.
Available to Report:	The number of RUM reports that are available to send to CSSM. This is the total number of reports in an `OPEN` or `CLOSED` state, where the product instance still has tracking information.
Collecting Data:	Number of reports where the product instance is currently collecting measurements.
Maximum Display:	Number of reports available for display in a **show** command's output.
In Storage:	Number of reports currently stored on the disk
MIA:	The number of reports missing.

Table 18: show license tech rum: Field Descriptions for Header "Smart Licensing Usage Report Detail"

Field Name	Description
Version:	Displays the format of the report during transmission. Starting with Cisco IOS XE Cupertino 17.7.1, RUM reports are stored in a new format that reduces processing time. This field indicates if the product instance is using the old format or the new format.

Field Name	Description
Storage State:	Indicates if a given report is currently in storage. In addition to the displaying the current storage state of the RUM report, with these possible values: EXIST, DELETED, PURGED, MISSING, if a "(1)" is displayed next to the label (`Storage State (1)`), this means the RUM report is in the older (pre-17.7.1 format) and will be processed accordingly. If the RUM report is in the new format, the field is displayed as `Storage State` - without any extra information.
Storage State Change Reason:	Displays the reason for the change in the storage state change. Not all state changes provide a reason. • NONE: This means no reason was recorded for the the storage state change. • PROCESSED: This means the RUM report was deleted after CISCO has processed the data. • LIMIT_STORAGE: This means the RUM report was deleted because the product instance reached it's storage limit. • LIMIT_TIME: This means the RUM report was deleted because the report reached the persisted time limit.
Transaction ID: Transaction Message:	If the transaction ID displays a correlation ID and an error status is displayed, the product instance displays the error code field in this section. If there are no errors, no data is displayed here.
Report Size	This field displays two numbers. The first number is the size of raw report for communication, in bytes. The second number is the disk space used for saving the report, also in bytes. The second number is displayed only if report is stored in the new format.

show license tech support on Cisco Catalyst 9800-CL Wireless Controller

The following is sample output from the **show license tech support** command on a Cisco Catalyst 98000-CL Wireless Controller running software version Cisco IOS XE Cupertino 17.7.1:

```
Device# show license tech support
Smart Licensing Tech Support info

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

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED
```

```
Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: <none>
  Virtual Account: <none>

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

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Address: <empty>
    Port: <empty>
    Username: <empty>
    Password: <empty>
  Server Identity Check: True
  VRF: <empty>

Miscellaneous:
  Custom Id: <empty>

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

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting) State(1) InPolicy(0)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>

License Usage
=============
Handle: 1
  License: air-network-advantage
  Entitlement Tag:
regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
  Description: air-network-advantage
  Count: 0
```

```
  Version: 1.0
  Status: NOT IN USE(1)
  Status time: Oct 05 22:24:24 2021 UTC
  Request Time: None
  Export status: NOT RESTRICTED
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 0
      Current Report: 0       Previous: 0
  Soft Enforced: True

Handle: 2
  License: air-dna-advantage
  Entitlement Tag: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790

  Description: air-dna-advantage
  Count: 0
  Version: 1.0
  Status: NOT IN USE(1)
  Status time: Oct 05 22:24:24 2021 UTC
  Request Time: None
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 0
      Current Report: 0       Previous: 0
  Soft Enforced: True

Product Information
===================
UDI: PID:C9800-CL-K9,SN:9KGIXIDOXFE

HA UDI List:
    Active:PID:C9800-CL-K9,SN:9KGIXIDOXFE
    Standby:PID:C9800-CL-K9,SN:9UBKZU955E4

Agent Version
=============
Smart Agent for Licensing: 5.3.14_rel/47

Upcoming Scheduled Jobs
=======================
Current time: Oct 06 00:38:46 2021 UTC
Daily: Oct 06 21:24:22 2021 UTC (20 hours, 45 minutes, 36 seconds remaining)
Authorization Renewal: Expired Not Rescheduled
Init Flag Check: Expired Not Rescheduled
Reservation configuration mismatch between nodes in HA mode: Expired Not Rescheduled
Start Utility Measurements: Oct 06 00:39:25 2021 UTC (39 seconds remaining)
Send Utility RUM reports: Oct 06 22:24:54 2021 UTC (21 hours, 46 minutes, 8 seconds remaining)
Save unreported RUM Reports: Oct 06 01:24:35 2021 UTC (45 minutes, 49 seconds remaining)
Data Synchronization: Expired Not Rescheduled
External Event: Expired Not Rescheduled
Operational Model: Expired Not Rescheduled
```

```
Communication Statistics:
=======================
Communication Level Allowed: INDIRECT
Overall State: Insufficient trust for direct communication
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=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>
Result Polling:
  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 Request:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Confirmation:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Return:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Sync:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Hello Message:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>

License Certificates
====================
Production Cert: False
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: False

Reservation Info
================
License reservation: DISABLED

Overall status:
  Active: PID:C9800-CL-K9,SN:9KGIXIDOXFE
      Reservation status: NOT INSTALLED
      Request code: <none>
      Last return code: <none>
      Last Confirmation code: <none>
      Reservation authorization code: <none>
  Standby: PID:C9800-CL-K9,SN:9UBKZU955E4
      Reservation status: NOT INSTALLED
      Request code: <none>
      Last return code: <none>
      Last Confirmation code: <none>
      Reservation authorization code: <none>

Specified license reservations:

Purchased Licenses:
  No Purchase Information Available

Usage Report Summary:
=====================
Total: 0,  Purged: 0(0)
Total Acknowledged Received: 0,  Waiting for Ack: 0(0)
Available to Report: 0  Collecting Data: 0
Maximum Display: 0  In Storage: 0,  MIA: 0(0)
Report Module Status: Ready

Other Info
==========
Software ID: regid.2018-05.com.cisco.WLC_9500C,1.0_85665885-b865-4e32-8184-5510412fcb54
Agent State: authorized
TS enable: True
Transport: Smart
  Default URL: https://smartreceiver.cisco.com/licservice/license
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char)  : 1
sizeof(int)   : 4
sizeof(long)  : 4
sizeof(char *): 8
sizeof(time_t): 4
sizeof(size_t): 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: 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
Check Point Interface: True
Config Management Interface: False
License Map Interface: True
HA Interface: True
Trusted Store Interface: True
Platform Data Interface: True
Crypto Version 2 Interface: False
SAPluginMgmtInterfaceMutex: True
SAPluginMgmtIPDomainName: True
SmartTransportVRFSupport: True
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartTransportServerIdCheck: True
SmartTransportProxySupport: True
SmartAgentPolicyDisplayFormat: 0
SmartAgentReportOnUpgrade: False
SmartAgentIndividualRUMEncrypt: 2
SmartAgentMaxRumMemory: 2
SmartAgentConcurrentThreadMax: 10
SmartAgentPolicyControllerModel: False
SmartAgentPolicyModel: True
SmartAgentFederalLicense: True
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: True
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
HighAvailabilityOverrideEvent: UnknownPlatformEvent
platformIndependentOverrideEvent: UnknownPlatformEvent
platformOverrideEvent: UnknownPlatformEvent
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 3 KB
P:C9800-CL-K9,S:9KGIXIDOXFE: No Trust Data
P:C9800-CL-K9,S:9UBKZU955E4: No Trust Data
Overall Trust: No ID
```

```
Clock sync-ed with NTP: True

Platform Provided Mapping Table
===============================
  C9800-CL-K9: Total licenses found: 5
Enforced Licenses:
  P:C9800-CL-K9,S:9KGIXIDOXFE:
    No PD enforced licenses
  P:C9800-CL-K9,S:9UBKZU955E4:
    No PD enforced licenses
```

Example (Smart Licensing Using Policy)

The following is sample output from the **show license tech support** command.

```
Device# show license tech support

Smart Licensing Tech Support info

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 Nov 02 03:16:01 2020 IST

License Authorization:
  Status: AUTHORIZED - RESERVED on Nov 02 03:16:01 2020 IST

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: Smart
  URL: https://smartreceiver.cisco.com/licservice/license

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 89 days, 23 hours, 42 minutes, 47 seconds

License Usage
=============
Handle: 1
  License: AP Perpetual Networkstack Advantage
  Entitlement tag:
regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
  Description: AP Perpetual Network Stack entitled with DNA-A
  Count: 1
  Version: 1.0
```

```
  Status: AUTHORIZED(3)
  Status time: Nov 02 03:16:01 2020 IST
  Request Time: Nov 02 02:55:34 2020 IST
  Export status: NOT RESTRICTED
  Soft Enforced: True

Handle: 2
  License: Aironet DNA Advantage Term Licenses
  Entitlement tag: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790

  Description: DNA Advantage for Wireless
  Count: 1
  Version: 1.0
  Status: AUTHORIZED(3)
  Status time: Nov 02 03:16:01 2020 IST
  Request Time: Nov 02 02:55:34 2020 IST
  Export status: NOT RESTRICTED
  Soft Enforced: True

Product Information
===================
UDI: PID:C9800-CL-K9,SN:93BBAH93MGS

HA UDI List:
    Active:PID:C9800-CL-K9,SN:93BBAH93MGS
    Standby:PID:C9800-CL-K9,SN:9XECPSUU4XN

Agent Version
=============
Smart Agent for Licensing: 4.8.7_rel/52

Upcoming Scheduled Jobs
=======================
Current time: Nov 02 03:17:23 2020 IST
Daily: Nov 03 02:47:04 2020 IST (23 hours, 29 minutes, 41 seconds remaining)
Certificate Renewal: Not Available
Certificate Expiration Check: Not Available
Authorization Renewal: Not Available
Authorization Expiration Check: Not Available
Init Flag Check: Not Available
Evaluation Expiration Check: Not Available
Ack Expiration Check: Not Available
Evaluation Expiration Warning: Not Available
IdCert Expiration Warning: Not Available
Reservation request in progress warning: Not Available
Reservation configuration mismatch between nodes in HA mode: Nov 09 03:16:30 2020 IST (6
days, 23 hours, 59 minutes, 7 seconds remaining)
Endpoint Report Request: Not Available

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: False
```

```
Reservation Info
================
License reservation: ENABLED

Overall status:
  Active: PID:C9800-CL-K9,SN:93BBAH93MGS
      Reservation status: SPECIFIC INSTALLED on Nov 02 03:16:01 2020 IST
      Export-Controlled Functionality: ALLOWED
      Request code: <none>
      Last return code: <none>
      Last Confirmation code: 102fc949
      Reservation authorization code:
<specificPLR><authorizationCode><flag>A</flag><version>C</version><piid>[illegible]</piid><timestamp>[illegible]</timestamp><entitlements><entitlement><tag>regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790</tag><count>5</count><startDate>2020-Oct-14
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>Aironet DNA Advantage Term
Licenses</displayName><tagDescription>DNA Advantage for
Wireless</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790</tag><count>5</count><startDate>2020-Jun-18
 UTC</startDate><endDate>2020-Dec-15
UTC</endDate><licenseType>TERM</licenseType><displayName>Aironet DNA Advantage Term
Licenses</displayName><tagDescription>DNA Advantage for
Wireless</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896</tag><count>5</count><startDate>2020-Oct-14
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>AP Perpetual Networkstack
Advantage</displayName><tagDescription>AP Perpetual Network Stack entitled with
DNA-A</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896</tag><count>5</count><startDate>2020-Jun-18
 UTC</startDate><endDate>2020-Dec-15
UTC</endDate><licenseType>TERM</licenseType><displayName>AP Perpetual Networkstack
Advantage</displayName><tagDescription>AP Perpetual Network Stack entitled with
DNA-A</tagDescription><subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode><signature>[illegible]</signature><udi>P:C9800-CL-K9,S:93BBAH93MGS</udi></specificPLR>

  Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
      Reservation status: SPECIFIC INSTALLED on Nov 02 03:15:45 2020 IST
      Export-Controlled Functionality: ALLOWED
      Request code: <none>
      Last return code: <none>
      Last Confirmation code: ad4382fe
      Reservation authorization code:
<specificPLR><authorizationCode><flag>A</flag><version>C</version><piid>[illegible]</piid><timestamp>[illegible]</timestamp><entitlements><entitlement><tag>regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896</tag><count>10</count><startDate>2020-Oct-14
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>AP Perpetual Networkstack
Advantage</displayName><tagDescription>AP Perpetual Network Stack entitled with
DNA-A</tagDescription><subscriptionID></subscriptionID></entitlement><entitlement><tag>regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790</tag><count>10</count><startDate>2020-Oct-14
 UTC</startDate><endDate>2021-Apr-12
UTC</endDate><licenseType>TERM</licenseType><displayName>Aironet DNA Advantage Term
Licenses</displayName><tagDescription>DNA Advantage for
Wireless</tagDescription><subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode><signature>[illegible]</signature><udi>P:C9800-CL-K9,S:9XECPSUU4XN</udi></specificPLR>

Specified license reservations:
  Aironet DNA Advantage Term Licenses (AIR-DNA-A):
    Description: DNA Advantage for Wireless
    Total reserved count: 20
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
          Subscription ID: <none>
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
          Subscription ID: <none>
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
```

```
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
          Subscription ID: <none>
  AP Perpetual Networkstack Advantage (DNA_NWStack):
    Description: AP Perpetual Network Stack entitled with DNA-A
    Total reserved count: 20
    Term information:
      Active: PID:C9800-CL-K9,SN:93BBAH93MGS
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 5
          Subscription ID: <none>
        License type: TERM
          Start Date: 2020-JUN-18 UTC
          End Date: 2020-DEC-15 UTC
          Term Count: 5
          Subscription ID: <none>
      Standby: PID:C9800-CL-K9,SN:9XECPSUU4XN
        License type: TERM
          Start Date: 2020-OCT-14 UTC
          End Date: 2021-APR-12 UTC
          Term Count: 10
          Subscription ID: <none>

Other Info
==========
Software ID: regid.2018-05.com.cisco.WLC_9500C,1.0_85665885-b865-4e32-8184-5510412fcb54
Agent State: authorized
TS enable: True
Transport: Smart
  Default URL: https://smartreceiver.cisco.com/licservice/license
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char)  : 1
sizeof(int)   : 4
sizeof(long)  : 4
sizeof(char *): 8
sizeof(time_t): 4
sizeof(size_t): 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: 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
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
```

```
systemInitByEvent: True
SmartAgentFederalLicense: True
SmartAgent_Crypto_Exit_CB: 0x55B353357A20
SmartAgent_Crypto_Start_CB: 0x55B353357A10
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: True
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
platformOverrideEvent: UnknownPlatformEvent
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 21 KB

Platform Provided Mapping Table
===============================
<empty>
```

CHAPTER 7

Troubleshooting Smart Licensing Using Policy

This section provides the list of Smart Licensing Using Policy-related system messages you may encounter, possible reasons for failure, and recommended action.

System Message Overview

The system software sends system messages to the console (and, optionally, to a logging server on another system). Not all system messages mean problems with your system. Some messages are informational, and others can help diagnose problems with communications lines, internal hardware, or the system software.

How to Read System Messages

System log messages can contain up to 80 characters. Each system message begins with a percent sign (%) and is structured as follows:

```
%FACILITY-SEVERITY-MNEMONIC: Message-text
```

%FACILITY

Two or more uppercase letters that show the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software

SEVERITY

A single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation.

Table 19: Message Severity Levels

Severity Level	Description
0 - emergency	System is unusable.
1 - alert	Immediate action required.
2 - critical	Critical condition.

Severity Level	Description
3 - error	Error condition.
4 - warning	Warning condition.
5 - notification	Normal but significant condition.
6 - informational	Informational message only.
7 - debugging	Message that appears during debugging only.

MNEMONIC

A code that uniquely identifies the message.

Message-text

Message-text is a text string describing the condition. This portion of the message sometimes contains detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because the information in these variable fields changes from message to message, it is represented here by short strings enclosed in square brackets ([ ]). A decimal number, for example, is represented as [dec].

Table 20: Variable Fields in Messages

Severity Level	Description
[char]	Single character
[chars]	Character string
[dec]	Decimal number
[enet]	Ethernet address (for example, 0000.FEED.00C0)
[hex]	Hexadecimal number
[inet]	Internet address (for example, 10.0.2.16)
[int]	Integer
[node]	Address or node name
[t-line]	Terminal line number in octal (or in decimal if the decimal-TTY service is enabled)
[clock]	Clock (for example, 01:20:08 UTC Tue Mar 2 1993

System Messages

This section provides the list of Smart Licensing Using Policy-related system messages you may encounter, possible reasons for failure (incase it is a failure message), and recommended action (if action is required).

For all error messages, if you are not able to solve the problem, contact your Cisco technical support representative with the following information:

The message, exactly as it appears on the console or in the system log.

The output from the **show license tech support**, **show license history message**, and the **show platform software sl-infra** privileged EXEC commands.

- %SMART_LIC-3-POLICY_INSTALL_FAILED
- %SMART_LIC-3-AUTHORIZATION_INSTALL_FAILED
- %SMART_LIC-3-COMM_FAILED
- %SMART_LIC-3-COMM_RESTORED
- %SMART_LIC-3-POLICY_REMOVED
- %SMART_LIC-3-TRUST_CODE_INSTALL_FAILED
- %SMART_LIC-4-REPORTING_NOT_SUPPORTED
- %SMART_LIC-6-POLICY_INSTALL_SUCCESS
- %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS
- %SMART_LIC-6-AUTHORIZATION_REMOVED
- %SMART_LIC-6-REPORTING_REQUIRED
- %SMART_LIC-6-TRUST_CODE_INSTALL_SUCCESS
- %IOSXE_RP_EWLC_NOT-2-MSGDEVICENOTREG
- %CAPWAPAC_TRACE_MSG-3-MAX_LICENSE_AP_LIMIT_REACHED

```
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.

Note The device should have a valid clock and the NTP configuration.

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, and 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].
```

This message is not applicable to Cisco Catalyst Access, Core, and Aggregation Switches, because there are no enforced or export-controlled licenses on these product instances.

```
Error Message %SMART_LIC-3-COMM_FAILED: Communications failure with the [chars] :
[chars]
```

Explanation: Smart Licensing communication either with CSSM, or CSLU, or SSM On-Prem failed. The first [chars] is the currently configured transport type, and the second [chars] is the error string with details of the failure. This message appears for every communication attempt that fails.

Possible reasons for failure include:

- CSSM, CSLU, SSM On-Prem is not reachable: This means that there is a network reachability problem.
- 404 host not found: This means the CSSM server is down.
- A TLS or SSL handshake failure caused by a missing client certificate. The certificate is required for TLS authentication of the two communicating sides. A recent server upgrade may have cause the certificate to be removed. This reason applies only to a topology where the product instance is directly connected to CSSM.

> **Note** If the error message is displayed for this reason, there is no actual configuration error or disruption in the communication with CSSM.

For topologies where the product instance initiates the sending of RUM reports (Connected to CSSM Through CSLU: Product Instance-Initiated Communication, Connected Directly to CSSM, CSLU Disconnected from CSSM: Product Instance-Initiated Communication, and SSM On-Prem Deployment: Product Instance-Initiated Communication) if this communication failure message coincides with scheduled reporting (**license smart usage interval** *interval_in_days* global configuration command), the product instance attempts to send out the RUM report for up to four hours after the scheduled time has expired. If it is still unable to send out the report (because the communication failure persists), the system resets the interval to 15 minutes. Once the communication failure is resolved, the system reverts the reporting interval to last configured value.

Recommended Action:

Troubleshooting steps are provided for when CSSM is not reachable or there is a missing client certificate, when CSLU is not reachable, and when SSM On-Prem is not reachable.

- If a client certificate is missing and there is no actual configuration error or disruption in the communication with CSSM:

To resolve the error, configure the **ip http client secure-trustpoint** *trustpoint-name* command in global configuration mode. For *trustpoint-name*, enter only `SLA-TrustPoint`. This command specifies that the secure HTTP client should use the certificate associated with the trustpoint indicated by the trustpoint-name argument.

- If CSSM is not reachable and the configured transport type is **smart**:

  1. Check if the smart URL is configured correctly. Use the **show license status** command in privileged EXEC mode, to check if the URL is exactly as follows: https://smartreceiver.cisco.com/licservice/license. If it is not, reconfigure the **license smart url smart** *smar_URL* command in global configuration mode.

  2. Check DNS resolution. Verify that the product instance can ping `smartreceiver.cisco.com` or the nslookup translated IP. The following example shows how to ping the translated IP

```
Device# ping 171.70.168.183
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 171.70.168.183, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

- If CSSM is not reachable and the configured transport type is **callhome**:

  1. Check if the URL is entered correctly. Use the **show license status** command in privileged EXEC mode, to check if the URL is exactly as follows: https://tools.cisco.com/its/service/oddce/services/DDCEService.

  2. Check if Call Home profile `CiscoTAC-1` is active and destination URL is correct. Use the **show call-home profile all** command in privileged EXEC mode:

```
Current smart-licensing transport settings:
 Smart-license messages: enabled
 Profile: CiscoTAC-1 (status: ACTIVE)
 Destination  URL(s):  https://tools.cisco.com/its/service/oddce/services/DDCEService
```

  3. Check DNS Resolution. Verify that the product instance can ping `tools.cisco.com`, or the nslookup translated IP.

```
Device# ping tools.cisco.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.37.145.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 41/41/42 ms
```

  If the above does not work check the following: if the product instance is set, 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 80

   From a Web browser on the device where CSLU is installed, verify `https://<product-instance-ip>/`. This ensures that the REST API from CSLU to the product instance works as expected.

- If SSM On-Prem is not reachable:

1. For product instance-initiated communication, check if the SSM On-Prem transport type and URL are configured correctly.

   In the **show license all** command output, under the `Transport:` header check the following: The `Type:` must be `cslu`and `Cslu address:` must have the hostname or the IP address of the server where you have installed SSM On-Prem and <tenantID> of the *default* local virtual account. See the example below:

```
Transport:
  Type: cslu
  Cslu address: https://192.168.0.1/cslu/v1/pi/on-prem-default
```

Check if you have the correct URL from SSM On-Prem (Retrieving the Transport URL (SSM On-Prem UI), on page 88) and then configure **license smart transport cslu** and **license smart url cslu** *http://<ip>/cslu/v1/pi/<tenant ID>* commands in global configuration mode.

Check that you have configured any other required commands for your network as mentioned in Ensuring Network Reachability for Product Instance-Initiated Communication, on page 85.

2. For SSM On-Prem-initiated communication, check HTTPs connectivity.

   Use the **show ip http server session-module** command in privileged EXEC mode. In the output, under header `HTTP server current connections:`, check that `SL_HTTP` is active. If it is not re-configure the **ip http** commands as mentioned in Ensuring Network Reachability for SSM On-Prem-Initiated Communication, on page 91.

3. Check trustpoint and that certificates are accepted.

   For both forms of communication in an SSM On-Prem Deployment, ensure that the correct trustpoint is used and that the necessary certificates are accepted:

```
Device(config)# crypto pki trustpoint SLA-TrustPoint
Device(ca-trustpoint)#
Device(ca-trustpoint)# enrollment terminal
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# end
Device# copy running-config startup-config
```

If the above does not work and 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)
        - Cisco Smart License utility (CSLU)
Smart Agent communication with either the Cisco Smart Software Manager (CSSM) or the Cisco
 Smart License
utility (CSLU) has been restored. No action required.
```

Explanation: Product instance communication with either the CSSM, or CSLU, or SSM On-Prem is restored.

Recommended Action: No action required.

```
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
```

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

Explanation: A previously installed *custom* licensing policy has been removed. The `Cisco default` policy is then automatically effective. This may cause a change in the behavior of smart licensing.

Possible reasons for failure include:

If you have entered the **license smart factory reset** command in privileged EXEC mode all licensing information including the policy is removed.

Recommended Action:

If the policy was removed intentionally, then no further action is required.

If the policy was removed inadvertantly, you can reapply the policy. Depending on the topology you have implemented, follow the corresponding method to retrieve the policy:

- Connected Directly to CSSM:

  Enter **show license status**, and check field `Trust Code Installed:`. If trust is established, then CSSM will automatically return the policy again. The policy is automatically re-installed on product instances of the corresponding Virtual Account.

  If trust has not been established, complete these tasks: Generating a New Token for a Trust Code from CSSM, on page 106 and Installing a Trust Code, on page 106. 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 78. 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:Export to CSSM (CSLU Interface), on page 79 > Uploading Data or Requests to CSSM and Downloading a File, on page 108 > Import from CSSM (CSLU Interface), on page 80.

  - For CSLU-initiated communication, complete this task: Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 78. This causes CSLU to detect and re-furnish the missing policy in an ACK response. Then complete these tasks in the given order: Export to CSSM (CSLU Interface), on page 79 > Uploading Data or Requests to CSSM and Downloading a File, on page 108 > Import from CSSM (CSLU Interface), on page 80.

- 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 108.

  Then complete this task on the product instance: Installing a File on the Product Instance, on page 109.

- SSM On-Prem Deployment

  - For product instance-initiated communication), enter the **license smart sync** command in privileged EXEC mode. The causes the product instance to synchronize with SSM On-Prem and restore any required or missing information. Then synchronize SSM On-Prem with CSSM if required:

  - For SSM On-Prem-initiated communication: In the SSM On-Prem UI, navigate to **Reports** > **Synchronization pull schedule with the devices** > **Synchronize now with the device**.

  For both forms of communication in an SSM On-Prem Deployment, synchronize with CSSM using either option:

- SSM On-Prem is connected to CSSM: In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports** > **Usage Schedules** > **Synchronize now with Cisco**.
- SSM On-Prem is not connected to CSSM: Exporting and Importing Usage Data (SSM On-Prem UI), on page 89.

```
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 106 and Installing a Trust Code, on page 106.
- Timestamp mismatch and signature mismatch: Configure the **ntp server** command in global configuration mode. For example:

  ```
  Device(config)# ntp server 198.51.100.100 version 2 prefer
  ```

```
Error Message    %SMART_LIC-4-REPORTING_NOT_SUPPORTED: The CSSM OnPrem that this
product instance is connected to is down rev and does not support the enhanced policy and
usage
reporting mode.
```

Explanation: Cisco Smart Software Manager On-Prem (formerly known as Cisco Smart Software Manager satellite) is supported in the Smart Licensing Using Policy environment starting with Cisco IOS XE Amsterdam 17.3.3 only (See Cisco Smart Software Manager On-Prem (SSM On-Prem), on page 11). In *unsupported* releases, the product instance will behave as follows:

- Stop sending registration renewals and authorization renewals.
- Start recording usage and saving RUM reports locally.

Recommended Action:

You have the following options:

- Refer to and implement one of the supported topologies instead. See: Connecting to Cisco SSM, on page 13.
- Upgrade to a release where SSM On-Prem is supported with Smart Licensing Using Policy. See Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy, on page 67.

```
------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
```

```
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].
```

This message is not applicable to Cisco Catalyst Access, Core, and Aggregation Switches, because there are no enforced or export-controlled licenses on these product instances.

```
------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
```

```
Error Message %SMART_LIC-6-AUTHORIZATION_REMOVED: A licensing authorization code has
 been removed from [chars]
```

Explanation: [chars] is the UDI where the authorization code was installed. The authorization code has been removed. This removes the licenses from the product instance and may cause a change in the behavior of smart licensing and the features using licenses.

Recommended Action: No action is required. If you want to see the current state of the license, enter the **show license all** command in privileged EXEC mode.

```
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
```

```
Error Message %SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement
will be required in [dec] days.
```

Explanation: This is an alert which means that RUM reporting to Cisco is required. [dec] is the amount of time (in days) left to meet this reporting requirements.

Recommended Action: Ensure that RUM reports are sent within the requested time. The topology you have implemented determines the reporting method.

- Connected to CSSM Through CSLU
  - For product instance-initiated communication: Enter the **license smart sync** command in privileged EXEC mode. If CSLU is currently logged into CSSM the reports will be automatically sent to the associated Smart Account and Virtual Account in CSSM.
  - For CSLU-initiated communication, complete this task: Collecting Usage Reports: CSLU Initiated (CSLU Interface), on page 78.
- Connected Directly to CSSM: Enter the **license smart sync** command in privileged EXEC mode.
- Connected to CSSM Through a Controller: If the product instance is managed by a controller, the controller will send the RUM report at the scheduled time.

  If you are using Cisco Catalyst Center as the controller, you have the option of ad-hoc reporting. See the *Cisco Catalyst Center Administrator Guide* of the required release (Release 2.2.2 onwards) > *Manage Licenses* > *Upload Resource Utilization Details to CSSM*.
- CSLU Disconnected from CSSM: If the product instance is connected to CSLU, synchronize with the product instance as shown for "Connected to CSSM Through CSLU"above, then complete these tasks: Export to CSSM (CSLU Interface), on page 79, Uploading Data or Requests to CSSM and Downloading a File, on page 108, and Import from CSSM (CSLU Interface), on page 80.
- No Connectivity to CSSM and No CSLU: Enter the **license smart save usage** command in privileged EXEC mode, to save the required usage information in a file. Then, from a workstation where you have connectivity to CSSM, complete these tasks: Uploading Data or Requests to CSSM and Downloading a File, on page 108 > Installing a File on the Product Instance, on page 109.
- SSM On-Prem Deployment:

  Synchronize the product instance with SSM On-Prem:
  - For product instance-initiated communication: Enter the **license smart sync** command in privileged EXEC mode. If CSLU is currently logged into CSSM the reports will be automatically sent to the associated Smart Account and Virtual Account in CSSM.
  - For SSM On-Prem-initiated communication, complete this task: In the SSM On-Prem UI, navigate to **Reports** > **Synchronization pull schedule with the devices** > **Synchronize now with the device**.

Synchronize usage information with CSSM (*choose one*)

- SSM On-Prem is connected to CSSM: In the SSM On-Prem UI, Smart Licensing workspace, navigate to **Reports** > **Usage Schedules** > **Synchronize now with Cisco**.
- SSM On-Prem is not connected to CSSM: Exporting and Importing Usage Data (SSM On-Prem UI), on page 89.

```
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
```

```
Error Message %SMART_LIC-6-TRUST_CODE_INSTALL_SUCCESS: A new licensing trust code
 was successfully installed on [chars].
```

Explanation:[chars] is the UDI where the trust code was successfully installed.

Recommended Action: No action is required. If you want to verify that the trust code is installed, enter the **show license status** command in privileged EXEC mode. Look for the updated timestamp under header `Trust Code Installed:` in the output.

```
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
```

```
Error Message %IOSXE_RP_EWLC_NOT-2-MSGDEVICENOTREG: Unregistered 9800-CL can only
be used in lab. For production usage, please register this device in [int] days. Failure
to do so
will result in a limited number [50] of Access Points being allowed post this.
```

Explanation: An ACK is required on this product instance. [int] is the amount of time left to install an ACK on the product instance.

This is system message is displayed only if the product instance is a Cisco Catalyst 9800-CL Wireless Controller running Cisco IOS XE Cupertino 17.7.1 or a later release. For more information, see RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72.

This system message is displayed once everyday, until the first ACK is made available on the product instance.

Recommended Action:

Implement one of the supported topologies and complete usage reporting. The method you can use to send the RUM report to CSSM and ACK installation depends on the topology you implement. See: Connecting to Cisco SSM, on page 13 and Implementing Smart Licensing Using Policy, on page 27.

```
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
```

```
Error Message %CAPWAPAC_TRACE_MSG-3-MAX_LICENSE_AP_LIMIT_REACHED: Chassis 1 R0/0:
wncmgrd: Ap MAC: [enet] is not allowed to join. Please start reporting licensing to Cisco
to get the
 ACK for resumption of usual operation.
```

Explanation: The ACK deadline for this product instance has passed and an ACK has still not been installed. [enet] is the MAC address of the AP that is trying to join the Cisco Catalyst 9800-CL Wireless Controller but is not allowed because the requisite ACK is not installed.

This is system message is displayed only if the product instance is a Cisco Catalyst 9800-CL Wireless Controller running Cisco IOS XE Cupertino 17.7.1 or a later release. For more information, see RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72.

Recommended Action:

Implement one of the supported topologies and complete usage reporting. The method you can use to send the RUM report to CSSM and ACK installation depends on the topology you implement. See: Connecting to Cisco SSM, on page 13 and Implementing Smart Licensing Using Policy, on page 27.

CHAPTER 8

Additional References for Smart Licensing Using Policy

Topic	Document Title
For complete syntax and usage information for the commands used in this chapter, see the Command Reference of the corresponding release.	Cisco Catalyst 9800 Series Wireless Controller Command Reference
Cisco Smart Software Manager Help	Smart Software Manager Help
Cisco Smart License Utility (CSLU) installation and user guides	Cisco Smart License Utility Quick Start Setup Guide Cisco Smart License Utility User Guide

CHAPTER 9

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.

Release	Feature	Feature Information
Cisco IOS XE Gibraltar 16.10.1	Smart Licensing	A cloud-based, software license management solution that allows you to manage and track the status of your license, hardware, and software usage trends.
Cisco IOS XE Amsterdam 17.3.2a	Smart Licensing Using Policy	An enhanced version of Smart Licensing, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use. Starting with this release, Smart Licensing Using Policy is automatically enabled on the device. This is also the case when you upgrade to this release. By default, your Smart Account and Virtual Account in CSSM is enabled for Smart Licensing Using Policy.
	Cisco Catalyst Center Support for Smart Licensing Using Policy	Cisco Catalyst Center supports Smart Licensing Using Policy functionality starting with Cisco Catalyst Center Release 2.2.2. When you use Cisco Catalyst Center to manage a product instance, Cisco Catalyst 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 Controller, on page 10. For information about this topology, see Connected to CSSM Through a Controller, on page 18 and Workflow for Topology: Connected to CSSM Through a Controller, on page 31.

Release	Feature	Feature Information
Cisco IOS XE Amsterdam 17.3.3	Smart Software Manager On-Prem (SSM On-Prem) Support for Smart Licensing Using Policy	SSM On-Prem is an asset manager, which works in conjunction with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM. For information about the compatible SSM On-Prem and product instance versions, see: Cisco Smart Software Manager On-Prem (SSM On-Prem), on page 11. For an overview of this topology, and to know how to implement it see SSM On-Prem Deployment, on page 21 and Workflow for Topology: SSM On-Prem Deployment, on page 36. For information about migrating from an existing version of SSM On-Prem, to one that supports Smart Licensing Using Policy, see Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy, on page 67.
Cisco IOS XE Bengaluru 17.4.1	Option to opt-out of AIR DNA licenses and change in default license level for EWC-APs.	The option to opt-out of purchasing an AIR DNA license was introduced. This option is available only through the Cisco Commerce portal. When you opt-out, you use only the AIR Network Essentials license, and Smart Licensing Using Policy functionality is disabled on the product instance. For more information, see the *Configuring an AIR License* section in this guide. Starting with this release, the default license on an EWC-AP was also changed to AIR Network Essentials.

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.7.1	RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller	If you are using a Cisco Catalyst 9800-CL Wireless Controller, you must complete RUM reporting and ensure that the Acknowledgment (ACK) is made available on the product instance - at least once. This is to ensure that correct and up-to-date usage information is reflected in CSSM. For more information, see RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72.
	Factory-installed trust code	For new hardware orders, a trust code is now installed at the time of manufacturing. Note: You cannot use a factory-installed trust code to communicate with CSSM. See Trust Code, on page 6.
	Support for trust code in additional topologies	A trust code is automatically obtained in topologies where the product instance initiates the sending of data to *CSLU* and in topologies where the product instance is in an air-gapped network. See:Trust Code, on page 6
	RUM Report optimization and availability of statistics	RUM report generation and related processes have been optimized. This includes a reduction in the time it takes to process RUM reports, better memory and disk space utilization, and visibility into the RUM reports on the product instance (how many there are, the processing state each one is in, if there are errors in any of them, and so on). See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller, on page 72. Also see the **show license rum**, **show license all**, and **show license tech** commands in the command reference of the applicable release.
	Support to collect software version in a RUM report	If version privacy is disabled (**no license smart privacy version** global configuration command), the Cisco IOS-XE software version running on the product instance and Smart Agent version information is *included* in the RUM report. See the **license smart** global configuration command in the command reference of the applicable release.
	Account information included in the ACK and **show** command outputs	

Release	Feature	Feature Information
		A RUM acknowledgement (ACK) includes the Smart Account and Virtual Account that was reported to, in CSSM. You can then display account information using various **show** commands. The account information that is displayed is always as per the latest available ACK on the product instance. See the **show license all**, **show license summary**, **show license status**, and **show license tech** commands in the command reference of the applicable release.
	CSLU support for Linux	CSLU can now be deployed on a machine (laptop or desktop) running Linux. See Cisco Smart License Utility (CSLU), on page 10, Workflow for Topology: Connected to CSSM Through CSLU, on page 27, and CSLU Disconnected from CSSM, on page 17.

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	New mechanism to send data privacy related information	A new mechanism to send all data privacy related information was introduced. This information is no longer included in a RUM report.If data privacy is disabled (**no license smart privacy** { **all** | **hostname** | **version**} global configuration command), data privacy related information is sent in a separate sync message or offline file. Depending on the topology you have implemented, the product instance initiates the sending of this information in a separate message, or CSLU and SSM On-Prem initiates the retrieval of this information from the product instance, or this information is saved in the offline file that is generated when you enter the license smart save usage privileged EXEC command In the command reference of the corresponding release, see the license smart (global config) command.
	Hostname support	If you configure a hostname on the product instance and disable the corresponding privacy setting (**no license smart privacy hostname** global configuration command), hostname information is sent from the product instance. Depending on the topology you have implemented, the hostname information is received by CSSM, and CSLU or SSM On-Prem. It is then displayed on the corresponding user interface. In the command reference of the corresponding release, see the **license smart** (global config) command.
	Support for trust code in additional topologies	A trust code is automatically obtained in topologies where CSLU initiates the retrieval of data from the product instance. See: Trust Code, on page 6, Connected to CSSM Through CSLU, on page 13, CSLU Disconnected from CSSM, on page 17.
	RUM Report Throttling	

Release	Feature	Feature Information
		For all topologies where the product instance initiates communication, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. The affected topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated communication), *CSLU Disconnected from CSSM* (product instance-initiated communication), and *SSM On-Prem Deployment* (product instance-initiated communication). You can override the reporting frequency throttling, by entering the **license smart sync** command in privileged EXEC mode. This triggers an on-demand synchronization with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. RUM report throttling also applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to *all* subsequent releases. See: Connected to CSSM Through CSLU, on page 13, Connected to CSSM Through CSLU, on page 13, CSLU Disconnected from CSSM, on page 17, and SSM On-Prem Deployment, on page 21.