

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

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.

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 9800-80 Wireless Controller	Cisco IOS XE Amsterdam 17.3.2a

Cisco Catalyst Wireless Controllers	When Support for Smart Licensing Using Policy was Introduced
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 CW9800H1 Wireless Controller	Cisco IOS XE Dublin 17.14.1
Cisco Catalyst CW9800H2 Wireless Controller	Cisco IOS XE Dublin 17.14.1
Cisco Catalyst CW9800M Wireless Controller	Cisco IOS XE Dublin 17.14.1
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. If you want to return an SLR authorization code, see Removing and Returning an Authorization Code.

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 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.

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.

- 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.

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.