Information About Smart Licensing Using Policy

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

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

Benefits of Smart Licensing Using Policy

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

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

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

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

Benefits of Smart Licensing Using Policy

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

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

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

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

Supported Products

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

Table 1: Smart Licensing Using Policy: Supported Products

Product Category	Product Series	Introductory Release When Support was Introduced
Cisco Aggregation, Integrated, and Cloud Service Routers		
	Cisco 1000 Series Integrated Services Routers	Cisco IOS XE Amsterdam 17.3.2
	Cisco 4000 Series Integrated Services Routers	Cisco IOS XE Amsterdam 17.3.2
	Cisco ASR 1000 Series Aggregation Services Routers	Cisco IOS XE Amsterdam 17.3.2
	Cisco Cloud Services Router 1000v (Requires upgrade from a CSRv .bin image to a Catalyst 8000V software image.)	Cisco IOS XE Bengaluru 17.4.1
	Cisco Integrated Services Virtual Router (Requires upgrade from an ISRv .bin image to a Catalyst 8000V software image.)	Cisco IOS XE Bengaluru 17.4.1
Cisco Catalyst 8000 Edge Platforms Family		
	Catalyst 8200 Series Edge Platforms	Cisco IOS XE Bengaluru 17.4.1
	Catalyst 8300 Series Edge Platforms	Cisco IOS XE Amsterdam 17.3.2
	Catalyst 8500 Series Edge Platforms	Cisco IOS XE Amsterdam 17.3.2
	Catalyst 8000V Edge Software	Cisco IOS XE Bengaluru 17.4.1
Cisco Terminal Services Gateways		

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

Key Concepts of Smart Licensing Using Policy

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

License Enforcement Types

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

Unenforced or Not Enforced

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

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

Enforced

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

Export-Controlled

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

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

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

License Duration

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

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

Authorization Code

The Smart Licensing Authorization Code (SLAC) allows activation and continued use of a license that is export-controlled or enforced. Installing SLAC on a device enables the use of the license.

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

Table 2: License That Requires SLAC

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

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

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

Table 3: Throughput Level That Requires SLAC

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

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

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

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

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

SLR Authorization Codes

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

Policy

A policy provides the product instance with these reporting instructions:

- License usage report acknowledgement requirement (Reporting ACK required): The license usage report is known as a RUM Report and the acknowledgement is referred to as an ACK. This is a yes or no value which specifies if the report for this product instance requires CSSM acknowledgement or not. The default policy is always set to **yes**. For more information, see RUM Report and Report Acknowledgement.
- First report requirement (days): The first report must be sent within the duration specified here. If the value here is zero, no first report is required.
- Reporting frequency (days): The next RUM report must be sent within the duration specified here. If the value here is zero, it means no further reporting is required *unless* there is a usage change.
- Report on change (days): In case of a change in license usage, a report must be sent within the duration specified here. If the value here is zero, no report is required on usage change.

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

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

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

Understanding Policy Selection

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

`Cisco default` is the default policy that is always available in the product instance. If no other policy is applied, the product instance applies this default policy. The table below (Table 4: Policy: Cisco default, on page 7) shows the `Cisco default` policy values.

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

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

Table 4: Policy: Cisco default

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

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

RUM Report and Report Acknowledgement

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

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

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

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

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

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

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

RUM report generation, storage, and management

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

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

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

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

Trust Code

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

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

There are multiple ways to obtain a trust code.

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

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

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

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

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

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

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

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

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