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 Fuji 16.9.1	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. Starting from this release, Smart Licensing is the default and the only available method to manage licenses. Starting from Cisco IOS XE Fuji 16.9.1, the Right-To-Use (RTU) licensing mode is deprecated, and the associated **license right-to-use** command is no longer available on the CLI. This feature was introduced on: • Cisco Catalyst 9300 Series Switches • Cisco Catalyst 9400 Series Switches • Cisco Catalyst 9500 Series Switches

Release	Feature	Feature Information
Cisco IOS XE Fuji 16.9.2	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. Starting from this release, Smart Licensing is the default and the only available method to manage licenses. Starting from Cisco IOS XE Fuji 16.9.1, the Right-To-Use (RTU) licensing mode is deprecated, and the associated **license right-to-use** command is no longer available on the CLI. This feature was introduced on Cisco Catalyst 9200 Series Switches.
Cisco IOS XE Gibraltar 16.11.1	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. Smart Licensing is the default and the only available method to manage licenses. This feature was introduced on Cisco Catalyst 9600 Series Switches.

Release	Feature	Feature Information
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 DNA Center support for Smart Licensing Using Policy	Cisco DNA Center supports Smart Licensing Using Policy functionality starting with Cisco DNA Center Release 2.2.2. When you use Cisco DNA Center to manage a product instance, Cisco DNA Center connects to CSSM, and is the interface for all communication to and from CSSM. For information about the comptabile controller and product instance versions, see Controller. For information about this topology, see Workflow for Topology: Connected to Cisco SSM Through a Controller.
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 comptabile SSM On-Prem and product instance versions, see: SSM On-Prem Deployment. For an overview of this topology, see Workflow for Topology: SSM On-Prem Deployment. For information about migrating from an exisiting version of SSM On-Prem, to one that supports Smart Licensing Using Policy, see Migrating to a Version of SSM On-Prem That Supports Smart Licensing Using Policy.

Release	Feature	Feature Information
Cisco IOS XE Bengaluru 17.6.2	Export Control Key for High Security (HSECK9 key)	The HSECK9 key was introduced on the Cisco Catalyst 9300X Series Switches. The HSECK9 key is an export-controlled license, which authorizes the use of cryptographic features that are restricted by U.S. export control laws. If you want to use a restricted cryptographic feature, an HSECK9 key is required. See Authorization Code. On product instances where the HSECK9 key is supported, you can obtain and install SLAC by implementing one of these topologies: • Workflow for Topology: Connected to Cisco SSM Through CSLU • Workflow for Topology: Connected Directly to Cisco SSM • Workflow for Topology: CSLU Disconnected from Cisco SSM • Workflow for Topology: No Connectivity to Cisco SSM and No CSLU • Workflow for Topology: SSM On-Prem Deployment

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.7.1	CSLU support for Linux	Support for CSLU deployment on a machine (laptop or desktop) running Linux. See Cisco Smart License Utility (CSLU), Workflow for Topology: Connected to Cisco SSM Through CSLU, and Workflow for Topology: CSLU Disconnected from Cisco SSM.
	Factory-installed trust code	For new hardware orders, Cisco installs a trust code at the time of manufacturing. For more information, see Trust Code.
	Trust code request and installation 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 • Workflow for Topology: Connected to Cisco SSM Through CSLU and Tasks for Product Instance-Initiated Communication • Workflow for Topology: CSLU Disconnected from Cisco SSM and Tasks for Product Instance-Initiated Communication • Workflow for Topology: No Connectivity to Cisco SSM and No CSLU and Workflow for Topology: No Connectivity to Cisco SSM and No CSLU • In the command reference of the corresponding release, see the **license smart** privileged EXEC command.
	Ability to save SLAC request and return in a file in an air-gapped network	

Release	Feature	Feature Information
		Option to save a SLAC request file on the product instance. The SLAC request file must be uploaded to CSSM and the file containing the SLAC code can then be downloaded and installed it on the product instance - the same as a RUM report and ACK. With this method you do not have to gather and enter the required details on the CSSM Web UI to generate a SLAC Similarly, an authorization code that is saved to a file can also be uploaded the same way as a RUM report. In the command reference of the corresponding release, see the **license smart** privileged EXEC command. See Workflow for Topology: No Connectivity to Cisco SSM and No CSLU and Workflow for Topology: No Connectivity to Cisco SSM and No CSLU.
	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 the Smart Agent version information is *included* in the RUM report. In the command reference of the corresponding release, see the **license smart** global configuration command.
	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 Report and Report Acknowledgement, Upgrades Within the Smart Licensing Using Policy Environment, and Downgrades Within the Smart Licensing Using Policy Environment. In the command reference of the corresponding release, see the **show license rum**, **show license all**, and **show license tech** privileged EXEC commands.
	Account information included in **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. In the command reference of the corresponding release, see the **show license summary**, **show license status**, **show license all**, and **show license tech** privileged EXEC commands.
Cisco IOS XE Cupertino 17.7.1	Smart Licensing Using Policy	Smart Licensing Using Policy was implemented on the following product instances: • C9500X-28C8D, which was introduced in this release. C9500X-28C8D is part of the new Cisco Catalyst 9500X Series Switches, which is still part of the overall Cisco Catalyst 9500 Series Switches. • Catalyst 9600 Series Supervisor Engine 2 (C9600X-SUP-2), which was introduced this release • Cisco Catalyst 9400 Series Supervisor Modules 2 and 2XL (C9400X-SUP-2 and C9400X-SUP-2XL), which were introduced in this release

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.8.1	Export Control Key for High Security (HSECK9 key)	This feature was implemented on the following product instances: • Cisco Catalyst 9500X Series Switches • Catalyst 9600 Series Supervisor Engine 2 with associated line cards. See Authorization Code. On product instances where the HSECK9 key is supported, you can obtain and install Smart Licensing Authorization Code (SLAC) for the HSECK9 key, by implementing one of these topologies: • Workflow for Topology: Connected to Cisco SSM Through CSLU • Workflow for Topology: Connected Directly to Cisco SSM • Workflow for Topology: CSLU Disconnected from Cisco SSM • Workflow for Topology: No Connectivity to Cisco SSM and No CSLU • Workflow for Topology: SSM On-Prem Deployment

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 configuration 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 configuration command.
	Trust code request and installation	From this release, trust code request and installation is supported in the CSLU-initiated mode as well. See Trust Code, Workflow for Topology: Connected to Cisco SSM Through CSLU, and Workflow for Topology: CSLU Disconnected from Cisco SSM.
	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 Workflow for Topology: Connected to Cisco SSM Through CSLU, Workflow for Topology: Connected Directly to Cisco SSM, Workflow for Topology: CSLU Disconnected from Cisco SSM, and Workflow for Topology: SSM On-Prem Deployment.
	Smart Licensing Using Policy	This feature was implemented on C9200CX-12P-2X2G, C9200CX-8P-2X2G, and C9200CX-12T-2X2G models of the Cisco Catalyst 9200CX Series Switches.

Release	Feature	Feature Information
Cisco IOS XE Dublin 17.11.1	Export Control Key for High Security (HSECK9 key)	This feature was implemented on Cisco Catalyst 9400 Series Supervisor 2 and 2XL Modules (C9400X-SUP-2 and C9400X-SUP-2XL). See Authorization Code. On product instances where the HSECK9 key is supported, you can obtain and install Smart Licensing Authorization Code (SLAC) for the HSECK9 key, by implementing one of these topologies: • Workflow for Topology: Connected to Cisco SSM Through CSLU • Workflow for Topology: Connected Directly to Cisco SSM • Workflow for Topology: CSLU Disconnected from Cisco SSM • Workflow for Topology: No Connectivity to Cisco SSM and No CSLU • Workflow for Topology: SSM On-Prem Deployment

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