The bridge to possible

Data sheet
Cisco public

Cisco Smart Licensing Security

(updated November 2020)

Contents

Introduction

In a move to simplify software license management for our customers, Cisco has implemented Cisco® Smart Software Licensing, a flexible software licensing model that streamlines the way customers activate and manage Cisco software licenses across their organization. Smart Licenses provide greater insight into software license ownership and consumption, so customers know what they own and how it is being used. Gone are the days of lost or unknown PAKs. Cisco Smart Licensing establishes a pool of licenses or entitlements that can be used across the entire organization in a flexible and automated manner.

Different deployment options for different security profiles

With Smart Licensing, you control the level of security required for your environment. There are multiple options for usage reporting – Cisco understands there is no "one size fits all" approach when it comes to security. You can choose one deployment option, or a mix-and-match approach of options, based on what is most convenient and best suited for your organization.

Direct (at Cisco) license management and reporting

The simplest deployment method is direct cloud access, where a Cisco product sends usage information directly over the Internet or through an HTTP proxy server. If your Cisco products have connectivity to **tools.cisco.com** over the Internet, this solution is by far the simplest, because it requires no additional configuration steps - it works "out of the box."

Mediated (on-premises) license management and reporting

The Cisco Smart Software Manager (SSM) On-Prem license server is most often the go-to solution used by financial institutions, utilities, service providers, and government organizations. Allowing infrastructure devices to have connectivity over the Internet, either directly or through an HTTP proxy server, may violate security policies, requiring an on-premises license management solution.

Using the free download, a customer or partner can deploy the Cisco SSM On-Prem license server to keep device communication contained within the customer's local network. The Cisco SSM On-Prem license server uses a "synchronization process" to exchange license information with Cisco Smart Software Manager (Cisco SSM). This can be accomplished either with an automatic network-based transfer or an offline manual transfer.

Disconnected (License Reservation) license usage

For customers who need to have a full air-gapped environment where a disconnected SSM On-Prem license server is not an option (for example, remote deployments or low-high side operations), the License Reservation option, which requires no ongoing communications or additional infrastructure, may be more efficient. If deploying more than about 30 Cisco devices, the disconnected SSM On-Prem license server deployment model is recommended instead, to simplify license changes and RMA processes.

For the highest degree of security, Cisco offers full offline access through License Reservation. In this environment, all license changes are processed manually. License Reservation uses copy-and-pasted information between the product and Cisco.com to manually check licenses in and out. The functionality is equivalent to node locking, but with Smart License tracking.

Smart Licensing Using Policy

A new deployment method for Smart Licensing simplifies the way end customers activate and manage their licenses. Smart Licensing now supports simpler and more flexible offering structures, allowing customers to have an easier, faster, and more consistent way to purchase, renew, or upgrade their licenses. Based on the product policy, reporting software usage is required, but per device registration and on-going communication with Cisco have been relaxed.

Cisco Smart Licensing online

Cisco is committed to helping our customers and partners by protecting and respecting personal data, no matter where it comes from or where it flows. Cisco complies with mandatory privacy laws worldwide. We have established long-standing security, data protection, and privacy programs, which already included many of the same requirements derived from our commitments to comply with regulations, customer's needs, and our own corporate code of conduct.

Cisco Online Privacy Statement summary

The **Cisco Online Privacy Statement** (https://www.cisco.com/c/en/us/about/legal/privacy-full.html), and this summary, apply to Cisco's websites and our affiliates' websites that link to the Statement. Cisco respects and is committed to protecting your personal information. Our privacy statements reflect current global principles and standards on handling personal information – notice and choice of data use, data access and integrity, security, onward transfer, and enforcement and oversight.

Cisco Data Protection Program

As part of our privacy efforts, we are deepening our commitment to privacy engineering by embedding privacy by design/default principles in the development lifecycle of our offerings, starting from the ideation phase, and including strengthening security controls.

Our data protection program covers data throughout its lifecycle. It begins with security and privacy by design, managing collection, use, processing, and storage; addressing operational needs such as reporting and oversight; and secure disposition or destruction at end of life.

General Data Protection Regulation (GDPR)

The European Union General Data Protection Regulation (GDPR) brings long-anticipated consistency to the data protection landscape in Europe. GDPR embodies the well-recognized privacy principles of transparency, fairness, and accountability. By introducing a risk-based approach, GDPR will enable innovation and participation in the global digital economy while respecting individual rights.

Cisco is certified under both the EU and Swiss–U.S. Privacy Shield. We have achieved accreditation under the EU Binding Corporate Rules with policies fully aligned to GDPR.

Legally and securely transferring data (worldwide)

As part of our privacy efforts, we are deepening our commitment to privacy engineering by embedding privacy by design/default principles in the development lifecycle of our offerings, starting from the ideation phase, and including strengthening security controls.

- **Binding Corporate Rules (BCR):** Cisco's data protection and privacy policies, standards, and related documentation ("BCR-C") have been approved by the European data protection supervisory authorities.
- **EU-U.S. and Swiss-U.S. Privacy Shield:** Cisco is certified under both frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, processing, and cross-border transfer of personal data from the EU and Switzerland to the United States, respectively. (https://www.cisco.com/c/en/us/about/legal/privacy.html)
- **APEC Cross-Border Privacy Rules and PRP Systems:** The U.S. APEC Accountability Agent certified that the Cisco global privacy program complies with the Asia Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPRs) and Privacy Recognition for Processors (PRP) systems.
- **Cisco Master Data Protection Agreement with EU Model Clauses:** To protect the free movement of personal data (both Cisco's and Cisco's customers') as needed around the world, we have made available a Master Data Protection Agreement (MDPA), which we require from our suppliers and offer to our customers.

Smart Licensing data sharing

Cisco loosely follows the ISO 19770 protocol specification for an IT Asset Management (ITAM) platform. As part of this Cisco collects the following data:

- License(s) being used
- Unique device identifications (For hardware, that is usually product IDs and serial numbers. For software, it is often a universally unique identifier [UUID].)
- Serial numbers of devices using the license(s)
- Quantity of licenses being used

Optional data, including the product's host name, can be shared with Cisco to improve your report generation. This is controlled through configuration on the product. If using an SSM On-Prem license server, you can independently choose not to send this information to Cisco. The items you have the option to share are:

- Host name: The host name of the registered Cisco product
- IP address: The IP address of the registered Cisco product
- MAC address: The Media Access Control (MAC) address of the registered Cisco product

Smart Licensing cryptography

Cisco has implemented Certificate Authorities (CAs) to provide a source of publicly trusted identities for clients and servers using Secure Sockets Layer (SSL) and Transport Layer Security (TLS) communications. These Certificate Authorities consist of systems, products, and services that both protect the CA's private key and manage the X.509 certificates (SSL certificates) issued by the Certificate Authority.

Certificates used by Cisco products

Cisco products report feature usage back to Cisco Smart Software Manager (Cisco SSM) (or Cisco SSM On-Prem) to indicate license usage. In order to ensure the validity of the license data Cisco and Cisco products use a number of notable cryptographic certificates:

Cisco Licensing root certificate

- Embedded in Cisco products that include a Smart Agent, this is the root of the trust chain.

Cisco Sub-CA

- Generated by Cisco and sent to the Cisco product during registration.

ID Certificate (IDCERT)

- The IDCERT is generated by Cisco SSM (or Cisco SSM On-Prem) using the product's UDI during the registration process. It is used to verify the product (though its UDI) and, through the product, to validate the signing authority of Cisco SSM or an SSM On-Prem license server. The IDCERT has a lifetime of one year and is automatically renewed every six months.

Signing certificate

- Generated in the SSM or satellite on registration or renewal and sent to the Cisco product. The signing certificate contains the CISCO SSM public key, which is used to verify the signatures on response messages exchanged between a Cisco product and Cisco.

Cisco products with Smart License

Cisco products that support Smart Licensing use the following message to send license usage reports to Cisco license servers.

Request messages sent by the Cisco product

Cisco products use the private key generated during registration to sign all outgoing request messages. Upon receipt, the Cisco license server will use the public key from the Certificate Signing Request (CSR) in registration to verify the signature on any received request message. The certificate is an SHA256 digital signature.

Response messages sent by Cisco license servers (Cisco SSM or Cisco SSM On-Prem)

Cisco license servers (Cisco SSM or Cisco SSM On-Prem) use the private key generated during registration to sign all outgoing response messages. Cisco products then use the public key in the signing certificate received during registration to validate the signature on a received message. The certificate is an SHA256 digital signature. Upon receipt, the Cisco license server will use the Cisco public key from the Certificate Signing Request (CSR) in registration to verify the signature on any received request message.

Verifying data integrity in data exchange

The data is exchanged between the Cisco products, and Cisco SSM is signed with one of the signing certificates listed in this document. To independently audit the signing process, the public key can be extracted from the signing certificate, and through the use a cryptography tool (such as OpenSSL), you can verify the certificates against the signature.

Cisco products with Smart License Using Policy and Managed Service License Agreement (MSLA)

Cisco products that support Smart Licensing Using Policy and Managed Service License Agreement (MSLA) accumulate usage reports in the form of Reported Usage Measurements (RUMs) as defined in ISO 19770, which must then be transferred to Cisco license servers.

Collection of usage data directly from Cisco products

Customers can send usage reports from each Cisco product and uploads to the reports to the Cisco license server. This can be accomplished by configuring the product to directly send usage data to Cisco (push mode) or an authorized Cisco utility, or by using NETCONF/YANG to retrieve the data (pull mode). Pull mode is not supported for MSLA.

Collection of usage data through a Cisco Smart Licensing Utility (CSLU) or SSM On-Prem

Cisco also provides no-cost software options for automation of the data collection from Cisco products. These solutions allow for the products to push (send reports) or pull (retrieve reports) from products. This data is then stored locally to be proxied to the Cisco license server in a store and forward fashion.

Verifying data integrity in usage data exchange

The usage data originating from Cisco products will be signed to ensure data integrity and validated by a Cisco license server to ensure integrity of the data before processing the records. Depending on the deployment options, different keys can be used by a device to generate signatures. The goal is to incrementally enhance the trust between the product and Cisco, as outlined later in this document.

Authorizations

The Smart Licensing Using Policy enables the downloads of authorization codes for export control features in accordance with Cisco trade control.

Policy download

Smart Licensing Using Policy provides a flexible method for reporting. The policy contains the reporting interval required for sending usage reports to Cisco and durations for reporting for perpetual and subscriptions licenses. In certain business situations covered by a Cisco Smart Account, this policy may be changed, and the policy will be downloaded either through a direct connect method or Cisco Smart Licensing Utility (CSLU).

Certificates used by Cisco SSM On-Prem

When you initially register to Cisco SSM, the SSM On-Prem license server sends a registration file that contains Certificate Signing Requests (CSRs) which will be signed by the Cisco License Crypto Service (LCS).

Cisco SSM On-Prem certificates used for Smart Licensing

To ensure the integrity of the Smart License information, Cisco products depend on a number of certificates to validate the locally installed on-premises license server. These certificates are not used for data encryption, but instead are used to establish that the server is authorized and can be trusted. These certificates are signed off the Cisco Licensing Root Certificate and cannot be changed.

During normal operation of the Cisco SSM On-Prem license server, telemetry is exchanged during the initial registration, and subsequent synchronization, between the SSM On-Prem license server and Cisco SSM:

- **Registration Request file:** The SSM On-Prem license server sends a registration request file to Cisco SSM.
- **Registration Authorization file:** After Cisco SSM receives and processes the registration request, Cisco SSM returns an authorization file back to the SSM On-Prem license server indicating that the SSM On-Prem license server has been registered with Cisco SSM and the details of the full synchronization.
- **Synchronization Request file:** The SSM On-Prem license server sends a synchronization request file to Cisco SSM.
- **Synchronization Response file:** After Cisco SSM receives and processes the request, Cisco SSM returns a synchronization response file back to the SSM On-Prem license server indicating that the registration or synchronization has completed.

To ensure the content of the exchanged files maintain their integrity, the files are signed with the signing certificates (listed in this document), when created, and validated when received. To verify the content against the signature, the public key from the signing certificate is used to verify the content against the signature. The signing certificate and signature are Base64-encoded and must be decoded while verifying.

Cisco SSM On-Prem certificates used for communications

In addition to the Cisco Smart License certificates returned, Cisco will also provide a certificate, called a TG_CERT, that is used to accept secure connections and allow the Cisco SSM On-Prem license server to communicate over a secured connection (HTTPS) with Cisco products.

Cisco product security

Cisco product development practices specifically prohibit any intentional behaviors or product features that are designed to allow unauthorized device or network access, exposure of sensitive device information, or a bypass of security features or restrictions. These include but are not limited to:

- Undisclosed device access methods or " backdoors"
- Hardcoded or undocumented account credentials
- Covert communication channels
- Undocumented traffic diversion

Cisco considers such product behaviors to be serious vulnerabilities. Cisco will address any issues of this nature with the highest priority and encourages all parties to report suspected vulnerabilities to the Cisco Product Security Incident Response Team (PSIRT) for immediate investigation. Internal and external reports of these vulnerabilities will be managed and disclosed under the terms of the Cisco Security Vulnerability policy.

Cisco Product Security Incident Response Team (PSIRT)

The Cisco Product Security Incident Response Team (PSIRT) is responsible for responding to Cisco product security incidents. The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of information about security vulnerabilities and issues related to Cisco products and networks.

https://www.cisco.com/c/dam/en_us/about/security/psirt/Cisco-PSIRT-Infographic.pdf‘

Cisco Security Vulnerability Policy

Cisco defines a security vulnerability as an unintended weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of the product. Cisco PSIRT adheres to ISO/IEC 29147. Cisco PSIRT is on call and works 24 hours a day with Cisco customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security vulnerabilities and issues with Cisco products and networks.

https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html

Cisco Security Advisories

The Cisco Security portal provides actionable intelligence for security threats and vulnerabilities in Cisco products and services and third-party products.

https://tools.cisco.com/security/center/publicationListing

Third-party software vulnerabilities

If there is a vulnerability in a third-party software component that is used in a Cisco product, Cisco typically uses the Common Vulnerability Scoring System (CVSS) score provided by the component creator. Cisco may adjust the CVSS score to reflect the impact on Cisco products.

Cisco will consider a third-party vulnerability “high profile” if it meets one or more of the following criteria:

- The vulnerability exists in a third-party component.
- Multiple Cisco products are affected.
- The CVSS score is 5.0 or above.
- The vulnerability has gathered significant public attention.
- The vulnerability is expected to be, or is being, actively exploited.

For high-profile, third-party vulnerabilities, Cisco will begin assessing all potentially affected products that have not reached end-of-support (with priority given to those products that have not reached end-of-software-maintenance) and will publish a Security Advisory within 24 hours after Cisco classifies the vulnerability as high profile. All known affected Cisco products will be detailed in an update to the initial Security Advisory, which will be published within seven days of Cisco's initial disclosure. A Cisco bug will be created for each vulnerable product so that registered customers can view them via the Cisco Bug Search Toolkit. Third-party vulnerabilities that are not classified as high profile will be disclosed in a release note enclosure.

Cisco SSM On-Prem application security

The Cisco SSM On-Prem license server adheres to the internal Cisco Secure Development Lifecycle (SDL), which establishes a repeatable and measurable process designed to increase Cisco product resiliency and trustworthiness.

The combination of tools, processes, and awareness training introduced during the development lifecycle promotes defense-in-depth, provides a holistic approach to product resiliency, and establishes a culture of security awareness.

Each quarter, Cisco releases an update for the SSM On-Prem license server that contains features and bug fixes as well as available critical and high common vulnerabilities and exposures (CVEs) reported against third-party software. Customers are encouraged to keep the SSM On-Prem license server updated to the latest software version to ensure the highest level of product security.

Cisco Smart Licensing products

Product communication

Smart-enabled Cisco products periodically send information about license consumption to either the Cisco Smart Software Manager (Cisco SSM) at Cisco or, if configured, to your Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem) license server. The information sent and the formats in which it is sent, are identical regardless of the destination.

By default, products are preconfigured to communicate with Cisco SSM at Cisco. If needed, the product can be manually configured to change the destination URL to direct traffic to the Cisco SSM On-Prem license server or through a proxy. Please see specific product documentation on how to perform this configuration.

Smart License Message transport

The communication is normally encrypted using HTTPS (HTTP over TLS), which is the default. There is a possible exception by configuring the Cisco product to use straight HTTP to communicate with the Cisco SSM On-Prem license server or a proxy. The only reason to do this would be to capture packets locally for decoding and inspection. All communication with Cisco's back end, whether a Cisco product directly to Cisco SSM or the SSM On-Prem license server to Cisco SSM, should be encrypted using HTTPS. If a Cisco product attempted an unencrypted HTTP communication, the session would fail. Because Smart Licensing relies on the product's implementation of TLS, the TLS version will vary based on what version the product supports.

During registration, the Cisco product will create a public/private key pair and a Certificate Signing Request (CSR). The public key is sent to Cisco SSM or the SSM On-Prem license server in the CSR. The Cisco product signs outgoing messages with the private key. Cisco SSM (or Cisco SSM On-Prem) validates the signature with the public key.

Smart Call Home

To send the Smart License Messages to Cisco, Cisco SSM uses Smart Call Home API endpoints to relay the Smart License message to the Cisco SSM server. While some products can also send Smart Call Home information for product improvement and troubleshooting, Smart Licensing does not depend on the full capabilities of the Smart Call Home server, and information sent to Cisco can be limited in the Smart Call Home configuration.

Cisco products reporting license usage to Cisco use a well-known Cisco API: tools.cisco.com. The servers are supported through a number of regional load balances to the best server in your geographic location. Cisco products reporting license usage to a Cisco SSM On-Prem license server will use the URL (or IP address) of the license server. Smart Call Home can be configured to use either HTTP or HTTPS based on the URL format. HTTPS is strongly recommended. For details on Smart Call Home, please see: https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/smart_call_home/SCH_Deployment_Guide.pdf

Smart Transport

Smart Transport is another transport protocol available for use with supporting Cisco products. There is no difference from a Smart License "functional" perspective. The introduction of Smart Transport was due to some customers (military) having a policy against using Smart Call Home, to the point that they will not allow the configurations to be present. This meant that we had to have a new method to get Smart License messages to Cisco that did not use the Smart Call Home configuration or the Smart Call Home transport.

The primary difference is in the transport encoding and the API gateway in use, as shown below:

Transport	Product support	API gateway	Access points	Protocol	VRF support	Proxy support
Smart Call Home	All (enabled by default)	tools.cisco.com	Regional	HTTP/HTTPS (SOAP)	Yes	Yes
Smart Transport	Some	smartreceiver.cisco.com	USA	HTTPS (JSON)	No	Yes

For most customers, staying with Smart Call Home is the choice, due to its larger product support, management VRF support, simplified firewall impact, and standardization of configuration.

Smart Transport supports both HTTP (unencrypted) and HTTPS (encrypted) modes based on the URL format. The Cisco SSM On-Prem license server will accept either format, but Cisco SSM will only accept HTTPS sessions.

Smart License protocols and ports

Smart Licensing-related communication is initiated by the Cisco product, and neither the Cisco SSM at Cisco nor a Cisco SSM On-Prem license server can initiate communication. They can only respond to requests from Cisco products. Your firewall rules can, and should, reflect this.

The Cisco product must have reachability to the appropriate endpoint – Cisco SSM or an SSM On-Prem license server. This may require configuring firewall rules and/or any intermediate proxies. The channels and ports used will depend on which transport protocol is used. This is shown below.

Smart Call Home

- HTTP(80): tools.cisco.com
- HTTPS(443): tools.cisco.com

Smart Transport

- HTTPS(443): smartreceiver.cisco.com

Cisco product registration ID Tokens

For Cisco products to register with a Cisco SSM On-Prem license server, they need to be provided a valid ID Token from the target local Virtual Account. When a Cisco product is registered an ID Token is sent by the product to the Cisco license server, where it is looked up and checked to ensure it is valid (not expired or revoked).

Because each ID Token must be unique, they are created by taking a random 32-byte array, referred to as the KEY, along with the local Virtual Account ID and the current timestamp, referred to as the TBS, when the token is created, the result is signed with the KEY, Base64-encoded; the TBS is appended to the string, and it is Base64 encoded once again. This is then stored in the local database.

Message content

The information that is sent from the Cisco product to Cisco SSM or a Cisco SSM On-Prem license server includes:

- The Smart Account and Virtual Account that the product is associated with. This is essentially the product owner and is determined during product registration. This information is initially conveyed by way of the ID Token, and thereafter by the PIID and UDI.
- The product's Unique Device Identifier (UDI). This is usually the Product Type (PID) plus serial number for hardware products. Software-only products use a Universally Unique Identifier (UUID). This is used to prevent double counting of license consumption and in customer reports.
- What licenses are being consumed and in what quantity
- Optionally, the Cisco product can be configured to send its host name to Cisco, or the Cisco SSM On-Prem license server. Host names are used in customer consumable reports. Many customers find host names useful in reports. The alternative is to show consumption by UDI.

A number of the data elements in the Smart License messages follow the format defined in the International Standards Organization (ISO) specification ISO/IEC-19770. ISO/IEC-19770 is a set of standards for IT Asset Management (ITAM) that address managing software assets and related IT assets. Cisco Smart Software Licensing is primarily concerned with three parts of the standard:

- ISO/IEC 19770-2 provides a data standard for software identification tags ("SWID").
- ISO/IEC 19770-3 provides a data standard for software entitlement tags, including usage rights, limitations, and metrics ("ENT").
- ISO/IEC 19770-4 provides a data standard for Resource Utilization Measurement ("RUM").

Cisco uses these standards to define the formats of various data fields such as software identification tags, software entitlement tags, and RUM reports. For a complete description, please see ISO/IEC 19770-5: Overview and Vocabulary (https://www.iso.org/obp/ui/#iso:std:iso-iec:19770:-5:ed-1:v1:en).

Smart Licensing Message types and frequency

There are for major types of Smart Licensing messages initiated by Cisco products:

- Registration, renewal, and deregistration
- Entitlement (license) requests
- Conversion requests
- Specialized requests not supported by all products

Registration: The initial registration registers a Cisco product to a Virtual Account on Cisco SSM or an SSM On-Prem license server using an ID Token generated from that Virtual Account. ID Tokens can only be created by an authorized user of the Virtual Account; this mechanism is used to establish product ownership and trust. Please see ID Tokens for a description of ID Tokens. Along with the ID Token, the Cisco product sends its UDI, the UDI of any high-availability peers, and an ISO 19770-2 software ID tag identifying the product type. A successful registration includes assigning an X.509 ID Certificate, an X.509 signing certificate, and unique Cisco Product Identifier (PIID) to the Cisco product. The ID Certificate is used for identity and trust.

The primary purpose of registration renewals is to renew the ID Certificate. ID Certificates have a one-year life span. By default, Cisco products renew their ID Certificate every six months. Users can issue a command to force a registration renewal immediately upon issuing the command.

Deregistration is just that: it deregisters the product from the Smart Account and Virtual Account.

Entitlement request: Entitlement requests, sometimes called authorization requests, are used to send license usage information to Cisco SSM or an SSM On-Prem license server. Generally, products send entitlement requests any time that license consumption changes (with a slight delay to include multiple changes, if appropriate), and every thirty days to keep usage and status information in synchronization. Some products that typically change license consumption frequently (such as dynamic session count licenses) throttle requests. Typically, these products send requests only once a day, regardless of how many changes occur during that period.

An entitlement request contains the Cisco product UDI, PIID, HA peer information, and what licenses are being consumed. Licenses are identified with an ISO 19770-2 entitlement tag with the count of how many are in use. The response includes the compliance status of the Virtual Account the Cisco product is associated with, the next request interval (always 30 days, but can be over-ridden by the product), and the authorization life (always 90 days).

Conversion request: Conversion requests are normally used to convert after a product is upgraded from a software level that only supports a legacy license model to one that supports Smart Licensing. The message is initiated by a command (CLI: **license smart conversion start** or GUI) on a Cisco product and is used for automatically converting the Cisco product's traditional licenses to Smart Licenses. It is normally only sent once by a product unless there is a failure. The information that is sent with the request include the Cisco product UDI, Cisco product identifier, software ID tag, and conversion data. The conversion data includes any license files that are stored on the Cisco product, the entitlement tags, and the number of any "trust-based" licenses that are configured on the product. A response is returned that includes the success or failure of converting the licenses in the request.

Specialized request: There are also several other types of messages sent for specialized situations and not supported by all products. These are:

- Endpoint reports: used to report endpoints that use licenses, but are reported by multiple controllers, such as a Wireless LAN controller reporting access points
- Export Authorization Requests: requests an Export Authorization Key to allow use of a U.S. Export Controlled functionality. (See "U.S. Export Control," below, for more information.)
- Third-party key requests: request third-party data, typically a license key from a third party
- Poll requests: these poll a Cisco SSM or an SSM On-Prem license server for a response. These are typically made to get a response that was not available when an initial request was made.

Smart License Using Policy Message transport

All communication exchanged between a product and Cisco is encrypted using HTTPS (HTTP over TLS). All information sent by the product includes both usage data and return codes and will be signed by the product and validated by Cisco to ensure the integrity of the data before processing the records. Please see the Appendix for detailed flows.

U.S. Export Control

U.S. Export Control regulations prohibit Cisco from shipping some functionalities (typically strong encryption of user data at speed) to some entities, approximately governments and military in emerging market countries, unless a special permission, called an Export License, is granted. There are regulatory implications of shipping restricted functionality to any entity and special rules and limitations for embargoed entities and entities under sanction. Adherence to these regulations is not optional and is fully supported by Cisco. Licensing has been one of the primary mechanisms that has been used to ensure regulatory compliance. For a full description, please see: https://www.cisco.com/c/en/us/about/legal/global-export-trade.html.

There are two types of export checks that are done. The first is performed when the Smart Account is set up, at which time Cisco attempts to determine any export related restrictions associated with the company which will own the Smart Account, and the second at the time of ordering, when the parties to the transaction are determined and screened. In some cases, and with some products, these checks are enough to allow a particular customer to enable restricted functionality. In other cases, and with some products, a special Export Authorization Key tied to a particular Cisco product must be installed on the product to allow enablement of the restricted functionality. Export Authorization Requests and responses are used to request and install the required keys.

Third -party licenses

Cisco products have the capability to use Smart Licensing to request license information from outside of Smart Licensing. They are used to retrieve licenses, typically license files, for third-party software capabilities that require licenses. One example would be a collaboration “speech to text” feature that requires a Nuance license.

The third-party license request that comes from a Cisco product includes the product UDI, PIID, who the third party is, what data is requested (key name and/or ID) and any other data required to fulfill the request. The response includes the Virtual Account the product is associated with, confirmation of the UDI and PIID of the Cisco product, and the requested key or keys.

License Reservation

License Reservation is a capability that is supported by some products for fully air-gapped environments where a Disconnected Cisco SSM On-Prem license server is not an option (such as remote deployments and low-high side operations). This option requires no ongoing communications and no additional infrastructure. License Reservation does provide for Smart License tracking. It is roughly equivalent to node locking. Since License Reservation inherently cannot utilize the automatic processes associated with online communication it may entail more operational overhead, especially for operations such as moving licenses between Cisco products or changing license consumption. It amounts to permanently reserving licenses for specific Cisco products until the reservation is either updated or removed from the Cisco product.

License Reservation is accomplished by generating a request code from the Cisco product that is entered into Cisco SSM, and then reserves the required licenses on Cisco SSM. Cisco SSM will then generate an Authorization Code that must be entered into the Cisco product. Removing a License Reservation, to release the licenses for other use, is similarly accomplished by revoking the reservation on the Cisco product, copying the resultant Confirmation Code, and entering the Confirmation Code into Cisco SSM. Cisco SSM will then cancel the reservation. Updating a reservation, to increase or decrease the licenses included in the reservation, is accomplished by navigating to the Cisco product on Cisco SSM and changing the reservation. Cisco SSM will generate a new Authorization Code that must be entered into the Cisco product. The Cisco product will generate a Confirmation Code that can, in turn, be entered into Cisco SSM. At that point Cisco SSM will release any licenses that were removed from the reservation. If no licenses were removed from the reservation, only added to the reservation, entering the Confirmation Code into Cisco SSM is optional.

The License Reservation Request Code is an ASCII string that, except the UDI, is BASE58 encoded so that it can be unambiguously typed. It includes a version, sequence number, product UDI, SW ID tag (hashed to nine characters), and a two-character hash.

The Specific License Reservation Authorization Code is an XML formatted file that contains a signature to prevent tampering. It includes the Virtual Account the product is associated with, the confirming UDI and PIID of the Cisco product and for each reserved license, the license type (perpetual, term, or subscription), entitlement tag, count, start and end date of term or perpetual licenses, license name and description, subscription ID if applicable, and a signature to prevent tampering. The same Authorization Code is the same regardless of whether it is an initial authorization or a change.

The Confirmation Code that is used to confirm changes is a hash that is calculated on the UDI, sequence number, PIID, and timestamp from the SLR authorization code. The hash will be BASE58-encoded. Return Codes that confirm the deletion of a License Reservation also use a BASE58- encoded ASCII string that includes the version, the PIID of the Cisco product, and a signature.

Smart License States

The licensing state machine is transparent to users most of the time. Understanding it is primarily useful in troubleshooting and may be useful to distinguish when states change.

The normal sequence of events when installing a Smart-enabled product or upgrading to Smart Licensing from traditional licensing is shown below.

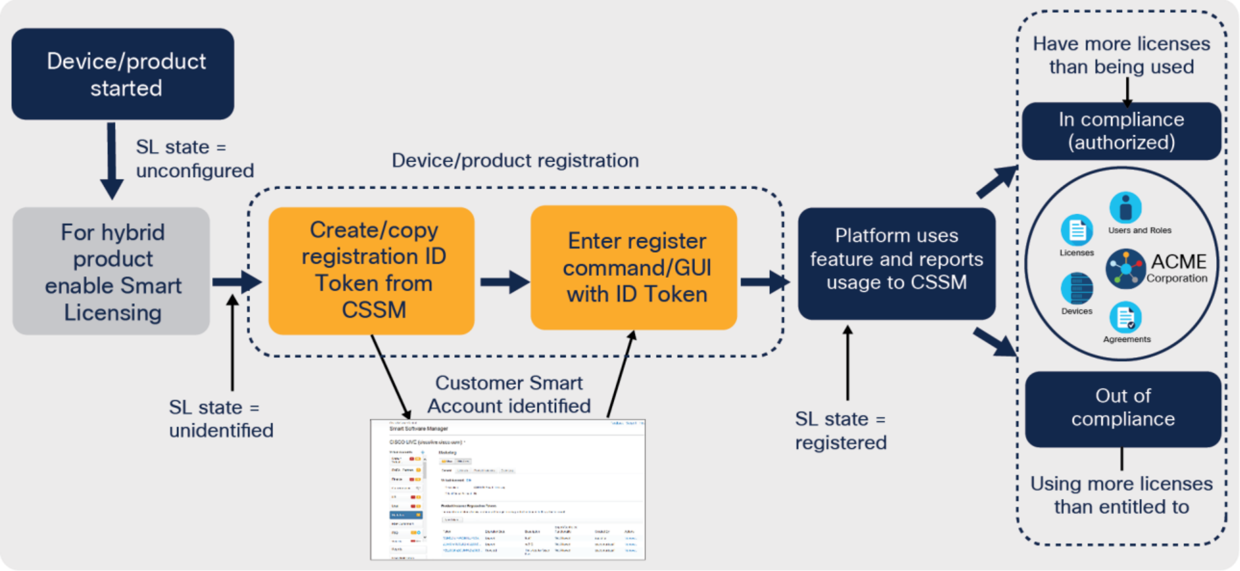

Device/product started
SL state = unconfigured
For hybrid product enable Smart Licensing
SL state = unidentified
Device/product registration
Create/copy registration ID Token from CSSM
Enter register command/GUI with ID Token
Customer Smart Account identified
Platform uses feature and reports usage to CSSM
SL state = registered
Have more licenses than being used
In compliance (authorized)
Users and Roles
Licenses
ACME Corporation
Devices
Agreements
Out of compliance
Using more licenses than entitled to

Figure 1.
Smart Licensing Workflow

The process starts with Smart enablement for products that support both traditional and Smart Licensing. For these products the default is the traditional licensing to minimize disruption during an upgrade. This step is not necessary for products that only support Smart Licensing as they will always be Smart-enabled.

The next step is to register the Cisco product to the desired Smart Account and Virtual Account.1 This is done with an ID Token generated from the Smart Account/Virtual Account (SA/VA) on either Cisco SSM or an SSM On-Prem license server, depending on which the Cisco product is configured to communicate with. An ID Token is simply a way to associate the Cisco product with the SA/VA. ID Tokens are not product specific, and a single ID Token can be used any number of times (unless a limit was set on creation) and with any product type. ID Tokens are only used for initial registration and are not stored on the Cisco product. When ID Tokens expire, that has no impact on Cisco products already registered. ID Token expiration simply means that it cannot be used to register any additional Cisco products.

In most cases, no other action is needed. Registration includes assigning an X.509 ID Certificate to the Cisco product, used for ongoing identity, and establishes trust with Cisco SSM or the SSM On-Prem license server. The Cisco product will automatically send license-consumption information and receive status updates as well as periodically renew ID Certificate lifetimes.

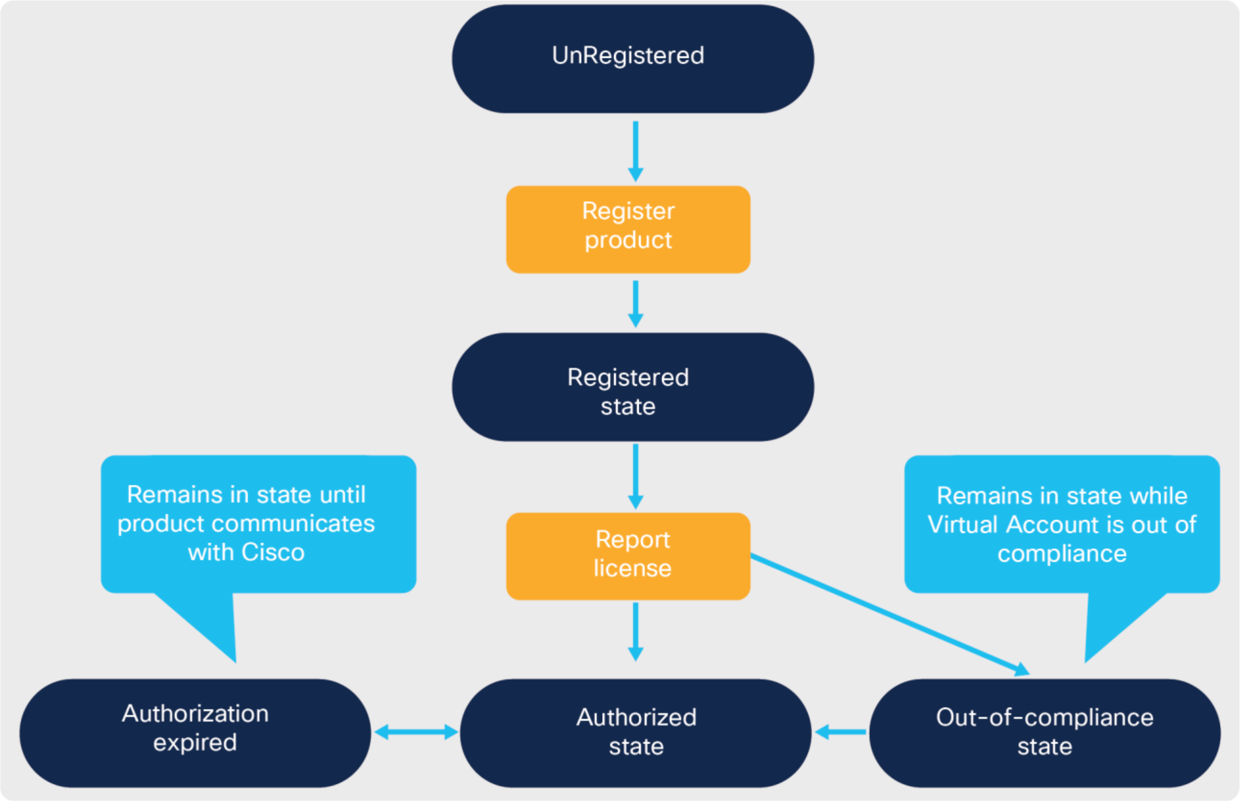


Figure 2.
Smart License Product States

There are a number of states that Smart Licensing could be in. The figure below shows these states.

Unregistered state: The initial Smart Licensing state is "Unregistered." This is the state that the product is in after Smart Licensing is enabled – on boot up for a Smart Only product – but before it is registered to either Cisco SSM or a Cisco SSM On-Prem license server.

Evaluation mode: Often, Cisco products will initially be in "Evaluation mode." Evaluation is a period when an unregistered product is consuming a license. Products have a one-time (life of the product) 90-day evaluation timer that runs when the product is operational. consuming a license, and unregistered. The evaluation mode can be re-entered if there is time left, and any time those three criteria are met. Evaluation can be suspended indefinitely by registering the Cisco product or deconfiguring all license consumption.

Registered state: Once a Cisco product is successfully registered, it will automatically send an authorization request that includes the licenses it is consuming. Authorization requests are sent any time license consumption changes, up or down, and every 30 days, to keep information synchronized.

Authorized state: A Cisco product will then receive a response that includes the license consumption status of the Virtual Account. That is, are there enough licenses in the Virtual Account to satisfy the authorization requests from all the Cisco products associated to that Virtual Account that are consuming that license? If there are enough licenses in the Virtual Account, the license is considered "authorized."

Out-of-compliance state: If not, then the license is considered "out of compliance." Any product that is consuming a license that is out of compliance is in an out-of-compliance state. However, please note that this is the status of the Virtual Account, not the Cisco product, though there may be implications for the Cisco product. Since licenses are pooled within a Virtual Account, individual licenses are not assigned to specific Cisco products (except with License Reservation), and there is no notion of a specific Cisco product being out of compliance while another is authorized. One implication of this is that a Cisco product will only learn of any change in its license status when it sends an authorization request and gets a response. Users have the option to manually force an authorization request (see product documentation for instructions) to shortcut status updates.

A possible scenario that can interrupt the normal processes described above is a communication failure. This is a case when a registered Cisco product is not able to successfully complete an authorization request/response sequence. There are many reasons why a failure could occur, from a downed link to a new firewall rule that isolates the Cisco product. When a communication failure happens, the Cisco product will post an error (console and syslog) and retry the request. The retry interval will vary depending on the authorization state:

- If the product is in an authorized state, the retry is every 23 hours (We don't want to retry at exactly the same time every day.)
- If a product is in an out-of-compliance state, the retry is every 15 minutes for two hours, then back to once every four hours after that.
- If a product is in an authorization-expired state, the retry is once every hour.

Authorization-expired state: Should the communication failure persist over an extended period, the isolated Cisco products' license authorizations may expire. License authorizations are valid for 90 days, and when they expire, Cisco products enter authorization-expired state and post weekly syslog error messages.

ID Certificates that are the cornerstone of Cisco product identity and the basis of trust have a one-year life. These ID Certificates are normally automatically renewed every six months. When a communication failure occurs, the ID Certificates renewal will fail and the Cisco product will retry the renewal every hour until the ID Certificate expires. Additionally, the Cisco product will post syslog messages on each retry communication failure and ID Certificate expiry warnings:

- 60 days before expiration
- 30 days before expiration
- Every week during the last 30 days
- Every day during the last week and
- Every hour on the last day

ID Certificate expiration: Should the communication failure persist long enough, the ID Certificate will expire, resulting in a major error that requires that the product to be re-registered to be corrected. At the point the ID Certificate expires, the Cisco product will return to an unidentified state and reenter evaluation mode. If there is any time left for time evaluation, product instances also enter the unidentified state if they are deregistered.

Product behavior in nonauthorized states

Cisco expects that customers will remedy nonauthorized states and bring the product back into compliance state – providing at least as many licenses in the Virtual Account as are being consumed. This can be done in one of four ways:

1. Address the communications failure such that products can report license usage.
2. Purchase more licenses and have them delivered to the Virtual Account.
3. Transfer licenses from a Virtual Account with an excess of the license to the Virtual Account that has the deficit.
4. Deconfigure the functionality that requires the license on enough Cisco® products associated with the Virtual Account to reduce the license consumption to no more than what is available.

Most products do not take any action due to their Cisco product being in a nonauthorized state. This does not relieve users of the responsibility to bring their Cisco product (and/or) Cisco Smart Account back into compliance. A few products will take some action if they are not returned to an authorized state, primarily by restricting adding functionality.

Please see product documentation or https://www.cisco.com/go/smartlicensing for product-specific behavior in the various states and scenarios.

Evaluation

As described above, evaluation can last up to 90 days over the life of the Cisco product when the product is not registered/unidentified and consuming licenses. Because of U.S. export regulations do not allow Cisco products to operate export-restricted functionality in the initial evaluation period (because Cisco cannot confirm the party operating the Cisco product) unless there is a separate Export Authorization Key installed on the Cisco product or another export compliance mechanism. Most hardware-based products allow unlimited use of non-export-restricted functionality during the evaluation period. Many, but not all, software-based products do have functional limits, typically restricting throughput.

Out of compliance

When a Virtual Account is out of compliance, several alarms and notifications are sent so that users are aware of the situation. Cisco SSM at Cisco will send an email notification to those users who have subscribed to out-of-compliance notifications. Both Cisco SSM and the Cisco SSM On-Prem license server will post errors notifying users when they are out of compliance. Product instances that are consuming an out-of-compliance license will send syslog error messages once a week.

Authorization expired

Most hardware-based products do not take any further action beyond posting syslog errors; however, several software-only products do take action. The typical action is restricting configuring additional functionality.

ID Certificate expired

When a Cisco product's ID Certificate expires and it enters unidentified mode, more products take action than they do when out of compliance or for authorization expiration, though many take no action. Those that do typically restrict adding functionality.

Cisco SSM On-Prem license sever

The Cisco SSM On-Prem license server is a license management system that manages the software licenses across Cisco products. It enables customers to locally manage, track, and renew Cisco Software licenses. It also provides information about license ownership and consumption through a single user interface.

Cisco SSM On-Prem data sharing and privacy

When you first register a Cisco SSM On-Prem license server to Cisco SSM, two files are exchanged between the Cisco SSM On-Prem license server and Cisco SSM:

- **Registration Request file:** The Cisco SSM On-Prem license server sends a registration request file to Cisco SSM.
- **Authorization Response file:** After Cisco SSM receives and processes the registration request, Cisco SSM returns an authorization file back to the Cisco SSM On-Prem license server indicating that the Cisco SSM On-Prem license server has be registered with Cisco SSM and the details of the full synchronization.

During regular synchronization, the Cisco SSM On-Prem license server and Cisco SSM exchange two additional files:

- **Synchronization Request file:** The Cisco SSM On-Prem license server sends a synchronization request file to Cisco SSM.
- **Synchronization Response file:** After Cisco SSM receives and processes the request, Cisco SSM returns a synchronization response file back to the Cisco SSM On-Prem license server indicating that the registration or synchronization has completed.

Cisco SSM On-Prem host OS security

Linux kernel

The Cisco SSM On-Prem license server is based on the CentOS 1804 system, which, utilizing SCAP Security Guide (SSG), has been configured and hardened to meet government-level regulations. The host OS is further secured by ensuring that unused communication ports are closed, by removing "'root'" access, and through the use of a single 'admin' user.

Deployment profiles

The Cisco SSM On-Prem license server provides two different profiles, which can be used when deploying the software;

- **Standard profile:** When logged in, you will be placed into the standard CentOS bash shell with the option to use the Cisco SSM On-Prem license server console. This profile provides the standard security features, usually required by nondefense and finance organizations.
- **DISA STIG profile:** When logged in, you will be placed into the Cisco SSM On-Prem license server On-Prem Console. This console provides a menu of “white-listed” commands and prevents ‘**sudo**’ and/or ‘**root**’ level access. Select this security profile at installation if STIG compliance is required. This profile selection enables security features required for Department of Defense security systems. In addition, the features enabled with this profile selection are compliant with Security Technical Implementation Guide (STIG) standards.

Host OS access

The Cisco SSM On-Prem license server console provides a secure approach for managing the Cisco SSM On-Prem license server though the use of a built-in Command Line Interpreter (CLI). For most customers, the primary differences between the profiles govern the level of access you will have to the host OS in production. The **Standard profile** offers Bash access, while the **DISA STIG profile** offers only the hardened shell, and a higher level of security.

Cisco SSM On-Prem application security

Communications protocol and port

The Cisco SSM On-Prem license server uses Hypertext Transfer Protocol Secure (HTTPS) for secure communication between your network and Cisco. Optionally, products can use either HTTP or HTTPS based on the configured destination URL. The Cisco SSM On-Prem license server uses the default, HTTPS TCP port 443 and 8443, while. HTTP, which is only available to products, uses port 80. The following table outlines the ports currently in use by the Cisco SSM On-Prem license server.

	Products	Browser	High availability
Encrypted	443	8443	5432 (Version 7) 22 (Version 8)
Unencrypted	80	N/A	N/A

Product communication with Cisco SSM On-Prem

The Cisco SSM On-Prem license server replicates only the subset of the Smart Call Home APIs that provide Smart Licensing. Just as with the Cisco SSM license servers, the Cisco SSM On-prem license server provides both HTTPS (443) and HTTP (80), based on your network needs.

Cisco SSM On-Prem communication with Cisco SSM

Cisco SSM On-Prem license server exchanges data with Cisco through the use of a public Cisco Software API, swapi.cisco.com, which is available through an anycast address;

- HTTPS (443): swapi.cisco.com
- IPv4: 146.112.59.25
- IPv6: 2a04:e4c7:fffe::4

In addition to the Cisco Software API, the single-sign-on sever, cloudsso.cisco.com, is also used to authenticate your CCOID during local account registration.

Cisco products registration to Cisco SSM On-Prem

Before the Cisco SSM On-Prem license server can accept a registration request from a Cisco product, the Cisco SSM On-Prem license server has to be register with Cisco Smart Software Manager portal. During the registration process, the Cisco SSM On-Prem license server will receive a set of certificates; a 3-tier certificate, and a 4-tier certificate.

If your Cisco products have not implemented the latest Smart Agent code and only require 3-tier certificates from Cisco SSM, you must wait 48 hours after registering the Cisco SSM On-Prem license server with Cisco SSM. The certificates are manually signed. After 48 hours the 3-tier certificates are embedded in the:local_sub_ca_cert: response field. At this point, the 3-tier devices can then be registered to the Cisco SSM On-Prem license server.

To facilitate automatic validation of the trust chain, the certificate path-length was extended to four levels (4-tier). When using 4-tier certificate, the Smart Agents validates the entire certificates path-length. Received for the Cisco SSM On-Prem license server to ensure it was signed by the Cisco Licensing Root certificate.

During the initial registration, the CSR from a Cisco SSM On-Prem license server to Cisco SSM is signed immediately. However, you must make changes to the product Smart Agents, the Cisco SSM On-Prem license server, and Cisco SSM for the trust chain to work automatically.

Appendix

Terminology

Cisco SSM or CSSM – Cisco Smart Software Manager	**PIDs** – Product IDs
CSR – Certificate Signing Request	**PLR** – Permanent License Reservation
DLC – Device Led Conversion	**SA** – Smart Account
DNS – Domain Name Server	**SBP** – Subscription Billing Platform
FQDN – Fully Qualified Domain Name	**SCH** – Smart Call-Home
LCS – License Crypto-Module Support	**SKU** – Stock Keeping Units
LVA – Local Virtual Accounts	**SLR** – Specific License Reservation
MSLA – Managed Service License Agreements	**TPL** – Third (3rd) Party Licensing
OOC – Out of Compliance	**UUID** – Universally Unique Identifier
PI – Product Instances	**VA** – Virtual Accounts

Data definitions

Customer data: Customer data is all data (including text, audio, video, or image files) that is provided to Cisco in connection with your use of our products or services. Customer data does not include administrative data, payment data, support data, or telemetry data, as defined below.

Administrative data: Administrative data is information about customer representatives provided during signup, purchase, or contracting, or management of products or services. This may include name, address, phone number, IP address, and email address, whether collected at the time of the initial agreement or later during management of the products or services.

Payment data: Payment data is the information that you provide when making a purchase or entering into a licensing agreement for products or services. This may include name, billing address, payment instrument number, the security code associated with your payment instrument, and other financial data.

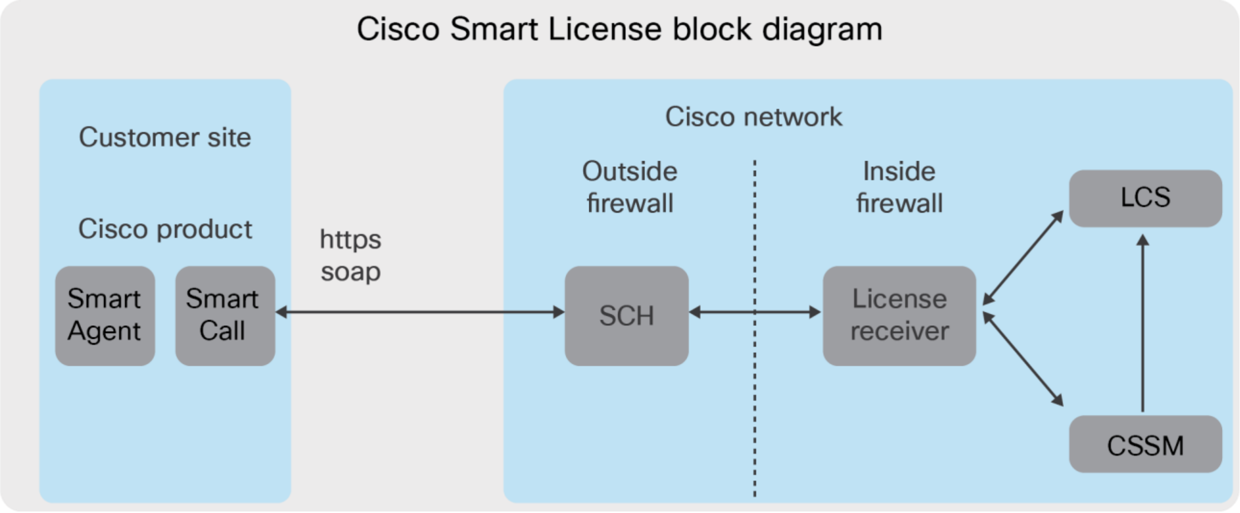
Support data: Support data is the information we collect when you submit a request for support services or other troubleshooting; it may include information about hardware, software, and other details related to the support incident. Examples of these details include authentication information, information about the condition of the product, system and registry data about software installations and hardware configurations, and error-tracking files. Support data does not include log, configuration or firmware files, or core dumps, which are taken from a product and provided to us to help us troubleshoot an issue in connection with a support request.

Telemetry data: Telemetry data is samples of email and web and network traffic, including but not limited to data on email-message and web-request attributes and information on how different types of email messages and web requests were handled by or routed through Cisco products. Email message metadata and web requests included in telemetry data are anonymized or otherwise obfuscated to remove any personally identifiable information prior to disclosure to any unrelated third party.

Usage reports: A form of Reported Usage Measurements (RUMs) as defined in ISO 19770 used for Smart Licensing Using Policy and MSLA usage reporting.

Cisco product protocol overview

This document will explain how the Smart Agent registers with Cisco SSM, how certificates are used, and how messages are signed.



Cisco product registration

Registration request from a Cisco product

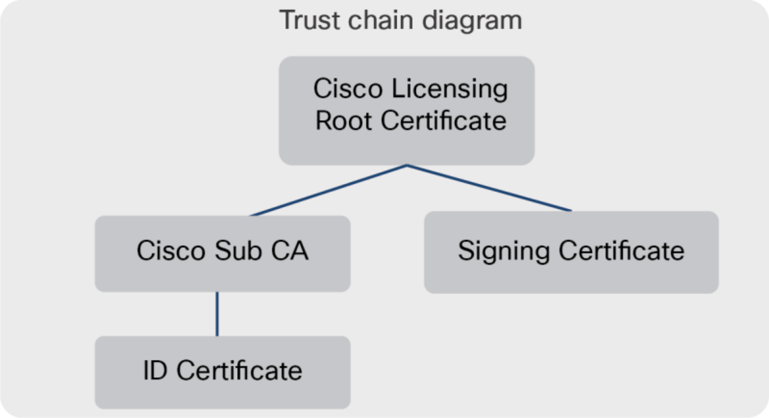
- The customer gets an ID Token from their Cisco Smart Account using the Cisco SSM portal.
  - The ID Token is simply a secure method of identifying a customer.
- Customer uses the registration command on the Cisco product with the ID Token to start the registration process in the Cisco Smart Agent.
  - Note: After registration, the ID Token is no longer needed.
- Smart Agent generates a CSR (Certificate Signing Request).
  - Signature is SHA256.
  - The Cisco product UDI is put in the CN (Common Name) field.
- Smart Agent will generate private/public key pair; the length is 2048.
  - The Cisco Smart Agent uses the private key to sign request messages that it sends to Cisco SSM.
  - The public key goes in the CSR, the Smart Agent saves the private key in its Trusted Store.
  - The Cisco SSM uses the public key to verify signatures on messages it receives.
- Smart Agent sends the following in a registration request to Cisco SSM:
  - CSR
  - ID Token
  - Software ID tag
  - UDI
- The registration message is sent via the Smart Call Home component, which uses HTTPS and SOAP.
  - Smart Call Home is responsible for getting the necessary certificates into the PKI trust pool to secure the HTTPS message.
- After receiving the registration response, the Smart Agent will send an ACK to Cisco SSM so that Cisco SSM knows the Smart Agent received the certificates.

Registration response from the Cisco SSM license server

- Cisco SSM with the help of LCS creates three certificates and a public/private key pair.
  - Cisco SSM will save the private key and sign response messages that it sends, to the Cisco product, with it.
  - Sub-CA
  - Signing certificate
    - Contains the public key that the Cisco Smart Agent will use to verify response message signatures.
  - ID Certificate
- Cisco SSM creates a Cisco Product ID (PIID) to uniquely identify this registration instance.
  - Cisco SSM links the certificates, UDI, and PIID in its data base.
- Cisco SSM will send the certificates and the PIID back to the Cisco product.
- Smart Agent will save the certificates and the PIID in its Trusted Store, so they will be available after a restart.

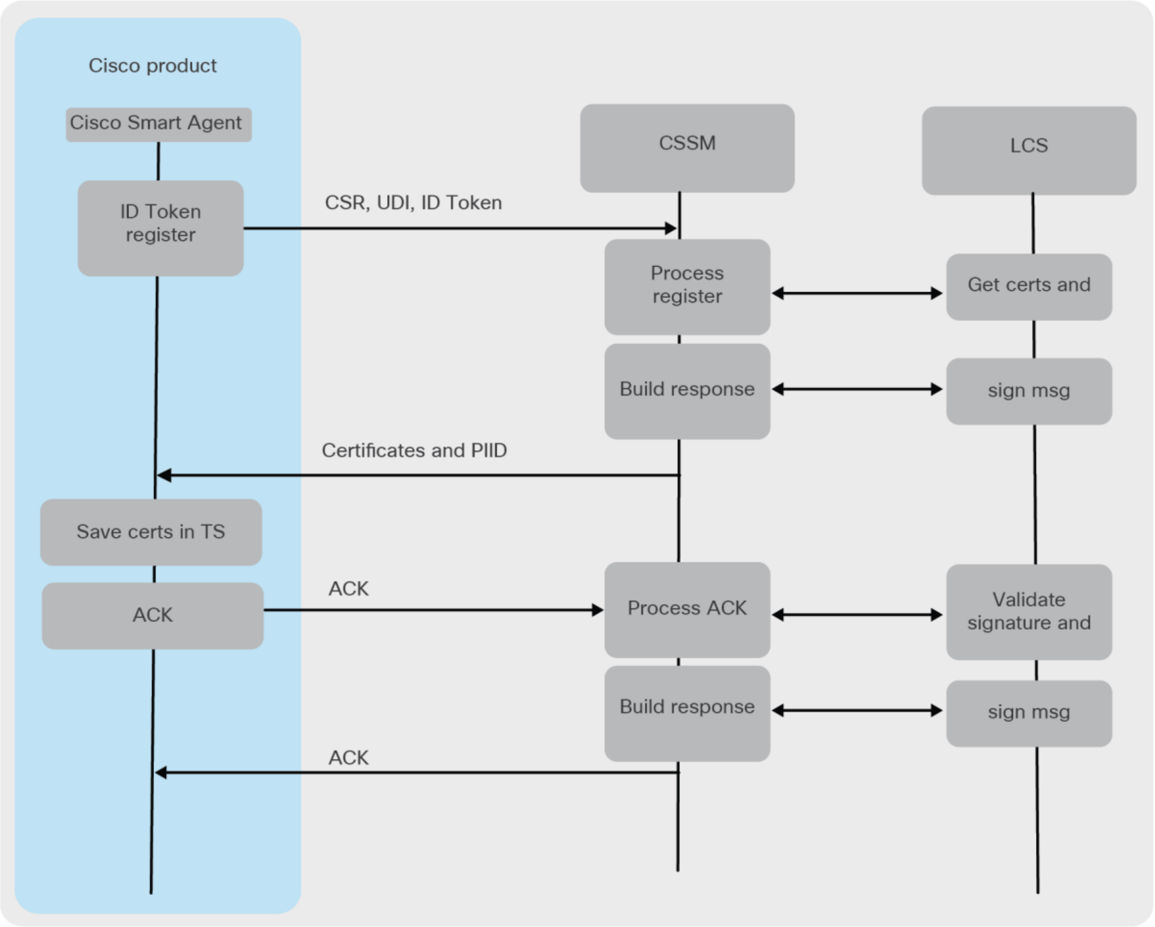
Registration response validation

1. The Cisco Smart Agent will validate the trust chain of the certificates it has received all the way to the root certificate, which is embedded and obfuscated in the Smart Agent code.
2. Validates that the UDI in the ID Certificate matches the UDI of the Cisco product.



3. Saves the certificates in Trusted Store.
4. Sends ACK to the Cisco SSM.

Figure illustrating registration flows



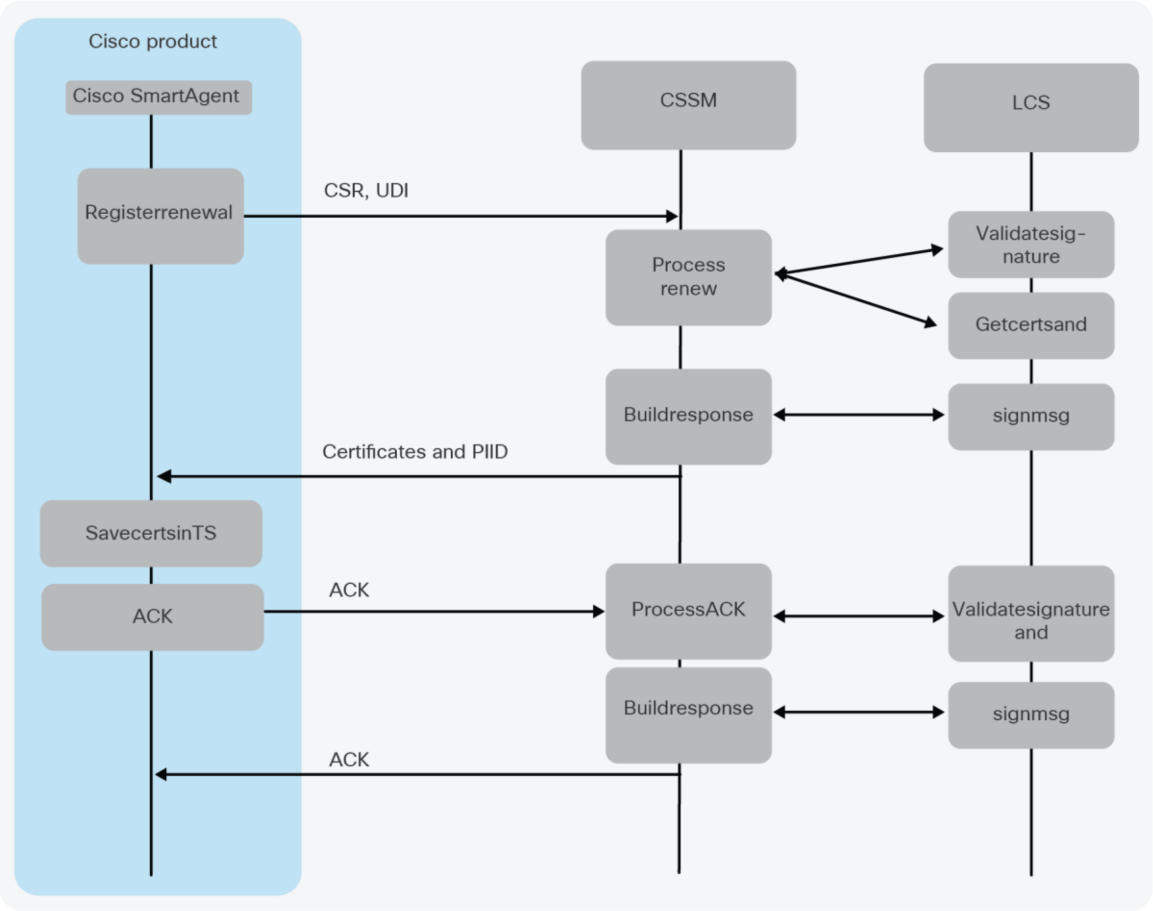
Cisco product registration renewal

The lifetime of an ID Certificate is one year from the day it was issued. The Cisco Smart Agent will automatically try to renew the certificate after six months. When a renewal is triggered on the Cisco Smart Agent, the flow is much the same as a registration:

- Smart Agent generates a new CSR.
- Smart Agent generates a new private/public key pair; the length is 2048.
- Smart Agent sends the following in the renewal request to the Cisco SSM via the Smart Call Home server:
  - CSR
  - Software ID tag
  - UDI
  - Note: There is no ID Token. It is not used or saved after the initial registration.

- Cisco SSM creates three new certificates and a public/private key pair.
    - Sub-CA
    - Signing certificate
    - ID Certificate
- Cisco SSM will send the certificates back to the Cisco product.
- After receiving the registration response, the Cisco Smart Agent will send an ACK to the Cisco SSM so the Cisco SSM knows the Smart Agent received the certificates.
- The Cisco SSM will send a final ACK back to the Smart Agent.
- At this point the Smart Agent will delete the old certificates and start using the new certificates.
- Smart Agent saves the new certificates in its Trusted Store.
- If there was a communications failure somewhere in the process, the Smart Agent will start the renewal process over again, and continue to use the old certificates until it receives that final ACK.

Figure illustrating renewal flows



Cisco product certificates

- Cisco Licensing Root Certificate
  - Embedded and obfuscated in the image that includes the Cisco Smart Agent. This will never change. This is the root of the trust chain.
- Cisco Sub-CA
  - Generated by Cisco and sent to the Smart Agent
- ID (node) Certificate
  - Generated in the Cisco SSM or SSM On-Prem license server on registration or renewal and sent to the Smart Agent
  - Lifetime of one year
  - The ID Certificate also has the Cisco product UDI embedded in it, so we can verify it is for the correct Cisco product. Verified when received and at boot time.
  - Smart Agent will automatically renew this certificate every six months.
- Signing certificate
  - Generated in the Cisco SSM or SSM On-Prem license server on registration or renewal and sent to the Smart Agent
  - Contains the Cisco SSM public key, which is used to verify the signatures on response messages received by the Cisco Smart Agent

Cisco product message signing

- Cisco Smart Agent signing
  - The Cisco Smart Agent will use the private key it generated during registration to sign all outgoing request messages.
  - The Cisco SSM or SSM On-Prem license server will use the public key sent in the CSR during registration to validate the signature on a received message.
  - SHA256 digital signature
- Cisco SSM verification
  - Uses the public key from CSR in registration to verify the signature on any received request message

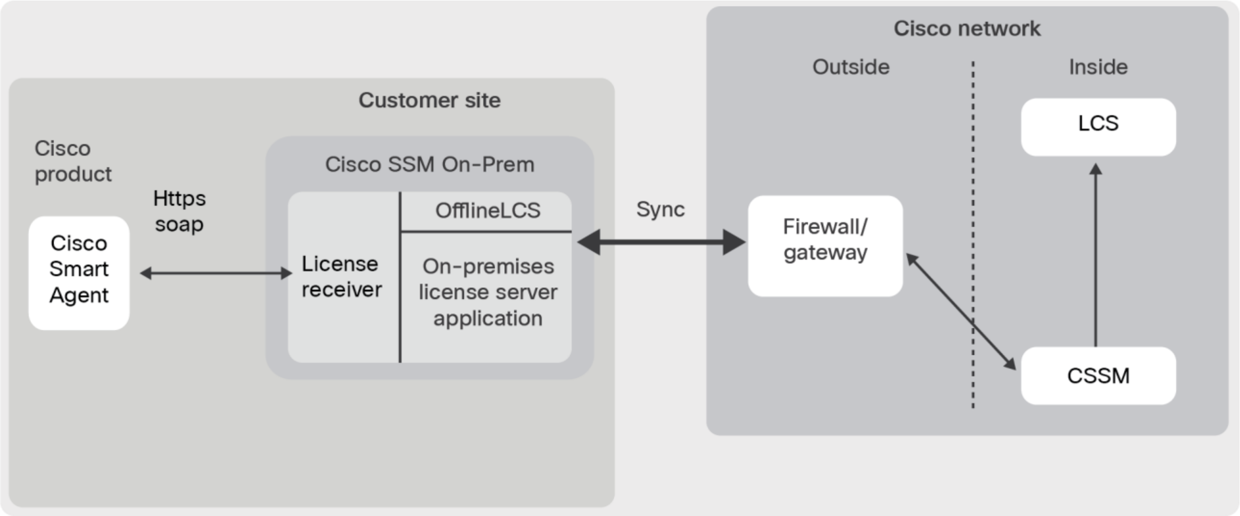
Cisco SSM license server message signing

- Cisco SSM message signing
    - Cisco SSM will use the private key it generated during registration to sign all outgoing response messages.
    - The Cisco Smart Agent will use the public key that is in the signing certificate it received during registration to validate the signature on a received message.
    - SHA256 digital signature
- Smart Agent verification
    - Uses the public key from CSR in registration to verify the signature on any received request message

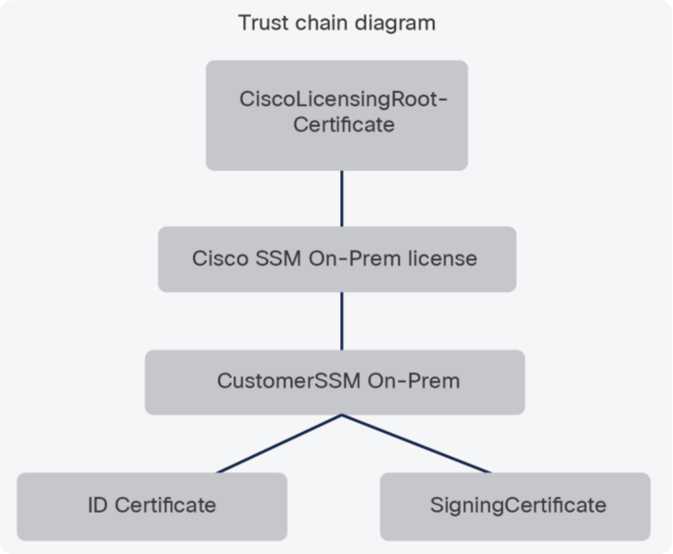
Cisco SSM On-Prem protocol overview

Certificate usage when the Cisco Smart Agent is connected to the Cisco SSM On-Prem license server is almost the same as described above. This section will call out the differences.

Cisco SSM On-Prem license server block diagram



The certificates created when connected to a Cisco SSM On-Prem license server are slightly different. Instead of a 3-tier trust chain, a 4-tier trust chain is used.



Cisco SSM On-Prem license server certificates

- Cisco SSM On-Prem license server Sub-CA
  - Generated in Cisco SSM when a satellite register. Sent to the Cisco SSM On-Prem license server, then later sent to the Cisco Smart Agent when it registers with the Cisco SSM On-Prem license server.
- Customer SSM On-Prem license server Sub-CA
  - Generated in Cisco SSM when a Cisco SSM On-Prem license server registers. Sent to the Cisco SSM On-Prem license server, then later sent to the Cisco Smart Agent when it registers with the Cisco SSM On-Prem license server.

Registration request file

When you initially register your SSM On-Prem license server to Cisco SSM, the Cisco SSM On-Prem license server sends a Registration file to Cisco SSM to establish a link to a specific Virtual Account within your Smart Account. The Registration file contains the key information outlined in Table 1, along with three Certificate Signing Requests (CSRs), which will be signed by Cisco and returned in for use by the Cisco SSM On-Prem license server.

Table 1. Components of the registration request file

Component	Description
instance_id:	This is a 128-bit Universally Unique Identifier (UUID) for the Cisco SSM On-Prem license server, standardized by the Open Software Foundation. For additional information, see the IEEE RFC122.
exported_timestamp:	This is the timestamp when the Registration Request file was created.
lcs_csr:	Certificate signing requests for the LCS (License Crypto Service) used to sign the IDCERT used by Cisco products to establish trust with a Cisco SSM On-Prem license server.
tg_csr:	Certificate signing requests used to secure the HTTPS communication between the Cisco SSM On-Prem license server and Cisco products.
ssms_csr:	Certificate signing requests used to secure the HTTPS communication between the Cisco SSM On-Prem license server user interface and your browser.

Authorization response file

Upon receiving the Registration Request file, Cisco SSM will associate the UUID of the Cisco SSM On-Prem license server with the target Virtual Account and create an Authorization Response file, which will contain key information required for the Cisco SSM On-Prem license server to become fully operational. Specifically of interest, the Authorization Response file has eight different certificates signed by Cisco, which are needed for Cisco product (PI) registration.

Table 2. Authorization response file certificates

Certificate	Description
id_cert:	The Cisco SSM On-Prem license server uses this certificate to identify all Cisco products. CSSM uses this certificate to identify Cisco SSM On-Prem license servers. This certificate is renewed every time the Cisco SSM On-Prem license server and CSSM synchronize.
sub_ca_cert:	The licensing agent installed on any Cisco product uses this certificate to identify the Sub-CA.
signing_cert:	The Cisco SSM On-Prem license server uses this certificate to verify that the **id_cert** was signed by **licensing_root_ca**.
local_sub_ca_cert_1_1:	The local SSM On-Prem license server LCS and Cisco SSM On-Prem license server use this certificate to handle registrations for 4-tier Cisco products For additional information on 3-tier and 4-tier certificates, see the **3-Tier vs. 4-Tier Certificates** section on page 9). The LCS uses this certificate to sign the **id_cert** when sending data to the product. The registration response files return the **sub_ca_cert**.
tg_ssl_cert:	The Transport Gateway (TG) uses this certificate to accepts secure connections and communicate over a secured connection (HTTPS).
tg_issuer_cert:	The TG uses this certificate to establish CA issuer hierarchy. For example, the licensing root certificate (embedded in TG source code) issues the **tg_issuer_cert** which issues the **tg_ssl_cert**.

Certificate	Description
satellite_cert:	The online LCS uses this certificate to sign the **local_sub_ca_cert_1_1** for the local offline LCS
ssms_ssl_cert:	The SSM On-Prem license server uses this certificate to accept secure connections allowing the web browser to communicate to the SSM On-Prem license server over a secured connection (HTTPS).

CSSM also returns the Cisco Smart Account assigned and SSM On-Prem license server information.

Key	Description
status:	Registration success or failure status
uuid:	This is the ID assigned to this SSM On-Prem license server
smart_account:	Name of the Cisco Smart Account registered to
account_domain:	Domain associated with the Smart Account
satellite_name:	Name of the Local Account being registered

Synchronization request file

When a Cisco SSM On-Prem license server synchronizes with CSSM, the SSM On-Prem license server sends a synchronization request file to CSSM. This file contains information about registered Products and license usage and sends CSRs with two certificates to CSSM.

Table 3. Components of the synchronization request file

Component	Description
sync_version:	This is the version of the synchronization code with CSSM.
ssms_version:	This is version of the Cisco SSM On-Prem license server.
id_cert, signing_cert:	CSSM uses these certificates to verify that the SSM On-Prem license server is valid.
collector_id	This is the UUID used to uniquely identify this SSM On-Prem license server.
csr (lcs csr):	This CSR is no longer used.
tg_csr:	The SSM On-Prem license server sends this CSR to CSSM anytime the IP address for the SSM On-Prem license server is changed. The CSR is used to establish secure communication between the Product and the SSM On-Prem license server.
ssms_csr:	The SSM On-Prem license server only sends this CSR to CSSM if the administrator IP address changes or the SSM On-Prem license server is restored to a different host (different IP address). Browser to SSM On-Prem license server.
last-sync:	This is the timestamp of the last time the SSM On-Prem license server and CSSM synchronized and is used to identify the new data since that synchronization.

Component	Description
last_generated:	This is the timestamp of the last time the Synchronization Request file was generated and is used to identify changed data.
virtual_accounts:	These are virtual accounts, products, and licenses registered in the SSM On-Prem license server.

In addition to the base sync control information contained in the Synchronization Request file, the file will also contain product and license usage formation used to update the Cisco Virtual Account. Table 4 defines the components in the Virtual Account section of the Synchronization Request file.

Table 4. Virtual account section of the synchronization request file

Component	Description
:id:	Unique number used to identify the Virtual Account the Cisco SSM On-Prem license server is registered to.
:name:	The name given to the SSM On-Prem license server either at time of registration, or later if changed at CSSM portal.
:product_instances:	Starts the YAML section that identifies the products registered to the SSM On-Prem license server.
:id:	A unique number assigned by SSM On-Prem license server to identify one Cisco product. Each Cisco product will have a number assigned to it at the time the product is registered.
:is_active:	True if the product is currently registered, or false if it is being removed from the Cisco Virtual Account.
:software_tag_identifier:	The software tag as defined by ISO 19770, which identifies the product entitlement.
:udi_pid:	The product identifier (PID).
:hostname:	The hostname configured on the product. [*1]
:ip_address:	The IP address of the device using the license. [*1]
:mac_address:	The MAC address of the device using the license. [*1]
:host_identifier:	Not used.
:license:	Starts the YAML section that list the license in use by the product.
:id:	A unique number used by the registered product to identify the license being used. This number is assigned by SSM On-Prem license server.
:tag:	The software tag as defined by ISO 19770, which identifies the license being used by the product.
:consumed_quantity:	Number of licenses in use.

[*1] By default, the hostname, IP address, and MAC address is sent with the request. If you do not want the Synchronization Request file to include this information, you can be disabled using the Data Privacy Setting (Refer to the SSM On-Prem license server User Guide)

Synchronization response file

After receiving a Synchronization Request file from a Cisco SSM On-Prem license server, CSSM sends the Synchronization response to authorize and synchronizes with SSM On-Prem license server.

A full synchronization occurs when SSM On-Prem license server initially registers with CSSM and is reflected in the Synchronization Response file. The content of the synchronization section of the Synchronization Response file is the same for both the synchronization of the Authorization file and in the Synchronization Response file.

When the SSM On-Prem license server requests a periodic synchronization with CSSM, CSSM provides in the Synchronization Response file certificate information, and information about the virtual accounts and licenses from CSSM to SSM On-Prem license server (Figure 6).

Table 5 lists the certificates in the Synchronization Response File.

Table 5. Certifications in the synchronization request file

Certificate	Description
id_cert	CSSM uses these certificates to verify that the Cisco SSM On-Prem license server is valid.
sub_ca_cert:	The licensing agent installed on any Cisco product uses this certificate to identify the sub-CA.
signing_cert:	The SSM On-Prem license server uses this certificate to verify that the id_cert was signed **by licensing_root_ca**
local_sub_ca_cert:	The SSM On-Prem license server and LCS use this certificate to process registrations for 3-tier Cisco products. This certificate is only included in the Synchronization Response file if the SSM On-Prem license server has been registered for more than 48 hours. For additional information on 3-tier and 4-tier certificates, see the **3-Tier vs 4-Tier Certificates** section on page 9).
local_sub_ca_cert_1_1:	The local SSM On-Prem license server LCS and SSM On-Prem license server use this certificate to process registrations for 4-tier Cisco products. The LCS uses this certificate to sign the **id_cert** when sending data to the product. The registration response files return the **sub_ca_cert.**
tg_ssl_cert:	The Transport Gateway (TG) uses this certificate to accept secure connections and communicate over a secured connection (HTTPS).
tg_issuer_cert:	The TG uses this certificate to establish CA issue hierarchy. For example, the licensing root certificate, embedded in TG source code, issues the **tg_issuer_cert** which issues the **tg_ssl_cert.**
satellite_cert:	The online LCS uses this certificate to sign the **local_sub_ca_cert_1_1** for the local offline LCS.
ssms_ssl_cert:	The SSM On-Prem license server uses this certificate to establish a secure connection between the user's web browser and the Cisco SSM On-Prem license server (HTTPS). This is currently not used.

Table 6. Additional components in the synchronization response file

Component	Definition
collector_instance_id:	This is the ID assigned to this SSM On-Prem license server to uniquely identify the SSM On-Prem license server.
satellite_name:	This is the name of the SSM On-Prem license server that you configured in the **Administration** workspace.
last_generated:	This is the timestamp of the last time the Synchronization Request file was generated and is used to identify changed data.
last-sync:	This is the timestamp of the last time the SSM On-Prem license server and CSSM synchronized and is used to identify the new data since that synchronization.
Synchronization:	These lines identify the Cisco products, types, and licenses registered in the SSM On-Prem license server and synchronized to CSSM.
virtual_accounts:	These lines identify Cisco virtual accounts registered in the SSM On-Prem license server and synchronized to CSSM.

Third-party provider information

Cisco SSM can send provider information in the Synchronization Response file during a full synchronization with the Cisco SSM On-Prem license server. The provider information can indicate third-party support for SpeechView, Apple Push Notifications, and PnP, respectively.

Device-Led Conversion (DLC)

When using Device-Led Conversion (DLC) support, Cisco SSM provides the Cisco SSM On-Prem license server conversion information in the device_conversion_response: section of the Synchronization Response file. The device_conversion_response: section lists status information for each Cisco product registered to the Cisco SSM On-Prem license server that initiated DLC.

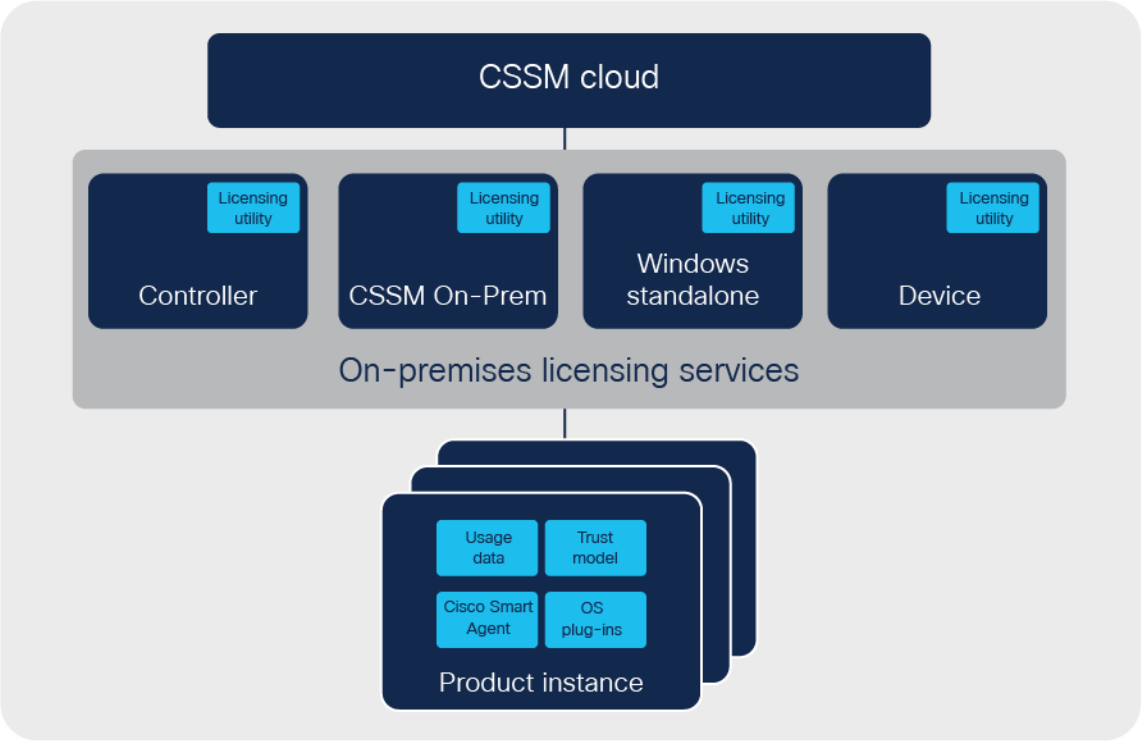
Table 7. Components in the DLC section of the synchronization response file

Component	Description
:udi_pid:	This is the product identifier.
:udi_serial_number:	This is the serial number for the PI.
:conversion_status:	This indicates if the conversion COMPLETED or FAILED.
:status_message:	If the conversion failed, then this field provides information on why the conversion FAILED. This field is blank if the conversion COMPLETED.
:status_message_localized:	If the conversion FAILED, then this field provides information on why the conversion failed in the localized language. This field is blank if the conversion COMPLETED.
:software_tag_identifier:	This is the identification tag for the software loaded onto the **udi_pid**.

Cisco Smart License Using Policy

The new deployment method for Smart Licensing simplifies the way end customers activate and manage their licenses. Smart Licensing now supports simpler and more flexible offering structures, allowing customers to have an easier, faster, and more consistent way to purchase, renew, or upgrade their licenses.

- No evaluation mode at product boot, no registration required at Cisco.com
- No on-going communication with Cisco cloud per device
- Reporting of software use is required.
- No network deployment operating expense



Information sent from product to Cisco

Information sent by the product includes both usage data and return codes and will be signed by the product and validated by Cisco to ensure the integrity of the data before processing the records.

- **Default signature key:** Each Cisco product will have a product specific key.
- **Product signing keys:** When a Cisco product communicates with Cisco, asymmetric keys are used to secure the communications. Each product has a unique private key (RSA-2048) that can be used to sign data sent back to Cisco. The key will be certified and tied to the Cisco root.

Information returned from Cisco to product

Any privileged authorization will need to be signed by Cisco and tied to the entity being authorized. Authorizations could include the rights to use enforced licenses or policies to allow unlimited use of enforced licenses. In every case, this document assumes Cisco is the sole authority to generate these authorizations. To ensure that the signing is secure, Cisco will own the private key (ECDSA) used to sign records. Clients receiving these signed records will have the Cisco root along with the public certificate that can be used to verify these signatures.

Using on-premises licensing services

Cisco provides the ability to collect and report license usage through the Cisco Smart Licensing Utility (CSLU), a standalone Window application, and the SSM On-Prem license server. Each of these software options can support an online or offline connectivity model for usage data reporting.

Cisco SSM On-Prem license server

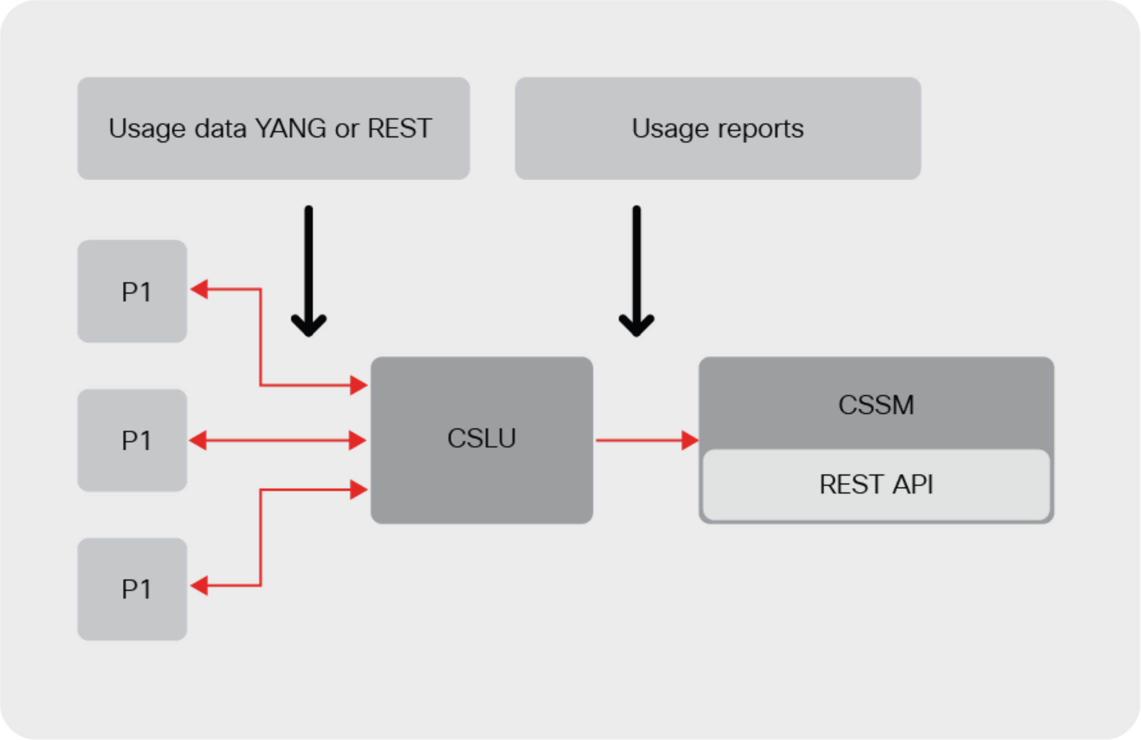
When the Cisco SSM On-Prem is present, it will support the Smart License Using Policy functionality to automate the collection and reporting of usage data, as it supports Smart License today.

Using Cisco DNA Center (DNAC) licensing services

Cisco provides the capability to use Cisco DNA Center (DNAC) for license-usage data collection and, similarly, reporting to the CSLU the behavior given in the figure below. Please see DNAC product literature for a description of this functionality and security aspects.

Cisco Smart Licensing Utility (CSLU)

The Cisco Smart Licensing Utility is a “store and forward” windows application that allows users to collect, and send, license-usage data from Cisco products to the Cisco license server for compliance visibility.



The CSLU usage report format is based on ISO 19770-4 standard RUM report format. It is delivered in JSON format and signed per trust model. The usage report will first be hashed using SHA-256, then the hash will be signed using the supplied key from either the default signature key, or the product signing keys.

ID Token registration and Smart License Using Policy

No registration or ID Token is required in this model. However, for backward compatibility, the current ID Token can be used by the customer, as an option, to establish trust with CSSM, in an online manner, so that signed messages can be exchanged. In this mode, there is no registration expiration, no authorization renewal, no registration renewal, and no registered state.

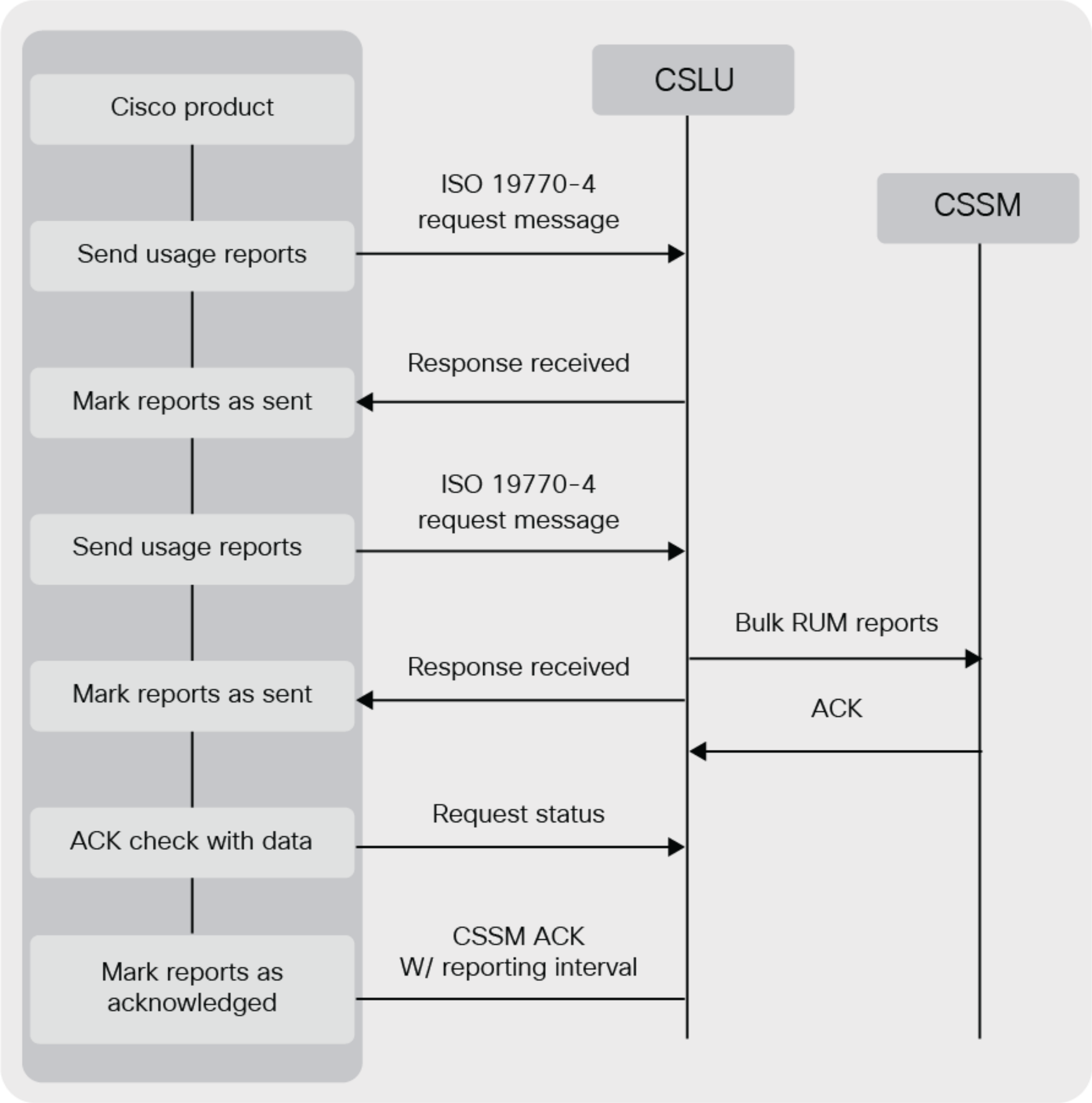
Product sending usage data

When the product sends usage reports directly to the CSLU REST endpoint, the product will need configuration options to set the following:

CSLU endpoint

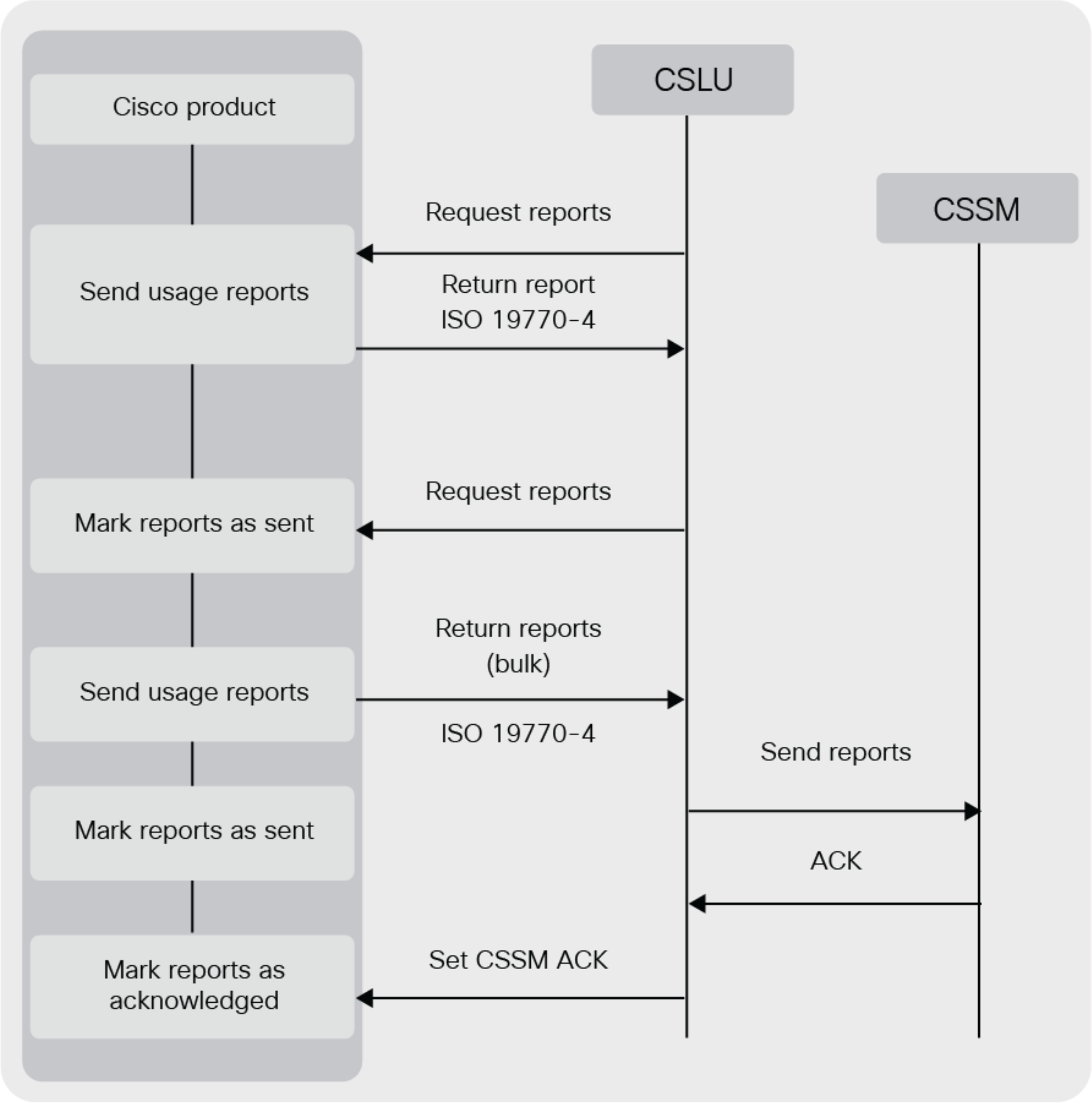
Set reporting period interval

The product will create a usage report that contains many usage reports, and send it to the CSLU. The product will also poll the CSLU for any ACK responses on a regular schedule.



CSLU retrieving usage reports

Note that the communication with CSSM may be online or offline. The CSLU will send any ACK responses to the product when it has them.



Licensing policies

Licensing policies contain the license entitlement parameters, which include, but are not limited, to first-time reporting, report frequency, reporting enforcement, feature enforcement for renewals, export classification, and overuse. While there is a default set of parameters, and then parameters specific to the customer’s EA (Cisco enterprise agreement), or other license agreements with Cisco.

Trust model

Communications are established between the product and the Cisco Smart Licensing Utility (CSLU) and from the CSLU to the Cisco SSM-Cloud. The trust method for communications from the product to the CSLU is considered a responsibility of the customer as part of their network. The trust method for communication from the CSLU to Cisco OAUTH is the method used for Cisco SSM-Cloud APIs in use today. License usage data will be signed using one of the following methods:

1. A trust code is installed.
    a. The factory registration (offline trust establishment) will set up a public/private key pair and install a trust code. The private key will be used to sign the usage reports.
    b. This method is reasonably secure, because the private key on the product is saved in the local trusted store.
    c. This method uses the trust code that is installed on the product at the time of manufacture.
2. There will be a key stored in the product trust store.
    a. The product will use an HMAC-SHA246 signing algorithm.
    b. There is a different key for each product license type.
    c. Generated, encrypted, and base64 are encoded by Cisco.

Basic reporting rules for Smart License Using Policy

Any product that goes through manufacturing will have information installed on the product that describes the licenses purchased. During the manufacturing process these purchased licenses will automatically be reported as in use. The installed policy will define the need for continued reporting.

In general:

1. Reporting is not required for any perpetual license/entitlement that is part of the “purchased info” described above, if the product is not using more counts than are available in the “purchased info.”
2. Reporting is required for subscription licenses and perpetual licenses where the product is using more counts than are available in the “purchased info,” or where the license is not part of the " purchased info.”

References

1. Cisco Security
(https://tools.cisco.com/security/center/home.x)

2. Cisco Root CA 2048 Certification Practice Statement
(https://www.cisco.com/security/pki/policies/CiscoRootCA2048-CPS.pdf

3. Cisco Security Vulnerability Policy
(https://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html)

4. Vendor Vulnerability Reporting and Disclosure Policy
(https://www.cisco.com/c/en/us/about/security-center/vendor-vulnerability-policy.html)

5. Third-Party Code Attestation Policy
(https://www.cisco.com/c/en/us/about/security-center/third-party-attestation-policy.html)

6. Trust and Transparency Center
(https://trust.cisco.com/)

7. Cisco Secure Development Lifecycle
(https://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle.html)

Americas Headquarters	Asia Pacific Headquarters	Europe Headquarters
Cisco Systems, Inc. San Jose, CA	Cisco Systems (USA) Pte. Ltd. Singapore	Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-743812-01 12/20