ı|ııı|ı
CISCO
The bridge to possible

Cisco Smart Licensing Whitepaper

Updated May 2024

Contents

Introduction

In the ever-evolving landscape of network technology management, efficient and streamlined licensing models are essential for organizations to effectively utilize their Cisco software and devices. The advent of Cisco Smart Licensing marked a significant shift away from the complexities of traditional licensing mechanisms, offering a centralized and simplified cloud-based solution. Building upon this innovation, Cisco then introduced an advanced iteration known as Cisco Smart Licensing using Policy. This white paper aims to explore the intricacies of both licensing approaches, underscoring the enhancements in transparency, control, and operational flexibility that are vital for modern network environments.

Cisco Smart Licensing (SL)

Cisco Smart Licensing is a flexible licensing model that provides a centralized, cloud-based system to manage licenses across Cisco products. It simplifies the traditional licensing model by removing the need for Product Activation Keys (PAKs) and device-level tracking of licenses. With Smart Licensing, customers create a Cisco Smart Account, which is an online repository where all licenses are stored. Devices communicate with the Cisco Smart Software Manager (CSSM) over the internet to register themselves and report their license usage. This process ensures that customers have the right to use the software features they've purchased without having to manage complex license files or activation codes.

Cisco Smart Licensing using Policy (SLP)

Cisco Smart Licensing using Policy is an evolution of the Smart Licensing model. It was introduced to provide more transparency and control over how licenses are consumed. This model employs a policy-based approach that determines the actions a device can take if it is out of compliance. In this model, devices no longer need to communicate with CSSM for day-to-day operations. Instead, they operate according to the policy set within the license agreement. This approach is designed to give customers better visibility into their license usage and compliance, while also providing a more flexible and less intrusive way of managing licenses.

Both licensing models are part of Cisco's effort to streamline the license management process, but Smart Licensing using Policy offers a more flexible approach that can be more suitable for environments where devices cannot always maintain a connection to the Cisco licensing servers.

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 may choose one deployment option or a mix-and-match approach of the various deployment options, based on what is most convenient for them.

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 devices have connectivity to Smartreceiver.cisco.com over the Internet, this solution is by far the simplest as it requires no additional configuration steps – works "out of the box."

Mediated (On-Premises) License Management and Reporting

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, violates security policies, requiring an on-premises license management solution.

Using the free download, a customer or partner can deploy the SSM On-Prem license server to keep device communication contained within the customer's local network. The SSM On-Prem license server uses a "synchronization process" to exchange license information with Cisco Smart Software Manager (Cloud) or software.cisco.com. 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 the Disconnected CSSM On-Prem license server is not an option (remote deployments, low-high side operations), the License Reservation option requires no ongoing communications or additional infrastructure and 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 the RMA process.

For the highest degree of security, Cisco offers full offline access through License Reservation. In this environment, all license changes are processed manually. Cisco provides the customer with a node locked license file they can install that can be tracked with Smart License tracking.

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, customers' needs, and our corporate code of conduct.

Cisco Online Privacy Statement Summary

The **Cisco Online Privacy Statement** 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/oversight. Below are some of the highlights of our Online Privacy Statement.

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, 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 securing 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-US 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, 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-US and Swiss-US 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 found in the framework texts; [EU-US and SWISS-US](#).

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

- Software ID tag that identifies the product

- License being used

- Unique Device Identification, for hardware platforms, is usually the Product ID & Serial Number. For software platforms, it is often a UUID

- Serial Number of devices using the license

- Quantity of license being used

- Locale set on the product

Optional Data that can be shared with Cisco to improve your report generation includes the product hostname. This is an option and is controlled through product configuration.

If using the SSM On-Prem license server, you can independently choose to not send this information to Cisco. The items you can optionally share are:

- Hostname: The hostname of registered Cisco product and the software version

The following data is not sent to Cisco:

- 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 Systems 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 from the Certificate Authority.

Certificates used by Cisco Products

Cisco Products report feature usage back to CSSM (or SSM On-Prem) to indicate license usage. To ensure the validity of the license data Cisco and Cisco Products use several notable cryptographic certificates:

- **Cisco Licensing Root Certificate:** Embedded in the Cisco Products that include the Smart Agent and is the root of the trust chain.

- **Cisco Sub-CA:** Generated by Cisco and sent to the Cisco Product during registration.

- **ID Certificate (IDCERT):** For Smart Licensing, the IDCERT is generated by CSSM (or SSM On-Prem) using the product's UDI during the registration process. It is used to verify the product (though its UDI) and by the product to validate the signing authority of the SSM or SSM On-Prem license server. The IDCERT has a lifetime of one year and is automatically renewed every six months. In the case of Smart Licensing Use Policy (SLP) the license lifetime is for 10 years and is not renewed as it is a permanent license.

- **Signing certificate:** Generated in the SSM or satellite on registration or renewal and sent to the Cisco Product. The signing certificate contains the Cisco Smart Software Manager public key which is used to verify the signatures on response **messages exchanged between a Cisco product and Cisco.**

Cisco Product Registration and Trust Establishment

- In the original SL mode of operation, a device needs to be registered with the CSSM. This process requires the customer to obtain an ID token from their smart account and then use the device Command Line Interface (CLI) to enter that ID token and initiate the registration process with the CSSM. Once complete, the registration lifetime is one year, and smart licensing on the device automatically renews the license every 6 months.

- In SLP, once trust is established, it is permanent and there is no automatic renewal.

- Smart licensing on the device and CSSM exchange public/private key pairs are used to sign and verify communications between the two.

Request messages sent by the Cisco Product

Cisco Products use the private key generated during registration or trust establishment to sign all outgoing request messages. Upon receipt, the Cisco license server will use the public key from CSR in registration to verify the SHA256 digital signature on any received request message.

Response messages sent by Cisco License Servers (SSM or SSM On-Prem)

Cisco License servers (SSM or SSM On-Prem) use the private key it generated during registration to sign all outgoing response messages. Cisco Products then use the public key in the signing certificate it received during registration to validate the SHA digital signature on a received message. Upon receipt, the Cisco, the Cisco public key from 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 a 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 using 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) utility

Cisco products that support Smart Licensing using Policy and Managed Service License Agreement (MSLA) utility mode 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.

MSLA is supported in both Smart License and Smart License Use Policy modes. In Smart License mode, MSLA requires the use of a Smart License On-Prem to get Reported Usage Measurement Reports (RUM) and send them to Cisco. Note: Netconf/YANG is not supported by this method.

MSLA in SLP can be directly connected to CSSM, On-Prem or operate in an air-gapped mode using a file upload. Netconf/YANG is supported in SLP mode.

Collection of usage data directly from Cisco products

Customers can send usage reports from each Cisco product 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 RUM 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, Cisco Smart Licensing Utility (CSLU) or On Prem.

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 several certificates to validate the locally installed On-Prem license server. These certificates are not used for data encryption but

instead are used to establish the server is authorized and can be trusted. These certificates are signed off the Cisco Smart License Root CA and cannot be changed.

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

- **Registration Authorization file**—After Cisco SSM receives and processes the registration request, Cisco SSM returns an authorization file to the Cisco SSM On-Prem license server indicating that the Cisco SSM On-Prem license server has been registered with Cisco SSM and the details of the full synchronization.

- **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 been completed.

To ensure the exchange maintains 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, a 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 user for Communications

In addition to the Cisco Smart License certificates returned, Cisco will also provide a certificate, called the TG_CERT, which is used to accept secure connections and allow the 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 an 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 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 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. Learn more about Cisco PSIRT.

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. The Cisco PSIRT adheres to ISO/IEC 29147. The on-call Cisco PSIRT 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. See more in the Vendor Vulnerability Reporting and Disclosure Policy.

Cisco Security Advisories

The Cisco Security portal provides actionable intelligence for security threats and vulnerabilities in Cisco products and services and third-party products. See more in the Third Party Code Attestation Policy.

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 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 likely to have exploits available and is expected to be, or is being, actively exploited.

For high profile, third-party vulnerabilities, Cisco will begin assessing all potentially impacted products that have not reached End-of-Support (with priority given to those products that have not reached End-of-Software-Maintenance) and 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 7 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 which contains features, bug fixes, as well as available critical and high CVEs reported against third-party software. Customers are encouraged to stay updated to the latest 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 (CSSM) at Cisco or, if configured, to your Cisco Smart Software Manager On-Prem (CSSM On-Prem) license server, as mentioned above. The information sent and the formats in which it is sent are identical regardless of the destination.

By default, products are pre-configured to communicate with CSSM at Cisco. If needed, the product can be manually configured to change the destination URL to direct traffic to the 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) and this is the default. There is a possible exception by configuring the Cisco Product to use straight HTTP to communicate with the CSSM 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 Cisco Product directly to CSSM or CSSM On-Prem license server to CSSM 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 TLS implementation, the TLS version will vary based on what version the product supports.

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

Smart License Protocol and Ports

Smart Licensing related communication is initiated by the Cisco product, and neither the CSSM at Cisco nor a CSSM 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 – CSSM, SSM On-Prem or CSLU license server. This may require configuring firewall rules and or any intermediate proxies. Channels and ports used will depend on which transport protocol is used and are shown below.

Smart Call Home:

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

Smart Transport:

- HTTPS (443): smartreceiver.cisco.com

Smart Transport

Smart Transport is the preferred transport protocol available for use with supporting Cisco Products because it is more reliable and has better throughput and thus a better Smart Licensing experience.

The primary difference is in the transport encoding and API gateway in use as shown below. Please consider migrating to Smart Transport if you are using Smart Call Home as it is more reliable.

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	All	smartreceiver.cisco.com	USA	HTTPS (json)	No	Yes

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

Smart Call Home

Smart Transport is the preferred transport protocol. Call Home should only be used in legacy deployments. At some time in the future Cisco will stop using Call Home for licensing communications.

While some products can also send 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 Call Home configuration.

Smart Call Home can be configured to use either HTTP or HTTPS based on the URL format. HTTPS is strongly recommended. Learn more in the Smart Call Home Deployment Guide.

Cisco Product Registration ID Tokens

For Cisco SL mode Products to register with the SSM On-Prem license server or CSSM, they need to be provided a valid ID Token from the target Local Virtual Account. For when the Cisco Product is registered, the ID Token is sent by the product to the Cisco license server, where it is looked up, and check to ensure it is valid (not expired or revoked).

For SLP mode products the id token is required to establish with the CSSM. An ID token is not required to establish trust to the SSM On-Prem as trust establishment is automatic.

As the 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 CSSM or 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 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 (can be limited in product configuration), the Cisco Product can also send its hostname and system version number. Hostnames are used in customer consumable reports. Many customers find hostnames useful in reports. The alternative is to show consumption by UDI.

Several 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 the overview and vocabulary in the ISO/IEC 19770-5: Information technology – IT asset management.

SL Mode Message Types and Frequency

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

- Registration, Renewal, & Deregistration

- Entitlement (License) Requests

- Conversion Requests

- Specialized Request not supported by all products

Registration – The initial registration registers a Cisco Product to a Virtual Account on CSSM or CSSM 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 Smart enabled Cisco products periodically send information about license consumption to either the Cisco Smart Software Manager (CSSM) at Cisco or, if configured, to your Cisco Smart Software Manager On-Prem (CSSM On-Prem) license server, as mentioned above. The information sent and the formats in which it is sent are identical regardless of the destination.

By default, products are pre-configured to communicate with CSSM at Cisco. If needed, the product can be manually configured to change the destination URL to direct traffic to the SSM On-Prem license server or through a proxy. Please see specific product documentation on how to perform this configuration for a description of ID Tokens. Along with the ID Token the Cisco Product sends its UDI, the UDI of any HA 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 a 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. 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 CSSM or CSSM On-Prem license server. Generally, products send entitlement requests any time 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 includes 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 counts 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 the use of Export Controlled functionality.

- Third-Party Key Requests – Requests third-party data, typically a license key from a third party.

- Poll Requests – these poll a CSSM or CSSM On-Prem license server for a response. This is typically to get a response that was not available when the initial request was made.

-

Export Control

US Export Control regulations prohibit Cisco from shipping some functionality, typically strong encryption of user data at speed, to some entities, governments, and military in emerging market countries, unless 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 have been used to ensure regulatory compliance. For a full description, please see Global Export Trade site.

Two types of export checks are done. The first Smart Account set up where Cisco attempts to determine the entity restrictions and the second is at time of order with 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 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. It is used to retrieve licenses, typically license files, for third-party software capability that requires licenses. One example would be a Collaboration "speech to text" feature that requires a Nuance license.

The third-party license request that comes from the 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, confirming 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 the Disconnected CSSM On-Prem license server is not an option (remote deployments, low-high side operations), this option requires no ongoing communications, and requires 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 Smart Software Manager (CSSM) then reserving the required licenses on CSSM. CSSM 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 Return Code, and entering the Return Code into CSSM. CSSM 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 CSSM and changing the reservation. CSSM will generate a new Authorization Code that must be entered into the Cisco product. The Cisco Product will generate a Return Code that can, in turn, be entered into CSSM. At that point, CSSM 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 Return Code into CSSM is optional.

The License Reservation Request Code is an ASCII string that, except the UDI, is base-58 encoded so that it can be unambiguously typed. It includes a version, sequence number, product UDI, SW ID tag (hashed to 9 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, 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 Return 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 BASE58 encoded ASCII string that includes a version, PIID of the Cisco product, and a signature.

SL mode Smart License States

The licensing state machine is transparent to users most of the time. Understanding 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.
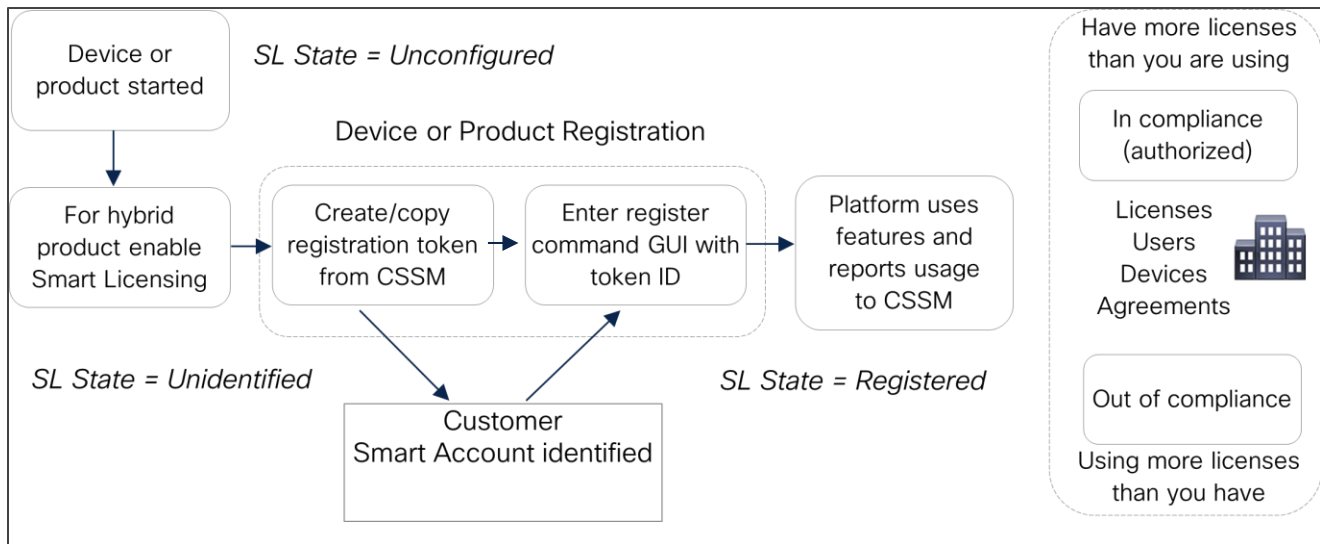
Figure 1. Smart Licensing Workflow

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 Account1. This is done with an ID Token generated from the Smart Account/Virtual Account (SA/VA) on either CSSM or CSSM 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 establishing trust with CSSM or CSSM 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.

There are several states that Smart Licensing could be in. The figure below shows these states.
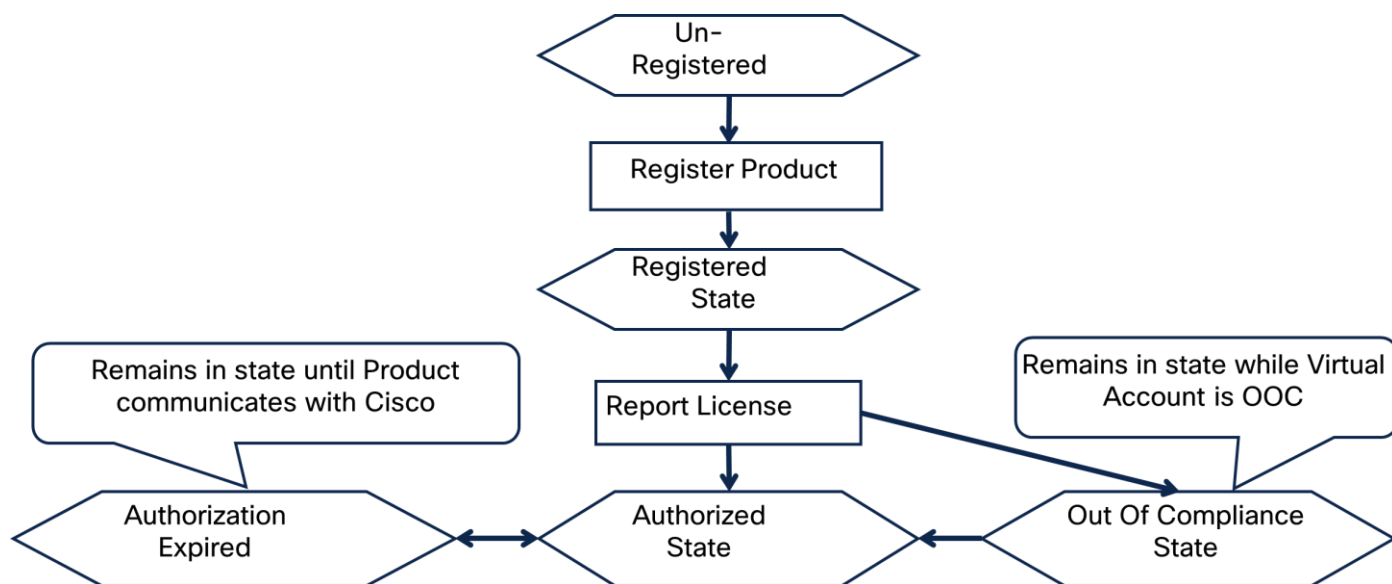
Figure 2. Smart License Product States

Un-Registered State – The initial Smart Licensing state is "Un-Registered." 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 CSSM or CSSM On-Prem license server.

Evaluation State – Often, Cisco products will initially be in "Evaluation". Evaluation is a period where an un-registered 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 de-configuring all license consumption.

Registered State – Once the Cisco Product is successfully registered, it will automatically send an Authorization Request that includes the licenses that 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 – The 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 with that Virtual Account that is consuming that license. If there are enough licenses in the Virtual Account, the license is considered "Authorized."

Out of Compliance State – 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 on one specific Cisco Product being Out of Compliance while another is Authorized. One implication is that Cisco products will only learn of any change in a 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 where a registered Cisco Product is not able to complete the Authorization Request/Response sequence. There are many reasons why a failure could occur, from a downlink 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 the authorized state, the retry is every 23 hours (we do not want to retry at the same time every day)

- If the product is in the OOC state, the retry is every 15 minutes for two hours then backs off to once every 4 hours after.

- If the product is in the 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 in the last 30 days,

- Every day in the last week, and

- Every hour in 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 be re-registered to be corrected. At the point the ID Certificate expires, the Cisco Product will return to the unidentified state and re-enter evaluation mode, if there is any time evaluation time left. Product Instances also enter the un-identified state if they are de-registered.

Product Behavior in Non-Authorized States

A Non-Authorized state is any that is not "Authorized", including:

- Evaluation period expired,

- Out Of Compliance,

- Not-Authorized,

- Authorization expired.

All of these states indicate the product is consuming more licenses than they are authorized to.

Cisco expects that customers will remedy any non-authorized states and bring the product back into Compliance State and provide 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. Unconfigure 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 non-authorized 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, primarily by restricting adding functionality.

Please see product documentation or 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. Due to US Export Regulations do not allow Cisco products to operate export restricted functionality in the initial evaluation period (Cisco cannot confirm the party operating the Cisco product) unless there is a separate Export Authorization Key installed on the Cisco Product or other 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. CSSM at Cisco will send an email notification to those users who have subscribed to the Out of Compliance notification. Both CSSM and CSSM On-Prem license servers will post errors notifying users of the Out of Compliance. Product instances that are consuming the 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 the 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 do in Out of Compliance or Authorization Expired, though many take no action. Those that do typically restrict adding functionality.

Cisco On-Prem license server

Cisco 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 been 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 been completed.

Cisco SSM On-Prem Host OS Security

Linux Kernel

The SSM On-Prem license server is based on 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 unused communication ports are closed, and removing 'root' access, instead replaced by a single admin user.

Deployment Profiles

The SSM On-Prem license server provides two different profiles which can be used when deploying the software which are:

- **Standard Profile**: When you log into the shell, you are default CENTOS bash shell with the option to use the On-Prem license server console. This profile provides the standard security features, usually required by non-defense/finance organizations.

- **DISA STIG Profile**: When you log into the shell, you are placed into the whitelisted console which will prevent root access and limit you to using only the whitelisted console commands in the On-Prem license server console. Select this security profile at installation if Security Technical Implementation Guide (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 STIG standards.

Host OS Access

The SSM On-Prem license server console provides a secure approach for managing the SSM On-Prem license server using 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. **Standard Profile** offers bash access, while the **DISA STIG Profile** only offers the hardened shell offering a higher level of security.

Cisco SSM On-Prem Application Security

Communications Protocol and Port

The 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. 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 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 SSM On-Prem:

The 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 SSM On-prem license server provides both HTTPS (443) and HTTP (80) based on your network needs.

SSM On-Prem communication with Cisco SSM:

The Cisco SSM On-Prem license server exchanged data with Cisco uses a well-known Cisco 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 SSM APIs, the single-sign-on server, cloudsso.cisco.com, is also used to authenticate your CCOID during Local Account registration.

Cisco products Registration to SSM On-Prem

Before the SSM On-Prem license server can accept registrations from Cisco products, it must register with CSSM. Cisco products utilize either 3-Tier certificates or 4-Tier certificates.

If your Cisco products have not implemented the latest smart agent code and only require a 3-Tier certificate from CSSM, you must wait 48 hours after registering the SSM On-Prem license server with CSSM. 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 SSM On-Prem license server.

To facilitate automatic validation of the trust chain, an additional certificate was added to set: four levels of certificates (4-Tier). When using a 4-tier certificate, the Smart Agents, SSM On-Prem license server, and CSSM must exchange information to validate the certificates and make them available automatically.

During the initial Registration, the CSR from an SSM On-Prem license server to a CSSM is signed immediately. However, you must make changes to the product smart agents, SSM On-Prem license server, and CSSM for the trust chain to work automatically.

Cisco Smart License using Policy

This 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
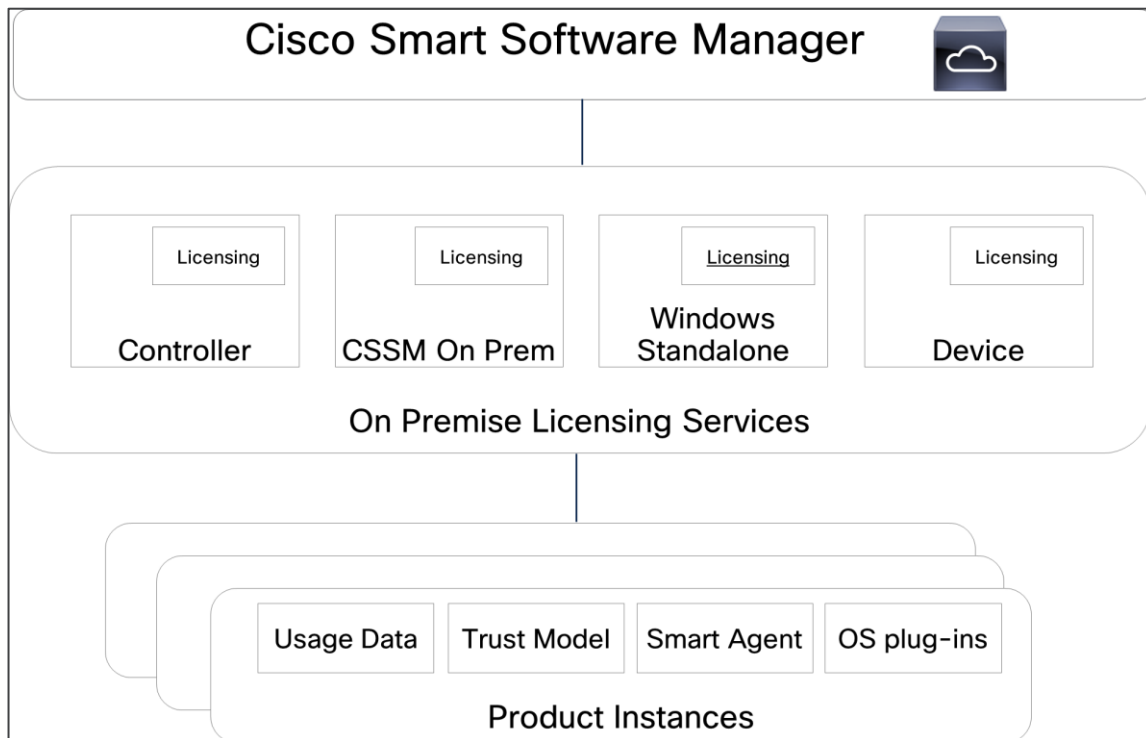
Information sent from product to Cisco

License usage data is sent in the form of ISO19770-4 RUM reports 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, export restricted 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.
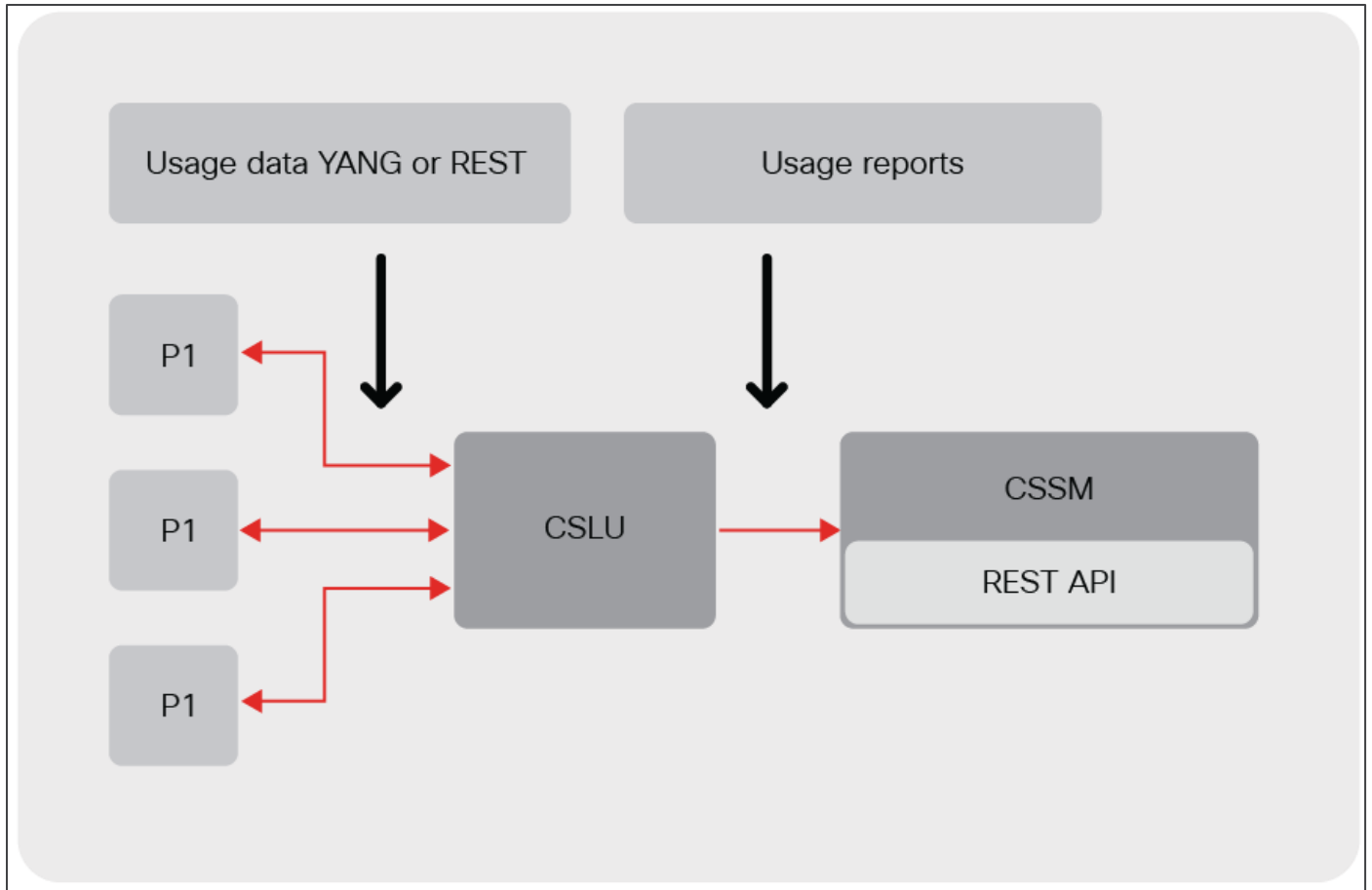
The CSLU usage report format is based on ISO 19770-4 standard RUM report format. It is delivered in JSON format and signed per trust model. The usage report will first be hashed using SHA-256, then the hash will be signed using the supplied key from either the default signature key, or the product signing keys.

ID Token registration and Smart License Using Policy

No registration or ID Token is required for SLP mode when connected via On-Prem or air-gapped. An ID token is required to establish trust when the product instance is directly connected to CSSM. 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.
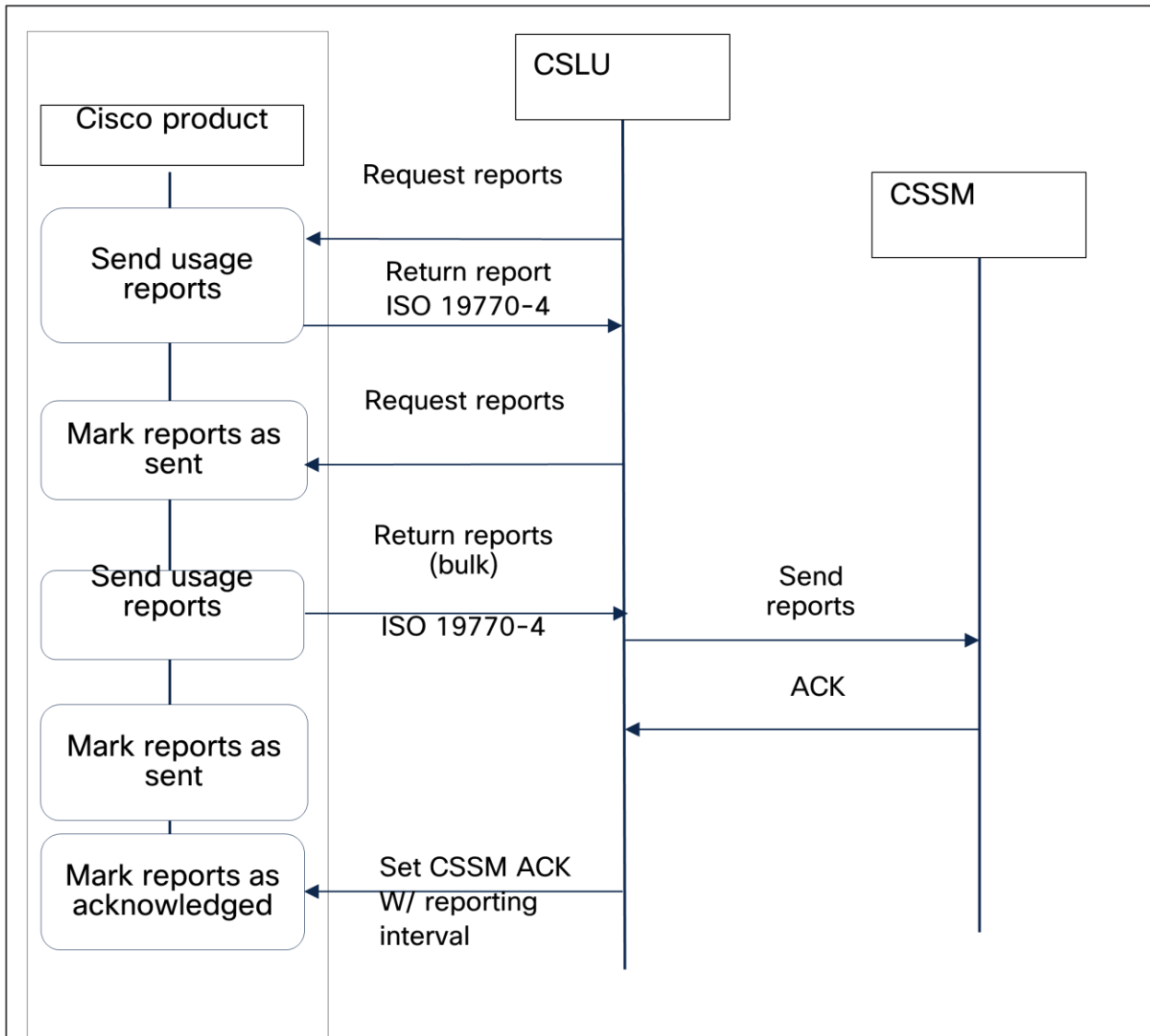
Licensing policies

Licensing policies contain the license entitlement parameters, which include, but are not limited, to first-time reporting, report frequency, reporting enforcement. 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.

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.

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."

Appendix

Terminology

CSSM or SSM – Cisco Smart Software Manager

CSR – Certificate Signing Request

DLC – Device Led Conversion

DNS – Domain Name Server

FQDN - Fully Qualified Domain Name

LCS – License Crypto-Module Support

LVA – Local Virtual Accounts

MSLA – Managed Service License Agreements (Utility)

OOC – Out of Compliance

PI – Product Instances

PIDs – Product IDs

PIID – Product Instance IDs

PLR – Permanent License Reservation

SA – Smart Account

SBP – Subscription Billing Platform

SCH – Smart Call-Home

SKU – Stock Keeping Units

SLR – Specific License Reservation

TPL – Third (3rd) Party Licensing

UUID – Universally Unique Identifier

VA – Virtual Accounts

SLP – Smart Licensing using Policy

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 sign-up, 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 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, 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, web, and network traffic, including but not limited to data on an email message and web request attributes and information on how different types of email messages and web requests were managed 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 before 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 or establishes trust with the CSSM, how certificates are used, and how messages are signed.

Cisco Smart License Block Diagram
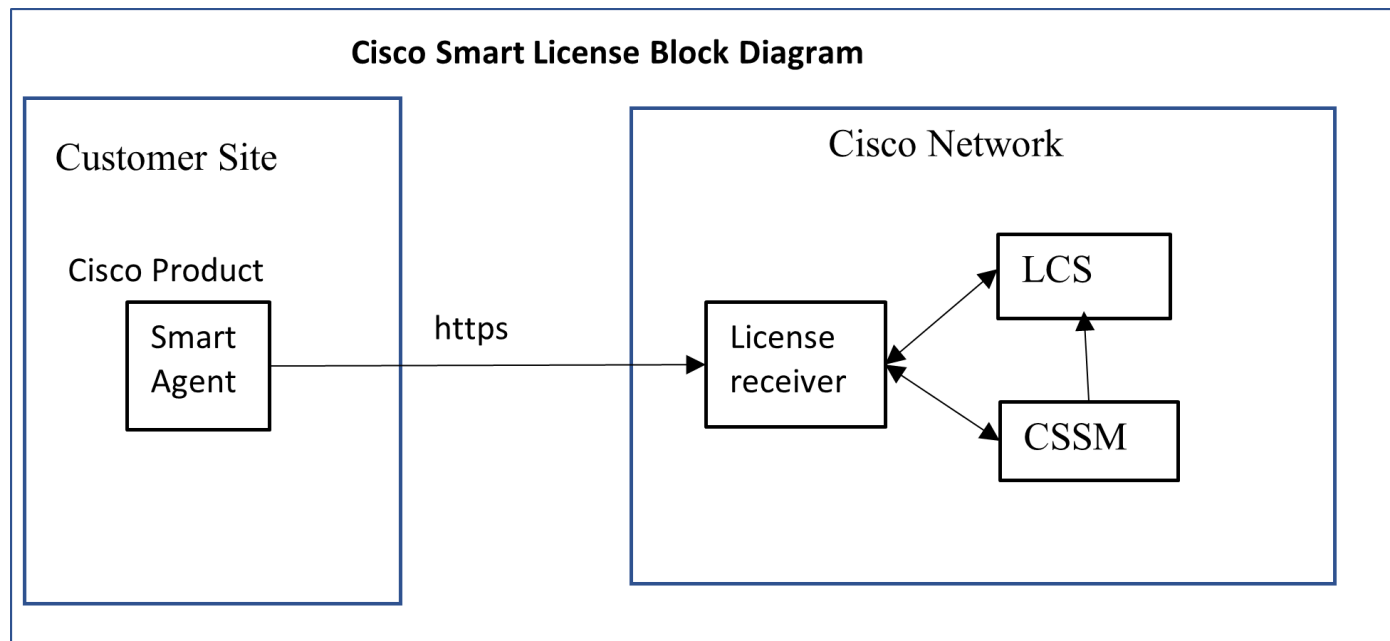
Cisco Product Registration or SLP trust establishment

In SL mode the product will register with Cisco. In SLP mode the product will establish trust with Cisco. The process is the same for either one.

- The customer gets an ID Token from their Smart Account using the Cisco SSM portal.
    - o The ID Token is simply a secure method of identifying a customer.
- The customer uses the registration or trust command on the Cisco Product with the ID Token to start the process in the Smart Agent.
    - o Note: After the process is complete, the ID Token is no longer needed.
- Smart Agent generates a CSR (Certificate Signing Request).
    - o Signature is SHA256
    - o The Cisco Product UDI is put in the CN (Common Name) field.
- The Smart Agent will generate private/public key pair, the length is 2048.
    - o The Cisco Smart Agent uses the private key to sign request messages that it sends to Cisco SSM

- o The public key goes in the CSR, The Cisco Smart Agent saves the private key in a trusted store.
- o The Cisco SSM uses the public key to verify signatures on messages it receives.
- The Cisco Smart Agent sends the following in a request to the Cisco SSM:
  - o CSR
  - o ID Token
  - o Software Id Tag
  - o UDI
- The message is sent via HTTPS .
- After receiving the response, The Cisco Smart Agent will send an ACK to the Cisco SSM, so the Cisco SSM knows The Cisco Smart Agent received the certificates.

Registration/Trust Response from Cisco SSM license server

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

Registration/Trust Response Validation

1. The Smart Agent will validate the trust chain of the certificates it has received to the root certificate which is embedded and obfuscated in the Smart Agent code.
2. Validate the UDI in the ID certificate matches the UDI of the Cisco Product.

Trust chain diagram
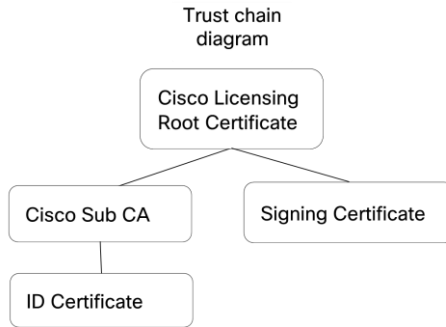
3. Save the certificates in Trusted Store

4. Send ACK to the Cisco SSM

Figure illustrating registration/trust flows
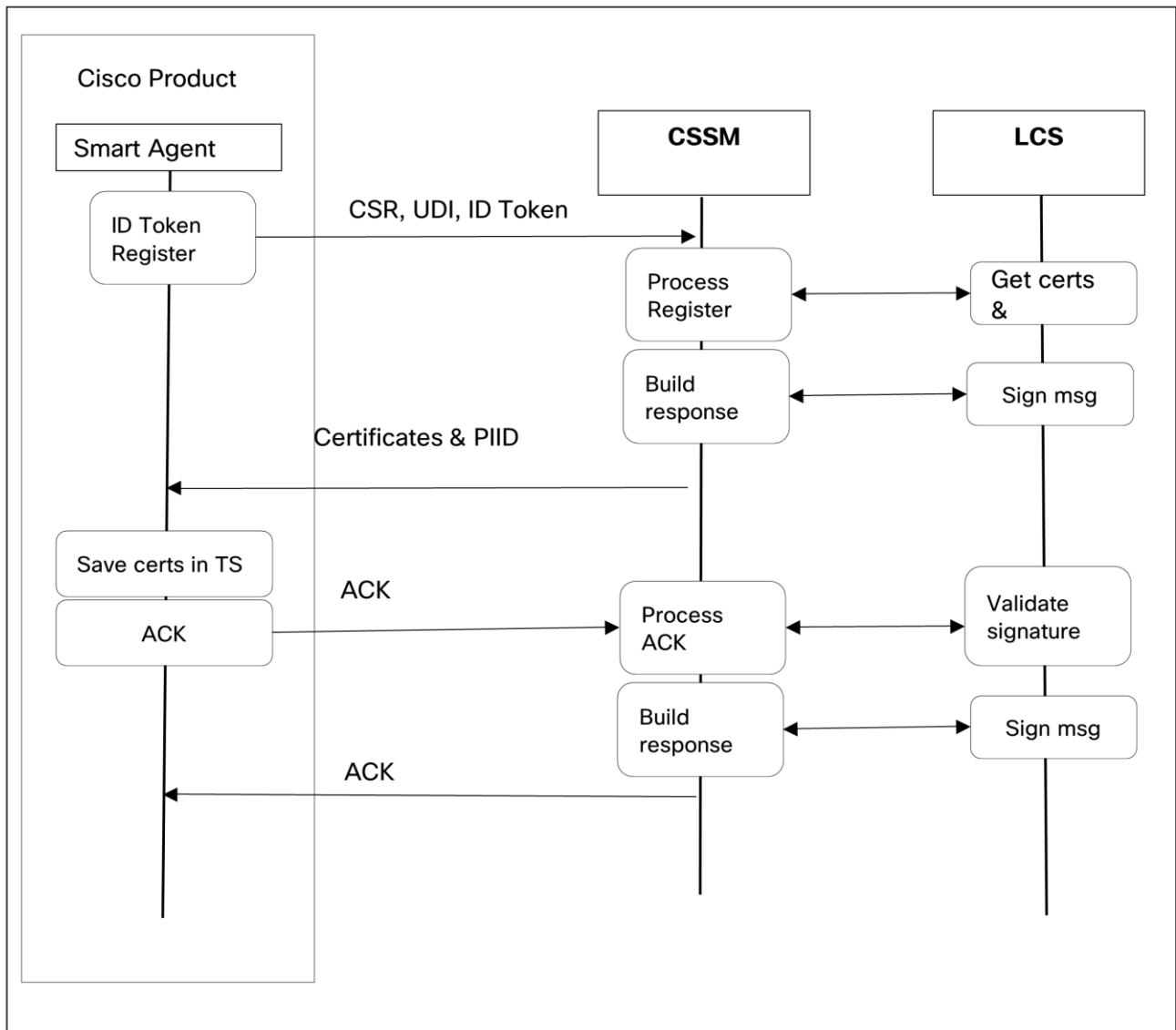
Cisco Product Registration Renewal

Registration renewal is only for classic SL mode operations. In SLP mode the trust code is permanent so no renewal is necessary.

The lifetime of the 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 registration.

- Smart Agent generates a new CSR.

- Smart Agent generates a new private/public key pair, the length is 2048.

- The Cisco Smart Agent sends the following in the renewal request to the Cisco SSM via the Smart Call Home server:

  o CSR

  o Software ID Tag

  o UDI

  o 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.

  o Sub-CA

  o Signing certificate

  o 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 Cisco Smart Agent received the certificates.

- The Cisco SSM will send a final ACK back to the Cisco Smart Agent.

- At this point, The Cisco Smart Agent will delete the old certificates and start using the new certificates.

- The Cisco Smart Agent saves the new certificates in its trusted store.

- If there was a communications failure somewhere in the process The Cisco Smart Agent will start the renewal process over and continue to use the old certificates until it receives that final ACK.

Figure illustrating renewal flows
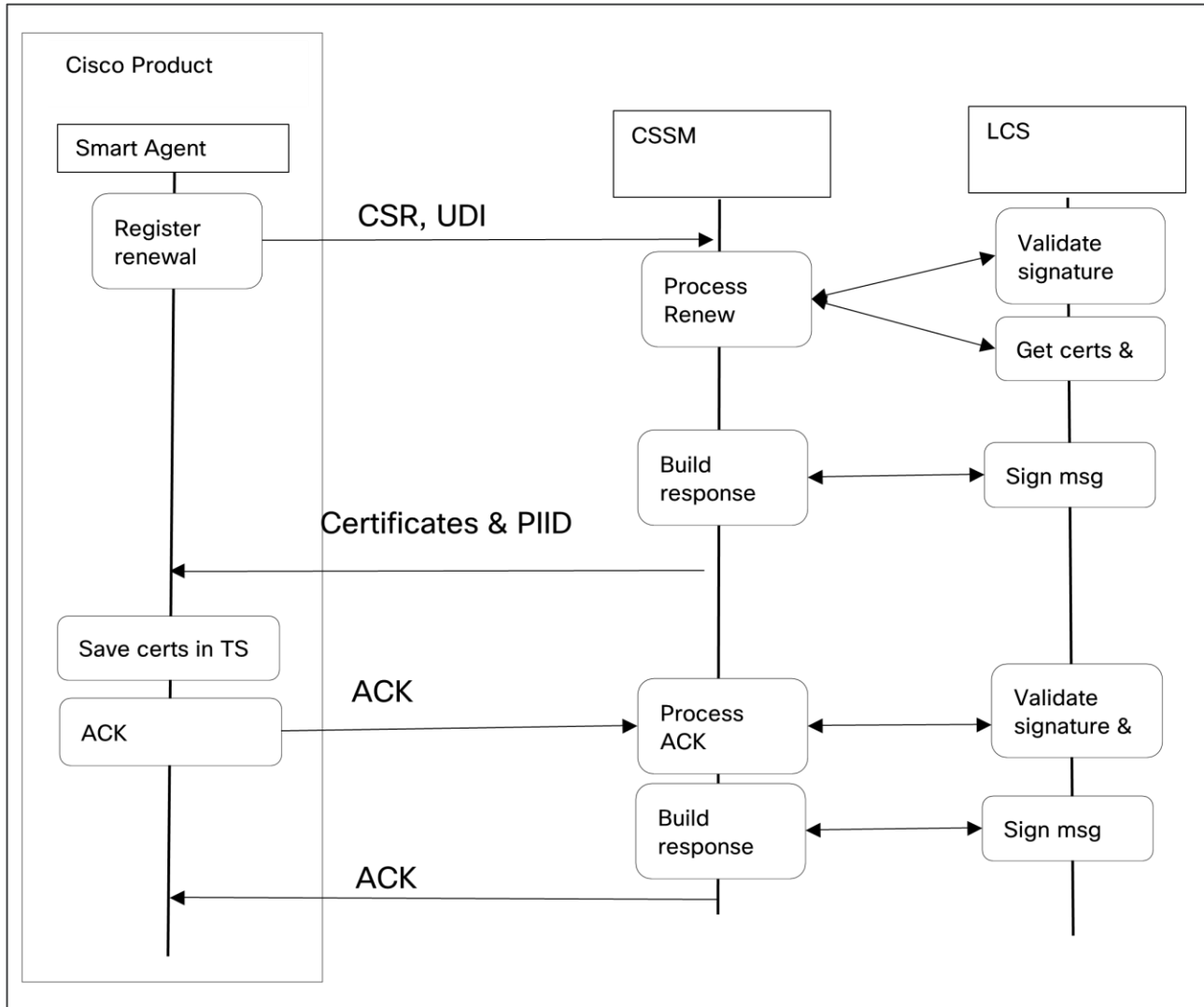
Cisco Product Certificates

This applies to both SL and SLP modes.

- Cisco Licensing Root Certificate

    - Embedded and obfuscated in the image that includes the Smart Agent. This will never change. This is the root of the trust chain.

- Cisco Sub-CA

    - Generated Cisco and sent it 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.

    - A lifetime of one year.

    - The ID Certificates also have the Cisco Product UDI embedded in them so we can verify it is for the correct Cisco Product. Verified when received and at boot time.

- o   Smart Agent will automatically renew this certificate every six months.

- Signing certificate

  - o   Generated in the Cisco SSM or SSM On-Prem license server on registration or renewal and sent to the Smart Agent.

  - o   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

- Smart Agent signing

  - o   The Cisco Smart Agent will use the private key it generated during registration to sign all outgoing request messages.

  - o   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.

  - o   SHA256 digital signature

- Cisco SSM verification

  - o   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

  - o   The Cisco SSM will use the private key it generated during registration to sign all outgoing response messages.

  - o   The Cisco Smart Agent will use the public that is in the signing certificate it received during registration to validate the signature on a received message.

  - o   SHA256 digital signature

- Smart Agent verification

  - o   Uses the public key from CSR in registration to verify the signature on any received request message.

SSM On-Prem Protocol Overview

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

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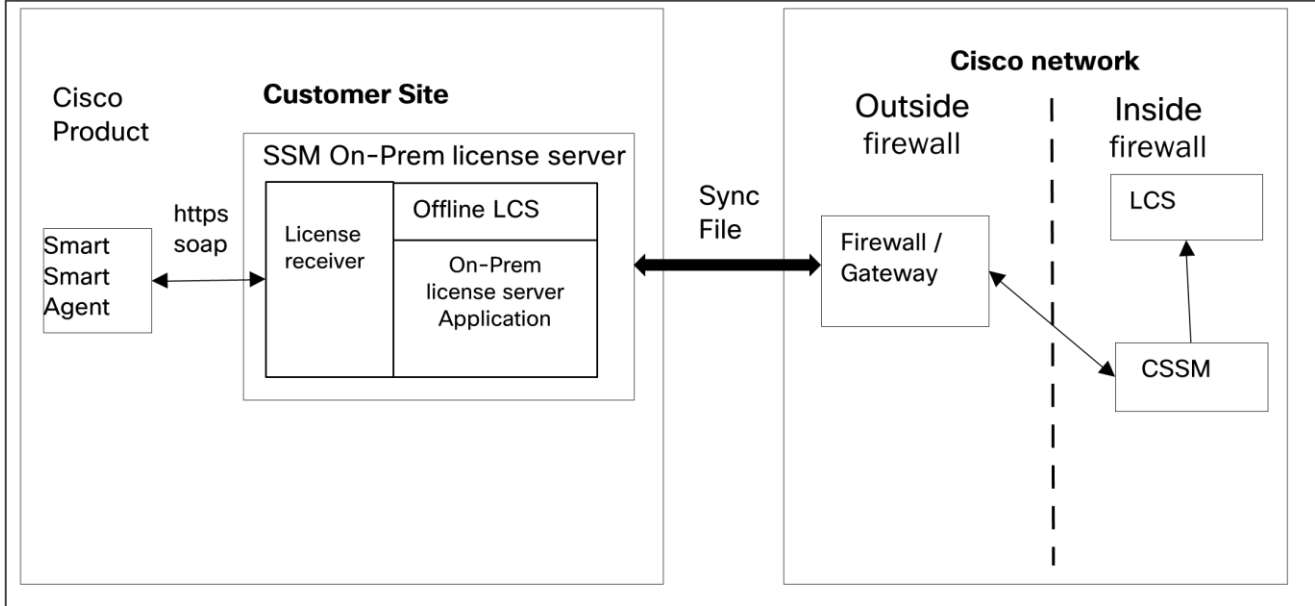
The certificates created when connected to an SSM On-Prem license server are slightly different. Instead of a 3-tier trust chain, a 4-tier trust chain is used.
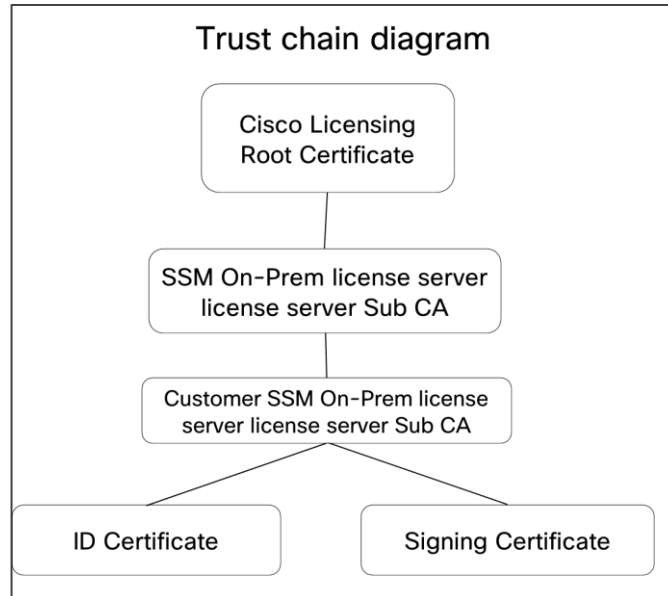
Cisco SSM On-Prem license server certificates

- SSM On-Prem license server Sub-CA

- Generated in the Cisco SSM when the satellites register. Sent to the SSM On-Prem license server then later sent to the Smart Agent when it registers with the SSM On-Prem license server.

- Customer SSM On-Prem license server Sub-CA

    - Generated in the Cisco SSM when the satellites registers. Sent to the SSM On-Prem license server then later sent to the Smart Agent when it registers with the SSM On-Prem license server.

Registration Request file

When you initially register your SSM On-Prem license server to CSSM, the SSM On-Prem license server sends a Registration Request file to CSSM to establish a link to a specific Virtual Account within your Smart Account. The Registration Request file contains the key information outlined in Table 1, along with three Certificates Signing Requests (CSRs) which will be signed by Cisco and returned for use by the 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 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:	Certificates Signing Requests for the LCS (License Crypto Service) used to sign the IDCERT used by Cisco products to establish trust with a SSM On-Prem license server.
tg_csr:	Certificates Signing Requests are used to secure the HTTPS communication between the SSM On-Prem license server and Cisco Products.
ssms_csr:	Certificates Signing Requests are used to secure the HTTPS communication between the SSM On-Prem license server User Interface and your Browser.

Authorization Response file

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

Table 2.   Authorization Response File Certificates

Certificate	Description
id_cert:	The SSM On-Prem license server uses this certificate to identify all Cisco products. CSSM uses this certificate to identify SSM On-Prem license servers. This certificate is renewed every time the 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 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 SSM On-Prem license server use this certificate to manage 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 the 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**.
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 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 a version of the 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 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.
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 Cisco Virtual Account section of the Synchronization Request file.

Table 4.   Virtual Account Section of the Synchronization Request File

Component	Description
:id:	A unique number is used to identify the Virtual Account the SSM On-Prem license server is registered.
:name:	The name is given to the SSM On-Prem license server either at the time of registration or later if changed at the CSSM portal.
:product_instances:	Starts the YAML section that identifies the products registered to the SSM On-Prem license server.
:id:	A unique number is assigned by the 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 is defined by ISO 19770, which identifies the product entitlement.
:udi_pid:	The product identifier (PID).
:hostname:	The hostname is 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 lists the license in use by the product.
:id:	A unique number is used by the registered product to identify the license being used. This number is assigned by the SSM On-Prem license server.
:tag:	The software tag is defined by ISO 19770, which identifies the license being used by the product.
:consumed_quantity:	The number of licenses in use.

[1] By default, the hostname, IP address, and MAC address are sent with the request. If you do not want the file to include this information, it 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 an SSM On-Prem license server, CSSM sends the Synchronization response to authorize and synchronize with the SSM On-Prem license server.

A full synchronization occurs when the 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 the information about the virtual accounts and licenses from CSSM to SSM On-Prem license server. 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 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.
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 the 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 accept secure connections allowing the web browser to communicate to the SSM On-Prem license server over a secured connection (HTTPS).

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 were synchronized to CSSM.
virtual_accounts:	These lines identify Cisco virtual accounts registered in the SSM On-Prem license server and were synchronized to CSSM.

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 is 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**.

Third-Party Provider Information

CSSM can send provider information in the Synchronization Response file during a full synchronization with the 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, CSSM provides SSM On-Prem license server conversion information in the ***device_conversion_response:*** section of the Synchronization Response file (Figure 8). The ***device_conversion_response:*** section lists status information for each Cisco Product registered to the SSM On-Prem license server that initiated DLC.

Table 8. 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**.

References

1. Cisco Security
   (https://sec.cloudapps.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://www.cisco.com/c/en/us/about/trust-center.html)

7. Cisco Secure Development Lifecycle
   (https://www.cisco.com/c/en/us/about/trust-center/technology-built-in-security.html#~processes)