Cisco Smart Software Manager On-Prem User Guide

Version 9 Release 202406

First Published: 01/16/2016
Last Modified: 6/14/2024

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Preface

This preface describes the objectives and organization of this document and explains how to find additional information on related products and services.

Objectives

This document provides an overview of software functionality that is specific to SSM On-Prem. It is not intended as a comprehensive guide to all the software features that can be run, but only the software aspects that are specific to this application.

Related Documentation

This section refers you to other documentation that also might be useful as you configure your SSM On-Prem. This document covers valuable information for the SSM On-Prem and is available online.

Listed below are other guides, references, and release notes associated with Cisco Smart Software On-Prem.

- *Cisco Smart Software Manager On-Prem Quick Start Guide*
- *Cisco Smart Software Manager On-Prem Installation Guide*
- *Cisco Smart Software Manager On-Prem Console Reference Guide*
- *Cisco Smart Software Manager On-Prem Migration Guide*
- *Cisco Smart Software Manager On-Prem Release Notes*

Document Conventions

This documentation uses the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords used in one or more step(s).
Italic	Italic text indicates arguments for which the user supplies the values or a citation from another document
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
variable	Indicates a variable for which you supply a value, in context where italics cannot be used.

Callout Conventions

This document uses the following callout conventions:

NOTE: Means reader pay special attention. Notes contain helpful suggestions or references to material not covered in the manual.

CAUTION: Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed, paste this URL into your RSS reader: What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.

Introduction

Cisco Smart Software Manager On-Prem (SSM On-Prem) is an IT Asset Management solution that enables customers to administer Cisco products and licenses on their premises. It is designed as an extension of **Cisco Smart Software Manager** and provides a similar set of features.
However, instead of being hosted on cisco.com, it is available as an "on premises" version. SSM On-Prem has a Licensing Workspace where you can request an account, request access to an existing account, and manage an existing account.
SSM On-Prem also has a License workspace where you can track and manage licenses through Smart Licensing.

- SSM On-Prem is targeted for all customers:
  - who want to manage their assets on premises,
  - whose policies prevent products from reporting to Cisco directly,
  - where deployments which are air-gaped and reporting to Cisco directly is not possible.
- Supports multiple Local Accounts (multi-tenant).
- Scales up to a total 300,000 product instances with a maximum capacity of 25,000 Product Instances per account using 1 license each.
- Provides online or offline connectivity to Cisco.
- Managed Service License Agreement (MSLA) support: On-Prem supports aggregates usage-based measurements from product instances and relays them to Software Billing Platform (SBP) for rating and billing. See On-Prem Support of Utility Billing (MSLA)

System Requirements

Cisco Smart Account Access

Ensure that you have access to a Cisco Smart Account before you proceed with the tasks mentioned in this section.

Supported Web Browsers

The following web browsers are supported:

- Chrome 36.0 and later versions
- Firefox 30.0 and later versions
- Internet Explorer 11.0 and later versions

NOTE: JavaScript must be enabled in your browser.

Logging into Cisco SSM On-Prem

(Included into SSM On-Prem in the 201910 release.)

SSM On-Prem has an initial login configuration feature that allows you to set the native language, create a new password, and to set your Host Common Name. The Host Common Name must match the value you plan to use for the host portion of the destination URL. This will either be an IP address, or the FQDN (recommended) of the SSM On-Prem server.

Initial Login Procedure

You initially log into SSM On-Prem with your username and password. After you have logged into the application, a Wizard screen opens asking you to:

- Set the default language
- Reset your password
- Check your Common Name
- Review all your selections before logging into the application.

Complete these steps when you perform your initial login.

Step	Action
Step 1	Log into SSM On-Prem for the first time with your: • **Userid** • **Password** The Wizard opens asking you to select your default language. **NOTE**: At any point you can click **Back** to return to the previous page.
Step 2	Select the **default** language (English, French, Japanese, Chinese, Korean).
Step 3	Enter your **new password**.
Step 4	Confirm your **new password**.
Step 5	Enter or confirm your **Common Name**.
Step 6	Review your **changes**. If they are correct, click **Next**. The Wizard returns you to the Login screen. Where you can log into SSM On-Prem using your new password.

Step	Action
	If they are incorrect, click **Back** and you are returned to the previous screen.

Logging into SSM On-Prem using OAuth2 ADFS

(Added for SSM On-Prem 7 Release 201910)

Once you have enabled the OAuth2 ADFS Secondary Authentication, click **Save** and configure your ADFS server, you can now log into SSM On-Prem with either SSM On-Prem login or OAuth2 ADFS login. The login screen now shows two buttons:

- **Log in**: Allows you to log into the system using your SSM On-Prem credentials.

NOTE: The local SSM On-Prem administrator would continue to use this login method.

- **OAuth2 ADFS Log in**: Redirects you to the ADFS screen where you log into the system using your ADFS credentials.

NOTE: If you use the OAuth2 ADFS Log in button, do not fill in your SSM On-Prem credentials since they will be ignored. Use the SSM On-Prem credentials only for an SSM On-Prem local login.

Application Overview

Cisco Smart Software Manager On-Prem (SSM On-Prem) is linked to the cloud-based Cisco Smart Software Manager (CSSM Cloud) through a single management workspace. SSM On-Prem enables you to support multiple SSM On-Prem Local Accounts. When created, each Local Account is linked to a unique cloud Virtual Account within your Cisco Smart Account/Cisco Virtual Account pair located on CSSM Cloud.

A Local Account groups multiple SSM On-Prem Local Virtual Accounts, which contain your product instances and associated licenses. All SSM On-Prem Local Virtual Accounts are wrapped into a default Local Virtual Account named Default. SSM On-Prem uses the Default Local Virtual Account to communicate with CSSM Cloud. You can use each SSM On-Prem Local Virtual Account to group your licenses by department, geographic region, function, and so on.

On the one hand, CSSM Cloud functions as the “source of truth” for all license entitlements (purchases), Cisco Virtual Accounts, and metadata information. On the other hand, SSM On-Prem functions as the “source of truth” for product instance registration and license consumption. This means that each system accepts whatever is sent by the other system as an undeniable source. In addition, when a Local Account synchronizes with CSSM Cloud, it gets a new ID certificate (364-day duration) that allows uninterrupted functioning.

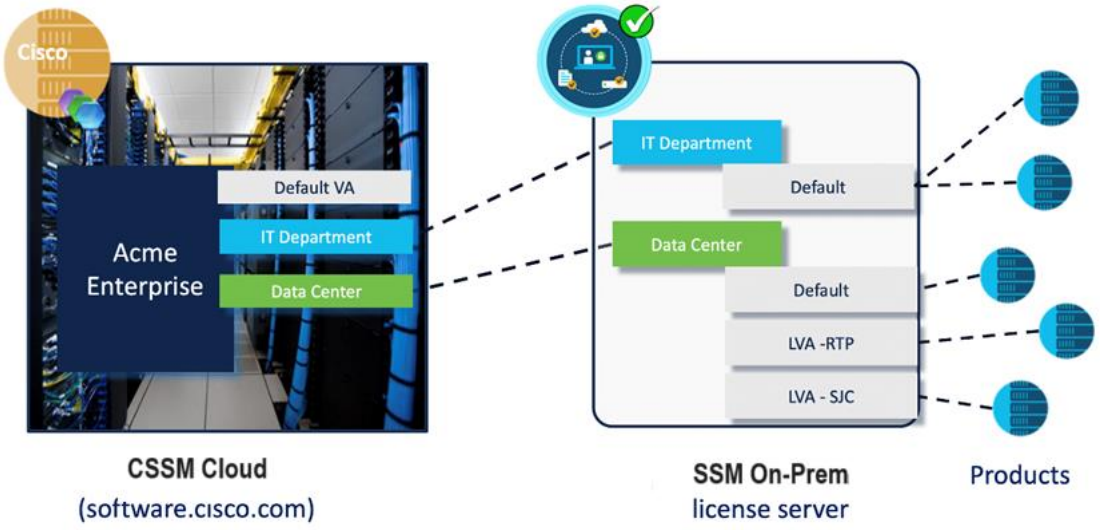

Figure 1 - Today's SSM On-Prem structure

SSM On-Prem has architecture and updated user interface (see About Accounts and Local Virtual Accounts) that provides these features:

- Separate Licensing and Administration workspaces
- Multi-tenancy capability with RBAC (Role Based Access Control) for license management
- External authentication such as: LDAP, AD, and ADFS
- Syslog
- Proxy
- Other miscellaneous functions

Accounts and Local Virtual Accounts

There are four different types of accounts in the SSM On-Prem architecture that containerize licenses and product instances. Of these four account types, two are found in the cloud software.cisco.com for CSSM Cloud and two are found in the SSM On-Prem. For CSSM Cloud, you have **Cisco Smart Accounts** and **Cisco Virtual Accounts**. For SSM On-Prem you have **Local Accounts** and **Local Virtual Accounts**.

NOTE: The **name** of the Local Account listed in SSM On-Prem is the **Local Account** and will differ from the name of the Smart Account listed in CSSM Cloud. Therefore, if you register a Product Instance with an SSM On-Prem, the Local Account name will be the SSM On-Prem name and not the name listed on the CSSM Cloud.

Accounts Located in CSSM Cloud

Accounts that reside in CSSM Cloud are **Cisco Smart Accounts** and **Cisco Virtual Accounts**. Each Cisco Smart Account, in turn, contains **one** or **more** subaccounts called **Cisco Virtual Accounts**. A customer typically uses a single Cisco Smart Account; however, more than one

Smart Account can be used with the understanding that there is **no relationship** as it is not possible to directly transfer information between Cisco Smart Accounts.

Accounts Located in Smart Software Manager On-Prem

Accounts that reside in SSM On-Prem are **local Accounts** and **Local Virtual Accounts**. Each SSM On-Prem Local Account is linked to a single Cisco Virtual Account and can contain one or more Local Virtual Accounts. Each Local Virtual Account can contain one or more registered product instances and associated licenses. One of these Local Virtual Accounts is always designated the **Default Local Virtual Account** and is named **Default.**

NOTE: The default Local Virtual Account name can be changed by a customer, see Modifying the Default Virtual Account Name.

The Default Local Virtual Account is special because it is the account used to communicate product instance and license information back and forth between CSSM Cloud and an SSM On-Prem application instance. Transferring product instances and licenses from the Default Local Virtual Account to another Local Virtual Account within the same Local Account **has the effect of hiding network information from Cisco**.

About the Relationship between CSSM Cloud and SSM On-Prem Accounts

There is a one-to-one relationship where one Cisco Virtual Account is directly related to one SSM On-Prem Local Account.

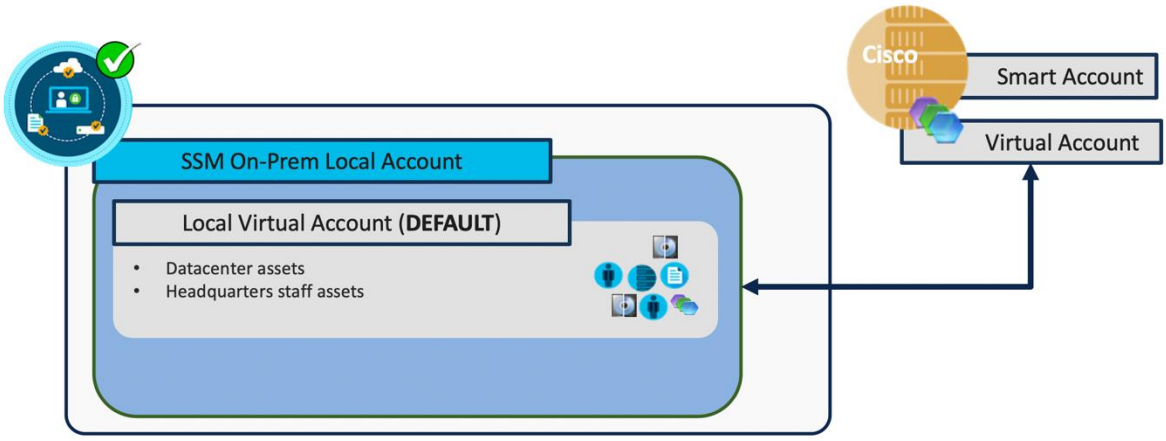

Figure 2 – Relationship between Cisco Virtual Account and SSM On-Prem Account In this relationship, product instance and license information are synchronized between these two accounts for the CSSM Cloud and SSM On-Prem systems respectively.

Following this one-to-one relationship, if a license(s) is added, it will show up in the Default Local Virtual Account associated with that SSM On-Prem Local Account. Conversely, if a license is removed from the Cisco Virtual Account, it will also be removed first from the Default Local Virtual Account and then from other user-created Local Virtual Accounts, in alphabetical order, until the required number of licenses are removed to satisfy the number of licenses removed from the CSSM Cloud.

NOTE: While the relationship between CSSM Cloud and SSM On-Prem Accounts is one-to-one, it is permissible to create multiple Local Accounts within a single SSM On-Prem application instance.

Licenses

- Licenses are required for all Cisco products and often for different feature sets of given product. The following types of product licenses vary depending on the Cisco product:
- **Term Licenses**: Licenses that automatically expire and are removed after a set amount of time: one year, three years, or whatever term was purchased.
- **Perpetual Licenses**: Licenses that do not expire.
- **Demo Licenses**: Some Cisco Products offer Demo or Trial licenses to allow for evaluation or testing of the product prior to purchase. Demo licenses typically last 30 days but may vary based on the Cisco product. Demo licenses are not intended for production use and are automatically removed at the end of the demo period.
- **Reporting-Only Licenses**: Licenses that are zero-dollar base and bundled with the hardware. After a device registers and reports the use of these reporting-only licenses, CSSM Cloud will begin to show consumption of such licenses in the Smart Account/Virtual Account to which the device is registered. Please note: CSSM Cloud will always show purchased quantity for such licenses equal to the in-use quantity and there will never be a surplus of reporting-only licenses in the inventory.

Overview

- SSM On-Prem is tailored to maximize Cisco's licensing features. This section describes, in detail, the five key features in Cisco Licenses.
    - **Application Redundancy Support**: Application Redundancy (or Application High Availability) is a method to achieve high availability of applications within the product instance. In the application redundancy model, the role of an application can be different from the role of the system (product instance). For example, an application can be in Standby state on an Active system (product instance) or vice-a-versa.
    - **Export Control (EC)**: Export control allows Smart License enabled products that connect to SSM On-Prem to generate restricted tokens for trusted customers (for example, category A and B Customers) as well as activate restricted functionality according to Export Control laws.
    - Device-Led Migration (DLC): Today, classic-to-Smart license conversion takes place on Long Range Proximity or CSSM Cloud portals based on information available in the SWIFT database. DLC allows the device/product instance to initiate a conversion of classic licenses (such as Remote Terminal Unit) to Smart licenses that are not on the SWIFT database. Upon conversion, these Smart Licenses are deposited into CSSM Cloud. Products must be upgraded to a DLC-enabled version, connected to a DLC-enabled CSSM Cloud or SSM On-Prem for this feature to work.

- **Third-Party License (TPL)**: TPL, such as Speech View in Unity Connection and Apple Push Notification (APNs) in Cisco Unified Communication Manager (CUCM), is used to authorize Smart License enabled Cisco products to use their services.
- **Future Dated License:** SSM On-Prem supports future-dated transactions starting at SSM On-Prem Release 8-202206. The licenses with a start date less than the current date are future dated licenses. Future-dated licenses should not be consumed until the start date becomes current.

The key features of SSM On-Prem include the following features listed in the table below.

Feature	Description
Multi-tenancy	Can manage multiple customer Local Accounts in a single management workspace.
System Security Enhancements	SSM On-Prem is packaged as a deployable ISO with a AlmaLinux Security Hardened Kernel and is Nessus Scanned with Critical and Major (CVE) issues addressed. SSM On-Prem is fully compliant with FIPS-140-2. NOTE: TACACS+ uses MD5 hashing algorithm which is not FIPS compliant. If FIPS compliance is a requirement of your organization, please use an alternative secondary authentication method.
LDAP Authentication	A System Administrator can set the authentication method to use LDAP or OAuth2 LDFS. If not specified, it will use local authentication.
LDAP Groups	LDAP user group operations such as role assignment can be applied to multiple LDAP users within the group. If not specified, it will use local authentication.
User Groups	When using local authentication, group user operations, such as role assignment, can be applied to multiple users within the group instead of individual users.
Account and Licensing Management	Combines Local Account and Licensing management in a single workspace with the same look-and-feel as Cisco Smart Software Manager and Virtual Account Administration.
Multiple Network Interfaces	You can configure multiple interfaces for traffic separation between management and product instance registrations. Some restrictions apply.
Syslog Support	You can configure Local Account events, so they are sent to a syslog server.
Proxy Support	SSM On-Prem can have a proxy between itself and CSSM Cloud for traffic separation.
API Support	Applications can call SSM On-Prem APIs for virtual account, token, license, product instance, reporting, alerts, and other operations.
Virtual Account Tagging	You can tag Local Virtual Accounts for easy virtual account classification, grouping, locating and/or role assignment.
License Tagging	You can define and assign tags to licenses, which is useful for classifying, locating, and grouping licenses.

License Administration Features

The SSM On-Prem has a License Administration workspace application that contains a group of configuration Widgets. These Widgets enable an administrator to configure the system, user creation, Local Account creation, registration, synchronization, network, system, security settings and more. The License Administration Workspace is accessed via: https://<ip address>:8443/admin.

NOTE: See your network administrator for the hostname or IP address. This administration workspace is restricted to authorized users.

Licensing Workspace Features

The SSM On-Prem has a Licensing workspace with a similar functionality to CSSM Cloud (located on software.cisco.com) where users can manage their Local Accounts, users, product instances, licenses, and so on. The Licensing Workspace is accessed via:

https://<ip-address>:8443

License Transfers

CSSM Cloud (software.cisco.com) is the “single source of truth” for all license entitlements and SSM On-Prem is the “single source of truth” for product instance registrations and license consumption. This distinction dictates that licenses cannot transfer outside of CSSM Cloud. However, in SSM On-Prem, because all licenses in the Local Virtual Accounts are not visible to CSSM Cloud, the license transfer behavior between Local Virtual Accounts in SSM On-Prem is similar to the license transfer behavior in CSSM Cloud. During a synchronization of SSM On-Prem to CSSM Cloud, all product instances and licenses are aggregated across all Cisco SSM On-Prem Local Virtual Accounts and updated in CSSM Cloud and vice versa.

CSSM Cloud and SSM On-Prem have the following behaviors for license transfers:

- Non-export-restricted license transfers:
  - Only purchased quantity licenses are transferred (not in-use quantity) on the **On-Prem License Workspace > Smart Licensing > Inventory** tab **> Licenses** subtab. If all licenses are in-use (for example, Purchased = 5, In-use=5, Balance =0), and you transfer all the purchased quantity (maximum allowed), it will render the "From Local VA" Out-of-Compliance (OOC).
  - You cannot transfer licenses if the Local Virtual Account is already OOC. The **Transfer/Preview** button is grayed out.
- Export-restricted license transfers:
  - **Case 1**: If there are available restricted licenses and no in-use restricted licenses, CSSM Cloud/SSM On-Prem allows the license transfer for the available quantity (balance) and does not add any export control verbiage.
  - **Case 2**: If there are available restricted licenses and some in-use restricted licenses, CSSM Cloud/SSM On-Prem allows the license transfer for the available quantity (balance) with this export control verbiage as shown:

```
Because this license restricted encryption technology, instances of the
license that are currently assigned to product instances cannot be
transferred. Those licenses must be removed from the product instances
before they will be available for transfer.
```

- **Case 3**: If there are available restricted licenses and they are all in-use, CSSM Cloud/SSM On-Prem do not allow the license transfer because allowing transfer would render the "From VA" OOC, and OOC for Export Control is not allowed. The Transfer/Preview is grayed out.

License Hierarchy

When using a smart licensing product, the product instance reports back to SSM On-Prem allowing SSM On-Prem to account for the licenses that are being used. If a license being used is not available for consumption in SSM On-Prem, rather than letting the requested license go out of compliance, a higher tier license can be utilized to satisfy the license request (providing the license exists in the Virtual Account).

For example, if a free Network Advantage license (parent) exists, it can be used (borrowed) to satisfy a request for lower tier licenses such as: LAN, Network, TEI, FAB, ACI, and BASIC. SSM On-Prem supports license hierarchies that support multiple parents or multiple children.

Hierarchy Weights

(Added for On-Prem-8 202010 Release)

NOTE: When you are upgrading to SSM On-Prem Release 8-202008 with hierarchy weights, after you upgrade, you must synchronize your account with CSSM Cloud so that you can view **In Use** counts.

Hierarchy weights determine which licenses take precedence in a situation where there are insufficient licenses. Weights are assigned to products to allow SSM On-Prem to make a calculated decision without the need for human interaction in every event where such a situation occurs.

NOTE: License sharing can only happen in one Product Instance, and therefore, licenses cannot be shared across Product Instances.

License Hierarchy introduces a new challenge in determining which devices should be allocated a borrowed license based on their priority or importance. To address this vital need, a "Weighting" has been introduced that allows a degree of autonomy in deciding the prioritization of license entitlements.

Weights are assigned in descending order from parent to a child. If there are multiple parents and multiple children, the algorithm establishes a specific order for sharing licenses.

For example, if two children require a license, and there is only one license available, the weight algorithm establishes which product receives the license and which will not, resulting in one device becoming Out of Compliance (OOC).

To check if license hierarchy is implemented, navigate to the **On-Prem License Workspace > Smart Licensing > Inventory** tab **> Licenses** subtab. The licenses table displays these columns:

- **License**: Lists the name of the license.
- **Billing**: Lists what status the license is in such as, Prepaid.
- **Available to Use**: Total number of licenses that have been purchased shows as a positive number and any borrowed licenses will be in parenthesis as a negative number. If there is any borrowing/lending happening, it will be listed after the purchases amount with borrowed licenses as a positive number and any lent licenses as a negative number.
- **In Use**: Lists the number of licenses that are in use.
- **Substitution**: Shows the number of licenses that were borrowed and from what level (shared to lower or borrowed from higher) they were borrowed from.
- **Balance**: Lists the difference of the total number of licenses minus the licenses that are being used.
- **Alerts**: Lists any alerts that can affect the license (for example, being out of date).
- **Actions**: Lists any actions that need to be taken for that license.

To view the status within a license that has a hierarchy, click the License Name. A pop-up model opens showing the Local Virtual Account Usage in a pie graph.

Hierarchy Ratios

(Added for On-Prem-8 202102 Release)

Hierarchy ratios utilize an algorithm that calculates the quantity of licenses that can be borrowed from parent nodes and shared amongst child nodes. The children will be assigned specific ratios according to a common algorithm which spans CSSM Cloud, and On-Prem.

Licenses for a specific account are listed in On-Prem in hierarchical order. Therefore, the top license listed will be the parent and bottom license will be the lowest child node.

The number of borrowed licenses is shown in the **Substitution** column represented as a ratio, (the explanation here refers to the table below):

- The license being lent will show a ratio of 1:1 whereas the child license has a ratio of 3:1. Therefore, in the **Purchased** column the parent license will show 1 but in the **Substitution** column the license count will show a number within that ratio depending on the request.
- By clicking on the link in the **Substitution** column, in the pop-up you see what level the license was borrowed from.
- If the license request must go through multiple parents in the hierarchy, then the ratio will be included in the number. For example, if a license request is directed for the child License C (N93-16-Y in table below) with a ratio of 3:1, these actions occur:
  - License C (N93-16-Y in table below) will first check to see if it has enough licenses.
  - If it does not have enough licenses, then it will go up the hierarchy in search of its parents for sufficient licenses. For example, if License B (DCMN-LAN in table below) does not have any licenses but is assigned a ratio of 3:1, then the 3:1 ratio is also included when License C (N93-16-Y in table below) searches for licenses in the next parent, License A

(ACI- Adv in table below), which has a ratio of 1:1. Therefore, the number that shows up in the Substitution column will be a number between 1-9. (3x3).

This table provides a specific example of a license sharing transaction. There are five licenses listed where ACI Advantage is the parent node and NX-OX is the lowest child node.

License	Billing	Available to Use	In Use	Substitution	Balance	Alerts	Actions
ACI Advantage	Prepaid	1	0	To Lower -1	0		
DCMN LAN	Prepaid	0	2	From Higher +1	-2	Insufficient Licenses	
N93-16-Y	Prepaid	0	3	From Higher +3	0		

To see if a license hierarchy is being used, navigate to the **On-Prem License Workspace > Smart Licensing > Inventory** tab **> Licenses** subtab. The licenses table provides these information columns:

- **License**: Lists the name of the license from parent to child.
- **Billing**: Lists what status the license is in such as, for example, Prepaid.
- **Available to Use**: Total number of licenses that have been purchased shows as a positive number. ACI Adv has purchased 1 license.
- **In Use**: Lists the number of licenses that are in use. The children DCMN-LAN and N93-16-Y.
- **Substitution**: When using ratios, this column has been added to show the number of licenses that were borrowed and from what level (shared to lower or borrowed from higher) they were borrowed from. For example, by clicking on the provided link, you can view what licenses were borrowed from what level (represented by a negative number) and the level that received the license(s) (represented by a positive number).
- **Balance**: Lists the difference of the total number of licenses minus the licenses that are being used, for example, DCMN-LAN shows -2 which means it does not have sufficient licenses to fill the request.
- **Alerts**: Lists any alerts that can affect the license (for example, DCMN-LAN shows insufficient licenses.).
- **Actions**: Lists any actions that need to be taken for that license.

To view the status within a license that has a hierarchy, click the **License Name**. A pop-up model opens showing the **Local Virtual Account Usage** in a pie graph.

Application Redundancy Support

Application Redundancy (or Application High Availability) is a method to achieve high availability of applications such as Zone-Based Firewall (ZBFW), Network Address Translation (NAT), VPN (Virtual Private Network), Session Border Controller (SBC), within the product instance. In this application redundancy model, the role of an application can be different from the role of the

system (product instance), for example, an application can be in Standby state on an Active system (product instance) or vice-a-versa.

Currently, product High Availability (HA) assumes that redundancy and fail-over occurs at a Product Instance (mapped to a serial number or UUID) level, and that any given product instance will have a single, consistent state – either active, standby, or in some cases, a member of a HA cluster. In this model, the application redundancy enabled product assumes that there can only be a single active product instance within the HA cluster, and license consumption is reported only by the active product instance.

- In an application redundancy-enabled product (used to prevent double counting of licenses on a fail-over) the application making an entitlement request must provide additional information beyond what is needed for non-redundant applications. The information provided includes:
- An indicator that this is an application redundant configuration
- An active or standby role
- Peer information
- An application unique identifier (UID) so CSSM Cloud or SSM On-Prem can match up multiple usages of the same license

With this additional information, CSSM Cloud and SSM On-Prem know that a specific license in-use is being shared between two applications and they also know the Unique Device Identifier (UDI)s of the devices hosting those applications.

With this additional information, CSSM Cloud and SSM On-Prem show the following:

- In a normal configuration of Active and Active peers, license usage instances are shown as being consumed by both applications.
- In a normal configuration of Active and Standby peers, license usage instances are shared between an active/standby application.
    - On a fail-over, the Standby peer uses the license count from the previous active to avoid double counting.
    - To show which licenses that are in use are shared on a device (product instance).

Application Redundant Enabled Product Instance Workflow

This is the workflow used by application redundant enabled product instances.

1. Register product instances to SSM On-Prem (See Registering Product Instances).

    2. Configure one application as Active and its peer as Standby (Active/Standby) or Active (Active/Active) on product instances with the appropriate commands and peer information (refer to the associated product documentation for the correct configuration).

    - Configure the Active peer so that it points to the Standby peer and vice versa. For example, [DeviceA, TagA, ApplicationA, ID1, Active], reports using 1 license and has peer of [DeviceB, TagB, ApplicationB , ID2, Standby].
    - Alternatively, configure the Active/Active peers with similar information.

    3. Request licenses on both Active and Standby (or Active/Active) peers. Since Cisco SSM and SSM On-Prem have the information on Application Redundant peers, it would show

in the Product instance High Availability tab that the Active peer is consuming license(s), and the Standby is not.

4. In an Active/Standby configuration, if the Active application fails, the Standby peer needs to be specifically reconfigured (via a set of product specific commands) and then declare itself an Active application (without a peer) so that CSSM Cloud or SSM On-Prem would be able to show that the license is now consumed by the new Active (old Standby).

Synchronization File Changes for Application Redundancy

SSM On-Prem adds the Application Redundancy information to the synchronization request when it synchronizes with CSSM Cloud. This action ensures that CSSM Cloud has the same peer information. This way, the CSSM Cloud's **Product** and **License** tabs match SSM On-Prem.

Reporting for Application Redundant Enabled Products

The Licenses and Product Instances tabs have additional subtabs to reflect peer information. You will see the updated **Overview**, **High Availability** and **Events** tabs under the **Product Instances** tab.

Export Control Support

Previous export control support on SSM On-Prem includes the ability to use export restricted functionality for customers that are located inside the EULF/ENC set of countries, roughly US, Canada, EU, Japan, Australia and New Zealand (85% of Cisco customers), and non-public sector customers located outside of the EULF/ENC that require screening to ensure that they are, in fact, non-public sector (approximately 14% of Cisco customers). A Local Account representing the customer is classified as to whether they are subject to Export restrictions. If a customer is classified in the above categories, they can generate export-control-allowed registration tokens such that after registration, the product registered to this customer via this token can turn on export-controlled functionality.

There is a small set of customers (less than 1%), roughly public sector (including government, military, and government-owned enterprises) located outside of the EULF/ENC where US export restrictions apply. These customers are not allowed to generate export control allowed tokens today. However, these customers can apply and receive special permissions for Export Licenses and turn on specific restricted functionality authorized by those Export Licenses.

Enhanced Export Control Authorization Workflow

At a high level, the new Export Control support on SSM On-Prem includes these steps.

1. The Product generates a "Not-allowed" registration token from a Local Virtual Account on SSM On-Prem and registers to it.

NOTE: This type of customer cannot generate an "Allowed" registration token (for example, this option is not available on the Licensing workspace for them).

2. The Product requests a restricted license and quantity from SSM On-Prem via a command or Graphical User Interface (GUI) action that needs to be authorized from CSSM Cloud.
3. When a request is received from a product for a restricted license, it notifies the product to poll it for status, once per hour.

NOTE: Because requests are only polled once per hour. It can take up to 1 hour (3600 seconds) for you to receive product status.

4. SSM On-Prem updates its GUI under the **On-Prem License Workspace > Smart Licensing > Inventory** tab **> Product Instances** tab to indicate the status of the request (License Authorization Pending).
5. When a synchronization is initiated on SSM On-Prem, it sends the restricted license request it receives from the product to CSSM Cloud.
   - If SSM On-Prem is in manual mode, there is a dismissible alert in the **On-Prem Admin Workspace** to remind the user to perform a manual synchronization so that the CSSM Cloud authorization can transmit down to SSM On-Prem.
   - If SSM On-Prem is in network mode, the next synchronization request to CSSM Cloud will contain the export control restricted license authorization response.
6. When SSM On-Prem receives the response from CSSM Cloud, it processes the request and updates the alerts accordingly with a success or failure message and associated reason(s).
   - If authorized, SSM On-Prem updates its **On-Prem License Workspace > Smart Licensing > Inventory** tab **> Product Instances** tab indicating the correct reserved export license count.
   - If not authorized due to the license not being available, a status is reflected on the **On-Prem License Workspace > Smart Licensing > Inventory** tab **> Product Instances** tab. If there are other types of errors such as bad format or invalid export control tag, the status is sent to the products only and is not available on the SSM On-Prem GUI.
7. If the export license is no longer needed, the feature can be disabled, and the product will send a cancellation/return of the Export Control Authorization, returning the license to the Local Virtual Account for use by other product instances. The cancellation request works similarly to the original authorization request in that SSM On-Prem would get the cancellation request from the product, inform the product to check in later for the cancellation authorization status, and send it along for authorization from CSSM Cloud.

Export Control Alerts

There are several alerts in the **On-Prem License Workspace > Smart Licensing > Inventory** tab **> Product Instances** tab on the SSM On-Prem GUI when an export control license is requested.

- **License Request Pending**: When a product requests an Export Control license and is waiting for an authorization from CSSM Cloud.
- **License Return Pending**: When a product requests a cancellation of an Export Control license and is waiting for an authorization from CSSM Cloud.
- **Failed to Connect**: When the product either fails to send an ID, certificate renew (365 days) or when a de-registration is successful, but the de-authorization fails resulting in the export control license not being released.
- **Failed to Renew**: When a device consuming both restricted and non-restricted licenses (regular authorization) and non-restricted authorization renew is expired.

- **Export License Not Available**: When an Export Control license has been requested by the product, but no license is available in the Local Virtual Account.

NOTE: If a “License not Sufficient” error occurs, perform the following action:
Before requesting an export restricted license from a Local Virtual Account, it's best to transfer the export license to the Local Virtual Account.
Also: If requesting an export restricted license from a Local Virtual Account with export licenses in the default account, the device will continue to poll until the user moves the license into the Local Virtual Account and synchronizations.

Future Dated License

(Added for On-Prem-8-202206 Release)

The Future Dated license feature is integrated into SSM On-Prem and enables you to have a license with a future start date. The Future Dated license is processed when the start date < current date, so that Future-dated licenses will not be consumed until the start date becomes current. The purchase count will only be reflected based on license transactions that have a present start date.

NOTE: Future date feature is only supported for Prepaid type licenses.

The License Hierarchy algorithm will not use the future dated licenses. When the future dates become current, it will rerun the License Hierarchy calculations.

The following bullets pertain to the table located in the **Smart Licensing > Inventory** tab **> Licenses** subtab:

- The **Available to Use** column does not include a future start date transaction quantity. The calculations that specify the number in the **Balance** column are used to populate the **Available to Use** and **In Use** columns.
- Hovering the mouse pointer over the **Available to Use** column heading displays the following message: "Available to use does not reflect purchased licenses that have a future start date."

NOTE: Future dated transactions are allowed to transfer between Local Virtual Accounts similar to a normal license.

- If the future start date quantity is greater than 0, the “Awaiting Start Date” message is displayed in the **Alerts** column.
- Click a license name in the **License** column. The **Overview** tab appears and displays the following information:
  - The right pane of the **Overview** tab displays the following message: "out of total 'x' purchased licenses, 'y' of them have a future start date and are not included in **Available to Use**." In this message, "x" purchased licenses are mapped to **entitled_quantity + future start date.**

- In the **Overview** tab, the pie chart reflects the **Available to Use**, **In Use**, and **Balance** columns of the table located in the **Smart Licensing > Inventory** tab **> Licenses** subtab.

Cisco Smart License Using Policy Support

(Added for On-Prem-8-202102 Release)

The Cisco Smart License Using Policy (SL Using Policy) Support feature is integrated into SSM On-Prem and enables you to manage devices (Product Instances) without deploying additional Asset Management Services. After you have installed SSM On-Prem and registered your accounts, you can begin to utilize Smart License Policy Support functionality.

The SSM On-Prem integration with SL Using Policy support provides these capabilities:

- Provide new, update current, and remove obsolete devices utilizing the SSM On-Prem UI. (See Managing Devices)
- Enable import capabilities for devices from CSSM Cloud. (See Authorization Code Requests)
- Provide export capabilities for usage reports and importing Acknowledgement (ACK) from CSSM Cloud.
- SL Using Policy Support will be able to import directly from a device when not connected with CSSM Cloud. (Collecting Usage Reports)
- Provide additional validation of devices for added security (See Validating Devices)

On-Prem SL Using Policy Support Multiple Account Capabilities

There is a drop-down list of associated Accounts (sometimes referred as Tenants) at the top-right corner of the **On-Prem License Workspace**. Use this feature to select the account to work with and to transfer the devices from one registered account to another.

On-Prem SL Using Policy Support Operational Modes

There are two principle operational modes that SSM On-Prem SL Using Policy Support uses. They are:

- **Unconnected** (offline): When SSM On-Prem SL Using Policy is not logged into CSSM Cloud, it can only gather (pull) usage information directly from Product Instances as *.csv files. The **Collect Usage** option is used for the unconnected mode.

NOTE: Product Instances must have already been configured in the system before you can obtain usage data.

- **Connected** (online): When On-Prem SL Using Policy Support is logged into CSSM Cloud, it can export as well as import information, such as auth codes and Acknowledgement (ACK) files, to and from CSSM Cloud. The **Export/Import ALL...** button in the **SL Using Policy** screen is used for these operations in the connected mode.

General Workflow for SL Using Policy Support

For complete procedure for obtaining usages reports, see Using SL Policy Transport URL for Adding Product Instances and Obtaining Usage Data Directly from a Product Instance into On-Prem. For procedures specific to each phase of the process, see SL Using Policy Tab.

1. Add and Register Accounts on to SSM On-Prem.

NOTE: SSM On-Prem SLP feature supports SSM On-Prem Account names with spaces (and other special characters). The SSM On-Prem account name does not affect the SA/VA names, which may contain spaces and do not require any changes.

2. Add and Configure Devices for each account.
3. Add devices to SL Using Policy in SSM On-Prem.

NOTE: Make sure the devices are configured with a single IP; otherwise, there will be unpredictable results.

4. Collect usage data from devices:
    - Push Mode – Using the CLI, navigate to the device location and add devices. After synching with SSM On-Prem, devices are listed in the **On-Prem License Workspace > Smart Licensing > Inventory** tab **> SL Using Policy** table and in the **Product Instance** tab.
    - Pull Mode – In the **On-Prem License Workspace > Smart Licensing > Inventory** tab **> SL Using Policy** subtab, use **Add Single Product**. In the **SL Using Policy** window, choose **Actions for Selected > Collect Usage** to obtain usage reports (*.csv files) Export usage reports to CSSM Cloud.
5. Import acknowledgement reports from CSSM Cloud.
6. Export acknowledgements to devices.
7. Import authentication (auth code) from CSSM Cloud.
8. On-Prem sends auth code to device, which will then auto install authentications and enable features on devices.

SLP Compliance

SSM On-Prem displays and assigns the compliance status for all SLP devices. This Leads to improved compliance visibility for all SL and SLP devices. The SLP device sends the RUM reports to On-Prem, the On-Prem responds back with **OOC** to the device. The On-Prem needs to synchronize with CSSM to get the SLP compliance status as **AUTHORIZED** or **OOC** depending on the availability of purchased licenses in CSSM.

Once the synchronization is successful, depending on the device polling between On-Prem and device, the updated SLP compliance status from the On-Prem is sent to the device.

This applies only for IOS XR version: 24.1.1 (r241x) and above; with the associated Smart Licensing Agent version: 5.9.25_rel/115.

Using SL Using Policy Transport URL for Adding Product Instances (Push Mode)

You must use the CLI when using the SL Using Policy Transport URL. You use this transport method when exporting license information directly from a device to CSSM Cloud.

NOTE: If you need bulk loading of devices for SL Using Policy, use this method.

Complete these steps to export information from a Product Instance to CSSM Cloud using the SL Using Policy Transport URL and the CLI.

List	Action
Loading Product Instances to UI with Usage Data	
Step 1	Log into On-Prem and select the Smart Licensing workspace. screen, and then select the **Inventory** tab.
Step 2	Select a **Local Virtual Account** (top right corner) from the local Virtual Account drop-down list.
Step 3	In the **General** tab, click the **CSLU Transport URL** link. The Product Registration URL pop-up opens listing the URL with the **Tenant ID**.
Step 4	Copy the **URL** Tenant ID listed in the pop-up.
Step 5	Next, using the CLI, connect to the **SLE device** (Smart License Enterprise) you want to manage using either using ssh or telnet. Use the following sequence to obtain a usage report. a. Connect to the **SLE Device** (PI) using either ssh or telnet. b. Enter the **password**. c. Next, use the configuration command: **conf t** and then press **Enter**. d. Change the transport type command to: **#lice smart url cslu <IPaddress>** (paste the url from **step 4** for the IPaddress). Press **Enter**. e. Type **#show lice status** and press **Enter** to show the license status.
Step 6	Next, you can check whether the ack has been received by entering this command: **show license all** Press **Enter**. You receive a list of acknowledgements (ack) received.
Step 7	To send the **Open reports** to On-Prem, you will need to run a **synchronization request**. In the CLI, use this command: **#license smart synch local** Press **Enter**. Refresh the screen and current open status states have been updated (will be in unacknowledged status). The Product Instance is added to the SL Using Policy table. At this stage you can then begin the export process.

List	Action
Exporting Usage Data to CSSM Cloud	
Step 1	Return to On-Prem UI and navigate to **SL Using Policy** tab to begin the export process from On-Prem to CSSM Cloud. a. Select a **device(s) (PI)** from the list. b. Select **Export/Import All > Export Usage to Cisco**. c. A pop-up window opens to list the ack file (***.tar**) that has been generated. d. Click **OK** to save the file. Now the ack file is ready to export to Cisco.
Step 2	To export, log into **CSSM Cloud** and navigate to **Smart Software Licensing > Reports > Usage Data File** tab. **NOTE**: The Usage Data Files are listed in the Reporting Status column and also in the Acknowledgement column as **download**.
Step 3	To download the ack file (*.tar), click on the **download link** in the Acknowledgement column. The file is downloaded to On-Prem and is listed in the download directory.
Step 4	To import the file back to On-Prem, return to **device list** in On-Prem, select the device, and from the Export/Import All tab, select **Import from Cisco**.
Step 5	The Import from Cisco pop-up opens where you can either **browse** for the file (in the download directory) or **drag & drop** the file from the library list. **NOTE**: If you use browse, select the file, and then click **Open**. The file will be imported and a “successfully imported data” notice opens at the bottom of the screen which means that you have successfully obtained usage data from CSSM Cloud.

Obtaining Usage Data Directly from a Product Instance into On-Prem (Pull Mode)

This section describes the steps used to obtain usage data directly from a Product Instance to SSM On-Prem using SL Using Policy. You can use this procedure when you are not connected to CSSM Cloud, and you only want to add one device.

Complete these steps to pull a device into On-Prem.

List	Action
Step 1	In On-Prem, navigate to the **Inventory** tab, and then select a **Local Virtual Account** from the local Virtual Account drop-down list (top right corner).
Step 2	In the Inventory table, select the **SL using policy** tab. The Smart License screen opens.
Step 3	Click **Add a Single Product** to open the Add product pop-up screen. **NOTE**: If you need to import usage information from multiple devices, select **SL using policy >Import Product List**. Using this option will import all the devices into the SL Using Policy table.
Step 4	Enter the **Host** (IPAddress) for the device.
Step 5	Select the **Connect Method**: • Product Instance Initiated Only

List	Action
	• NetConf • RestConf • REST API
Step 6	Click **Product Instance Login Credentials** located in the right column. The Product Instance Login Credentials screen opens. **NOTE**: You need the login credentials if the Product Instances need an authorization code. You need to have added a valid SA/VA **before** any authentication requests can be serviced.
Step 7	Enter the **UserID** and **Password**.
Step 8	Click **Save**. Once validated, the Product Instance is added to the list in the Policy Actions table.
Step 9	Select the **Product Instance** from the list, and from the **Actions for Selected...** button, select **Collect Usage**. When the file is imported (downloaded) a "successfully imported data" message opens at the bottom of the screen. **NOTE**: Collect Usage in when you are not connected to CSSM Cloud is the same synchronization when you are connected.
Obtaining Usage Reports from CSSM Cloud	
Step 1	Click **Export to Cisco** and then wait for the acknowledgement file to be generated.
Step 2	Log into CSSM Cloud and navigate to **Reports > Usage Data Files**. The Acknowledgement (*.tar) file is listed in the table with a **Download** status showing for the Product Instance (Acknowledgement column.)
Step 3	Select the Product Instance record and click **Download**.
Step 4	To import the file back to On-Prem, return to **device list** in On-Prem, select the device, and from the Export/Import All tab, select **Import from Cisco**.
Step 5	The Import from Cisco pop-up opens where you can either **browse** for the file (in the download directory) or **drag & drop** the file from the library list. **NOTE**: If you use browse, select the file, and click **Open**. The file will be imported and a "successfully imported data" notice opens at the bottom of the screen which means that you have successfully obtained usage data from CSSM Cloud.

Product Instances

A product instance is an individual Cisco product (such as a router) with a unique device identifier (UDI) that is registered using a product instance registration token. You can register several instances of a product with a single registration token. Each product instance can have one or more licenses that reside in the same virtual account.

Product instances must periodically connect to the SSM On-Prem server during a specific renewal period. If a product instance fails to connect, it is marked as having a license shortage, but continues to use the license. If you remove the product instance, its licenses are released and made available within the virtual account. (For more information, see Managing Product Instance Registration Tokens.)

Product Instance Registration

When the SSM On-Prem is operational, smart-enabled product instances can register to SSM On-Prem and report license consumption. This registration is between the product instances to SSM On-Prem and is different from the registration between SSM On-Prem and CSSM Cloud.

For products that support Smart Transport, you must configure the "license smart url" on the product to use the Smart Transport Registration URL. For legacy products that still use Smart Call-Home, you must configure the "destination address http" on the product to use the Smart Call-Home Registration URL. The recommended method is Smart Transport. Please consult your Products Configuration Guide for setting the destination URL value.

The following information is required to register a product instance to SSM On-Prem:

- **SSM ON-PREM-URL**: The SSM ON-PREM-URL is the Common Name (CN). The Common Name (CN) is set in the System Administration workspace within the Security Widget, and is entered in the form of a Fully Qualified Domain Name (FQDN), hostname, or IP address of SSM On-Prem.
- **Smart Transport URL**: Smart-enabled product instances need to be configured to send the registration request to SSM On-Prem. This is accomplished by setting the destination HTTP or HTTPS URL in the Smart Transport configuration section of the product configuration depending on the level of encryption used (HTTPS offers stronger encryption of communications then does HTTP). The URL should be set to: http://<SSM ON PREM-URL>:/SmartTransport

NOTE: HTTPS provides encrypted communication between a product and SSM On-Prem whereas HTTP provides clear text communication between a product and SSM On-Prem. Because of the stronger encryption capability, HTTPS is recommended unless there are issues with setting up certifications.

- **Smart Call-Home URL**: Smart-enabled product instances need to be configured to send the registration request to SSM On-Prem. This is accomplished by setting the destination http URL in the Smart Call-Home configuration section of product configuration. The URL should be set to;
  http:// <SSM ON PREM-URL>:/Transportgateway/services/DeviceRequestHandler.
- **TOKEN-ID**: The <TOKEN-ID > is used to associate the Product to the Specific Account and Local Virtual Account you selected on SSM On-Prem.
- **Configuration Guide**: Smart-enabled product instances vary in how they register to SSM On-Prem when using the CLI or GUI, as it depends on the product. For complete instructions on configuring a product instance to communicate with SSM On-Prem, see the documentation for your product.

NOTE: Products that support Strict SSL Cert Checking require **SSM On-Prem-URL** to match the SSM On-Prem Common Name. The common name is provided by navigating to the **Security Widget > Certificates** tab > **Product Certificate Section > Host Common Name** field (located at the top of the page).

NOTE: Products that support Strict SSL Cert Checking require **SSM On-Prem-URL** to match the SSM On-Prem Subject Alternative Name. The Subject Alternative name is provided by navigating to the **Security Widget > Certificates** tab > **Product Certificate Section > Subject Alternative Name** field (located at the top of the page).

NOTE: Products that are deployed in disconnected mode may require the PKI Certificate revocation to be disabled. See the documentation for your product for disabling revocation checks.

Registration Tokens

A product requires a registration token until you have registered the product. Registration tokens are stored in the Product Instance Registration Token Table that is created with your Local Account. When the product is registered, the registration token is no longer necessary and can be revoked and removed from the table. Registration tokens can be valid from 1 to 9999 days. Tokens can be generated with or without the export-controlled functionality feature being enabled. (For more information, see Creating a Product Instance Registration Token.)

Product Instance and License Transfer Behaviors

Product Instance (PI) and License transfer behaviors are different when a license is export restricted.

NOTE: The PI and license transfer behaviors described in this section are only for Local Virtual Accounts on SSM On-Prem.

About Product Instance Transfer

SSM On-Prem product instance (PI) transfer between Local Virtual Accounts is similar to the PI transfer in CSSM Cloud.

- Nonrestricted licenses being consumed by a PI.
  - The PI is transferred, and the in-use quantity is transferred to the destination Local Virtual Account. If the destination has no available licenses, it will render the destination Local Virtual Account Out-of-Compliance (OOC). You will get a warning message announcing a License Shortage.
  - The available license(s) (Purchased Qty) in “From Local VA” are not transferred with the PI transfer. You must transfer the available licenses (Purchased Qty) from the “From Local VA” yourself to the destination to resolve the OOC.

- Export-restricted licenses being consumed by a PI.
  - The PI transfer opens to a new modal with has this additional verbiage:

```
The following licenses that contain restricted encryption technology are
currently assigned to this product instance.
This license assignment will continue after the instance is transferred.
```

  - The transfer operation reflects both the “in-use” and the “available licenses (Purchased Qty)” to the destination Virtual Account because the PI would not have been able to consume a controlled license if it didn't have available licenses. So, the destination Virtual Account will never go OOC.

NOTE: The fundamental difference between transferring a PI versus a License for Export Control is that the available (Purchased Qty) licenses go with the PI transfer to avoid an OOC condition, which is not allowed when Export Control is enforced.

Cisco SSM On-Prem Role-Based Access (RBAC)

To use the capabilities of the Cisco SSM On-Prem license server, you must first login using a valid username and password. When authenticated, the access you have is based on the role you have been assigned. The SSM On-Prem license server offers role-based access control (RBAC) to restrict system access to ensure users only have access to information they have been authorized, or to limit system access according to user responsibility.

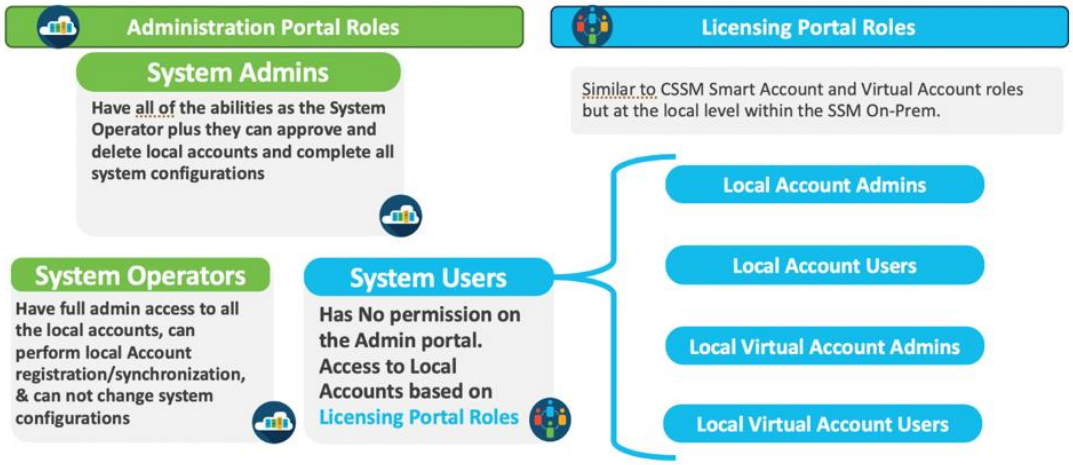

Figure 3: Cisco SSM On-Prem Role-Based Access.

About System Roles

RBAC is broken down into system level roles such as: administrator, operator, and user. The administrator and operator are granted system privileges to their roles. A user is granted system privileges specific to their role.

The available system roles and responsibilities are:

- **System Admin** (Full Access)

  - Full System access to all configuration settings
  - Full Access to all Accounts and Local Virtual Accounts
- **System Operator** (Limited Access)
  - No ability to change system configurations
  - Full Access to all Account(s) and Local Virtual Accounts
- **System User** (Restricted Access)
  - Access is restricted to License Workspace Only

NOTE: A user with the System User role attempting to access the **On-Prem Admin Workspace** is automatically be redirected to the **On-Prem License Workspace**.

  - Must be granted explicit access to Accounts and/or Local Virtual Accounts

About Smart License Roles

The System User role is restricted to the **On-Prem License Workspace** and only has access to Local Accounts if the user has been explicitly granted a **Smart License Role**. Each System User must have a Role assigned for a Local Account before they can gain access to that account. To provide finer grained access, System Users can be restricted to a special Local Virtual Account. The available account roles and responsibilities are:

- **Account Administrator can:**
  - Manage all aspects of the Smart Account and its Virtual Accounts
  - Assign Smart Account Approver role
- **Account User can:**
  - Manage assets within all Virtual Accounts but cannot add or delete Local Virtual Accounts or manage user access.
  - Add Administrator role to specific Local Virtual Accounts for other System Users
- **Local Virtual Account Administrator can:**
  - Allow User or Administrator access only to specific Virtual Accounts.
  - Add Administrator role to specific Local Virtual Accounts for other System Users
- **Virtual Account User can:**
  - Allow User or Administrator access only to specific Local Virtual Accounts

Cisco SSM On-Prem Idle Timeout Feature and ADFS

(ADFS feature included into SSM On-Prem in the 201910 release.)

SSM On-Prem provides a non-configurable timeout security feature that activates if there has been no activity for 10 minutes. After 10 minutes of no activity, the login screen opens requiring you to log into the system. This security feature guards against the possibility of unauthorized use if the workstation is left unattended.

If you are logged into SSM On-Prem using ADFS, and the timeout feature is activated, you are returned to the SSM On-Prem login page. From this page, you can continue to work in ADFS applications by clicking the **Login Using OAuth2 ADFS** link on the right side of the login screen. Because you remain logged into the ADFS server, but not SSM On-Prem, you are logged back into SSM On-Prem immediately and are able to use any applications that were open at the time you were logged out of SSM On-Prem.

NOTE: SSM On-Prem and ADFS are configured to function independently; therefore, when you are logged out of SSM On-Prem, ADFS, and all ADFS-related applications, remain running until either you close them or the default 12-hour ADFS idle time limit is reached. This means that logging out of SSM On-Prem does not log you out of ADFS until all other client applications log out of ADFS or the ADFS idle time limit is reached.

Endpoint Reporting Model (ERM)

Endpoint Reporting Model (ERM) is an additional API to Smart Licensing that allows binding licenses required by Access Points connected to WLAN Controllers such as WLC (Cisco WLAN Controller).

ERM uses an API call with the request type ENDPOINT_REPORT that binds the license with a particular Access Point. ERM eliminates the possibility of double counting licenses for customers when one WLAN controller is substituted for another WLAN Controller (Access Point moves from one controller to another) in the same Local Account, for example, when one controller fails.

Support for MSLA (Usage-Based Billing)

(Added for SSM On-Prem-8 202008 Release)

NOTE: The terms MSLA, Utility, Usage, or Post-paid are used interchangeably.

The Cisco Managed Service License Agreement (MSLA) program is a software licensing and consumption framework designed for Cisco customers and partners who offer managed software services to third parties. MSLA offers your Service Provider (SP) customers a simple way to buy software, which they can then offer as part of a service solution to their customers. MSLA offers SPs with an OpEx strategy for investing in Cisco software in a pay-as-you-go consumption model.

MSLA contracts have an initial three-year term. They automatically renew for a one-year term unless a new three-year term is negotiated. Listed here are the characteristics that comprise MSLA.

- Specific software products and solutions productized under the MSLA.
- Provides a fixed price for the term of the MSLA.
- Cisco software support with access to Cisco TAC 24/7/365, maintenance and minor updates, major upgrades, and Cisco online support knowledgebase.
- Ease of doing business with Smart Usage: one zero-dollar purchase order is all it takes to get started.

- Smart Account for visibility and management of license usage.
- Ability to deploy as many licenses as needed to deliver services to end customers. No additional paperwork or transactions required.
- Ability to reuse and redeploy licenses among an SP's end customers.
- SP generates usage report monthly for postpaid billing.

How It Works

- The Service Provider's account team submits a zero-dollar purchase order that includes the software Usage PIDs (or Subscription ID) for their customers who have signed the MSLA. The SPs then select the monthly usage SKUs within that subscription.
- The price of products available under MSLA currently is tied to the license and is a monthly usage fee. The monthly amount billed for a particular product will be:

  (monthly price per license) x (number of licenses used in that month)

- The subscription ID and license entitlements are deposited in the SP's Smart Account. Devices must connect to SSM On-Prem and enable **Usage mode** to send usage information.

NOTE: Devices connecting directly to CSSM cannot enable Usage mode and will be handled as pre-paid by CSSM. That is, CSSM currently does not support Usage billing for directly connected product instances.

- SSM On-Prem receives measurements from the products and periodically synchronizes with Cisco to exchange entitlement details and relay usage information to the Software Billing Platform (SBP) for rating and billing.

MSLA Data Reporting and Collection

Listed here are the stages that comprise the MSLA reporting and collection process.

- Product reports entitlement tag and usage count of that entitlement, so that every time an entitlement is used it is reported regardless of how long it was in use during that monitoring period.
- Product collects measurements every 15 minutes (the measurements show the maximum count in use.)
- Product reports to SSM On-Prem every 4 hours or 6 times a day.
- SSM On-Prem reports data to Smart Receiver once every 8 hours, or 3 times a day.
- Data is retained for up to 30 days on the product, so it can be resent if there is a communications failure or if SSM On-Prem loses the data because of a restore.

MSLA Workflow

The steps presented here describe the MSLA-based licensing workflow.

1. Customer purchases MSLA subscription and individual usage licenses on Cisco Commerce Workspace (CCW).

2. MSLA licenses are deposited on CSSM Cloud Default Virtual Account in the respective customer Smart Account.

NOTE: Cisco does not support usage licenses in Local Virtual Accounts.

3. SSM On-Prem registers and synchronizes with CSSM Cloud, so it will contain the entitlements of charge type usage.
4. Smart Agent enables Smart Licensing and Usage with CLIs.
5. Smart Agent registers to SSM On-Prem.
6. Smart Agent requests a license via an authorization-request.
7. SSM On-Prem checks whether that license is available in MSLA mode (a subscription ID and charge type = usage).
8. SSM On-Prem fulfills license in MSLA mode if a MSLA license is available. It responds to the authorization renew with the Subscription ID and informs the Smart Agent it can send the RUM report to SSM On-Prem.

NOTE: If MSLA mode is enabled and a MSLA license entitlement is not available, it fulfills the authorization request in pre-paid mode.

9. Smart Agent sends a RUM report.
10. SSM On-Prem accepts the RUM report from Smart Agent.
11. SSM On-Prem sends the RUM report to Smart Receiver every 8 hours.
12. Smart Receiver sends to SBP for billing once a day.
13. SSM On-Prem stores 90 days of raw data (For details, see Daily or Monthly Usage Report).

MSLA Workflow for SLP

(Added for SSM On-Prem-8 202206 Release)

The steps presented here describe the MSLA-based licensing workflow.

1. Customer purchases MSLA subscription and individual usage licenses on Cisco Commerce Workspace (CCW).
2. MSLA licenses are deposited on the CSSM Cloud Default Virtual Account in the respective customer Smart Account.

NOTE: Cisco does not support usage licenses in Local Virtual Accounts.

3. SSM On-Prem registers and synchronizes with CSSM Cloud, so it will contain the entitlements of charge type usage.
4. Smart Agent enables Smart Licensing and Usage with CLIs to Enable utility mode.

5. Device needs to be added to On-Prem CSSM with specific Smart Account/Virtual Account (PULL mode) before enabling utility flag and sending RUM reports.
6. RUM reports and all other messages sent to the SSM On-Prem will include a utility-enabled flag.
7. SSM On-Prem will forward RUM reports to CSSM Cloud and retrieve RUM ACK responses that it will send back to the PI.
8. CSSM sends back the RUM ACK along with subscription ID for each entitlement.
9. SLP RUM reports from then on will include the subscription ID for each entitlement tag in use when sent to CSSM Cloud.
10. CSSM Cloud sends the usage with subscription to SBP via Smart Receiver for billing once a day.

NOTE: If MSLA mode is enabled and a MSLA license entitlement is not available, it will be flagged as prepaid on CSSM.

11. The smart agent must receive an ACKs within 30 days for each RUM report.

Synchronization Changes for an MSLA-Enabled SSM On-Prem

These conditions define SSM On-Prem as in MSLA-enabled mode.

- You must have a subscription ID with the associated usage-based licenses.
- A device has registered to SSM On-Prem and enabled Smart License Utility mode (<conf t Smart License Utility>).
- There is at least one product instance consuming an entitlement tag of usage type.
- SSM On-Prem has received acknowledged RUM reports within the last 30 days.

The reason that SSM On-Prem must have connectivity to Cisco (swapi.cisco.com) is because customers cannot be billed unless RUM reports are being sent to Cisco (Smart Billing Platform) on a regular basis (every 8 hours).

NOTE: If you have upgraded from Cisco Smart Software Classic version 5.0.1, make sure when upgrading to SSM On-Prem version 8 that your firewall is open to both cloud.cisco.com and swapi.cisco.com. See *Cisco Smart Software On-Prem Installation Guide* for details on upgrading from previous versions.

The On-Prem-to-Smart Receiver synchronization is for SSM On-Prem to send RUM reports that are forwarded to the Software Billing Platform for billing. Furthermore, there is a requirement that SSM On-Prem must communicate with Cisco (swapi.cisco.com). If it fails to communicate within 30 days, it will shift from usage-based license consumption to pre-paid license consumption.

On a scheduled synchronization, SSM On-Prem performs the synchronization to CSSM Cloud at the configured scheduled time and the list of registered products in pre-paid and usage modes is sent to Cisco (swapi.cisco.com).

Authorization Renews from Smart Agents

Smart Agent authorization request and renew flows do not change when a product runs in MSLA mode. In MSLA mode, the Smart Agent sends RUM reports to SSM On-Prem periodically and the 90-day authorization-renew expiry is still in effect.

SSM On-Prem UI and License Reports in MSLA Mode

Supporting MSLA requires the SSM On-Prem UI and reports to be modified to represent post-paid billing types and usage reporting. When SSM On-Prem is in MSLA mode there are several UI changes.

License tab under a Virtual Account Modifications

The **License** tab has three modifications to it in MSLA mode. They are:

- **Billing, Purchased, In-Use, and Balance headings** reflect the post-paid licenses.
- **Purchase = "-"** shows that there is not a specific quantity required because the customers pay for what they use on a monthly, so they don't have to specifically purchase any quantity.
- **In-Use** indicates the number of Product Instances currently consuming these MSLA licenses.

Product Instances License Consumption

You can also get a report of the various Product Instances consuming licenses in a virtual account by selecting the **Product Instances** tab.

Complete these steps to view the Product Instances report.

Step	Action
Step 1	Select a **Virtual Account**. -
Step 2	Select **Licenses > License Name**.
Step 3	Select the **License** tab, then click **In Use Count** for that particular usage-based license. A list of products opens that is consuming that license.

Smart Agent Operational Changes for MSLA

Products must integrate a new Smart Agent (version 4.2.0) to report MSLA data. If the products have already integrated with a version earlier than 4.2.0 Smart Agent, they should move to 4.3 as soon as possible. For backward compatibility, a product with an older Smart Agent continues to work with the new MSLA-enabled SSM On-Prem.

- For non-MSLA enabled Products interacting with MSLA-enabled SSM On-Prem running in pre-paid mode will have these two operational characteristics.
  - Product continues to use the default Smart Call-Home (SCH) configuration.
  - Product registers to SSM On-Prem as before.
- For MSLA-enabled Products interacting with MSLA-enabled MSLA.
  - Product must explicitly enable Smart Usage through the smart license command.

```
-conf t
-license smart utility
```

- Product must explicitly enable Smart Transport with the license smart transport command.

```
-conf t
-license smart transport smart
-license smart <url>) command
```

- Product must explicitly configure the Smart Usage transport URL via the `license smart url <url>` command where URL is the satellite IP address or FQDN.

SSM On-Prem Operational Changes for MSLA

The following operational changes occur when SSM On-Prem is MSLA enabled.

- SSM On-Prem needs connectivity with Cisco.

NOTE: SSM On-Prem can also be manually synchronized, but if SSM On-Prem is MSLA enabled, there must be a connection to swapi.cisco.com.

- If no MSLA subscription exists and the product tries to consume MSLA (by sending MSLA data to SSM On-Prem), SSM On-Prem fulfills as "pre-paid."
- If an account has license type "usage" (MSLA), then both the **Available Actions** and **Actions** buttons for that license are disabled and you can only edit or delete license tags for that account. You cannot perform any other actions (**Actions** button) for that license whereas those limitations are not on a pre-paid license.

Changes to Enable MSLA Configuration

To enable MSLA on a Product, follow this command sequence.

1. Enable MSLA on the Product by using this command sequence:

```
Sushmaa_spla_83#config t
Enter configuration commands, one per line. End with CTRL+Z
Sushma_spla_83(config)#Lic
Sushma_spla_83(config)#License sm
Sushma_spla_83(config)#License smart ut
Sushma_spla_83(config)#License smart utility
Sushma_spla_83(config)#end
Sushma_spla_83#wr
```

2. Next, you will need to enable Smart Transport using this command sequence:

```
Sushma_spla_83(config)#License smart transport smart
Sushma_spla_83(config)#
```

3. In this step, you specifically configure the Smart Transport URL using this configuration command that points to SSM On-Prem IP Address:

```
Sushma_spla_83(config)#Lic
Sushma_spla_83(config)#License sm
Sushma_spla_83(config)#License sm ur
Sushma_spla_83(config)#License sm url
http://<ip_address>:80/Transportgateway/services/DeviceRequestHandler
     or for more security usr this URL
Sushma_spla_83(config)#License sm url Error! Hyperlink reference not
valid.
```

```
Sushma_spla_83(config)#wr
```

To check to see if MSLA is properly enabled on a product, use this TAC command:

```
show license tech support
```

Using this command will bring up the following information:

- Status information (enabled or disabled)
- Registration:
  - Status
  - Export-Controlled Functionality
- License Authorization
  - Status
  - Evaluation Period Remaining (Days, Hours, Minutes, Seconds)
- Usage Status and Usage Report:
  - Last success
  - Last attempt
  - Next attempt
- Usage Report Status
  - Last success
  - Last attempt
  - Next attempt

On-Prem Admin Workspace

The System Administration workspace is available to configure the SSM On-Prem system before it can be operational. It is accessible via the URL: https://<ip-address>:8443/admin.

The SSM On-Prem System Administration Workspace has a collection of Widgets each shown as a clickable circular image on the workspace. An overview of each Widget's function is described here.

NOTE: SSM On-Prem has an Idle Timeout security feature that activates if there has been no activity for 10 minutes. After 10 minutes of no activity, you are required to log into the system again.
If you are logged into SSM On-Prem using ADFS when the timeout feature activates, log into the system again by clicking the ADFS button on the login page.
For more details on this feature, see the Cisco SSM On-Prem Idle Timeout Feature.

- **Users Widget**: Allows the System Administrator (or System Operator) to create local users and configure advanced parameters such as setting passwords.

- **Access Management Widget**: Allows the Administrator to manage the configuration for LDAP, LDAP Users, LDAP Groups, OAuth2 ADFS, TACACS+ Configuration, as well as Single Sign On (SSO) Clients.
- **System Settings Widget**: Allows the Administrator to manage settings needed by SSM On-Prem such as: Messaging, Syslog, Language, Email, Time Settings including NTP Servers, CSLU, Event Log Settings and Message of the Day.
- **Network Widget**: Allows the Administrator to manage network IP, DNS servers, default gateway addresses, proxy parameters, and syslog configuration. It also supports both IPv4 and IPv6 settings.
- **Accounts Widget**: Allows the Administrator to add new accounts, manage existing accounts and account requests, and to view event logs for accounts (For detailed information on accounts, (see About Accounts and Virtual Accounts).
- **Synchronization Widget**: Allows the Administrator to view a list of Local Accounts, their status (alerts/alarms, if an account has warnings or alarms against it), to synchronize those accounts (their licenses) with CSSM Cloud, as well as synchronization schedules for each account.
- **API Toolkit Widget**: Allows the Administrator to create client and resource authentication credentials for accessing the SSM On-Prem public REST API.
- **Security Widget**: Allows the Administrator to manage certificates, password strength and expiration, rules, and password auto-lock features. It also provides an Events tab to track histories of these features.
- **High Availability Widget**: (The system must have a High Availability cluster installed and configured for this widget to be visible.) This Widget allows the Administrator to view basic cluster information with a simulated illustration. This widget also is functional for monitoring clusters utilizing TACACS+.
- **Support Center Widget**: Allows the Administrator to search, view, and download system logs directly from the GUI instead of the console.

System Health Status Readout

The right side of the Administration Workspace screen shows a status readout. This readout shows:

- System Health: This parameter shows the state of your machine, along with a statement such as, “Good - Your machine is working well. In addition, it shows:
  - The server name
  - The current version of SSM On-Prem installed on the server
  - Uptime: How long the SSM On-Prem server has been running
  - The Interface parameter that monitors the traffic load being used by that interface
- Resource Monitor Percentage: This parameter shows the SSM On-Prem server CPU, RAM, and Disk activity as both a bar graph and percentage.
- Recent Alerts: This parameter shows any alerts registered by the SSM On-Prem application.

- Connected Users: This parameter shows the users currently logged into the SSM On-Prem server.

NOTE: The System Health status along the right-hand panel is automatically displayed and cannot be turned off at this time.

Event Log Messages

(Added for the On-Prem 202008 release)

Each widget in the administration workspace has event logs. You can search for specific events using the search field or you can download a .csv (comma-separated value) file to a local drive.

This table lists the event logs associated to each widget.

Release	Category	Message Type	Description	Outcome	Level	Recommended Action
8-202008	Access Management	ADFS Configuration Updated	ADFS configuration updated	success	INFO	N/A
8-202008	Access Management	ADFS Configuration Updated	ADFS configuration updated	failure	WARN	Review additional log messages for causes of the error. Retry updating the ADFS configuration.
8-202008	Access Management	LDAP Configuration Updated	LDAP configuration updated	success	INFO	N/A
8-202008	Access Management	LDAP Configuration Updated	LDAP configuration updated	failure	WARN	Review additional log messages for causes of the error. Retry the LDAP configuration change.
8-202008	Access Management	LDAP Group Roles Assigned	LDAP group roles assigned	success	INFO	N/A
8-202008	Access Management	LDAP Group Roles Assigned	LDAP group roles assigned	failure	WARN	Review additional log messages for causes of the

Release	Category	Message Type	Description	Outcome	Level	Recommended Action
						error. Retry assigning the role(s).
8-202008	Access Management	LDAP Groups imported	LDAP group roles assigned	success	INFO	N/A
8-202008	Access Management	LDAP Groups imported	LDAP group roles assigned	failure	WARN	Review additional log messages for causes of the error. Retry importing the LDAP groups.
8-202008	Access Management	SSO Configuration Updated	SSO configuration updated	success	INFO	N/A
8-202008	Access Management	SSO Configuration Updated	SSO configuration updated	failure	WARN	Review additional log messages for causes of the error. Retry updating the SSO configuration.
8-202008	Access Management	IdP User Created	<idp> user <username> created	success	INFO	When a remote identity provider (IdP, such as ADFS / LDAP / SSO) user first logs on, a local user is created.
8-202008	Access Management	IdP User Created	<idp> user <username> created	failure	WARN	Review additional log messages for causes of the error. Verify the user on the remote identify provider (IdP). Attempt to log

Release	Category	Message Type	Description	Outcome	Level	Recommended Action
						the user on again.
8-202008	Account	Account Requested	Satellite Account was requested	success	INFO	Administrator should choose to approve or reject the request.
8-202008	Account	Account Request Rejected	On-Prem Account request was rejected	success	INFO	N/A
8-202008	Account	Account Registered	Satellite Account request was approved and registered with Cisco	success	INFO	N/A
8-202008	API Tool Kit	OAuth Client Created	OAuth client created: <name>	success	INFO	N/A
8-202008	API Tool Kit	OAuth Client Created	OAuth client created: <name>	failure	WARN	Review additional log messages for causes of the error. Retry creating the OAuth client.
8-202008	API Tool Kit	OAuth Client Deleted	OAuth client deleted: <names>	success	INFO	The message can contain one or more names of OAuth clients that have been deleted.
8-202008	API Tool Kit	OAuth Client Deleted	OAuth client deleted: <ids>	failure	WARN	The message can contain one or more ID numbers of OAuth clients that failed to be deleted. Review additional log messages for causes of the error. Retry

Release	Category	Message Type	Description	Outcome	Level	Recommended Action
						deleting the OAuth client(s).
8-202008	API Tool Kit	OAuth Client Updated	OAuth client updated: <name>	success	INFO	N/A
8-202008	API Tool Kit	OAuth Client Updated	OAuth client updated: <name>	failure	WARN	Review additional log messages for causes of the error. Retry updating the OAuth client.
8-202008	Network	Network Updated	general network configuration updated	success	INFO	N/A
8-202008	Network	Network Updated	general network configuration updated	failure	WARN	Review additional log messages for causes of the error. Retry the general network configuration change.
8-202008	Network	Network Updated	network interface <interface> configuration updated	success	INFO	N/A
8-202008	Network	Network Updated	network interface <interface> configuration updated	failure	WARN	Review additional log messages for causes of the error. Retry the network interface configuration change.
8-202008	Network	Proxy Updated	Proxy server <server>:<port> enabled	success	INFO	N/A
8-202008	Network	Proxy Updated	Proxy server <server>:<port> enabled	failure	WARN	Review additional log messages for causes of the

Release	Category	Message Type	Description	Outcome	Level	Recommended Action
						error. Retry the proxy settings change.
8-202008	Security	Auto Lock Settings Updated	Auto Lock settings updated. Login Attempts: <login_attempts>, Within (minutes): <within_minutes>, Lock Expiration (minutes): <lock_expiration_minutes>	success	INFO	N/A
8-202008	Security	Session Limit Settings Updated	Web session limit enabled. Limit: <limit>	success	INFO	N/A
8-202008	Security	Session Limit Settings Updated	Web session limit disabled.	success	INFO	N/A
8-202008	Security	Obsolete TLS Settings Updated	Obsolete TLS 1.1 protocol <enabled|disabled> for SSM On-Prem web server.	success	INFO	N/A. Please be aware that this restricts the SSM On-Prem web server to only support TLS 1.2.
8-202008	Security	Account Security Settings Updated	Account tab security settings (Auto Lock, Session Limit, Obsolete TLS toggle) failed to apply.	failure	WARN	Review additional log messages for causes of the error. Retry the account security change.
8-202008	Security	Password Settings Updated	Password settings updated.	success	INFO	
8-202008	Security	Password Settings Updated	Password settings updated.	failure	WARN	Review additional log messages for causes of the error. Retry the password

Release	Category	Message Type	Description	Outcome	Level	Recommended Action
						settings change.
8-202008	Security	Common Name updated	Common Name updated.	success	INFO	
8-202008	Security	Common Name updated	Common Name updated.	failure	WARN	Review additional log messages for causes of the error. Retry the common name change.
8-202008	Security	CSR Generated	CSR (Certificate Signing Request) generated.	success	INFO	
8-202008	Security	CSR Generated	CSR (Certificate Signing Request) generated.	failure	WARN	Review additional log messages for causes of the error. Retry generating a new CSR.
8-202008	Security	Certificate uploaded	Certificate uploaded.	success	INFO	
8-202008	Security	Certificate uploaded	Certificate uploaded.	failure	WARN	The certificate passed validation, but an internal error occurred. Review additional log messages for causes of the error. Retry uploading the certificate.
8-202008	Security	Certificate deleted	Certificate deleted.	success	INFO	**Note**: this action also removes any intermediate CA certificate(s) that were

Release	Category	Message Type	Description	Outcome	Level	Recommended Action
						originally uploaded with the signed identity certificate.
8-202008	Security	Certificate deleted	Certificate deleted.	failure	WARN	Review additional log messages for causes of the error. Retry deleting the certificate.
8-202008	Security	CA Certificate uploaded	CA Certificate uploaded.	success	INFO	
8-202008	Security	CA Certificate uploaded	CA Certificate uploaded.	failure	WARN	The certificate passed validation, but an internal error occurred. Review additional log messages for causes of the error. Retry uploading the CA certificate.
8-202008	Security	CA Certificate deleted	CA Certificate deleted.	success	INFO	
8-202008	Security	CA Certificate deleted	CA Certificate deleted.	failure	WARN	Review additional log messages for causes of the error. Retry deleting the CA certificate.
8-202008	Session	Session Created	Creating session <session id>	success	INFO	N/A
8-202008	Session	Session Destroyed	Destroying session <session id>	success	INFO	N/A

Release	Category	Message Type	Description	Outcome	Level	Recommended Action
8-202008	Session	Session Expired	Session <session id> expiring	success	INFO	N/A
8-202008	Settings	Banner Updated	Banner updated, <state>	success	INFO	N/A
8-202008	Settings	Banner Updated	Banner updated, <state>	failure	WARN	Review additional log messages for causes of the error. Retry the banner messaging change.
8-202008	Settings	Language Locale Updated	Locale changed to <locale_name>	success	INFO	N/A
8-202008	Settings	Language Locale Updated	Locale changed to <locale_name>	failure	WARN	Review additional log messages for causes of the error. Retry the language/locale change.
8-202008	Settings	Message of the Day Updated	Message of the day updated	success	INFO	N/A
8-202008	Settings	Message of the Day Updated	Message of the day updated	failure	WARN	Review additional log messages for causes of the error. Retry the message of the day settings change.
8-202008	Settings	Remote Syslog Updated	Remote syslog <server>:<port> updated, <state>	success	INFO	N/A
8-202008	Settings	Remote Syslog Updated	Remote syslog <server>:<port> updated, <state>	failure	WARN	Review additional log messages for causes of the error. Retry the remote syslog

Release	Category	Message Type	Description	Outcome	Level	Recommended Action
						configuration change.
8-202008	Settings	Email SMTP Settings Updated	SMTP settings updated	success	INFO	N/A
8-202008	Settings	Email SMTP Settings Updated	SMTP settings updated	failure	WARN	Review additional log messages for causes of the error. Retry the email settings configuration change.
8-202008	Settings	Time Settings Updated	Time settings updated	success	INFO	N/A
8-202008	Settings	Time Settings Updated	Time settings updated	failure	WARN	Review additional log messages for causes of the error. Retry the time settings change.
8-202008	User	User Login	Logging in user	success	INFO	N/A
8-202008	User	User Login	Logging in user	failure	WARN	Confirm that user exists, user is enabled and that the correct password was used.
8-202008	User	User Logout	Logging out user	success	INFO	N/A
8-202008	User	User Added	Creating new user <username>	success	INFO	N/A
8-202008	User	User Added	Creating new user <username>	failure	WARN	Review UI error messages or additional log messages. Retry and

Release	Category	Message Type	Description	Outcome	Level	Recommended Action
						contact support if error is repeated.
8-202008	User	User Deleted	Deleting user <username>	success	INFO	N/A
8-202008	User	User Deleted	Deleting user <username>	failure	WARN	Review UI error messages or additional log messages. Retry and contact support if error is repeated.
8-202008	User	User Password Changed	Changing password for user <username>	success	INFO	N/A
8-202008	User	User Settings Changed	Changing settings for user <username>	success	INFO	N/A
8-202008	User	User Disabled	Disabling user <username>	success	INFO	N/A
8-202008	User	User Disabled	Disabling user <username>	failure	WARN	Review UI error messages or additional log messages. Retry and contact support if error is repeated.
8-202008	User	User Enabled	Enabling user <username>	success	INFO	N/A
8-202008	User	User Enabled	Enabling user <username>	failure	WARN	Review UI error messages or additional log messages. Retry and contact support if error is repeated.

Release	Category	Message Type	Description	Outcome	Level	Recommended Action
8-202008	User	User System Role Changed	Changing system role to <role> for user <username>	success	INFO	N/A
8-202008	User	User System Role Changed	Changing system role to <role> for user <username>	failure	WARN	Review UI error messages or additional log messages. Retry and contact support if error is repeated.
8-202008	Satellites	Satellite File Synchronization	Satellite <satellite_name> synchronized via file synchronization	success	INFO	N/A
8-202008	Satellites	Satellite File Synchronization	Satellite <satellite_name> synchronized via file synchronization	failure	WARN	Review additional log messages for causes of the error. Retry the synch.
8-202008	Satellites	Satellite Network Synchronization	Satellite <satellite_name> synchronized via network synchronization	success	INFO	NOTE: This message also applies when Scheduled Synchs are triggered.
8-202008	Satellites	Satellite Network Synchronization	Satellite <satellite_name> synchronized via file synchronization	failure	WARN	Review additional log messages for causes of the error. Retry the sync.
8-202008	Satellites	Scheduled Synchronization	Scheduled Synchronization <enabled|disabled> for satellite "<satellite_name>"	Success	INFO	N/A
8-202008	Satellites	Scheduled Synchronization	Scheduled Synchronization <enabled|disabled> for	Failure	WARN	Review additional log messages for

Release	Category	Message Type	Description	Outcome	Level	Recommended Action
			satellite "<satellite_name>"			causes of the error. Retry
8-202008	Satellites	Satellite Synchronization Data Privacy Settings	Satellite synchronization data privacy settings modified, <enabled|disabled>, for satellite "<satellite_name>"	success	INFO	N/A
8-202008	Satellites	Satellite Synchronization Data Privacy Settings	Satellite synchronization data privacy settings modified, <enabled|disabled>, for satellite "<satellite_name>"	failure	WARN	Review additional log messages for causes of the error. Retry the settings change.
8-202008	Satellites	Scheduled Synchronization	Global Scheduled Synchronization modified, <enabled|disabled>.	success	INFO	N/A
8-202008	Satellites	Scheduled Synchronization	Global Scheduled Synchronization modified, <enabled|disabled>.	failure	WARN	Review additional log messages for causes of the error. Retry the settings change.
8-202008	Satellites	Global Synchronization Data Privacy Settings	Global synchronization data privacy settings modified	success	INFO	N/A
8-202008	Satellites	Global Synchronization Data Privacy Settings	Global synchronization data privacy settings modified	failure	WARN	Review additional log messages for causes of the error. Retry the settings change.
8-202008	Tags	Tag Created	Virtual account custom tag created: <tag_name>	success	INFO	N/A
8-202008	Tags	Tag Created	Virtual account custom tag created: <tag_name>	failure	WARN	Review additional log

Release	Category	Message Type	Description	Outcome	Level	Recommended Action
						messages for causes of the error. Retry creating the tag.
8-202008	Tags	Tag Modified	Virtual account custom tag modified: <tag_name>	success	INFO	N/A
8-202008	Tags	Tag Modified	Virtual account custom tag modified: <tag_name>	failure	WARN	Review additional log messages for causes of the error. Retry modifying the tag.
8-202008	Tags	Tag Deleted	Virtual account custom tag deleted: <tag_name>	success	INFO	N/A
8-202008	Tags	Tag Deleted	Virtual account custom tag deleted: <tag_name>	failure	WARN	Review additional log messages for causes of the error. Retry deleting the tag.
8-202008	Tags	Tag Created	License tag created: <tag_name>	success	INFO	N/A
8-202008	Tags	Tag Created	License tag created: <tag_name>	failure	WARN	Review additional log messages for causes of the error. Retry creating the tag.
8-202008	Tags	Tag Modified	License tag modified: <tag_name>	success	INFO	N/A
8-202008	Tags	Tag Modified	License tag modified: <tag_name>	failure	WARN	Review additional log messages for causes of the error. Retry

Release	Category	Message Type	Description	Outcome	Level	Recommended Action
						modifying the tag.
8-202008	Tags	Tag Deleted	License tag deleted: <tag_name>	success	INFO	N/A
8-202008	Tags	Tag Deleted	License tag deleted: <tag_name>	failure	WARN	Review additional log messages for causes of the error. Retry deleting the tag.

Access Management Widget

The Access Management widget in the SSM On-Prem Administration Workspace provides the following access management functionality:

NOTE: Local Authentication is the primary means of authentication using a local authentication database embedded in SSM-On Prem (not using an external authentication server). To use this form of authentication **do not enable LDAP, OAuth2 ADFS or SSO.**

- **LDAP** (Lightweight Directory Access Protocol) **Configuration tab**: Used to configure an LDAP server for SSM On-Prem as an external authentication mechanism using either Open LDAP or Active Directory.

NOTE: Consider the following scenario: two users share the same username; one of them is authenticated locally, while the other is authenticated through LDAP. In such cases, the system will first check the local user's password and their account status:

1. If the password matches and the account is enabled, the local user is granted access.
2. If the local user's password doesn't match, the system checks the LDAP user's password and grants access upon verification.
3. If the local user is disabled, the access is denied, and LDAP check is not performed.

- **LDAP Users tab**: This tab contains a list of the LDAP users. In one of our previous releases (8-202102) there was an ask to remove LDAP Users Tab from Access management widget. From

this point, any operations could be performed only on the LDAP groups and not a single user. However, it has not been justified by the customers' needs and you needed to bring back the functionality. So, in the release **8-202112**, the customers would be able to see LDAP Users Tab under Access Management widget on the Admin Portal. **The tab shows the highest system role assigned to the LDAP user** refer the example mentioned below**.**

Example:

Case1: User is a system admin on the LDAP group and as a system user in user widget.

If a user has a privilege of system admin on the LDAP group and as a privilege of system user on user widget, then the LDAP Users tab will show the highest privilege role among the system admin and system user roles, that is the system admin role.

Case2: User is a system user on the LDAP group and as a system admin in user widget.

If a user has a privilege of system user on the LDAP group and as a privilege of system admin on user widget, then the LDAP Users tab will show the highest privilege role among the system admin and system user roles, that is the system admin role.

- **LDAP Groups tab**: LDAP user groups are defined on the LDAP server and consist of groups of LDAP users. SSM On-Prem integration with LDAP allows it to assign RBAC to the accounts and Local Virtual Accounts for each LDAP group. Therefore, instead of assigning individual users one at a time for access to the Account and Local Virtual Accounts in SSM On-Prem Users tab, you can use the LDAP Groups tab to assign these resources to whole LDAP user groups.

NOTE: After upgrading to the On-Prem 8-202102 release, LDAP Users were not listed in either the Account Management > Users tabs. In addition, all existing LDAP Users in the User Groups tab are removed.
This tab has been introduced back in the On-Prem release 8-202112.

- **OAuth2 ADFS tab**: If you are using a Windows Server operating system with SSM On-Prem, you can use Active Directory Federation Services (ADFS) to authenticate users.
- **SSO Configuration tab**: Is used to configure secondary authentication information for a client.
- **TACACS+ Configuration tab**: Is used to direct authentication, Authorization, and Accounting to a centralized TACACS+ Server to process the need for maintaining local users on each device.

LDAP Configuration Tab

To enable SSM On-Prem to use an external LDAP server for external authentication, use the LDAP Configuration option.

- For LDAP authentication, enter the following information:
  - **Verify Server Certificate**: If you are establishing TLS connections to your server, use this option to verify that the verification of the server's certificate was signed by a trusted CA or by a custom CA that was uploaded. By enabling this option, communication to the

remote server will go over TLS which requires that the certificate is trusted. Go to Adding a CA Certificate for more information.

- **LDAP Title**: (Required) A title describing the LDAP configuration record that has meaning to your organization.
- **LDAP IP Address**: (Required) The IP address or Fully Qualified Domain Name (FQDN) of the LDAP server
- **Port**: (Required) Virtualization identifier defining the service endpoint
- **User Base DN**: (Required) A DN (Distinguished Name) is comprised of attribute=value pairs, separated by commas, which consist of the following basic elements (see DN in list below for a specific example):
  - **CN**: The Common Name of the object
  - **OU**: Organizational Unit
  - **DN**: Distinguished Name: "attribute=value pairs that define where your users are located within your LDAP tree. Examples are: cn=users, dc=some Host, dc=cisco, dc=com
- **UID**: (Required) This is the name of the unique identifier attribute that is used when looking up the user during an authentication request. For example, sAMAccountName. (for ActiveDirectory)
- **Encryption Method**: (Required) Select either:
  - **plain** (Plain Text Authentication) for no encryption
  - **simple-tls** (Transport Layer Security) for encryption

- **LDAP Type** (Required)
- **LDAP Authentication** (Required): Sets authentication parameters for LDAP
  - **Bind DN**: The bind DN binding credential used during authentication along with a password. For example, someUser@someHost.cisco.com, or cn=users, UID-root, DC=host name, DC=cisco, or DC=com.

NOTE: The LDAP Username will appear with the prefix distinction such as: cn=jane doe or dn=john smith.

  - **Password** (Required): The password for this LDAP server Bind DN. (See Editing LDAP password.
- **LDAP Group Import Settings** (Required): This designation enables you to automatically import LDAP groups. You will need to specify both these attributes:
  - **Group Base DN** (Required): Leads to your LDAP groups. For example, cn=users, dc=someHost, dc=cisco, dc=com, or o=someHost.cisco.com
  - **LDAP Type**: Either ActiveDirectory or OpenLDAP
  - **Filter** (Optional): This field allows you to specify specific LDAP groups to import.

When you have filled in the required information, click **Save**. When you have saved your information, select the **LDAP Groups** tab, and click **Update LDAP Data**.

- **Groups Object Class**

- **Group Unique ID Attribute**

Editing an LDAP Password

If you have an existing LDAP configuration and need to set your password, you can use the **Edit Password** button located on the LDAP Configuration tab.

NOTE: You cannot enter a password field that is empty.

Complete these steps to edit your Authentication password for LDAP.

Step	Action
Step 1	In the Administration Workspace, open the **Access Management Widget**.
Step 2	Select **LDAP Configuration**.
Step 3	Click **Edit Password** located to the right of the LDAP Authentication field. The Edit Password window opens.
Step 4	Enter a **New Password** and then **Reenter Password**.
Step 5	Click **Save**. The password has been changed.

Restricting LDAP User Privileges by Role

SSM On-Prem restricts role privileges which limits who can manage account access. Only System Administrators can configure access management. For example, as a System Administrator, for a group called “Example Group,” you add a System Operator role to that group. Then if that System Operator logs into On-Prem and attempts to update the group they will get a prompt, “You are not authorized to change these settings.”

NOTE: Only System Administrators can use the LDAP Configuration tab and save configuration changes.

LDAP Group of Names Support

Current On-Prem implementation supports only hardcoded groups object class:

- posixGroup for OpenLDAP
- group for ActiveDirectory

In the release **8-202112**, Support for “GroupOfNames” has also been added.

User has option to use custom Groups Object Class and Group Unique Id Attribute for OpenLDAP by two fields provided in LDAP Settings.

Groups Object Class (string) - objectClass of a group that On-Prem uses in its query when importing groups. For example: groupOfNames, posixGroup.

Group Unique Id Attribute (string) - the unique attribute to track the group identity. Only groups possessing this attribute can be imported into your On-Prem. For example: gidnumber, entryUUID.

Filtering LDAP Groups

You can filter a search for specific LDAP groups by using either standard syntax or a wild card.

NOTE: Go to https://tools.ietf.org/html/rfc2254 for a full list of standard syntax and wildcard variables.

To utilize these features of filtering, complete these steps.

Step	Action
Step 1	In the Administration Workspace, open the **Access Management Widget**.
Step 2	Select **LDAP Configuration**.
Step 3	Enter a standard **syntax variable** or **syntax with wildcard** or **extensible matching*** For example, to find an LDAP group labeled as “Users”, you can use cn=users. To find a LDAP group that begins with “s”, you can use cn=s with “*” acting as a wildcard.
Step 4	Click **Save**.
Step 5	Select the **LDAP Groups** tab.
Step 6	Click **Update LDAP Data**. The filtered groups are listed in the screen.

* Extensible matching is supported without OID. For more information on please see RFC2254

LDAP Groups Tab

CAUTION: If you were using LDAP groups on releases prior to 8-202102 this functionality has changed significantly. On-Prem v8-202102 now only supports adding LDAP Groups (versus users in previous versions). Before upgrading to v8-202102, and have upgraded to a more recent release, after logging into your upgraded version, you will need to navigate to **Admin Workspace > Access Management Widget >LDAP Groups Tab** and click **Update LDAP Data.** Your LDAP groups will be updated.

The LDAP Groups tab populates the LDAP Groups details after you log into the Licensing Workspace. For example, SSM On-Prem implements LDAP group posixGroup objectClass described in more detail at: https://ldapwiki.com/wiki/PosixGroup.

Each group defines one or more members. SSM On-Prem uses the member (DN of user) attribute for the DN of each member in the group. On-Prem also supports groups that only contain the memberUID attribute.

NOTE: It is strongly recommended to use groups that already contain the member attribute. Groups that use the **memberUID** attribute, require an additional query to run in the background, which will increase the processing time of the search. If the query is taking too long, please use the filter to narrow down the number of results.

Click **Update LDAP Data** to populate Group table with data from the LDAP server.

NOTE:

If an LDAP user is not part of an LDAP group, upon logging in, an error message **"Your username and/or password does not match our records, kindly try again. If the problem persists, please use 'Forgot Password', or contact your System Administrator" is displayed.**

Each LDAP group can be assigned RBAC to the various resources (System Role, Local Account, or Local Virtual Account).

Complete these steps to give universal access to accounts as either a System Administrator, System Operator, or Account User role.

Step	Action
Step 1	In the Administration Workspace, open the **Access Management Widget**.
Step 2	Select **LDAP Groups** tab.
Step 3	Select the **Group Name** that need to be updated/modified.
Step 4	Select the desired **System Role**. **NOTE**: If you select System Administrator or System Operator you can then click **Add**. But if you select **Per Account,** you will also need to specify the account and the account role.
Step 5	Click **Add** to add the role for the group.
Step 6	Click **Save**. All the users in that group will have that role assigned for that account. **NOTE**: If the system role was selected it takes precedence over account role.

Export LDAP Member Data

After updating LDAP group data, there is an option to download a report which consists of all member distinguished names (DNs) which are part of an LDAP group. The report is generated in a CSV format.

Step	Action
Step 1	In the Administration Workspace, open the **Access Management Widget**.
Step 2	Select **LDAP Groups** tab.
Step 3	Click on **Actions** next to the required LDAP group.
Step 4	Select **Export LDAP Member Data**.

Role-Based Access Control (RBAC) for LDAP

RBAC provides a convenient means of sorting users according to role. This is especially convenient with large numbers of users within a group.

Complete these steps to utilize RBAC for LDAP.

Step	Action
Step 1	In the Administration Workspace, open the **Access Management Widget**.
Step 2	Select **LDAP Groups** tab.
Step 3	Select the **group** you want for assigning a role by clicking on the **group name**.
Step 4	In the Group Details table, select the **Account** and the **Role**.

	NOTE: If you select **Per Account** as the role, you will need to select the Account and its associated Role before moving to Step 5. In other cases, there is no need to select account as the roles for all of them.
Step 5	Click **Add** and then click **Save**. The new role is listed in the group as a number beside the role label. **NOTE**: Groups are sorted by roles.

NOTE: Local Authentication is the primary means of authentication in SSM On-Prem. The other authentication methods (LDAP, SSO Client, ADFS) are optional secondary forms of authentication, and are only active when one of those methods is enabled and the associated authentication server is properly configured.

NOTE: When searching for LDAP Groups to add, only the first 1000 Groups will be returned. To narrow down the search, define a filter.

Elevating and Downgrading LDAP System Roles

SSM On-Prem allows you to change roles within an LDAP group which provides flexibility around role designation.

Step	Action
Step 1	In the Administration Workspace, open the **Access Management Widget**.
Step 2	Select the **LDAP Groups** tab.
Step 3	Select the **Group** that needs to be modified. The Group Details: Account screen opens.
Step 4	To change (elevate or downgrade) a System Role in the Group Details screen you can either: • Select the **Remove** option in the Actions column to remove an existing System Role and select new one. • Or, you can select **desired role** and click **add**, If the change is from/to System Administrator or System Operator, the role will be replaced. If the role is from per Account, the role will be added on top of existing per Account. If it is to per Account, the role would be replaced.
Step 5	Click **Add** and then click **Save**. Your changes are listed in the tab.

OAuth2 ADFS Configuration Tab

(Added for SSM On-Prem 7 Release 201910 and updated for SSM On-Prem 8 Release 202004)

NOTE: If you have enabled ADFS when using API Toolkit, only local authentication will work for Resource Owner Password Credentials (ROPC).

The OAuth2 ADFS tab provides ADFS authentication information for Windows Server operating systems when enabled.

Complete these steps to enable OAuth2 ADFS authentication.

Step	Action
NOTE: To get an explanation of the field, hover your cursor over the field which opens a tooltip that explains the function of the field. All the fields that have an [*] are required fields.	
Step 1	Select **Access Management > OAuth2 ADFS Configuration**.
Step 2	At the top left corner of the pane, enable **OAuth2 ADFS Secondary Authentication** (Default setting is disabled). **NOTE**: Once OAuth2 ADFS is enabled, a prompt opens under the field stating that OAuth2 ADFS is enabled and to use any other LDAP authentication process OAuth2 ADFS authentication must be disabled. As soon as the OAuth2 ADFS setting is enabled, all other tabs (LDAP Config, SSO Client, etc.) are disabled.
Step 3	(Optional) (Optional) If you are establishing TLS connections to your server, select **Verify Server Certificate** to verify that the verification of the server's certificate was signed by a trusted CA or by a custom CA that was uploaded. By enabling this option, communication to the remote server will go over TLS which requires that the certificate is trusted. Go to Adding a CA Certificate for more information. **NOTE**: This is a default setting for all new installations but needs to be activated for all existing customers.
Step 4	Enter the **ADFS Server URL**. (Host Name, FQDN, IPv4, or IPv6 must begin with https:// or http://)
Step 5	Select the **mode** of ADFS mode you are using: • ADFS V3 Mode: Allows ADFS on Microsoft Server 2012 • ADFS V4 Mode: Allows ADFS on Microsoft Server 2016+ • Import Claims: When enabled allows ADFS user claims to be mapped to SSM On-Prem user claims.
Step 6	Enter the **ADFS Resource Name**. A unique name in your organization that is used to identify the ADFS server.) Copy this **value** to your ADFS server's Relying party identifier field.)
Step 7	Enter the **Client ID**. (Copy the unique ID that you configured in your ADFS server into this field.)
Step 8	Copy the **Service Provider Redirect URI** (read-only field) to your ADFS server's Redirect URI field. **NOTE**: This URI is generated by assuming that you are logged into the same SSM On-Prem URL used by your users.
Step 9	Click **Save**.

After you have enabled the OAuth2 ADFS, you also should set your access control policy on the ADFS server by selecting your desired grants. For guidelines on enabling OAuth2 ADFS, see Appendix A.4. Setting up ADFS Server and Active Directory Groups and Claims.

SSO Client Tab

The SSO Client tab provides secondary authentication information for SSO when LDAP Secondary Authentication is disabled. See the LDAP Configuration tab for details on

authentication. There are two grant requests that can used depending on whether you are using an external server for an Auth Code grant.

If you are not using an external server for an Auth Code grant, you will select Password Grant when configuring SSO Client Secondary Authentication. If you are using an external server for an Auth Code grant, select Authorization Code Grant.

Configuring for an Internal SSO Client (Password Grant)

To utilize an internal SSO Client, complete these steps.

Step	Action
Step 1	Select **Access Management > SSO Client**.
Step 2	At the top left corner of the pane, turn the **SSO Client Secondary Authentication o**n or off. (Default is Off)
Step 3	(Optional) If you are establishing TLS connections to your server, select **Verify Server Certificate** to verify that the verification of the server's certificate was signed by a trusted CA or by a custom CA that was uploaded. By enabling this option, communication to the remote server will go over TLS which requires that the certificate is trusted. Go to Adding a CA Certificate for more information. **NOTE**: This is a default setting for all new installations but needs to be activated for existing customers and for all upgrades.
Step 4	Enter the **Authentication Server URL**.

Step 5	Select **Password Grant**.
	• **Password Grant**: Once selected, you will need to enter these two endpoints. (See Step 8 and 9)
	  ○ Token Endpoint
	  ○ Userinfo Endpoint

Step 6	Enter the **Application ID**.
Step 7	Enter the **Application Secret**.
Step 8	Enter the **Token Endpoint**.
Step 9	Enter the **Userinfo Endpoint**.
NOTE: The **Service Provider RedirectURI** is a read-only field. But you will likely need this URI to add to your server's list of valid redirect URI.	
Step 10	Click **Save**.
Step 10	Now users can log directly into the On-Prem workspaces.

After you have enabled the SSO Client, you also should set your access control policy on the SSO server by selecting your desired grants. In addition, you should set your issuance transform rules outlined in the example below.

Issuance transform rules example:

- Application Server: url = https://sso.pingdeveloper.com/OAuthPlayground/case1A-callback.jsp
- Application (client) ID = ac_oic_client
- Application (client) Secret = abc123DEFghijklmnop4567rZYXWnmlijhoauthplaygroundapplication

Configuring for an External SSO Client (Authorization Code Grant)

To utilize an external SSO Client, complete these steps.

Step	Action
Step 1	Select **Access Management > SSO Client**.
Step 2	At the top left corner of the pane, turn the **SSO Client Secondary Authentication** On or off. (Default is Off)
Step 3	(Optional) If you are establishing TLS connections to your server, select **Verify Server Certificate** to verify that the verification of the server's certificate was signed by a trusted CA or by a custom CA that was uploaded. By enabling this option, communication to the remote server will go over TLS which requires that the certificate is trusted. Go to Adding a CA Certificate for more information. **NOTE**: This is a default setting for all new installations but needs to be activated for existing customers and for all upgrades.
Step 4	Enter the **Authentication Server URL**.
Step 5	Select **Authorization Code Grant**. • **Authorization Code Grant**: Once selected, you will need to enter these four endpoints. (See Steps 8 thru 11) ○ Authorization Endpoint ○ Token Endpoint ○ Userinfo Endpoint ○ Logout Endpoint **NOTE**: The token and userinfo endpoints are server dependent. Please refer to the server you are using to get those public endpoints.
Step 6	Enter the **Application ID**.
Step 7	Enter the **Application Secret**.
Step 8	Enter the **Authorization Endpoint**.
Step 9	Enter the **Token Endpoint**.
Step 10	Enter the **Userinfo Endpoint**.
Step 11	Enter the **Logout Endpoint**.
NOTE: The **Service Provider RedirectURI** is a read-only field. But you will likely need this URI to add to your server's list of valid redirect URI.	
Step 9	Click **Save**.
Step 10	Log out of the Admin Workspace and then return to the On-Prem License workspace login page. You are automatically redirected to your **auth server** login page. Upon successful login, you are redirected back to On-Prem. **NOTE**: All users are initially granted **system user** access, higher-level privileges such as system operator, must be assigned by your system admin. **NOTE**: When you log out of On-Prem as the SSO user, you will also terminate the auth server's session.
ATTENTION: This feature is an Early Field Trial (ETF) feature. This feature has been tested within the lab with the Keycloak open-source identity provider but has not been fully integrated/tested with systems external customer may employ.	

TACACS+ Configuration Tab

ATTENTION: TACACS+ uses MD5 hashing algorithm which is not FIPS compliant. If FIPS compliance is a requirement of your organization, please use an alternative secondary authentication method.

The TACACS+ is an Access control system that uses Authentication, Authorization, and Accounting (AAA) protocols to allow centralized Access Controls to Network resources. Adding users to the TACACS+ system sets their privilege level once for access to all devices. This negates the need to create or add users to every system.

Within your TACACS+ system, you must create 3 TACACS+ profiles. Each profile represents a different SSM On-Prem system role.

The available SSM On-Prem system roles are:

- System User – Create a TACACS+ profile with the privilege between 1-9.
- System Operator – Create a TACACS+ profile with the privilege between 10-14.
- System Administrator – Create a TACACS+ profile with the privilege set to 15.

For a third-party TACACS+ server, it is mandatory to define the TacacsServiceDictionary name value as "priv-lvl" for SSM On-Prem to work. Below is an example of a tacacs service definition and attribute.

```
<TacacsServiceDictionary dispName="<service-display-name>" name="priv_lvl">
<ServiceAttribute dataType="Unsigned32" dispName="Privilege level" name="priv-lvl"/>
</TacacsServiceDictionary>
```

NOTE: The default privilege level is a mandatory argument and is used as a means for authorization.

Configuring TACACS+

NOTE: You must be logged into On-Prem as an Administrator to configure TACACS+ Authentication.

Complete these steps to configure TACACS+ Authentication:

Step	Action
Step 1	From the Administration workspace widget panel, select **Access Management Widget > TACACS+ Configuration**.
Step 2	At the top left corner of the pane, **enable TACACS+ Authentication** by sliding the toggle switch to the right.
Step 3	Enter **TACACS+ Title** (Title of the provider)
Step 4	Enter the **TACACS+ Primary Server IP Address** and **Port** (default port is 49) **NOTE**: The port can be changed if a custom configuration is required.
Step 5	Enter the **Primary Server Shared Secret** (Key). **NOTE**: When you create the shared secret, you cannot use these three characters. The system will give you an error message. • Space: " " • Pound sign: "#" • Backslash: "\"
Step 6	(Optional) Enter the **TACACS+ Secondary Server IP Address**, **Port**, and **Shared Secret**. **NOTE**: The secondary server can only be configured after the primary server has been configured.

Step	Action
Step 7	Select the **Authentication Method** • ASCII: Using Characters as Numbers • CHAP: Challenge Handshake Authentication Procedure (Recommended) • PAP: Password Authentication Procedure (Recommended)
Step 8	Set the **Authentication Timeout** limit (default is 5 seconds). **NOTE**: The maximum timeout is 10 seconds.
Step 9	Enable the **Allow Local Authentication** check box to allow local authentication/authorization after TACACS+ is configured. **NOTE**: If **Allow Local Authentication** check box is not enabled while configuring TACACS+, then login for non-TACACS+ users will be disabled.
Step 10	To test the server connection, click **Test Server Connection**. This test checks if the user and password are valid on the TACACS+ server **NOTE**: The test server connection button validates the server configuration with the user and password on the TACACS+ server. When the authentication is successful the **Save** button is enabled.
Step 11	When the validation is complete (successfully) click **Save** to save your configuration. You have now successfully configured the TACACS+ server. **NOTE**: After successful configuration, the Users Widget will list the TACACS users.
Step 12	Exit out of the Administration Workspace and **log into On-Prem** using your **TACACS+ UserID** and **Password**.
Step 13	Select the **License Workspace** and work as usual.

NOTE: The procedure above, is for the On-Prem GUI. To setup TACACS+ using the On-Prem Console (CLI), refer to **Appendix A7**. Configuring TACACS+ Through CLI.

TACACS+ Login Fallback to Default Local Account

When TACACS+ is selected as the primary authentication method so that all authentication requests of local users are validated only by the TACACS+ server. If for some reason the primary TACACS+ server does not respond within the specified authentication interval (see step 8 in TACACS+ configuration procedure). If both primary and secondary servers are not responding within the authentication interval, then On-Prem will check if the user is an On-Prem local user. If they are a local On-Prem user, On-Prem will validate the user's credentials and, if valid, they will be logged into On-Prem.

NOTE: Note: Once you logged in as TACACS+ user then you will not be able to create a local user with same name. On the other side when you already logged in as local user then you can login with TACACS user with same username.

Security Widget

(Updated functionality in SSM On-Prem 7 Release 201910)

The Security Widget screen has four tabs.

- **Account**: This tab allows you to enable or disable the auto lock feature as well as set the time an account is locked.
- **Password**: Provides password enforcement features and expiration settings.
- **Certificates**: This tab allows you to import, replace, renew, edit, and delete certificates.
- **Event Log**: Shows the event message, time and date of occurrence, and the user responsible for the occurrence.

Account Tab

The Account tab houses the Auto Lock feature. This feature enables a user with Administrator (or System Operator) role to lock the account after a specific number of failed login attempts.

- **Enable auto lock**: (Default setting is disabled) Sets the number of **login attempts** permitted and the **time span** (Within Minutes) the lockout is in effect.
- **Enable lock expiration**: Allows a locked account to be unlocked.
- **Enable session limit**: (Default setting is disabled) Allows user with admin privileges to set the number of sessions that can be opened for a user. The range is 1-999.
- **Enable obsolete TLS versions**: (Default setting is enabled) This setting allows the utilization of previous versions of TLS (such as TLS 1.1) that do not have adequate security protection for transfer between Cisco products and SSM On-Prem. This setting should only be used for backward compatibility with older Cisco products that have not upgraded to TLS 1.2 or TLS 1.3.

NOTE: SSM On-prem 8-202212 supports TLS 1.3.

- **Enable TLS 1.2 legacy ciphers**: (Default setting is disabled) This setting allows legacy Cisco products, such as Cisco Unity Connection and Cisco HCM-F, to communicate with SSM On-Prem.

Configuring Password Auto Lock and Lock Expiration Settings

Complete these steps to enable the password auto lock feature.

Step	Action
Step 1	From the **SSM On-Prem Admin Workspace**, click **Security Widget**. The Security Widget screen opens.
Step 2	In the account tab, slide the **Enable auto lock** toggle switch to the **right** (to enable auto lock).
Step 3	Set the **number of login attempts**.
Step 4	Set the **number of minutes** which is the time the account will remain locked, immediately after the number of failed login attempts is reached.
Step 5	Click **Apply**. **NOTE**: Click **Reset** if you need to reset the auto lock settings.
To configure lock expiration settings, complete these steps.	
Step 6	Select the **check box** entitled Enable lock expiration.
Step 7	Set the **time span** (greater than 1 minute) for the time the lock out will expire.

Step	Action
Step 8	Click **Apply** to save the settings to the system.

Enabling Session Limits in Security Widget

This feature allows a user with Admin privileges to limit the number of sessions that any single user (including Admin) can have. Complete these steps to enable session limits.

Step	Action
Step 1	From the **SSM On-Prem Admin Workspace**, click **Security Widget**. The Security Widget screen opens.
Step 2	Slide the **Enable session limit** toggle switch to the **right** (to enable session limit function).
Step 3	Set the **Maximum (count)**. The range is 1-999. (The default is 10) **NOTE**: This feature applies to all users listed in the Accounts widget.
Step 4	Click **Apply**. If a user attempts to exceed the session limit, they will get the following message: "This session limit has been reached for this user. Please contact your Administrator." **NOTE**: Click **Reset** if you need to reset the auto lock settings.

NOTE: All currently open sessions will be kept open until the user logs off. No new sessions can be opened after the limit is set.

Enabling Session Limits in the On-Prem Console

Complete these steps to set session limits in the On-Prem Console. (See SSM On-Prem Installation Guide for details.)

NOTE: If you have a High Availability (HA) cluster deployed on your system, you will also need to manually modify the session limits on each node from the corresponding On-Prem console.

Step	Action
Step 1	From the CLI, ssh as admin to your server IP address, and then to open the console, type the following command: `onprem-console` Hint: You can use tab completion to complete the command.
Step 2	Type **?** To open the On-Prem help section.
Step 3	Enter **shell_session_limit**. Set the **Maximum (count)** for each node. The range is 1-999. The default setting is 10. (See *SSM On-Prem Console Guide* for details on using the shell_session_limit command.) **NOTE**: This feature applies to all users including Admin role. Example of limiting sessions on a node:

Step	Action
	>> shell_session_limit No custom limit currently set. Using default limit of 10. >> shell_session_limit 11 Setting custom shell session limit... Done! This setting is not replicated between HA nodes. It must be manually set on each node. >> shell_session_limit Current custom limit: 11 **ATTENTION**: If you are deploying a High Availability (HA) cluster, session limits must be set up separately on each node.
Step 4	Press **Enter**. To save the setting. The session limit is set.

Enabling Obsolete TLS Versions

When enabled, this feature allows you to utilize previous versions of TLS (such as TLS 1.1) that do not have adequate security protection for transfer between Cisco products and SSM On-Prem. This setting should only be used for backward compatibility with older Cisco products that have not upgraded to TLS 1.2 or TLS 1.3.

NOTE: SSM On-prem 8-202212 supports TLS 1.3.

Step	Action
Step 1	From the **On-Prem Admin Workspace**, click **Security Widget**. The *Security* screen opens.
Step 2	Slide the **Enable obsolete TLS versions** toggle switch to the **right** (to enable obsolete TLS versions).
Step 4	Click **Apply** to save your changes.

Enabling TLS 1.2 Legacy Ciphers

When enabled, legacy Cisco products, such as Cisco Unity Connection and Cisco HCM-F, can communicate with Cisco SSM On-Prem.

Step	Action
Step 1	From the **On-Prem Admin Workspace**, click **Security Widget**. The *Security* screen opens.
Step 2	Slide the **Enable TLS 1.2 legacy ciphers** toggle switch to the **right** (to enable TLS 1.2 legacy ciphers).
Step 4	Click **Apply** to save your changes.

Password Tab

The Password tab houses the Password Settings and Password Expiration features. These features enable a user with Administrator (System Operator) role set specific parameters for passwords as well as how long a password can be viable.

Password Settings

(Added for SSM On-Prem 7 Release 201910)

The password settings menu is comprised of a list of four main options and seven sub-selections.

- Toggle switch: (default Enabled). When enabled, this setting allows users to see login error messages as well as password hints.
- Toggle switch: (default Disabled) Allow all local users to recover and reset their password by clicking **Forgot Password** option on the Login Screen.
- Toggle switch: (default Disabled) Force users to change password after the administrator resets the password: This option forces the user to create a new password after the administrator resets the password.

NOTE: After the administrator has reset the password, the user will be prompted to reset their password after their initial login.

- Toggle switch: (default Enabled) Apply password strength rules: This option has a series of other options that allows an administrator to tailor password strength. If this option is selected the administrator can select whether the passwords:

NOTE: The administrator can disable this option without altering a user's existing password values. New values will be used on next password reset.

  - Must not contain the user's name.
  - Must include upper- and lower-case letters (mixed case).
  - Must include numeric characters (0-9).
  - Must include special characters such as: exclamation points "!", question marks "?", dashes "-", etc.
  - Must not contain common passwords such as: "Password, MyName, Username, etc."
  - Must have a minimum length of characters (minimum length is 15 characters).
  - Must not use previously used password for a specific number of renewals (range is 1-99)

Click **Apply** to apply your settings or click **Reset** to return to the system default values.

Password Expiration

(Added for SSM On-Prem 7 Release 201910)

This feature allows the administrator to set specific expiration parameters to enhance password security.

When you enable Password Expiration, the following options can be selected (clicking the appropriate checkbox):

NOTE: The administrator can disable this option (after being enabled) without altering a user's existing password values. New values will be used on next password reset.

- The maximum number of days that the password is valid (default is 60 days).
- Prompt users to change their password a set number of days before it expires.
- Allows the user to change their password after the expiration date.
- Send expiration notification emails a set number of days before the password expires.

Click **Apply** to apply your settings or click **Reset** to return to previously saved settings.

Certificates Tab

(Added for SSM On-Prem 7 Release 201910)

The Certificates tab allows the administrator to:

- Set the Host Common Name
- Set the Subject Alternative Name
- Generate Browser Certificates
- Manage Browser Certificates

NOTE: The common name must match what is used on the product as part of the call-home configuration. See Product Instance Registration.

Filling in the Common Name

The Certificates tab's Common Name field lists the DNS resolvable hostname or **IP Address** connected to SSM On-Prem.

Complete these steps to enter a Host Common Name.

Step	Action
Step 1	Navigate to the **SSM On-Prem Administration Workspace** https://<ip address>:8443/admin. **NOTE**: Where the IP-address is the value used during installation.
Step 2	From the Administration Workspace, navigate to **Security Widget > Certificates**.
Step 3	In the Certificates tab, enter the **Host Common Name** (IP address). **NOTE**: This value must match the value user plan to use for the product destination URL. If it is part of the HA cluster, this value must match the value that the user plans to use it for the product destination URL, either as the FQDN or the virtual IP address.
Step 4	Click **Save**. The Host Common Name is updated.

NOTE: After you have updated the Host Common Name, make sure that your certificates are re-generated with the new Common Name by synchronizing your Local Accounts with CSSM Cloud.
You must synchronize **before** attempting to re-register the products with the new Common Name in the destination URL configuration. Not synchronizing can result in the products failing to register with the new Host Common Name.

Filling in the Subject Alternative Name (SAN)

(Added for SSM On-Prem 8 Release 202212)

The **Subject Alternative Name** (SAN) is an extension to the Host Common Name that allows users to specify additional host names for a single SSL certificate. An SSL certificate with more than one name is associated using the SAN extension. This provides the ability to configure SAN for the product certificate, so products can register either by using IP Address or the FQDN in the Smart Transport URL or the CSLU Transport URL.

NOTE: The Common Name is a part of the Subject Alternative Name by default.

Complete these steps to enter a Host Common Name.

Step	Action
Step 1	Navigate to the **SSM On-Prem Administration Workspace** https://<ip address>:8443/admin. **NOTE**: Where the IP-address is the value used during installation.
Step 2	From the Administration Workspace, navigate to **Security Widget > Certificates**.
Step 3	In the Certificates tab, enter the Subject Alternative Name. **NOTE**: This value must match the value user plan to use for the product destination URL. If it is part of the HA cluster, this value must match the value that the user plans to use it for the product destination URL, either as the FQDN or the virtual IP address.
Step 4	Click **Save**. The Subject Alternative Name is updated.

NOTE: After updating the Subject Alternative Name, make sure that the certificates are re-generated with the new host name by synchronizing your Local Accounts with CSSM Cloud.
User must synchronize **before** attempting to re-register the products with the new host name in the destination URL configuration, after adding or modifying the host name. Not synchronizing can result in the products failing to register with the new Subject Alternative Name.

Generating a Certificate Signing Request (CSR)

The Common Name tab contains the **Product Certificate** (IP Address or Domain Name). **Generate CSR** button, click this button to create a certificate from either your company or through a third party. Complete these steps to generate a CSR.

Step	Action
Step 1	In the Administration Workspace select **Security Widget > Certificates tab**.
Step 2	In the Browser Certificate section, click **Generate CSR**. The Generate CSR screen opens.
Step 3	Enter the following required information: a. **Common Name**: Name that you will be using for the CSR. (See note on Common Name tab screen It is auto filled on the form). b. **Organizational Unit**: Dept, Section, Unit that is using the certificate. c. **Country**: Select the country from the drop-down list. d. **State/Province**: Enter the appropriate state or province. e. **City/Locality**: Enter the appropriate city or locality. f. **Organization**: The name of the organization that is utilizing the CSR. g. **Key Size**: Select from the drop-down list. • 2048 • 4096 h. **Subject Alternative Name**: Another possible designation for the certificate. For example, an IP Address.
Step 4	Click **Generate**. The certificate signing request is downloaded and appears on the bottom of the browser window.
Step 5	Open the **Certificate Signing Request (CSR)** file. The CSR opens in a new pop-up window. **NOTE**: You must have the appropriate application installed on your system to open the CSR. Or you can open the file with Notepad and copy the contents and paste them in a file format to be sent and signed.
Step 6	Contact the **appropriate signing authority** to sign the CSR (typically received via email). A message opens at the bottom of the screen that the certificate is successfully created. Once the certificate is signed and loaded into your local drive, you are then able to add the certificate in Adding a Certificate.

Adding a Certificate

Once you have received your signed certificate from the commercial or third-party signing authority, you then add the certificate to SSM On-Prem, along with a private key so that other devices can use it.

NOTE: Make sure that you read the note concerning Common Name requirements located on screen.

Complete these steps to add a certificate.

Step	Action
Step 1	In the Administration Workspace select **Security Widget > Certificates tab**.
Step 2	In the Browser Certificate section click **Add**. The upload Certificate Wizard opens.
Step 3	Enter the following: • Description: Enter the **description** for the certificate. • Certificate: Click **Browse** to find the certificate on your drive.

Step	Action
	• Intermediate certificate: Click **Browse** to find the intermediate certificate on your local drive. **NOTE**: If there are several intermediate certificates, you will need to combine them into one intermediate certificate file. **NOTE**: You are prompted to correct any of the information that is incorrect. **NOTE**: • Intermediate certificates are optional for some certificate authority issued certificates. • Certificates must be in X.509 PEM format (no other formats are excepted) • Private keys must be in RSA format and cannot be "pass phrase." **NOTE**: If you have several intermediate certificates you need to use, create a new X.509 PEM formatted file, and then copy and paste all the certificates into that new file.
Step 4	Click **Apply**. A message opens stating, "Your certificate is being generated. Please wait 60 seconds for the process to complete. When generation is complete your screen will be refreshed." After 40 seconds, another pop-up with "Server Connection Error" opens directing you to reload the screen or let it automatically reload. Once the screen is reloaded to the Widgets screen, return to the Security Widget and open the Certificates tab and a certificate record is listed on the Browser Certificate section with the IP Address. An Expiration Date shows on the bottom right side of the screen.

Adding a CA Certificate

(Added for SSM On-Prem 8 Release 202008)

If you are using a proxy server connected via HTTPS and the root certificate served is not a trusted Certificate Authority certificate, you will need to export the root certificate and then import that certificate into On-Prem so it will be able to trust and connect to your proxy server.

You will import the root certificate using the CA Certificate section under the Certificate tab.

Complete these steps to add a CA certificate.

Step	Action
Step 1	In the Administration Workspace select **Security Widget > Certificates tab**.
Step 2	In the CA Certificate section, click **Add**. The Upload Certificate Modal opens.
Step 3	(Required) Enter a **Description** for the CA certificate.
Step 4	(Required) Click **Choose File** and browse for the **CA Certificate** file.
Step 5	Select the appropriate **CA Certificate** file.
Step 6	Click **OK**. The CA Certificate is listed in the CA Certificate table.

Deleting a Certificate

Each certificate has an expiration date. The Expiration Date pull down list is located on the right-hand side of the screen. If a certificate expires, you need to delete it using the Actions menu.

NOTE:
- The "Default or Self-signed certificate" cannot be deleted because it is used as a temporary replacement for an expired certificate.
- Make sure that any replacement certificate with "default status" has all the services needed by the other certificates being used.
- Self-signed certificates may not be compatible with all browsers. If the certificate is not compatible, your browser displays a warning message stating that your connection to SSM On-Prem Workspace Pages is not secure.

Complete these steps to delete a certificate.

Step	Action
Step 1	From the Certificate tab, select the **Certificate** to be deleted.
Step 2	From the Expiration Date field, click **Delete**. The certificate is deleted. If you need a temporary certificate, you can use the **Default Certificate**. Make sure the default certificate has all the services needed by the other certificates being used. **NOTE**: It can take up to 1 minute for the certificate to generate a self-signed certificate.

Event Log Tab

The Event Log tab table provides the following information:

- the date and time associated with a certificate,
- the type of event associated with a certificate,
- the event message associated with a certificate,
- the user that was associated with certificate activity.

Users Widget

The Users widget allows the System Administrator or System Operator to create local users and configure advanced parameters such as setting passwords, expiration rules and password auto-lock features.

NOTE: SSM On-Prem has an Idle Timeout security feature that activates if there has been no activity for 10 minutes. After 10 minutes of no activity, you are required to log into the system again.
If you are logged into SSM On-Prem using ADFS when the timeout feature activates, log into the system again by clicking the ADFS button on the login page. For more details on this feature, see Cisco SSM On-Prem Idle Timeout Feature.

When you create a user on the Administration Workspace, it is added to the local authentication database (not LDAP, SSO, OAuth2 ADFS, or another authentication server) with a default system role of System User (the lowest authority). When the authentication method is configured, an LDAP, ADFS, or SSO user is created within that authentication server where they can log into the Licensing Workspace. The user must then request access to an existing Local Account or a new Local Account before they can use the On-Prem Licensing workspace for Smart Licensing functions.

Adding a New User

Create a new user by completing these steps.

Step	Action
Step 1	From the System Administration click the **Users Widget**.
Step 2	Click **Create**.
Step 3	Fill in **the required information**. i. (Optional) Enter the user's **First Name**. j. (Optional) Enter the user's **Last Name**. k. (Optional) Enter a brief description of the user for example, user role, position, responsibilities in using SSM On-Prem). l. (Required) Enter a **User Name** for the user. m. (Optional but strongly recommended) Enter a valid **Email** for the user. n. (Required) Enter a **Password** for the user. o. (Required) Re-enter the **Password**.
Step 4	Click **Add User**. The user is added to the User Table.

Selecting a Role for the User

Once you have added a user, you need to select a role for them.

To select a user role:

Step	Action
Step 1	From the Administration Workspace, click the **Users Widget**.
Step 2	From the User Table, select the **User** that needs a role assignment.
Step 3	In the System Role column and select one of the following roles: • System User • System Operator • System Admin See SSM ON-Prem Roles for more information on role privileges.

NOTE: For TACACS Users, Dropdown for changing role and editing information about user is disabled and greyed out.

NOTE: A local user created here has a default role of **System User**. A System Administrator can change that role to the System Administrator or System Operator role.

NOTE: Local Authentication is the primary means of authentication in SSM On-Prem. The other authentication methods (LDAP, AD, or ADFS) are secondary forms of

authentication and are only active when the Access Management methods are used.

Action Menu

From the Actions column (right-hand column of the User table) you can select the appropriate action for each user.
A System Administrator or System Operator can select the following actions for a user.

- **Disable**: Disabling a User retains the user in the database, but the User is not able to login until re-enabled.
- **Remove**: Removing a User deletes the User record, and the user will need to be created again.

NOTE: **Actions** option is disabled and greyed out for TACACS Users, so they cannot select **Disable** or **Remove** options.

NOTE: If user with an LDAP associated account synchronization is removed, you will need to trigger a network sync and login to Cisco with a different user to allow scheduled synchronization to work properly.

NOTE: A System Administrator or System Operator cannot remove themselves.

Accounts Widget

The Accounts Widget allows the Administrator to add new accounts, manage existing accounts and account requests, and to view event logs for accounts.

A new or existing SSM On-Prem Local Account must exist and be registered before Smart Licensing functions can be performed in the licensing workspace. Until this process is completed, all other Smart Licensing options are grayed out.

NOTE: Once the Local Account has been requested, it must be **registered** to CSSM Cloud before it can be active and usable. Both network and manual registrations are supported.

Accounts Tab

During SSM On-Prem Local Account registration, a Cisco. Smart Account/Virtual Account pair must be specified. If the Cisco Virtual Account does not exist, CSSM Cloud creates it upon registration. Otherwise, it uses the existing Cisco Virtual Account.

Creating a New Local Account

A new Local Account can be created by a System Administrator or System Operator via the Accounts widget from the Administration workspace.

Complete the following steps to setup a new Local Account.

Step	Action
Step 1	Click the **Account** widget to open it.
Step 2	Select the **Accounts** tab.
Step 3	Click **New Account**.
Step 4	Enter the **required information** (the required fields are labeled with [*]) The fields are: • Account Name • Cisco Smart Account • Cisco Virtual Account **NOTE:** Cisco Virtual Accounts without product instances will appear as an option. Also note that when creating a new Cisco Virtual Account, you must use a unique name. • Email for Notification.
Step 5	Click **Submit**.
Step 6	Click **OK** at the message displayed that a new Account request has been created, and ready to be registered to Cisco. The Account request is then listed on the Account Requests tab in the Accounts widget.

De-activating a Local Account

A Local Account can be de-activated, activated, or deleted once it's been registered with Cisco. The De-activate option disables access to the Local Account in the Licensing Workspace.

NOTE: When a Local Account is deactivated, the Account is not removed from SSM On-Prem and no user permissions are changed.

Complete these steps to de-activate the Local Account.

Step	Action
Step 1	Click on the **Actions menu**.
Step 2	Select **Deactivate** from the Actions menu.
Step 3	Enter a **reason** for deactivation so it can be included in the email that is sent to the requestor.
Step 4	Click **Deactivate**.

Activating a De-activated Local Account

The Activate option is available for any account that has been de-activated. When the account is returned to the active state, the account will again be listed on the Licensing workspace and is available to any user that has authorization.

Complete these steps to activate a de-activated Local Account.

Step	Action
Step 1	Click on the **Actions menu**.
Step 2	Select **Activate** from the Actions menu.
Step 3	Enter a **reason** for activation so it can be included in the email that is sent to the requestor.
Step 4	Click **Activate**.

Deleting a Local Account

If a Local Account has been de-activated, the Delete function is visible enabling you to remove the Local Account.

Complete the following steps to delete a Local Account.

Step	Action
Step 1	Remove all Product Instances (**PIs)** on all Local Virtual Accounts in the SSM On-Prem Local Account. (See note below.)
Step 2	Synchronize with **SSM On-Prem** so that CSSM Cloud reflects that the PIs are no longer on SSM On-Prem.
Step 3	Deactivate the **Local Account**. Navigate to the Local Account and click **Deactivate**. The Local Account is listed as Inactive.
Step 4	From the Actions menu, select **Delete**.
Step 5	Click **OK**.
Step 6	Go to CSSM Cloud and **remove the SSM On-Prem** representing this Local Account. At this point, the Virtual Accounts (VA)s associated with this SSM On-Prem are empty because the PIs were removed in Step 1. To remove a SSM On-Prem account: p. Navigate to the **SSM On-Prem** pane. q. Select the **SSM On-Prem** corresponding to that Local Account. r. From the Actions menu, select **Remove**. s. Confirm **SSM On-Prem removal**.
Step 7	SSM On-Prem is removed from Cisco SSM and the Local Account can be re-registered again to the correct Cisco Smart Account/Virtual Account pair.

NOTE: The only way to remove PIs on SSM On-Prem and have them reflected on CSSM Cloud is to synchronize SSM On-Prem to CSSM Cloud after removing them from SSM On-Prem because SSM On-Prem is the source of truth for all PIs registered to it.

Re-Registering an Account

There is the possibility an SSM On-Prem Local Account could be deleted from your Smart Account. In the event this happens, the Account Re-Registration function allows you to re-register your Local Account without losing the existing users associated with the Account or having to re-register the product which has been previously registered. This process can be done either in connected (**Online**) or disconnected (**Offline**) mode.

NOTE: If SSM On-Prem in CSSM Cloud has products registered to it, you will need to open a Support Case with Cisco TAC to have a Cisco Admin remove product instance before proceeding.

Once you have removed the SSM On-Prem instance from CSSM Cloud, the associated Local Account must be deactivated (see De-activating a Local Account).

Re-Registering a Local Account (Online Mode)

Once a Local Account has been deactivated, the Re-register option becomes available.

NOTE: Re-registering a Local Account assumes there is an Internet connection to CSSM Cloud. Once you have completed re-registering a Local Account, a full synchronization will automatically be scheduled that runs in the background for the Account.

Complete these steps to re-register a Local Account.

Step	Action
Step 1	In the Admin Workspace screen, click **Account Widget**.
Step 2	Navigate to the Local Account you want to re-register and click **Actions**.
Step 3	From the Actions drop-down menu, select **Deactivate** (if not already de-activated).
Step 4	From the Actions drop-down menu, select **Re-register**. The Cisco Smart Account Administrator enters their Cisco credentials (Cisco Connection Online Identification CCO ID and Password).
Step 5	When prompted, click **Submit**. The Review Account Requests model opens.
Step 6	Enter the following information: • **Account Name**: Informational only • **Cisco Smart Account**: The Cisco Smart Account associated with the Local Account. • **Cisco Virtual Account**: The Cisco Virtual Account associated with the Local Account. (However, any eligible Cisco Virtual Account can be used.) • **Cisco Virtual Account**: The Cisco Virtual Account associated with the Local Account. (However, any eligible Cisco Virtual Account can be used.) • **Request Date**: Informational only • **Message to Approver**: Informational only
Step 7	Click **Next**. SSM On-Prem provides a status for the registration progress. Upon successful re-registration, a pop-up message opens stating that the Account was successfully re-registered.
Step 8	Click **Close**. In the Accounts tab, the Local Account shows as Active.

NOTE: The Re-registration option is only available in the drop-down menu if you have previously De-activated the Local Account.

Manually Re-Registering a Local Account (Offline Mode)

Once the Local Account has been deactivated, the Manual Re-Register action becomes available.

NOTE: Re-registering a Local Account assumes there is an Internet connection to CSSM Cloud. Once you have completed re-registering a Local Account, a full synchronization will automatically be scheduled that runs in the background for the Account.

Complete these steps to manually re-register a Local Account.

Step	Action
Step 1	In the **Admin Workspace** screen, click **Account Widget**.
Step 2	Navigate to the Local Account you want to re-register and click **Actions**.
Step 3	From the Actions drop-down menu, select **Deactivate** (if not already de-activated).
Step 4	From the Actions drop-down menu, select **Manual Re-register**. **NOTE**: This option is only available in the drop-down menu if you have previously **Deactivated** the Local Account.
Step 5	Click **Generate Re-Registration File**.
Step 6	Log into **CSSM Cloud**.
Step 7	Navigate to **On-Prem** tab
Step 8	Click **New SSM On-Prem**.
Step 9	Fill in the required **information**.
Step 10	Navigate to **Choose File** and select the **file** you created in Step 5.
Step 11	Click **Add**.
Step 12	Click **Generate Authorization File**.
Step 13	Click **Download Authorization File** and save the **file** to your local computer.
Step 14	Return to the **Admin Workspace** in step 5 and click **Choose File** and select the file downloaded in Step 11.
Step 15	Click **Upload**. SSM On-Prem provides a status of the registration progress. Upon successful registration, a message pop-up opens stating: Account was successfully re-registered.
Step 16	Click **Close**. In the Accounts tab, the Local Account shows as **Active**.

NOTE: A full synchronization must be manually performed as a final step in completing the Manually Re-Registering an Account procedure. Unless this step is performed, products cannot successfully report license usage to this **Account.**

Account Requests Tab

Once the Local Account has been requested, it must be registered to CSSM Cloud before it can be active and usable. The Local Account Request tab shows requests of Local Accounts pending for the System Administrator to approve and register. There are several actions which can be performed for Local Accounts.

Approving Account Requests (Online Mode)

A Local Account request shows up in Administration workspace Account Requests. The new Account request must be approved and registered by the System Administrator to become active. (As System Administrator) To approve an account request, complete these steps.

Step	Action
Step 1	Under Actions, select **Approve**. This action begins the registration process of the Local Account to CSSM Cloud.
Step 2	Click **Next.**
Step 3	To gain access to Cisco Account/Virtual Account CSSM Cloud, enter your **CCO ID credentials**.
Step 4	Click **Submit**. A status of the registration progress opens. Upon successful registration, a message pop-up opens stating that the Account was created successfully, and the Local Account is registered as Active under the Accounts tab.
Step 5	The Local Account is shown as SSM On-Prem registered on SSM On-Prem pane. **NOTE:** The Local Account name is the SSM On-Prem name on the General tab, and the Local Account name shows up under the **Virtual Accounts** tab.

NOTE: Only a single Cisco Virtual Account is supported per SSM On-Prem Local Account. If you add another Cisco Virtual Account to SSM On-Prem on the **SSM On-Prem** screen, only the Cisco Virtual Account originally registered is used to exchange license information during the synchronization. Additional Cisco Virtual Accounts will be ignored.

NOTE: Once the Local Account is registered, licensing functionality through the Licensing workspace becomes accessible.

Manual Registration (Offline Mode)

You can select the **Manual Registration** procedure instead of **Approve** procedure to manually register the Local Account to CSSM Cloud. While manual registration is supported, it's not recommended as you must keep track of the specific registration request/authorization file(s) for each registration.

Complete the following steps to manually register a Local Account to CSSM Cloud.

Step	Action
Step 1	In the Account Requests tab, find the account to be registered, and then select **Actions** > **Manual Registration**.
Step 2	Click **Generate Registration File** to download the file.
Step 3	Log into **CSSM Cloud**.
Step 4	Navigate to the **On-Prem** tab.

Step	Action
Step 5	Click **New SSM On-Prem**. a. Enter the **SSM On-Prem Name**. b. Select the **Virtual Account** from the drop-down list. c. Click **Add**. **NOTE**: Use same name as the account you created on SSM On-Prem and only select a single Virtual Account.
Step 6	In **Choose File**, select the **file** you generated in **Step 2**.
Step 7	Click **Generate Authorization File** and click **Download Authorization File**.
Step 8	Upload the **Account Authorization File** from CSSM Cloud to SSM On-Prem using the **Choose File** option and then click **Upload**. The file is uploaded, and the Local Account is registered.

Rejecting a Local Account

The System Administrator can also Reject the Local Account by providing a reason, which is included in the email sent to the requestor.

Complete these steps to reject a Local Account.

Step	Action
Step 1	From the Action tab, select **Reject**.
Step 2	Type a **message** or **reason** to be included in the email to be sent to the requestor. The Local Account will not be registered to CSSM Cloud.

Settings Widget

The Settings widget allows the System Administrator to configure the following settings needed by SSM On-Prem: Messaging, Syslog, Language, Email, Time Settings, and Message of the Day Settings.

Messaging Tab

The Messaging tab allows the user to configure messages for the application banner and login page. Complete these steps to configure these messages:

Step	Action
Step 1	(Optional) In the **Enter text to appear in banner** field, enter banner text.
Step 2	(Optional) Select **Display Message** (Selecting this option shows the message on the login screen.
Step 3	(Optional) Select **Text/Background Colors**. (Default is black text with red background.)
Step 4	(Optional) Select existing message and type your **Login Page Message**.
Step 5	Click **Save**.

Syslog Tab

SSM On-Prem syslog support enables SSM On-Prem Events to be sent to a remote syslog server.

Complete these steps to enable syslog support:

Step	Action
Step 1	Select **Enable Remote Logging**.
Step 2	Configure the **Syslog Server Address** and **UDP Port** number.
Step 3	Click **Save**.

The software sends syslog events based on the following severities:

- **INFO**: General notifications and events
- **WARN**: Minor alerts
- **ALERT**: Major alerts

Complete these steps to filter syslogs based on severity:

Step	Action
Step 1	Go to **Admin Workspace-> Settings**.
Step 2	Under Syslog, enter **Syslog Server Address** and server **PORT**.
Step 3	Select syslog level based on priority level selected. Available levels are: • **ALERT:** Major error log • **WARN:** Minor error and Warning log • **INFO:** Informational log
Step 4	Click **SAVE.**

All syslogs from selected severity level or higher are forwarded to the syslog server.

NOTE:

In the release 8-202102, users have switched to use Fluentd for remote logging solution. The Fluentd implementation captures significantly more logs than the previous implementation. The On-Prem used to send to remote logging server only event logs from the application. Now, it sends all captured logs and sets their facility based on the pattern:

- Application logs with all severity levels are mapped to local0 facility.
- Secure logs map to security/authorization facility.
- Event logs map to local1, local2, local3 and log audit.

CSLU Tab

The following switches are available in this tab:

- **Validate Device** – this controls the automatic creation of Product Instances when the usage report is received. When the Validate Device is ON, and an unknown Product Instance sends a usage report, the local database is examined to see if the device is present or not. If the device is present in the database, then the usage report is accepted. If the device is not present in the database, the usage report will be rejected. If you do not require the additional validation, make sure that the Validate Device switch is set to OFF (which is the default setting).
- **NAT Setup** – the default setting here is OFF, but the NAT Setup switch needs to be turned ON if the devices are behind a NAT (Network Address Translation) in the customer setup. This solution enables CSLU to capture unique device identification (UDI) data to identify the devices, instead of capturing their IP address (which would not be unique in a NAT setup).

- **Instant authorization request to CSSM** – the default setting is disabled. When you connect a device to SSM On-Prem, the device sends a SLAC request. SSM On-Prem forwards the SLAC request to the CSSM Cloud during synchronization. As part of the synchronization process, the CSSM Cloud responds by sending the SLAC to SSM On-Prem, which then sends the SLAC to the device. Because the communication between SSM On-Prem and the CSSM Cloud only occurs during the synchronization, there can be a long delay between when the device sends the request to SSM On-Prem and when the device receives the SLAC. The **Instant authorization request to CSSM** option enables you to bypass the synchronization requirement. When enabled, SSM On-Prem forwards the data immediately to the CSSM Cloud rather than waiting for a synchronization to occur.

NOTE:

- **Instant authorization request to CSSM** only supports push-mode devices. Pull-mode devices are not supported.
- **Instant authorization request to CSSM** is only supported in Connected-mode and not in Disconnected-mode.
- The Instant authorization is only applicable for the devices with IOS version 17.9 and above (Smart Agent version greater than 5.3).
- CSSM Cloud includes reserved licenses in the total number of licenses used. SSM On-Prem, however, does not. This causes CSSM Cloud and SSM-On Prem to show a different number of licenses in use after sending multiple SLAC requests.

Step	Action
Step 1	From the **SSM On-Prem Admin Workspace**, click **Security Widget**. The Security Widget screen opens.
Step 2	Select the **CSLU** tab.
Step 3	(Optional) Slide the **Validate Device** toggle switch to the **right** to enable device validation.
Step 4	(Optional) Slide the **NAT Setup** toggle switch to the **right** to enable NAT setup.
Step 5	(Optional) Slide the **Instant authorization request to CSSM** toggle switch to the **right** to enable instant authorization requests to CSSM.
Step 6	Click **Save**.

Language Tab

Currently, SSM On-Prem supports English, French, Korean, Chinese, and Japanese.

Complete these steps to select your language.

Step	Action
Step 1	From the drop-down list, select a **language**.
Step 2	Click **Save**.
Step 3	Navigate to **another screen**.
Step 4	Return to your **original screen**. The page now shows the new language.

NOTE: After you select and save a language, refresh the screen by navigating to another screen and then return to your original screen. The screen will now open in your selected language.

Email Tab

Configure the SMTP parameters listed here to get email notifications from SSM On-Prem.

Step	Action
Step 1	(Required) Enter the **SMTP Server** name.
Step 2	(Required) Enter the **SMTP Port** (default 25).
Step 3	(Required) Enter the **HELO Domain** name (FQDN).
Step 4	(Required) Enter the **Email From** address. **NOTE**: This must be a legitimate email address.
Step 5	(Optional) Select **Authentication Required**. **NOTE**: If this option is selected, then both a legitimate username and password must be entered (the username and password match that of the user record in the Users Widget) so that the user is notified of any role changes to his user account. a. (Required) Enter a **Username**. b. (Required) Enter a **Password**.
Step 6	Click **Save**. Your email settings are saved to the system.

Time Settings Tab

(Updated NTP procedure for multiple SHA settings for NTP/Chrony Server)

Currently, you can set the time manually or allow it to synchronize with NTP. The time zone for your SSM On-Prem system can also be set with UTC+0 which allows for all the timestamps to be displayed in UTC time. UTC+offset enables the timestamp to be displayed in the system's local time.

NOTE: When you change the time setting, all scheduled background jobs will also be rescheduled to reflect the changed time.

Complete these steps to configure Time Settings.

Step	Action
Step 1	Select **Time Zone** from the drop-down menu.
Step 2	Configuring the **Time Setting**. **NOTE**: The default setting for the Time Zone is UTC-0. If you want to manually set the time, turn on **Manually Set Time** by: c. Sliding **Manually Set Time** to **On** (slide to right). d. Selecting the **Date** (default to current date). e. Setting the **Hour**, **Minutes**, **Seconds**. If you want to synchronize with an NTP server, enable Synchronize with NTP Server by: a. Sliding the selector, **Synchronize with NTP Server,** to the right.

Step	Action
	b. Entering a **valid IP** Address or fully qualified domain name (FQDN) for Server Address 1. c. Entering a valid **Port** for Port 1. d. (Optional) If you have a second NTP Server, enter the IP Address or FQDN and Port for Server Address 2 and Port 2. **NOTE**: When you save the NTP server address configuration, SSM On-Prem checks to see if there is an incorrect IP Address. If the system finds that it cannot connect to the address for Server 1, the server will stop checking and show an error for server 1 (in red). If an error is listed for server 1, SSM On-Prem will **not** check to see if it can connect to Server 2 even though it may be able to do so. Additionally, if the system can connect to Server 1, it will attempt to connect to Server 2 and if it cannot connect to it, it will send back an error for Server 2.
Step 3 (Optional)	To use NTP/Chrony Authentication for one or both servers, complete these steps: a. Enable **Use NTP/Chrony Authentication for Server 1** by sliding the selector to the right, then select the **Key Type 1** from the drop-down list. The choices are: SHA1, SHA256, SHA384, SHA512. **NOTE**: For security reasons, it is strongly recommended that you select SHA256, SHA384, or SHA512. (SHA1 is no longer considered to be secure.) b. Enter the unique **Key ID** and **Key** obtained from the associated NTP server. (If you use Hexadecimal keys, select the **HEX** check box.) **NOTE**: The tooltip provides information on what HEX values must be used for SHA1, SHA256, or SHA512 as well as the range for an ASCII Key. **NOTE**: The HEX prefix is automatically included in the key. **NOTE**: For multiple NTP/Chrony servers, use Server Address 2, Port 2, and if authentication is used, Key Type 2, Key ID 2, Key 2, for the second address.
Step 4	Click **Apply**. **NOTE**: Click **Reset** if you need to reset the time settings. **NOTE**: Synchronize Time Now is enabled after the configuration has been saved or upon loading the dialog, but it is usually unnecessary, since synchronization occurs when saving the NTP configuration parameters. In addition, like other NTP clients, the SSM On-Prem NTP client automatically polls the NTP server to maintain server time.

Message of the Day Settings Tab

The options on this tab allow you to set the greeting message on the SSM On-Prem console when using ssh to connect to a terminal on the server.

- **Message of the Day**: Is displayed after the user logs into the application.
- **Before-login-Message**: Is the console display or greeting before the user is prompted to log into the system.

When you have configured these options, click **Save**.

Event Log Settings Tab

To provide a means of making sure that the database does not exceed space limits, the Event Log Settings tab establishes limitations on how long event log notifications are held. After the thresholds are reached, the system will "prune" the notifications from the database which will keep sufficient room on the database.

Complete these steps to set event log parameters.

Step	Action
Step 1	Open the Settings Widget, and select the **Event Log Settings** tab.
Step 2	In the Days Retention field, select the number of days for the records to be retained. **NOTE**: The number of days that records are retained must be 7 to 30.
Step 3	In the Prune Every field, select the number of days before pruning takes place. **NOTE**: The number of days before pruning must be greater than or equal to 1 day.
Step 4	Once the Event Log Setting parameters have been set. Click **Save**. The settings are saved to the system.

Update LDAP Data Settings Tab

This tab enables you to specify the frequency for fetching LDAP data.

Step	Action
Step 1	Open the Settings Widget, and select the **Update LDAP Data Setting** tab.
Step 2	In the Update Every * field, enter the frequency in hours for fetching LDAP data. **NOTE**: The number of hours must be 1 to 23.
Step 4	Click **Save**. The settings are saved to the system.

Event Log Tab

When you select the Event Log tab, the Event Log pane opens. Using search fields within the table, you can organize events according to Date Range, Event Type and/or User.

API Toolkit Widget

An application needs to be authenticated prior to using the SSM On-Prem APIs. Authentication is accomplished via the API Toolkit Widget. First, you need to create one or more credentials which can be used by your application. Your application will use the created credential when accessing APIs on the SSM On-Prem. If this is not done, your application will receive a **403 Access Restricted** error. You embedded an internal OAuth2 server embedded within the SSM On-Prem software (https://github.com/oauth-xx/oauth2) which authenticates all API calls.

API Console Access is enabled by the System Administrator through this Widget. Once access is enabled, an Admin or SysOps user can create Client or Resource credentials to get the Access Token (from the embedded OAuth2 server) to invoke the APIs. There are two types of credentials:

- **Client Credentials Grant**: Enable machine-to-machine access to the API so that it can issue the API call.

- **Resource Owner Grant**: Enable user-to-machine access to the API so that it can issue the API call. This is the case of a remote system user trying to initiate an API call through some client application.

Once the Client ID and Client Secret are generated, they need to be used by the application to request the OAuth2 server to generate the Access (Bearer) Token that is used as the header of the HTTP request(s) for the API endpoints. See Calling Access Tokens to generate this type of token.

NOTE: If you have enabled ADFS when using API Toolkit, only local authentication will work for Resource Owner Password Credentials (ROPC).

Enabling the API Console

The API Console toggle must be enabled by the System Administrator to create OAuth2 grants and to subsequently use API calls with these grants.

Complete these steps to enable the API Console.

Step	Action
Step 1	From the Administration workspace, click **API Toolkit**. The API Toolkit table opens.
Step 2	At the right-hand corner of the table, slide the **API Console** to **Enabled** (the default is **Disabled**). You can now create Access Tokens (from the embedded OAuth2 server) to invoke the APIs (see Creating OAuth2 Grants).
Step 3	Click **Add**.

Creating OAuth2 ADFS Grants

Once the API Console has been enabled, you can create grants. The Client Credentials Grant or the Resource Owner Grant needs to be generated to obtain the Access (Bearer)Tokens from the embedded OAuth2 ADFS server.

Complete these steps to create either a Client Credential or Resource Owner Grant.

Step	Action
Step 1	From the Administration Workspace, click **API Toolkit**. The API Toolkit table opens.
Step 2	Check if the API Console is **Enabled**.
Step 3	Click the **Create** tab to open menu.
Step 4	Depending on your need, select either the **Client Credentials Grant** or **Resource Owner Grant**.
Step 5	For Client Owner Grant: a. (Required) Enter the **Name** for the Grant. b. (Optional) Enter a short **Description** for the Grant. c. (Optional) Enter an **Expiration Date** (Hint: Click the calendar icon on the right side of the field. d. Review the **Client ID**. (Auto filled) e. (Required) Enter the **Client Secret**. (Hint: Click the “Eye” icon to view the secret.)

Step	Action
Step 6	(Optional) To open the API Access Control, click the **Click here to set API Access Control link**.
Step 7	(Optional) **Regenerate Client Secret**. **NOTE**: The Client Secret expires after 15 minutes. If it expires, click the link again to regenerate the secret. It is recommended that you click the "eye" icon so that you can view the secret change, then copy it (use the copy icon at the right side of the screen) so that you can use it when working with other applications.
Step 8	Click **Save**. The Grant Credential is listed in the table.

Setting API Access Control

NOTE: Be sure you have enabled the API Console and created Client Credentials Grant.

This procedure allows the application to access these resources in API endpoint calls.

Complete these steps to set API access control for one or more accounts.

Step	Action
Step 1	From the Client Credentials Grant table, click the **Click here to set API Access Control link**. The Client Credentials Grant table opens.
Step 2	Select an **Account** from the drop-down list.
Step 2	Select a **Role** (Account Admin, Account User, Per Virtual Account).
Step 3	Click **Add**. The Account and Role are listed at the bottom of the table.
Step 4	Click **Apply and Go Back**. You are notified that the access was created, and you are returned to the API Toolkit table.

API Call for Access Tokens

Both Client Credentials Grant and Resource Owner Grant use the same URL to call the SSM On-Prem: **POST "/oauth/token"**. Here is an example of how to generate an HTTP POST for a **Resource Owner Grant** (command is a single line):

```
curl -H 'Content-Type: application/json' -d '{"client_id":
"da52ae2c8dc2981e365b876ec15a7361db494d367a2eeff22607f4e6889e4c11",
"client_secret":
"ef8f1af6e49f375eea84ad0477633f184d508983baa83c0f367f1cf5b03725b1",
"grant_type": "password", "username": "admin", "password":
"CiscoAdmin!2345"}' https://<ip-address>:8443/oauth/token -v k
```

Here is an example of how to generate an HTTP POST for a **Client Credentials Grant** (command is a single line):

```
curl -H 'Content-Type: application/json' -d '{"client_id":
"da52ae2c8dc2981e365b876ec15a7361db494d367a2eeff22607f4e6889e4c11",
"client_secret":
"ef8f1af6e49f375eea84ad0477633f184d508983baa83c0f367f1cf5b03725b1",
"grant_type": "client_credentials"}' https://<ip-
address>:8443/oauth/token -v k
```

NOTE: For Windows command prompt, the curl command needs every string in double quotes and escape any double quotes within with a \.

```
curl -H "Content-Type: application/json" -d "{\"client_id\":
\"da52ae2c8dc2981e365b876ec15a7361db494d367a2eeff22607f4e6889e4
c11\", \"client_secret\":
\"ef8f1af6e49f375eea84ad0477633f184d508983baa83c0f367f1cf5b0372
5b1\", \"grant_type\": \"client_credentials\"}" https://<ip-
address>:8443/oauth/token -v k
```

NOTE: Replace the client id and client secret with the ones that you generated within the API Toolkit Widget. Replace username and password with your account credentials. This token expires within one hour of creation and a new client secret is needed after this time for the grant. The access token at the bottom of the output provides the Bearer token used for public API calls.

Using APIs

After receiving an access token described in the previous section, the remote systems will use that access token to call the SSM On-Prem APIs. In the case of Client Credentials Grant, the running of the API functions is authorized by roles granted to the OAuth Client Credential Grants (see Enabling API Access Control). In the case of Resource Owner Grant, the running of the API functions is authorized by the user roles in the system. Refer to: Using Smart Software Manager On-Prem APIs for the actual APIs that can be used and how to invoke them.

Support Center Widget

(Available in SSM On-Prem 7 201907)

The Support Center Widget allows the Administrator to search, view, and download system logs directly from the GUI instead of the console.

System Logs Tab

This table below describes the features and functionality in the Support Center Widget.

Feature	Functionality
Download All Logs	Clicking this button downloads all logs as a zip archive to the browser's default download directory. The contents of the log files consist of those messages accumulated at the time the request is processed by the server. This button is always enabled when log files are available to download.
Select a Log	Selects a log file to display. Log messages are displayed continuously in real-time as they are generated on the server. Available when there are logs available to display and Pause is not selected. **NOTE**: All features excluding Download All Logs are disabled, until a log file is selected from this list.
Download	Clicking this button downloads the currently selected log file to the browser's default download directory. The contents of the log file

Feature	Functionality
	consist of those messages accumulated at the time the request is processed by the server. This button is enabled once a log file has been selected.
Wrap Log Text	Checking this box makes long log messages wrap within the Support Center widget window. If unchecked log messages that exceed the length of the Support Center widget window must be scrolled to view their full text. This feature is active when a log file is selected.
Filter Realtime Text	Applies a Linux extended grep regular expression to log messages when they are coming from the server in real-time. (See Select a Log.) This feature is active when a log file is selected, and Pause is unselected.
Select Quick Search	Searches for a predefined case-insensitive string within the currently selected log file whose contents are those accumulated at the time the search is initiated. This list of strings is currently not configurable. Unlike Filter Realtime Text, this function searches the entire log file. Available when a log file is selected, and Pause is unselected.
Search Log Text	Applies a Linux extended grep regular expression to the currently selected log file whose contents are those accumulated at the time the search is initiated. Unlike Filter Realtime Text, this function searches the entire log file. Available when a log file is selected, and Pause is unselected.
Pause	When checked pauses real-time logging. When unchecked, restarts real-time logging, if real-time logging was enabled prior to selecting Pause. Available when a log file is selected.

Complete these steps to download your logs.

Step	Action
Step 1	If downloading a single log file, select the **log file** you want to view from the drop-down list.
Step 2	Download the file: • Either click **Download All Logs** to download a *.zip file containing all log files. • Or **Download** which will download the currently selected *.log file.

Network Widget

NOTE: SSM On-Prem supports configuration of IPv4, dual stack IPv4 and IPv6 addressing schemes.

The Network Widget allows the Administrator to configure network parameters such as: IP address, subnet mask/prefix, default gateways, and proxy settings used by SSM On-Prem.

SSM On-Prem adds support for up to four interfaces that can be configured and used for user management, product registration, and communications with CSSM Cloud. However, only two interfaces can use HTTPS. The number of interfaces listed in the Network Interface tab is dependent on the number of interfaces provisioned on the host.

NOTE: While all interfaces will show up, only **ens32** and **ens33** (these interface names are for example only and it changes according to your Infrastructure) can be used for strict HTTPS communication with products. The remaining interfaces can be used for either web access, or products which register with either HTTP, or that do not perform strict SSL checking.

NOTE: With customers that employ High Availability (HA) clusters, it is not possible to utilize **ens32** and **ens33** (Or any other interface) at the same time.

The Network Widget interface has three tabs:

- **General**: This tab lists the server name, DNS server, and default gateway information.
- **Network Interface tab**: This tab lists the connections available and the status of each connection.
- **Proxy tab**: This tab allows you to set up a proxy server.

NOTE: When High Availability is provisioned, editing of interface information is disabled and it is only possible to view the interface information.

General Tab

Complete these steps to configure the network settings.

Step	Action
Step 1	Select **Network Widget > General tab**
Step 2	Enter a DNS resolvable hostname or **IP Address** for the SSM On-Prem Name.
Step 3	Configure the IP Addresses for the Default Gateway Settings (either one or both). • IPv4 • IPv6
Step 4	Enter the **IP Address** for the Primary (and Alternate) DNS Settings (either one or both).
Step 5	Click **Apply**. **NOTE**: Click **Reset** if you need to reset the General Network settings.

NOTE: When either the Primary or Alternate DNS are changed an internal communications error is displayed stating, “An internal communications error within the server has occurred, page will reload.” This is expected behavior when the DNS settings have changed. Clicking **Reload Now** redirects you to the Login Page where you can restart the system.

Network Interface Tab

The Network Interface tab shows the various connections to the network. Each connection lists a specific status including firewall port requirements:

- **Connected**: The interface has a connection and is configured with an IP address.
- **Connected (Unconfigured)**: The interface has a connection but is not configured with an IP address.
- **Disconnected (Unconfigured)**: The interface does not have a connection and therefore is not configured with an IP address.

Editing an Interface

Interface properties are edited by expanding the **interface** section and then clicking **Edit Interface** (if HA is provisioned, this button is set to View Interface to disable editing). When the window opens, you can select either **IPv4** or **IPv6** depending on the network protocol being used (use the toggle switch located at the top left of either the IPv4 or IPv6 tabs).

IPv4 Settings

The **IPv4** window allows you to configure these settings (IP Addresses):

- Turn IPv4 on/off
- IP address
- Subnet Mask
- IPv4 Gateway

IPv6 Settings

The **IPv6** window allows for the configuration of these settings (IP Addresses):

- Turn IPv6 on/off
- IPv6 address
- IPv6 Prefix
- IPv6 Gateway

Default Gateway

This switch allows you to set the default gateway for one of the NICs. If it is set to **on**, that NIC defines the default gateway and firewall port requirements.

NOTE: Only one NIC can set the default gateway at a time, but up to four interfaces can be configured.

Firewall Port Requirements

The firewall configuration provides for traffic separation and security control (through specific ports).

You can set the type of access to SSM On-Prem through the following settings:

- Product and Management (Public: Access to SSM On-Prem open through either a browser, product, or Cisco.)

- Management Only (User: Access to SSM On-Prem is open just a browser.)
- Product is for product registration and authorization. (Product: Access open through the product.)
- Cisco Communication Only (DMZ: Restricted to inbound traffic only from Cisco.)

NOTE: If you add two network interfaces, then be sure to use specific configurations or the connectivity to SSM On-Prem will be lost.

NOTE: If you change the interface responsible for product registration and authorization, then you will also need to update Common Name. (See the Filling in the Common Name section for details.)

If you are setting up a DMZ (the last option listed), then you will need two network interfaces, Follow the steps in this example to configure specific static routes.

Example of DMZ Setup:

Step	Action
Step 1	Log into your Command Line Interface (CLI) as admin user using ssh.
Step 2	Start the On-Prem console by typing this command: `$ onprem-console`
Step 3	Next, run network manager from the console by typing this command `>> network_manager` Press **Enter** to open the Network Manager app opens.
Step 4	To route outbound traffic to Cisco, add the following custom routes to the DMZ network interface. a. From the main screen, select **Edit a Connection**. b. Next, select **Network Interface for DMZ**. c. Click **Edit**. **NOTE**: Network configuration, including IP addresses, DNS, and custom routes are not automatically configured during HA deployment. Log into both Primary and Secondary nodes and then follow steps 4-7 to set up custom routes for each network.
Step 5	In the Edit screen, navigate to the **routing section** and click **Edit**.

Step 6	In the next screen, click **Add** to add the first customer outward bound route. Repeat this step to add a second route using a gateway you have previously defined. (Using DMZ as gateway.)
	For example, if your DMZ network interface has a gateway IP address, you would add the following routes.
	`Destination1: 72.163.0.0/16`
	`Next Hop1: <YourIPGateway>`

Step	Action
	Destination2:173.37.0.0/16 Next Hop2: <YourIPGateway> Destination3: 146.112.0.0/16 Next Hop3: <YourIPGateway> **NOTE**: With this configuration, all requests to **swapi.cisco.com** and **cloudsso.cisco.com** go out through the **Proxy Network** interface.
Step 7	When you have finished configuring your firewall port configuration, **restart the system**.

Once you have configured your Network Interface settings, click **OK** to save your changes to the system.

Proxy Tab

The Proxy tab provides proxy services to SSM On-Prem. Basically, a proxy server is a device in the network that acts as an intermediary for requests from devices within the customer network and external servers. There are two types of proxy services supported by SSM On-Prem:

- Explicit proxy support
- Transparent proxy support

Explicit Proxy Support

SSM On-Prem is explicitly configured to use a proxy server, so that SSM On-Prem "knows" that all requests will go through a proxy. SSM On-Prem must be configured with the hostname/IP address of the proxy service. When information needs to be sent to Cisco, SSM On-Prem connects to the proxy and sends the request to it. The Proxy then relays the information to the Cisco servers.

Transparent Proxy Support

The proxy server is typically deployed at a gateway and the proxy service is configured to intercept traffic for a specified port (**443** in this case). SSM On-Prem is unaware that traffic is being processed by a proxy. Traffic sent via HTTP port 443 is intercepted by the proxy server and routed to the Cisco server.

The **Proxy Support** feature on SSM On-Prem enables HTTPS **Explicit Proxy** support between it and CSSM Cloud (**products > SSM On-Prem > HTTPS proxy > Cisco SSM**). This support enables customers to control or monitor traffic between SSM On-Prem and Cisco Servers.

NOTE: If you are using an HTTPS proxy, please make sure to follow the following steps:

- Create a certificate, and use IP of the proxy server as Common Name (CN)
- Have your certificate signed
- Upload the signed certificate to the proxy server and SSM On-Prem trusted key store.
- Fine tune the proxy server to allow the traffic from the ports that are used in SSM On-Prem
  User Interface: HTTPS (8443)
  Product Registration: HTTPS (443), HTTP (80)

- Please ensure that you firewall allows traffic to and from SSM On-Prem, and the following URLs are accessible:
  cloudsso.cisco.com
  swapi.cisco.com

Complete these steps to setup proxy support.

NOTE: The proxy should not interfere with the SSL inspection or bypass the CSSM Cloud root licensing certificate.

Step	Action
Step 1	Set **Use a Proxy Server** to **On**.
Step 2	Enter the **Proxy IP Address** and **Port**.
Step 3	Enter the **Proxy Username** and **Proxy Password**.
Step 4	Click **Apply**.

NOTE: Proxy settings only affect communication to Cisco during account registration and synchronization.

Editing a Proxy Password

If you have configured a Proxy server and have set your password, you can edit the password using the Edit Password button.

Complete these steps to edit your Proxy password.

Step	Action
Step 1	In the Administration Workspace, open the **Network Widget**.
Step 2	Select the **Proxy** tab.
Step 3	Click **Edit Password** located below the Proxy Credentials field. The Edit Password window opens.
Step 4	Enter a **New Password** and then **Reenter Password**.
Step 5	Click **Save**. The password has been changed.

Synchronization Widget

CSSM Cloud is the “source of truth” for all license entitlements (purchases), Cisco Virtual Accounts, and metadata information. On the other hand, SSM On-Prem is the “source of truth” for product instance registration and license consumption. This means that each system must take whatever is sent by the other system as an undeniable source. In addition, when a Local Account synchronizes with CSSM Cloud, it gets a new ID certificate (364-day duration) allowing uninterrupted functioning.

SSM On-Prem supports online manual, online scheduled, and offline manual synchronization. When you click the **Synchronization Widget**, you can view a list of Local Accounts, their status, and available options.

Synchronization Types

Either the **System Administrator** or **System Operator** can initiate full or partial synchronizations. See the following sections for more information on synchronization types.

Standard Synchronization

Under standard synchronization, SSM On-Prem and CSSM Cloud are operated on a delta synchronization model. This means that only incremental changes on product instances, license purchases, and consumption are sent and received.

Full Synchronization

In the case where the SSM On-Prem database is restored from a previous VM snapshot or backup, this incremental synchronization process can produce mismatched license entitlement/consumption and product instance counts. A full synchronization is used when CSSM Cloud detects that it needs SSM On-Prem to compile and send a complete list of its data, regardless of when it was created. In return, CSSM Cloud also gathers a complete list of its current “source of truth” elements and passes that list along to SSM On-Prem.

Synchronization Alerts

Below are the synchronization alerts, located on the right side of the screen, for Local Account non-synchronization with CSSM Cloud:

Alert	Description
(**Minor Alert**) Synchronization Overdue: Synchronization hasn't happened for 30 to 90 days	Synchronization Overdue: Local Account has not synchronized in X days." (X will be between 30th & 89th day, depending on last synchronization date)
(**Major Alert**) Synchronization overdue: Synchronization hasn't happened for 90 to 364 days	"Synchronization Overdue: On-Prem has not synchronized in X days." (X will be between 90th & 364th day, depending on last synchronization date)
(**Major Alert**) Re-registration Required: Synchronization has not happened in 365 days	Re-registration Required: On-Prem was not synchronized for 365 days and must be re-registered with CSSM Cloud

After 364 days of non-synchronization, the SSM On-Prem Local Account is still present (not deleted) on the CSSM Cloud; however, the ID certificate will have expired, and the SSM On-Prem Local Account can no longer be synchronized. License counts on SSM On-Prem and CSSM Cloud can be out-of-sync, and neither network nor manual synchronization can be performed. Existing products will not get valid responses from the SSM On-Prem, and no new products can be registered. However, it only affects this Local Account. The only recourse is to delete the SSM On-Prem Account, re-register it to CSSM Cloud, and re-register all the product instances to the Local Account. (For more information, see Re-registering a Local Account.) Account that resides on SSM On-Prem

Once registered, an SSM On-Prem Local Account is recommended to be synchronized with CSSM Cloud periodically to ensure the licensing information between the SSM On-Prem and CSSM Cloud is not out-of-sync. Scheduling is accomplished by setting up a scheduled synchronization. (For more information on scheduling synchronizations, see Scheduling Tab.

Accounts Tab

This view is a list of accounts on which you may perform synchronization actions.

NOTE: The **Name** and the **Satellite Name** columns refer to the Local Account Name on the SSM On-Prem, and the name of the account on CSSM Cloud respectively. They are typically the same, as giving these accounts the same name prevents confusion when dealing with multiple accounts.

In cases where a user changes the name to something else on CSSM Cloud, SSM On-Prem will reflect that new name in the **Satellite Name** field after it is detected in a synchronization response.

Most of the columns here refer to synchronization details (last sync date, sync due date, alerts, etc.) You may also select the name of the account to see the full list of details. If you click the **Name** of an account, the following information is listed:

- Account Name: The name of the account on SSM On-Prem.
- Cisco Smart Account Name: The name of the account on the CSSM Cloud.
- Cisco Virtual Account Name: Same as the Account Name.
- Cisco Satellite Name: The SSM On-Prem name on SSM On-Prem
- UID: The PI token assigned to the account.
- Date Registered: The date and time the account was registered.
- Last Synchronization: The date and time the account was last synchronized.
- Synchronization Due Date: The date and time for the next synchronization.

To perform synchronization activities, select the **Actions** button to the far right of the desired account name. See the following sections for more information on all available actions.

NOTE: Cisco SSM On-Prem version 8-202108 introduces the Bulk Sync feature that allows users to select multiple/all accounts and then trigger the network sync option for all of them. This bulk synchronization option is now available in the Admin Workspace for System Admin and System Operator roles through the **Sync Selected** button in the Accounts Tab.

Scheduled synchronization will take place irrespectively of the bulk sync completion.

Enable/Disable Scheduled Synchronizations

This action allows you to enable or disable scheduled synchronizations for a selected local account (the change is confirmed with a pop-up message). Global scheduled synchronizations options are available in the Synchronization Schedule section.

Data Privacy

This action enables you to define individual data privacy settings for a selected local account. This will override global data privacy settings. For more information on what settings are available, see the Global Synchronization Data Privacy Settings section.

Network Synchronization

Online synchronization assumes there is an Internet connection to CSSM Cloud from SSM On-Prem.

NOTE: If this is attempted for the first time (or if your session has expired), you will be required to re-authenticate with CSSM Cloud via a login screen to the Cisco Virtual Account in the SSM On-Prem Administration Workspace.

Follow these steps to perform an online synchronization:

Step	Action
Step 1	Open the **Synchronization** widget.
Step 2	On the Local Account, under Actions**,** select **network synchronization** and then select **Standard Synchronization Now...** or **Full Synchronization Now...**.
Step 3	Enter your **Cisco Smart Account** credentials.
Step 4	Click **OK**. The dynamic processing symbol appears, and the Alerts column shows the status of the synchronization as it progresses.

Manual Synchronization

Manual synchronization is used when the customer network is not connected to the Internet and you need to ensure product instance counts, license usage, and license entitlements are the same on both CSSM Cloud and SSM On-Prem.

NOTE: After 181 days, automatic synchronization will fail due to the expiration date of the access token, so manual online synchronization is required.

In this case, you can perform a manual synchronization which results in creating a Smart Software Manager On-Prem synchronization request file that is uploaded to CSSM Cloud. Once the file is received, a synchronization response file is sent to SSM On-Prem to reflect the same license information.

Follow these steps to perform a manual synchronization:

Step	Action
Step 1	Navigate to the SSM On-Prem Administration Workspace and click the **Synchronization widget** to open it.
Step 2	In the Accounts table under the Accounts tab, select **Actions**.
Step 3	Select **Manual Synchronization** and then either **Standard** or **Full Synchronization**.
Step 4	Click the **Download File** button to create and download the synchronization request file to your local hard disk. a. A **data file** is generated. b. Choose **a location** where you want to save the data file.
Step 5	Log into **CSSM Cloud** and click the **On-Prem** tab.

Step	Action
Step 6	In the SSM On-Prem page, locate **the SSM On-Prem** that you want to synchronize (Steps 7 & 8), or click **New On-Prem** to add a new SSM On-Prem (Skip to step 9).
Step 7	If you select an **existing SSM On-Prem** from the list, then from the Actions drop-down menu, select **File Sync** against the SSM On-Prem.
Step 8	In the Synchronize On-Prem dialog box, click **Choose File** to upload the data file that was generated in the SSM On-Prem in Step 4. (Skip to Step 10)
Step 9	If you are adding a **new SSM On-Prem**, a screen dialog opens. Follow these steps: a. Input the **new SSM On-Prem name** in the SSM On-Prem Name box. b. Click **Choose File** to select a registration file. Select the **new SSM On-Prem file name** in the dialog. c. Click the **On-Prem Virtual Accounts Name** box. d. Select from a list of existing On-Prem Local Virtual Accounts or select a **New local Virtual Account...**. e. If you select a new Local Virtual Account, enter the **name of the Local Virtual Account** and an optional description, and then click **Add**.
Step 10	Click **Generate Response File** to generate a response file that has the synchronized data.
Step 11	Go to the **SSM On-Prem name** in the table that you selected in Step 6. (You might have to search for the SSM On-Prem name.)
Step 12	Click **Download Response File** to download to your local hard disk.
Step 13	Return to the **Synchronization widget** in the SSM On-Prem.
Step 14	Click **Choose file** to select the synchronization response file you just downloaded in Step 11.
Step 15	Click the **Upload** dialog box to upload the response file and complete the manual synchronization process.

When the manual synchronization process is completed, the license entitlement and usage on both CSSM Cloud and Local Account are identical. All the licenses in the default and Local Virtual Accounts associated with the SSM On-Prem Local Account added together equal the count in the Cisco Virtual Accounts of that SSM On-Prem on CSSM Cloud.

Schedules Tab

SSM On-Prem provides the ability to schedule, at specified intervals, all Local Accounts to be synchronized with CSSM Cloud (see Enabling Scheduled Synchronizations). The recommended schedule is that synchronization is checked once every 30 days. The scheduled synchronization uses the access token acquired when the user logs into Cisco SSO when creating an account or triggering a network synchronization.

NOTE: As of September 25, 2020, the new default access token life is 180 days instead of 30 days. So, if an access token is expired, you will receive an "*Access Token not found Synchronization cannot proceed*" notice when you synchronize an account. If you receive an access token not found notice, you must select the **Accounts tab > Actions** and perform a standard or full synchronization for that account. Before the synchronization process begins, you are prompted to enter you login credentials

(COO). Once you log in, the synchronization process will proceed during the next scheduled interval.

CAUTION: After your access token expires, you must perform a network synchronization to trigger the CCO login which will refresh the access token. Once you log in, the synchronization process will proceed during the next scheduled interval.

Global Synchronization Data Privacy Settings

In the **Schedules** tab, you can set the Global Data Privacy for all Local Accounts. You can override these global parameters with these settings in the individual Local Accounts:

- **Hostname**: The host name of registered product instance. This data is excluded during transfer when you check this checkbox.
- **IP Address**: The IP Address of the registered product instance. This data is excluded during transfer when you check this checkbox.
- **MAC Address**: The Media Access Control (MAC) Address of the registered product instance. This data is excluded during transfer when you check this checkbox.

NOTE: It is possible to override the global synchronization data privacy settings for a given Local Account by selecting **Actions >Data Privacy...**

Synchronization Schedule

If Synchronization Schedule is enabled, all accounts are synchronized every 30 days from the completion of their last sync with their Cisco Smart Account. If desired, a synchronizations schedule frequency (Daily, Weekly, Monthly) and Time of Day can be set for synchronizing all Local Accounts (see Enabling Scheduled Synchronizations).

NOTE: As of September 25, 2020, the new default access token life is 180 days instead of 30 days. So, when an access token is expired, you will receive an "*Access Token not found Synchronization cannot proceed*" notice when you synchronize an account.
When you receive an access token not found notice, you must select the **Accounts tab > Actions** and perform a standard or full synchronization for that account.
Before the synchronization process begins, you are prompted to enter you login credentials (CCO). Once you log in, the synchronization process will proceed during the next scheduled interval.

CAUTION: After your access token expires, you must perform a network synchronization to trigger the CCO login which will refresh the access token. Once you log in, the synchronization process will proceed during the next scheduled interval.

Enabling Scheduled Synchronizations

If designed for it, a synchronizations schedule can be set globally for all Local Accounts. Complete these steps to globally set Local Accounts synchronization.

Step	Action
Step 1	From the Schedules tab, select **Scheduled Synchronization On** or **Off**.
Step 2	Select the **Frequency** (Daily, Weekly, Monthly), to begin synchronization of all Local Accounts.
Step 3	Set the **Time of Day** (hour: select a value between 0-23) and (minutes 0-59)
Step 4	Select the **Day of Week** or **Month**.
Step 5	Click **Apply**.

Disabling Scheduled Synchronizations

Currently, there is no way to globally disable scheduled synchronizations. Complete these steps to disable scheduled synchronization for individual Local Accounts.

Step	Action
Step 1	Select the **Account** do be disabled.
Step 2	Click **Disable Scheduled Synchronization**. This action will cause the scheduled synchronization for that Local Account to be skipped.

High Availability Status Widget

NOTE: This Widget is visible only if a functioning High Availability cluster is configured on your system. This widget is also functional for clusters monitoring TACACS+.

From the Administration Licensing workspace, you can view the status of the HA Cluster using the High Availability Status widget. The High Availability Status widget displays the basic information of the cluster with a simulated illustration. A warning/critical icon will also be shown when there is a system error. See the *Cisco Smart Software On-Prem Installation Guide: Appendix 4* for more information on deploying a High Availability (HA) cluster.

NOTE: Refer to the Cisco SSM On-Prem Console Reference Guide for instructions on using the console help system.

Host Tab

The Host tab shows the information about the configured servers in the cluster and the status of the cluster.

Cluster Status Server

At the top of the widget is the overall status of the High Availability (HA) cluster. It provides a status indicating if the cluster is running as expected, or if a system abnormality has been detected.

Status	Description
Normal	The cluster is working normally. Data is being replicated between the hosts and the auto failover function is available.

Degraded	The system has detected one or more critical errors in the cluster and the hosts are not able to run the usual services. All errors must be addressed as soon as possible.
Disconnected	The HA peer is offline. This state can occur when the peer node is offline.

Virtual IP (VIP) address

The middle section of the widget shows the Virtual IP (VIP) used by the cluster, and indicates which server is active and which is passive.

System Information

The bottom section of the widget shows the Virtual IP (VIP) used by the cluster, and indicates which server is active and which is passive. In this section, you can review the resources for the two servers. It is important that each server is provisioned with matching software versions and resources. You can check the following usage information in this part:

- **Physical Memory**: This information indicates how much memory was selected when the system was deployed.

NOTE: This is the amount of RAM reported by AlmaLinux and may not exactly match the amount allocated to the server when it was provisioned.

- **Disk Space**: This information indicates how much disk space was selected when the system was deployed.

NOTE: This is the disk size reported by AlmaLinux and may not exactly match the amount allocated to the server.

- **Current Version**: This is the version of the SSM On-Prem software running on each server. It is critical these versions are identical or unexpected server failure may occur.

Event Logs Tab

The Event Log tab displays these details on events specific to the High Availability (HA) cluster:

- Times the events occurred
- The type of event (currently always set to Cluster)
- Messages describing events
- Users associated with the event

On-Prem License Workspace

With Smart Software Manager License Workspace, you can organize and view your licenses in groups called Local Virtual Accounts.

This workspace consists of two major components:

- **Administration** (see this section for more information),
- **License** (see this section for more information).

Administration

After you log into SSM On-Prem Licensing Workspace, (if you have Administrator status) you can use the Administration section to:

- Request an Account
- Request Access to an Existing Account
- Manage an Account

The following sections provides information and procedures used in this section.

Request an Account

If a Local Account does not exist on CSSM On-Prem, then a Local Account request is needed. Once the request has been submitted, the System Administrator or System Operator can approve the request from the Administrative Workspace.

To request for a Local Account, complete these steps.

Step	Action
Step 1	Log into **SSM On-Prem**.
Step 2	In the Administration section of the Smart Software Manager On-Prem Home screen, click **Request an Account**. The Request an Account screen opens.
Step 3	In the "Would you like to create the Account now" section: a. Enter a valid **Email Address** (person's company email address). b. (Optional) Enter a **Message to Creator** (text).
Step 4	In the Account Information section enter this information: a. (Required) **Cisco Smart Account** **b.** (Required) **Cisco Virtual Account** **NOTE:** Cisco Virtual Accounts without product instances will appear as an option. Also note that when creating a new Cisco Virtual Account, you must use a unique name. **NOTE**: For more information, see creating a Local Account.
Step 5	Click **Continue**.

Once the submission is made, a System Administrator or System Operator will need to approve the request in the Administration workspace (see Approving Account Requests).

Request Access to an Existing Account

Requesting access to an existing Local Account is based on your current profile and allows you to associate a user account with an existing Local Account. To request user access to an existing Local Account, complete these steps.

Step	Action
Step 1	Log into **SSM On-Prem Licensing Workspace**.
Step 2	In the Administration section of the Smart Software Manager On-Prem Home screen, click **Request Access to an Existing Account**. The Request Access to an Existing Account screen opens.
Step 3	(Required) Enter the **Account Name**.

Step	Action
Step 4	Click **Submit**. The request is submitted.

Manage Account

You can manage an account from the Administration section of SSM On-Prem. To manage an account, click **Manage Account**. Using a series of tabs to organize your information, the Manage Account screen allows you to:

- View an account's properties and general information. This "read-only" tab provides the account status, account name, who requested the account, and the date it was requested.
- Create and modify Local Virtual Accounts where you can modify both the name and description of the default Local Virtual Account, or you can create a new Local Virtual Account. (See Creating a Local Virtual Account.)
- Create and manage users using the New User Wizard. (See Adding Users to a Local Virtual Account.)
- Create and manage custom tags using the New Virtual Account Custom Tag Wizard (See Adding a New Local Virtual Account Custom Tag.)
- Create and manage user groups and assign them to accounts. (See Adding New User Groups.)
- View search for and approve/decline access requests. (See Access Requests Tag.)
- Use the event log to search for various events that have occurred in a Local Account. (See Administration Event Log Tab.)

Account Properties Tab

This tab contains the following account-related information:

- account status,
- account name,
- account requested by,
- account request date.

You can use the blue button in the top-right corner to access the drop-down list. Select any of the available accounts to view its properties.

NOTE: Cisco SSM On-Prem version 8-202108 introduces the Triggered Sync feature that allows users to perform a standard network synchronization on a selected On-Prem account. You can perform this action via the **Sync Now** button in the Manage Account section of the On-Prem License Workspace. This standard network synchronization can be triggered by users with the following roles:

- System Admin
- System Operator
- Local Account Administrator
- Local Virtual Account Administrator

System Admins and System Operators can still trigger standard network synchronization using the Synchronization Widget in the On-Prem Admin Workspace. See this section for more information.

Virtual Accounts Tab

You can create Local Virtual Accounts using the Virtual Accounts tab. Complete these steps to create a new Local Virtual Account:

Step	Action
Step 1	Log into **SSM On-Prem Licensing Workspace**.
Step 2	In the Administration section of the Smart Software Manager On-Prem Home screen, click **Manage Account** and select the **Virtual Accounts tab**.
Step 3	In the Virtual Accounts pane, click **New Virtual Account...**
Step 4	In the New Virtual Account pane, enter the **Name** (required) and **Description** (optional).
Step 5	Click **Save**. A new Virtual Account is created and is added to the list of Local Virtual Accounts.

You can modify (change) the name of the Default Local Virtual Account. Complete these steps to change the name of the SSM On-Prem Default Local Virtual Account.

Step	Action
Step 1	Log into **SSM On-Prem Licensing Workspace**.
Step 2	In the Administration section of the Smart Software Manager On-Prem Home screen, click **Manage Account** and select the **Local Virtual Accounts tab**.
Step 3	In the Local Virtual Accounts pane, click the **Star** icon to the right of the Default Name. The Default pop-up window opens.
Step 4	Enter the **New Name** (required) and **Description** (optional).
Step 5	Click **Save**. The new Virtual Account Name is listed in the Virtual Account Name column in the Local Virtual Accounts table.

Users Tab

Complete these steps to add users to a Local Virtual Account.

Step	Action
Step 1	Log into **SSM On-Prem Licensing Workspace**.
Step 2	In the Administration section of the Smart Software Manager On-Prem Home screen, click **Manage Account** and select the **Users** tab.
Step 3	In the Local Virtual Accounts pane, click the **link** for the Virtual Account Name that needs users or click New User.... (Skip to Step 5.)
Step 4	In the dialog for that user, select the Role Management tab (Skip to Step 7.)
Step 5	In the dialog, enter either the **User ID** or **Email Address** for the user. **NOTE**: Users must exist in the system before you can add them to a Virtual Account. You can add Users using the Users Widget in System Administration.

Step 6	Click **Search**. If the user is found that user's information is listed in the bottom section of the screen. Click **Next**.
Step 7	Select the desired role from the first two options—Account User or Account Administrator. Selecting one of these two options has the side effect of assigning the user to the listed Local Virtual Accounts. Selecting the **Assign roles to specific Local Virtual Accounts only** option allows assignment of specific Local Virtual Accounts and roles to the specified user. Once you have made your selections, click **Next** (new user) or **Save** (existing user).
Step 8	Review the **User Information** and **Assigned Role** and click **Add User** if correct. The User is added to the Virtual Account. **NOTE**: If the information incorrect, click **Back** to modify it.

Custom Tags Tab

Custom tags tailor the Local Virtual Account to fit the Client's specific needs. For example, you could associate a department name or geographic location or other pertinent information with one or more Local Virtual Accounts. Custom tags have a name and one or more values associated with that name. When you create the custom tag, you can decide whether the tag can only have one value associated with it or multiple values. You can also decide if the tag is required for all Local Virtual Account or if it is optional. If the tags are optional, you can associate any combination of a tag's values with one or more Local Virtual Accounts. Once a tag is associated with a Local Virtual Accounts you can use it for classifying, locating, and grouping purposes.

Complete these steps to use the Wizard to add a new Custom Tag to a Local Virtual Account.

Step	Action
Step 1	Log into **SSM On-Prem Licensing Workspace**.
Step 2	In the Administration section of the Smart Software Manager On-Prem Home screen, click **Manage Account** and select the **Custom Tags** tab.
Step 3	Click **New Virtual Account Custom Tag**. The Wizard opens.
Step 4	In Step 1 of the Wizard, enter the **Tag Name** (required), and **Description** (optional).
Step 5	Select if the tag is to be **Required** or **Optional**.
Step 6	Select the appropriate Tag Value Assignment Options of either **One Tag Value Only** (see note below) or **Allow Multiple Tag Values**. Click **Next**.
Step 7	In Step 2 of the Wizard, enter the **Tag Value(s) (**separated by commas if there are more than one). Click **Add Tag Values**.
Step 8	If you choose to add optional tags to a group of Local Virtual Accounts, click **Manage All Tag Values**, select the tag you wish to add to Local Virtual Accounts, click **Add/Remove** and then select the Local Virtual Accounts you wish to associate with the given tag and move those accounts to the Tagged box within the shuttle and then click Ok. Alternatively, you can accomplish the same functionality by clicking the ellipsis button next to the tag value within the table. Click **Next**.
Step 9	Review the **Tag Information and** click **Add Virtual Account Custom Tag** if correct.

	NOTE: If any tags are set to "required" and you have not associated at least one tag value from that tag with each virtual account, then you are prompted with a dialog to select the tag values to associate with each currently unassociated virtual account. Press **Save** once you have set the associations. The Custom Tag is added with a success notification. **NOTE**: If the information incorrect, click **Back** to modify it.

Complete these steps to modify existing Custom Tags associated with or to remove Custom Tags from a Virtual Account using the Wizard.

Step	Action
Step 1	Log into **SSM On-Prem Licensing Workspace**.
Step 2	In the Administration section of the Smart Software Manager On-Prem Home screen, click **Manage Account** and select the **Custom Tags** tab.
Step 3	Click on the custom tag you wish to modify and then click on the **Tag Values Management** tab.
Step 4	Enter additional tag values, remove tag values or click on **Manage All Tag Values** or the ellipsis button to change the association between tag values and Local Virtual Accounts.
Step 5	Click **Save** when your changes are complete. **NOTE**: If any tags are set to required and you have not associated at least one tag value from that tag with each virtual account, then you will be prompted with a dialog to select the tag values to associate with each currently unassociated virtual account. Click **Save** once you have set the associations and then click **Save** again when your changes are complete.)

NOTE: When setting the Tag Value Assignment Options to One Tag Value Only, multiple tag values can be supplied for the tag, but only one from the group can be assigned to a given virtual account at a time. This differs from the Allow Multiple Tag Values option which allows assignment of one or more tags to a given virtual account simultaneously.

NOTE: It is not currently possible to view or modify the custom tags associated with a virtual account under the Local Virtual Accounts tab. All viewing and management of custom tags associated with Local Virtual Accounts must be done under the **Custom Tags** tab.

User Groups Tab

The User Groups tab provides a centralized place to manage large numbers of users. User groups are a convenient way of organizing users by function, department, region, etc.

Complete these steps to add a new User Group.

Step	Action
Step 1	Log into **SSM On-Prem Licensing Workspace**.
Step 2	In the Administration section of the Smart Software Manager On-Prem Home screen, click **Manage Account** and select the **User Groups** tab.

Step 3	Click **New User Group**.
Step 4	Enter the **User Group Name** (required), and **Description** (optional).
Step 5	Click **Create**. A success notification opens.
Step 6	In the **Add Members to Group** pane, add users by User ID or Email. **NOTE**: Users must exist in the system before you can add them to a Virtual Account. You can add Users using the Users Widget in System Administration Workspace.
Step 7	Select if the user will be a **Group Owner**. **NOTE**: You can choose to change a group owner within the user table after the user is added to the group.
Step 8	Click **Add**. The user is added to the group.
Step 9	When you have added all the users you need, click **Close** to close the screen.

NOTE: If you have a set of pre-defined users, you can upload users by using the **Upload Users** button to upload a file containing a list of user ids. If you choose to upload users from a file, you may download a csv template file to use. The file contains a header line, followed by rows of users. Each row is a user id comma-separated by a case-insensitive true or false to indicate ownership. Optional double quotes can be used to encapsulate special characters in the user id. For example:

"user_id", "is_owner"
"tthumb","true"
"ppan","false"

If you modify this file using Excel, make sure you save the file as a comma-separated-value (CSV) file.
After attempting to process the uploaded file, if the format of the file has errors in it or has user ids that are unknown, errors will be generated that can be reviewed.
Only one user can be set to be the owner of a group.)
In addition, you can download a group of users to your system but clicking the **Download Users** button that will export the user group as a <group name>.csv file.

Managing User Groups

Under the user groups tab, it is possible to manage the users associated with a user group, assign Local Virtual Accounts access, send a message to a user group or delete a user group. Complete these steps to access these functionalities.

Step	Action
Step 1	Log into **SSM On-Prem Licensing Workspace**.
Step 2	In the Administration section of the Smart Software Manager On-Prem Home screen, click **Manage Account** and select the **User Groups** tab.
Step 3	Click on the **I want to...** associated with the user group of interest.
Step 4	Choose one of **Manage Users** (you can also click on the user group name to access this option), **Assign Local Virtual Accounts Access**, S**end Message to User Group** or **Delete User Groups**.

Assigning Local Virtual Account Access

The search feature in this table allows you to search for Local Virtual Accounts by name or tag and then assign access control to it.

Step	Action
Step 1	Log into **SSM On-Prem Licensing Workspace**.
Step 2	In the Administration section of the Smart Software Manager On-Prem Home screen, click **Manage Account** and select the **User Groups** tab.
Step 3	Click on the **I want to...** associated with the user group of interest.
Step 4	Choose one of **Manage Users** (you can also click on the user group name to access this option), **Assign Local Virtual Accounts Access**, S**end Message to User Group** or **Delete User Groups**.
Step 5	Select **Actions** > **Assign Local Virtual Accounts Access**.
Step 6	Select the **Account(s)** (by name or tag).
Step 7	Click **Assign Roles to Selected Local Virtual Accounts**
Step 8	Select the **Role** for the VA from the drop-down list.
Step 9	Click **Apply**.

Access Requests Tab

When you select the **Access Requests tab**, the Access Request table opens. This table provides pertinent information about access requests such as:

- Who made the request (Requestor)
- The User ID of the Requestor
- The User's email address
- The Account that was requested for access
- The Company
- The Date of the Request
- The Status of the Request (if the status is Pending, clicking **the status** allows a System or Account Administrator to approve or decline the request)
- Who approved the request (Action By) (if status is Pending, this field is empty)

The Search field can be used to search for a specific request or group of requests by any of the parameters in the table (for example, Date of a Request).

Event Log Tab

When you select the **Event Log tab**, the Event Log pane opens. This pane shows the events captured for a particular Local Account—the one selected in the upper righthand corner of the screen. Using search fields within the table, you can organize events according to **Date Range, Event Type** and/or User.

License (Smart Licensing)

The License component contains the link leading to the Smart Licensing section of SSM On-Prem. You can perform the following license management actions while in the Smart Licensing section:

- Alerts tab: View alerts regarding status of licenses and product instances. This tab is also where you can export license information as *.csv files.
- Inventory tab: Create tokens, view license details, create and manage product instances, and view the event log.
- Convert to Smart Licensing: Manage license conversions to smart licensing, view license conversion history, and view the event log for specific license conversions.
- Reports tab: Run reports against your virtual account licenses, license subscriptions, and product instances. You can schedule synchronization schedules from Cisco or pull schedules from devices (PI?)
- Preferences tab: View or enable or disable (default) viewing license transaction details in the Inventory tab.
- Activity tab: Review license transactions.

You can export information pertaining to licenses, product instances, event logs, and user information as .csv files.

Complete these steps to export a license, product instance, event log, or user information as .csv files.

Step	Action
Step 1	In the Navigation pane, select a **virtual account**.
Step 2	On the License, Product Instances, Event Log, or Users page, click the **CSV** icon in the upper right of the screen.
Step 3	Use the **File Save** dialog box to save the file on to your hard drive.

NOTE: The system uses a platform-dependent dialog box to save the file. The dialog box varies slightly from page to page.

Alerts Tab

Smart Software Manager uses alert icons to bring your attention to actions required to effectively manage your smart products and devices. Major alerts are noted in red icons, with the number of major alerts noted. Minor alerts are indicated by yellow icons, with the number of minor alerts noted.

When you click the Alerts link in the Smart Licensing screen, a display opens that provides detailed information on all alerts generated for a specific Local Account plus alerts generated for all Local Virtual Accounts managed under that Local Account.

The Local Account alerts table provides the following information and management options:

Name	Description
Severity (Sev)	The **Sev column** provides an icon that defines each alert listed as either of Major or Minor importance. The default sort on the alerts is to list the alerts in order of Severity, and then Action Due.
Message	Alerts are generated for the following License and Product Instance events: • Insufficient Licenses • Product Instance Failed to Renew • Product Instance Failed to Connect • Updated Smart License Agreement • Synchronization Overdue • SSM On-Prem Unregistered and Removed • Smart Licensing Agreement Pending • Authorization Pending • Upcoming SSM On-Prem Sync Deadline (30 Day) • SSM On-Prem expired and removed (90 Days of no sync) • SSM On-Prem Authorization File Ready • Licenses Expired • Licenses Expiring • Reserved License Expired • Duplicate Licenses • Reserved Licenses Returned to Smart Account • Version Compatibility Note • Awaiting Start Date The message provides a description of what is required to address the alert and can provide a link to License or Product Instance information. Refer to License Information and Viewing Licenses in a Virtual Account.
Source	Provides a link to the **Smart Account** or **Virtual Account** information referenced by the alert.
Action Due	Identifies the time frame in which the alert must be addressed.
Actions	Provides drop down menu options for **Actions** that may be taken to address the alert.

Alert Actions

Various categories of alert messages require that specific actions be taken to manage Local Accounts effectively. The following table provides examples of Alert Actions, the Action that can be taken to address the alert, and the effect that Action has on the Behavior of the Alert message.

Alert	Action	Behavior
Insufficient Licenses: The Virtual Account "<pool>" has a shortage of <license> licenses. <count> license(s) is/are required to return to compliance.	Select **Transfer Licenses** to display the transfer options for the license type, and the licenses in overage (available for transfer) in the Virtual Account pool.	The alert cannot be dismissed. It is automatically dismissed when the licenses are brought back into compliance.
Updated Smart License Agreement: The Cisco Smart Licensing Agreement has been updated and this updated version must be accepted to continue using Smart Licensing.	Select **View/Accept Agreement** to display and accept license agreements.	The alert cannot be manually dismissed. It is automatically dismissed when the agreement is electronically signed.
NOTE: There are three types of Licenses – **Perpetual, Demo**, and **Term** – and each are valid for a different duration. **Perpetual** licenses remain valid in an ongoing, while **Demo** Licenses must be renewed after 60 days, and **Term** Licenses remain valid for specified periods of 1 to 3 years. Licenses are removed from Local Virtual Accounts as they expire.		
Licenses Expired: <count> <license> licenses in the virtual account "<pool>" expired on <date>.	Select **Dismiss** to hide the alert.	Use the **Dismiss** option in the **Actions** column to manually dismiss the alert.
Licenses Expiring: <count> <license> licenses in the virtual account "<pool>" are set to expire in 30 days on <date>.	Select **Remind** Later to hide the alert until the next warning period.	Select the **Remind Later** option to suppress the alert until the next warning period expires after a set number of days (e.g., 90, 60, 30, 14, 7, 3, 2, 1). If a previous warning has not been dismissed, it will be automatically dismissed when a new alert is generated.
Reserved License Expired: a term license in the reservation has expired.	Click the **update the reservation** link to select a different term license from the available surplus or the **dismiss** link to remove the alert.	The alert is dismissed when the Update Reserved Licenses process has been completed and validates the expiration of the selected term license or when you click the **dismiss link**.
Product Instance Failed to Connect: The product instance<instance> in the virtual account "<pool>" has not connected for its renewal period. The product instance may run in a degraded state if it does not connect within the next <days> days. If the product instance is not going to connect, you can remove it to immediately release the licenses it is consuming.	Select **Remove Instance** to remove the Product Instance and get a confirmation of that action. Select **Remind Later** to hide the alert until the next warning period.	Select **Remind Later** to suppress the alert until the next warning period expires after a set number of days (e.g., 90, 60, 30, 14, 7, 3, 2, 1). If a previous warning has not been dismissed, it will be automatically dismissed when a new alert is generated.

Alert	Action	Behavior
Duplicate Licenses: When the same entitlement is present from different subscriptions within the same Virtual Account.	• Either cancel the order in Cisco Commerce Workspace (CCW) and the entitlement will be removed from the Virtual Account OR • Transfer the entitlement to another Virtual Account that should not already have the same entitlement.	The alert is removed when either action is performed.
Reserved Licenses Returned to Smart Account: When a device with a factory-installed reserved license that was originally assigned to a specific Smart Account and/or Virtual Account is directly connected to CSSM Cloud or SSM On-Prem to a different Smart Account and/or Virtual Account, you will receive the following alert. The product instance "<PI Name>", which had licenses reserved, has been moved to another Smart Account. The licenses it was reserving will be returned to the original virtual account "<VA Name>". Licenses reserved: "<Ent 1>", "<Ent 2>".	Click **Dismiss** to remove the alert.	The alert is removed.
Product Instance Failed to Renew: The product instance "<instance>" in the Virtual Account "<pool>" failed to connect during its renewal period and may be running in a degraded state. The licenses it was consuming have been released for use by other product instances.	Select **Remove Instance** to remove a Product Instance, which will generate a message confirming its removal.	Select **Manual** to dismiss the alert.
NOTE: Product Instances are validated for 90 days from the date and time when they are first established. Smart-enabled products register contacts with the Cisco cloud, or their SSM On-Prem service, as the products are used. If a Product Instance does not contact Cisco for 30 days, a Minor Alert is sent to the License Administrator, indicating that there may be disruption of their Internet connection. Another Minor Alert is sent if the Product Instance does not contact Cisco for 60 days following its validation date. After 90 days, a Major Alert is issued. If the Product Instance does not connect with Cisco after that, the Product Instance is de-linked from the licenses used by the product. Those licenses are returned to the company's license Quantity pool to be used for another Product Instance.		

Inventory Tab

General Tab

The **General** tab displays information about the specific Local Virtual Account and the product instance registration tokens that are associated with the Local Virtual Account. From the **General** tab, you can perform the following actions:

- View information about the Local Virtual Account.
- View a list of existing **Product Instance** registration tokens.
- Create new **Product Instance** registration tokens.
- Using the Action drop-down list, you can copy, download, or revoke Product Instance **registration tokens**. Revoked Product Instance registration tokens can be left in the list or removed using the Actions drop-down list.

Viewing Local Virtual Account Information

Complete these steps to view Local Virtual Account information.

List	Action
Step 1	In the Smart Licensing screen, click the **Inventory** tab, and then select a **Local Virtual Account** from the local Virtual Account drop-down list.
Step 2	In the Inventory table, the **General** tab provides a description of the selected Local Virtual Account displayed along with Product Instance Registration Tokens. The **New Token...** button is used to create a registration token (See Creating a Product Instance Registration Token).

Creating Product Instance Registration Tokens

Product Instance Registration Tokens are used to register and consume a product for smart licensing. You must generate a token to register the product and add the product instance to a specified virtual account. When you create a new token, it is added to the **Product Instance Registration Tokens** table of that virtual account in which the product will be registered.

Complete these steps to create a new Product Instance Registration Token.

Step	Action
Step 1	From the Smart Licensing screen, click the Inventory tab, and select an **existing virtual account** from the Virtual Account drop-down list.
Step 2	From the General tab, click **New Token...**.
Step 3	From the Create Registration Token dialog box, fill in the following fields: **Virtual Account Field:** Displays the Local Virtual Account under which the registration token will be created. **Description Field**: (Optional) The description of the registration token. **NOTE**: Specify a description that will help you identify the token **Expire After Field:** The time limit for the token to be active from 1 up to 9999 days. **Max. Number of Uses:** (Optional) Limit number of times a token can be used prior to expiration date.

Step	Action
Step 4	**NOTE**: This field is visible for only those Local Accounts that are permitted to use this functionality. Select the **check box** to turn on the export-controlled functionality for tokens of a product instance you want to be export controlled in this Local Virtual Account. By selecting the checkbox and accepting the terms, you enable the tokens to use the restricted features on your product instances. You can de-select the check box if you do not want to allow the export-controlled functionality to be made available for use with this token. **CAUTION**: Use this option only if you are compliant with the export-controlled functionality. Some export-controlled features are restricted by the United States Department of Commerce. These features are restricted for products registered using this token when you uncheck the check box. The export-controlled functionality is available for only those tokens that comply with the regulations and policies of the United States Department of Commerce. ATTENTION: Any violations are subject to penalties and administrative charges.
Step 5	Select the **check box** to agree to the terms and conditions mentioned in the text box. **NOTE**: Read the conditions carefully before you choose your options.
Step 6	Click **Create Token**.

Viewing Product Instance Registration Tokens

You can view the registration tokens for a Local Virtual Account. These registration tokens can be used to register new product instances in the Local Virtual Account.

Complete these steps to view product instance registration tokens.

Step	Action	
Step 1	From the Smart Licensing screen, click the Inventory tab, and then select an existing virtual **account** from the Local Virtual Accounts dropdown menu.	
Step 2	Click the **General** tab.	
Step 3	In the Product Instance Registration Tokens section, the following details are displayed in this table.	
	Field Name	**Description**
	Tokens field	The token ID that is generated. You can click **the link** to view so that you can copy the entire length of the token string.
	Expiration Date field	The time limit for the token to be active.
	Uses field	The number of uses specified for this token before it expires, if this threshold is reached prior to the expiration date the token will expire. This field can be blank if no value was specified at token creation, this indicates that the token can be used without usage limitation until the expiration date. .
	Description field	The description of the product instance registration token.
	Export Controlled-Functionality field	Specifies if the export-controlled functionality is enabled for the generated token. **NOTE**: Enablement can only happen after the token has been undergone a government regulated vetting process.

Step	Action	
		NOTE: This field can be modified for only for those Local Accounts that are permitted to use this functionality. The export-controlled flag must be set to **Allowed** for the smart account in CSSM Cloud.
	Created By field	The userid of the person who created the token.
	Actions links	Perform **one** of the following actions: • Copy: Copy the token to your clipboard. • Download: Download the token to your local machine in a text file format. • Revoke: Revoke the token. Revoked tokens can no longer be used and will be rejected if an attempt is made to use them. Remove: Remove a revoked token from the Product Instance Registration Token table. The Remove action is only available if the token has first been revoked.

Managing Product Instance Registration Tokens

Step	Action
Step 1	In the Smart Licensing screen, click the **Inventory** tab, and select an existing virtual account from the **Local Virtual Accounts** drop-down list.
Step 2	On the **General** tab, locate the token in the **Product Instance Registration Token** table that you want to manage.
Step 3	In the **Product Instance Registration Token** table, perform one of the following actions (Actions menu): • **Copy**-Click on the token link to copy the token to your clipboard. • **Download**-Download the token to your local machine in a text file format and will be rejected if an attempt is made to use it. · • **Revoke**-Revoke the token. Revoked tokens can no longer be used. • **Remove**-Remove a revoked token from the Product Instance Registration Token table. The Remove action is only available if the token has first been revoked.

Licenses Tab

The Licenses tab displays information about all the licenses in your Local Virtual Account. From the Licenses tab screen, you can perform the following actions:

- View and Manage
  - All licenses in the Local Virtual Account
  - Detailed license information by checking the Show License Transactions check box

NOTE: To view detailed license information, you must first navigate to the Preferences Tab and set **Show License Transaction Details** in the Inventory Tab to **Enable**. Enabling Show License Transaction Details activates the Show License Transactions check box on the Licenses Tab. Selecting this setting shows the license details for that account.

  - Information about a specific license and which product is using it
  - Information about the transaction history

- Information about the alerts for specific licenses

- Search
  - Search licenses by name or by tag
  - Perform advanced search for licenses using user defined search criteria
- Manage License Tags
  - Edit and Delete in the Manage License Tags tabs
- Available Actions:
  - Transfer Licenses (individual or bulk), Port, and Upgrade Virtual Account
  - Add and remove license tags for licenses in the Available Actions
  - Bulk assign/delete license tags at both the Summary Level and License Transaction Detail Level.

Licenses Table

You can view the Licenses table either from the Summary Level or License Transaction Detail Level. The levels are described here.

NOTE: The **Show License Transactions** checkbox, that can be used to show the License Transaction Detail level, is only visible under the Licenses tab, if it is **enabled** under the Preferences tab.

View	Definition
Summary Level	Viewing the Licenses table at the Summary Level is the default top-level view. Each license at the Summary Level may be comprised of licenses from multiple sources (see License Transaction Detail Level below). This detail can be viewed only at the License Transaction Detail Level.
License Transaction Detail Level	Viewing the Licenses table at the License Transaction Detail Level is done by **checking the Show License Transactions*** check box. Click the plus (+) icon next to the license name to expand the view for each license. The license transaction details vary by source: • Device Migration Product SKU, Product SN, Device Details, Product Family, Quantity Purchased, Expiration Date • DLC Device Migration Product SKU, Product SN, License Family, Quantity Purchased, Expiration Date • PAK Migration PAK #, License SKU, License Family, Quantity Purchased, Expiration Date • EA Migration Transaction ID, Customer Suite Name, License SKU, License Family, Quantity Purchased, Expiration Date • Manual Fulfillment License SKU, License Family, Quantity Purchased, Expiration Date

View	Definition
	• Order PO #, Cisco Order #, Line #, Customer Name, Ship to Country, License SKU, License SKU Family Name, Quantity Purchased, Expiration Date • Device Transfer Product SKU, Product SN, License Family, Quantity Purchased, Expiration Date • Device Request Product SKU, Product SN, License Family, Quantity Purchased.
***All license tags associated to the entitlements in your Local Virtual Account at the License Transaction Detail Level are displayed only if the License Transaction Details drop-down list in the Preferences tab is set to **Enabled** AND the **Show License Transactions** check box is selected in the Licenses tab.	

The **Licenses** table provides the following information for each license you have for a Virtual Account.

Column Heading	Description
License	License identifier (name)
Billing	How the licenses are billed (Prepaid or By Usage)
Available to Use	Number (quantity) of licenses bought, which may include perpetual and/or term. If there are any upgrade pending licenses, they are identified by (+ quantity pending) in parentheses () next to the available quantity. For example, if there are 10 regular entitlements and 5 pending upgrade entitlements in a Local Virtual Account, it would appear as 10 (+5 pending). Please note licenses that are billed by usage do not have a predefined number purchased and this status is indicated by a dash (-) instead of a number. Hover over the dash to see the informational message. **NOTE**: There are three types of Licenses • Perpetual • Demo • Term Each license is valid for a different duration. **Perpetual** licenses remain valid in an ongoing fashion, while **Demo** Licenses must be renewed after 60 days, and **Term** Licenses remain valid for specified periods of 1 to 3 years. Licenses are removed from Local Virtual Accounts as they expire.
In Use	Number of licenses currently in use along with number of licenses reserved (standard or reporting) in parentheses (). Please note the following: The yellow warning icon appears when any reserved licenses are in transition. Hovering over the icon shows the details of why the licenses are in transition. Details are displayed along with the prompt on what to do to resolve the situation so that the licenses are no longer in transition. In-transition licenses will display if a reservation has been updated to reduce the quantity originally reserved. However, when that reservation has been updated to reduce the quantity, the licenses will not be marked as “In transition.” For licenses synchronized from SSM On-Prem, they are consumed and reflected here. If there are no licenses (by usage or prepaid) available in

Column Heading	Description
	the Virtual Account, then an out of compliance alert will appear for that license When a device that requires usage-based entitlements is directly connected to CSSM Cloud, it will not allow the device to consume the by-usage entitlements but instead start consuming in prepaid mode
Balance	Number of licenses that indicates either a surplus (+), shortage (-), or zero (0) Please note licenses that are billed by usage are billed monthly and therefore do not have an outstanding balance. Hover over the dash to read the informational message.
Alerts	Messages alerting the user about actions required (major, minor, informational). Upgrade Pending: Several upgrade licenses have been purchased but will not be available until the licenses being replaced have been identified. Click the Upgrade Pending link which will open a modal to complete the upgrade process. The alert is removed when the license upgrade process is completed.
Actions	Possible options available: • Transfer a number of licenses to/from another Local Virtual Account • Upgrade licenses

License Details

From the Inventory screen, select the **License** tab. A dialog opens to display a list of licenses for that Local Virtual Account. Click the **License** link to view the license details pop-up window that contains the following information:

- the **Overview** tab displays the Local Virtual Account usage pie chart, and the License Types table (that specifies license count, license type, start date, expiration date, and subscription ID),
- the **Product Instances** tab provides information on product instances, product type, and licenses used,
- the **Transaction History** tab displays license order history that includes transaction date, license SKU, quantity, expiration date, and order (line) number.

NOTE: Licenses that are duplicates or are pending upgrade are not included in these license count quantities.

Available Actions

The Available Actions tab is located on the Licenses table. It is activated when you select a license (checkbox). Once activated, you can perform the following operations:

- Add License Tags to a license.
- Remove License Tags from a license.

- Transfer a license to/from one account to another. (See Transferring Licenses)

Complete these steps to add a license tag to one or more licenses.

Step	Action
Step 1	In Smart Licensing, click the **Inventory** tab. **NOTE**: You can also search Local Virtual Accounts **By Name** or **By Tag** by entering the first few letters in the Search field to limit the number of available Local Virtual Accounts that are displayed.
Step 2	Click the **Licenses** tab, and then select the **Local Virtual Account** you want from the Virtual Account drop-down list.
Step 3	Summary Level a. In the Licenses table, check the **checkbox(es)** to select one or more licenses. b. Click **Available Actions** above the table. **NOTE**: Available Actions option is only enabled when checkbox(es) is/are checked. c. Select **Add License Tags**. d. Enter a **tag name**, click The Add License pop-up window opens **Enter**. The tag is listed in the window. **NOTE**: For multiple tags, repeat **step d**. e. Click **Save**. You are prompted that the tag is going to be created, do you want it created. You are notified that the tag was successfully created. f. Click **OK**. The tags are added to the license. Transaction Detail Level a. Above the Licenses table, check the **Show License Transactions*** check box and in the Licenses table. b. Click the **plus** [+] icon to choose the **individual lines** of each license transaction. c. Check the **checkbox(es)** to select one or more licenses. d. Click **Available Actions** above the table. e. Select **Add License Tags**.
Step 4	In the Add Tags to the Selected Licenses dialog, type in each **tags name.** Terminate the tag name with either a comma or the Enter key. **NOTE**: Since the comma is used as a terminator, it cannot be used in a tag name. In addition, duplicate tag names cannot be created, but tag names are case-sensitive, so aaa and AAA are recognized by the system as different tag names. Click **Save** and then click **OK.**
*****All license tags associated to the entitlements in your Local Virtual Account at the License Transaction Detail Level are displayed only if the License Transaction Details drop-down menu in the Preferences tab is set to Enable AND the Show License Transactions check box in the Licenses tab is checked.	

The Remove License Tags option allows you to remove a license tag(s) from specific licenses within an account.

NOTE: When you delete a tag, you delete the tags from the entire account.

Complete these steps to remove a license tag.

Step	Action
Step 1	In Smart Licensing work section, select **Inventory >** select a **Local Virtual Account** from the Virtual Account drop-down list. You can search Local Virtual Accounts **By Name** or **By Tag** by entering the first few letters in the Search field to limit the number of available Local Virtual Accounts that are displayed.
Step 2	Click the **Licenses** tab.
Step 3	Summary Level a. In the Licenses table, to select one or more licenses, select the **checkbox(es)**. b. Click **Available Actions** above the table. c. Select **Remove License Tags**. The Remove Tags from the Selected Licenses pop-up window opens d. Click the **x** on every tag you want removed. The tags are listed at the bottom of the window. e. Click **Remove**. You are prompted if you want to remove the tags. f. Click **OK**. You are notified that the tags have been successfully removed from the selected license. License Transaction Detail Level a. Above the Licenses table, check the **Show License Transactions*** check box and in the Licenses table, b. Click the **plus** [+] icon to choose the **individual lines** of each license transaction. c. Check the **checkbox(es)** to select one or more licenses. d. Click **Available Actions** above the table e. Select **Remove License Tags**.
Step 4	In the **Remove Tags from Selected Licenses** window, currently assigned tags are shown. Click the **x** to remove the tag(s) from selected licenses. Review the Tags selected for removal and then click **Save** to remove the selected tag(s) from the licenses.
***All license tags associated to the entitlements in your Virtual Account at the License Transaction Detail Level are displayed only if the License Transaction Details drop-down menu in the Preferences tab is set to Enabled AND the Show License Transactions check box in the Licenses tab is checked.	

Viewing Licenses in a Local Virtual Account

From the Licenses table, you can select a Local Virtual Account from the drop-down list. Click the **Licenses tab** to display the Licenses table.

Complete these steps to view licenses in a Local Virtual Account.

Step	Action
Step 1	In the **Smart Licensing** screen, select the **Inventory** tab, and then select an **existing Local Virtual Account** from the **Local Virtual Accounts** drop-down list. You can search Local Virtual Accounts **By Name** or **By Tag** by entering the first few letters in the **Search** field to limit the number of available Local Virtual Accounts that are displayed.
Step 2	Click the **Licenses** tab to display all the licenses in your **local Virtual Accounts**.

Step 3	(Optional) You can also export the license list to a **.csv file** from this pane. (File Icon).
Step 4	Click the **license name** to see detailed information about a license. The system displays the License Detailed Information dialog box. This dialog box has four tabs: Overview, Product Instances, Event Log, and Transaction History.

NOTE: Searching **By Tag** is only enabled if tags have been previously associated with Local Virtual Accounts or licenses.

Changing a Local Virtual Account Assignment

Duplicate licenses can either be moved or copied to a different Virtual Account(s). These licenses become active if the local Virtual Account(s) selected do not already contain the transferred licenses.

Complete these steps to change a Local Virtual Account assignment.

Step	Action
Step 1	Identify the duplicate license to be moved or copied. Click **Actions** and then select **Change Virtual Account Assignment**.
Step 2	Select the license **Subscription** to be transferred from the Subscription ID drop-down list. **NOTE**: The Subscription IDs that correspond to the **active entitlement** are marked as **Enabled**. The Subscription IDs that correspond to **duplicate entitlements** are marked as **Disabled**.
Step 3	Select the **Local Virtual Account**(s) from the available list to move or copy the license. The Local Virtual Account(s) that are checked mean the license is already there. To move the license, uncheck the local Virtual Accounts that currently have the license and select the other Local Virtual Accounts. To copy the license, leave the local Virtual Accounts that are checked as-is and select other Local Virtual Accounts to copy the license to. Click **Check All** if the license is to be copied to all available Local Virtual Accounts. **NOTE**: The **Duplicate Licenses** alert appears when either • The selected Local Virtual Account(s) has duplicate licenses or • The Local Virtual Account(s) will have duplicate licenses once the license has been copied or moved Click **OK**. The license is copied or moved to the selected Local Virtual Account(s).

Transferring Licenses between Local Virtual Accounts

This procedure can be conducted at either the Licenses pane (summary level) or at a detailed level (License Transaction Detail pop-up screen).

NOTE: Once an entitlement has been reserved, it cannot be transferred between Local Virtual Accounts.
Once a reserved term license has expired, the available quantity is reduced due to licenses being used to fulfill the expired reservation.

NOTE: License tags and their association with licenses are not transferred between Local Virtual Accounts.

Complete the following steps to transfer between Local Virtual Accounts at the summary level.

Step	Action	
Step 1	In **Smart Licensing** work section, select **Inventory >** then select the **virtual account** you want from the Local Virtual Accounts drop-down list.	
Step 2	Click the **Licenses** tab. The Licenses table opens.	
Step 3	If the **License Transaction Details** drop-down menu in the **Preferences** tab is set to **Disabled** OR the **Show License Transactions** check box in the Licenses tab is unchecked, check the **checkbox(es)** to choose **one or more licenses**. If the **License Transaction Details** drop-down menu in the **Preferences** tab is set to **Enabled** AND the **Show License Transactions** check box in the Licenses tab is checked, then click the ⊗ symbol for each desired license you want to transfer and then check the associated checkbox. Click **Available Actions** tab and select **Transfer...**.	
Step 4	In the Transfer Between Local Virtual Accounts screen, complete the information in the following fields:	
	Name	**Description**
	Transfer To/From drop-down menu next to the Transfer To/From drop-down menu	Choose one of the following: • **Transfer To**-Licenses are transferred from the current virtual account to the selected virtual account. • **Transfer From**-Licenses are transferred from the selected virtual account to the current virtual account.
	Virtual Account drop-down menu	Choose a **Local Virtual Account** to transfer the license(s) to/from.
	License	Shows the name of the license, the Local Virtual Account that it belongs to, and the number of licenses that are currently available.
	Billing	Shows how the licenses are billed (Prepaid or By Usage).
	Purchased	Shows the number (quantity) of licenses purchased, which may include **Perpetual** and/or **Term**. **NOTE:** Licenses billed by usage do not have a predefined number purchased and is indicated by a dash (-) instead of a number. Hover over the dash to see the informational message. **NOTE**: There are three types of Licenses: • Perpetual

Step	Action	
		• Demo • Term Each are valid for a different duration. **Perpetual** licenses remain valid in an ongoing, while **Demo** Licenses must be renewed after 60 days, and **Term** Licenses remain valid for specified periods of 1 to 3 years. Licenses are removed from Local Virtual Accounts as they expire.
	In Use	Shows the number of licenses currently in use, along with number of licenses reserved shown with the keyword **Reserved**.
	Balance	Shows the number of licenses available for transfer between Local Virtual Accounts.
	Transfer	Enter the number of licenses you want to transfer. This input field is enabled after you select a Local Virtual Account to transfer to/from.
Step 5	Click **Transfer** to transfer the licenses or click **Show Preview** to view a summary of the changes to be made. To exit the **Show Preview** screen, click **Hide Preview**. You can click **Cancel** if you wish to not go through with the license transfer.	

License Advanced Search

The Advanced Search feature allows you to filter using additional criteria, for example by product family, Expires By, PAK, and/or SKU.

NOTE: Advanced search is only available if the License Transaction Details drop-down menu in the **Preferences** tab is set to **Enabled** AND the Show License Transactions check box in the **Licenses** tab is **checked**. Refer to the Preferences tab for more details.

Complete these steps to run an advanced search.

Step	Action			
Step 1	In **Smart Licensing**, select **Inventory >** then select the Local Virtual Account you want from the **Local Virtual Accounts** drop-down list. You can search Local Virtual Accounts **By Name** or **By Tag** by entering the first few letters in the **Search** field to limit the number of available local Virtual Accounts that are displayed.			
Step 2	Next, click the **Licenses** tab.			
Step 3	Check the **Show License Transactions** check box and click the **Advanced Search** down arrow located at the right side of the pane.			
Step 4	Enter one or more of the following search field parameters and click **Apply**:			
	Search Field	**Search Criteria**	**Type of Search**	**Type Ahead**
	PAK	PAK #	Exact Match	Yes
	Product Family	License Product Family	Contains	

Step	Action			
	SKU	License or Product SKU	Contains	
	Expires By	Date Picker on "Term End Date"	Any license that has an expiration date on or before the selected	
Step 5	Click **Clear** to remove all search criteria and redisplay all unfiltered licenses.			

Search Licenses by Name or by Tag

In situations where you have a large number of licenses in an account, you can search for specific licenses or groups of licenses using the Search field. You can search for licenses by either Name or Tag. Each procedure is described below.

Complete these steps to search a license by name:

Step	Action
Step 1	In Smart Licensing, select the **Inventory** tab
Step 2	Click the **Licenses** tab.
Step 3	In the Licenses table, click **By Name** above the Search field.
Step 4	Click inside the **Search** field and type the first few letters of a license name. A list of all matching entitlements within your Virtual Account is displayed. Choose the license from the list. To remove the selected license name, click **x** in the search text box.

Complete these steps to search a license by tag:

Step	Action
Step 1	In Smart Licensing, select **Inventory** from the menu and then select **an existing Local Virtual Account** from the Virtual Account drop-down list. You can search Local Virtual Accounts by Tag by **entering the first few letters** in the Search field to limit the number of available Local Virtual Accounts that are displayed.
Step 2	Click the **Licenses** tab.
Step 3	Click **By Tag** above the Search field.
Step 4	Click **inside the Search field**. A list of license tags available within the Local Virtual Account is displayed. Enter the **first few letters** of a tag to filter the list. **NOTE**: All license tags associated to the entitlements in your Local Virtual Account at the License Transaction Detail Level are displayed only if the License Transaction Details drop-down menu in the Preferences tab is set to Enable AND the Show License Transactions check box in the Licenses tab is checked.
Step 5	Choose **one** or **more** tags. Only the entitlements associated to the selected tags are displayed. To remove selected license tags, click **x** against each tag.

Manage License Tags

License Tags are useful for classifying, locating, and grouping licenses.

Actions such as: adding, editing, and deleting license tags from the Inventory listed in the Smart Licensing can be accomplished using the Licenses tab.

Whereas the Available Actions tab allows you to Add or Remove License Tags, the Manage License Tags tab allows you to modify or delete your existing tags across your Local Virtual

Account. The License table lists the number of licenses and license transaction details that are associated with each tag.

When you modify or delete a license tag(s) in a Local Virtual Account, you modify ALL the licenses in that account. You cannot modify a single license. If you want to work with a specific license, you must use the **Available Actions** tab.

Complete these steps to modify or delete the license tags in a Local Virtual Account.

Step	Action
Step 1	In Smart Licensing, click the **Inventory** tab.
Step 2	Click the **Licenses** tab, and then select the **Local Virtual Account** you want from Local Virtual Account drop-down list. **NOTE**: You can also search Local Virtual Accounts **By Name** or **By Tag** by entering the first few letters in the Search field to limit the number of available Local Virtual Account that are displayed.
Step 3	Click **Manage License Tag...** tab. The Manage Tags pop-up window opens. From here you can edit or delete a tag(s). **NOTE**: If you modify or a delete a tag(s). ALL the tags associated with the account are modified or deleted.

Licensing Events

The table below provides an overview of licensing events. Users receive the following event messages, referencing the number of Licenses and Local Virtual Accounts, when licensing events occur in their Local Account.

Event	Message
New Licenses	<n> new <license-name> licenses were added to the Virtual Account "<va-name>"
Licenses Transferred	<n> <license-name> licenses were transferred from the Virtual Account "<from-va-name>" to the Virtual Account "<to-va-name>"
Licenses Expired	<n> "<license-name>" licenses expired and were removed from the Virtual Account "<va-name>"
Licenses Removed	<n> "<license-name>" licenses were removed from the Virtual Account "<va-name>"
Insufficient Licenses Detected	The Virtual Account "<va-name>" reported a shortage of <n> <license-name> licenses
Licenses Reserved	"The following licenses were reserved on product instance "XXXX" in Local Virtual Account "XXXX": <Quantity> "Ent 1" License(s) (<Quantity> expiring DD-MMM-YYYY, <Quantity> expiring DD-MMM-YYYY); <Quantity> "Ent 2" License(s) (<Quantity> expiring DD-MMM-YYYY, <Quantity> expiring DD-MMM-YYYY) and <Quantity> "Ent 3" license(s) (<Quantity> perpetual)."
License Upgrade	<n> new "<license-name>" term/perpetual licenses were added to the Virtual Account "<va-name>". These licenses will become available when the upgrade is completed by identifying the licenses to be replaced by the upgrade licenses.

Product Instances Tab

The Product Instances tab displays information about all the product instances in your Local Virtual Account. From the Product Instances tab, you can perform the following actions:

- View a list of all Product Instances.
- View information about specific Product Instances and what licenses it consumes.
- View information about the alerts for a specific Product Instance.
- Transfer a specific Product Instance(s) between Local Virtual Accounts.

NOTE: From CSSM Cloud, you cannot transfer or remove Product Instances from Local Virtual Accounts associated with an SSM On-Prem Account.

- Remove a specific Product Instance from the local Virtual Account which subsequently removes it from the Local Account.
- Export a list of Product Instances to a .csv file. (Export Icon)

Viewing Product Instances in a Local Virtual Account

Selecting a Local Virtual Account from the Inventory tab displays a Product Instances tab for that selected Local Virtual Account. Click the **Product Instances** tab to display the Product Instances table.

Complete these steps to view local Product Instances in a Local Virtual Account.

Step	Action
Step 1	In the Smart Licensing section, click the **Inventory** tab.
Step 2	From the **Inventory** screen, click the **Product Instances** tab.
Step 3	(Optional) You can export the list of product instances to a .csv file.
Step 4	**Click the Product Instance name to see detailed information about a product instance.** **NOTE**: A cluster setup icon by the right side of the product instance indicates a high availability of routers for that specific product instance. The system displays the Product Instance Details dialog box. This dialog box has two tabs: • Overview • Event Log.

Product Instances Table

The Product Instances table provides the following information for each product you have associated with a Local Virtual Account.

Column Heading	Description
Name	Product ID plus Product Instance name
Product Type	Lists the category of the Product Instance utilized.
Last Contact	Date the Product Instance was last contacted
Alerts	Messages alerting the user to actions required to maintain products
Actions	Option for removing a Product Instance, or transferring a Product Instance to another Local Virtual Account

Product Instance Details

Click on a Product Instance (Device) listed in the Product Instance table to display detailed information on that Virtual Account product. The information is organized under the following tabs.

Name	Description
Overview	In the **Description** section a product description is provided. In the **General** section, the following product instance details are displayed: • Name • Product • Host Identifier • MAC Address • PID • Serial Number • UUID • Local Virtual Account • Registration Date • Last Contact • Expiry Date The **License Usage** section displays the licenses in use and the number of each that are required. • The License Name. (NOTE: If there are no licenses available in the Local Virtual Account, then an Out of Compliance alert is generated for the license.) • When a device that requires usage-based entitlements is directly connected to CSSM Cloud, it will not allow the device to consume the by-usage entitlements but instead start consuming in prepaid mode • Expiration Date for term licenses • Never column lists Perpetual Licenses • Multiple terms link lists the combination of perpetual and term licenses or terms with different expiration dates • The Quantity of licenses reserved
High Availability	This tab lists the Product Instances that are utilized in a cluster. The information listed is: • Name • PID (Product ID) • Serial Number
Event Log	In the Event Tab, you can view the: • Times the event occurred • Event Type (See Product Instance Event Types) • Event: Shows product instance ID ○ Upward Arrow in blue box: Message that accompany the Event • The user who generated the message. (Either the account owner's CCO ID or "Cisco Support")

Product Instance Event Types

The table below provides an overview of **Product Instance** events. Users receive the following event messages, referencing the number () of Product Instances () and Local Virtual Accounts (), when product instance events occur in their Local Account.

Event	Message
New Product Instance	The product instance <instance-name> connected and was added to the Virtual Account "<va-name>".

Event	Message
New Product Instance (with redundancy)	The product instance <instance-name> was added to the Virtual Account "<va-name>" and configured for redundancy with the following Standbys: “<sb1-displayname>”, “<sb2-displayname>”.
Product Instance Transferred	The product instance <instance-name> was transferred from the Virtual Account "<from-va-name>" to the Virtual Account "<to-va-name>".
Product Instance Removed	The product instance "<instance-name>" was removed from Smart Software Manager.
Product Instance Requested License	The product instance <instance-name> in the Virtual Account "<va-name>" requested <n> "<license-name1>".
Product Instance Renewed Certificate	The product instance <instance-name> in the Virtual Account "<va-name>" connected and successfully renewed its identity certificate.
Product Instance Connected (with redundancy)	The product instance <instance-name> in the Virtual Account "<va-name>" connected and was configured for redundancy with the following Standbys: “<sb1-displayname>”, “<sb2-displayname>”.
Failure to Connect Detected	The product instance <instance-name> in the Virtual Account "<va-name>" failed to connect for its renewal period.
Product Instance Added via SSM On-Prem	The product instance <instance-name> was added to the Virtual Account "<va-name>" via synchronization with the SSM On-Prem "<SSM On-Prem-name>".
Product Instance Requested License via SSM On-Prem	The product instance <instance-name> in the Virtual Account "<va-name>" requested <n> "<license-name1>" via synchronization with the SSM On-Prem "<SSM On-Prem-name>".
Product Instance Removed via SSM On-Prem	The product instance <instance-name> was removed from the Virtual Account "<va-name>" via synchronization with the SSM On-Prem "<SSM On-Prem-name>".
Product Instance Detached	The product instance <instance-name> in the Virtual Account "<va-name>" was put in detached mode.
Product Instance Reattached	The product instance <instance-name> in the Virtual Account "<va-name>" was taken out of detached mode.
Product Instance Failed to Detach	The product instance <instance-name> in the Virtual Account "<va-name>" failed to go into detached mode.
Product Instance Failed to Re-attach	The product instance <instance-name> in the Virtual Account "<va-name>" failed to be taken out of detached mode.

Transferring a Product Instance

CAUTION Transferring a Product Instance from one Local Virtual Account to another Local Virtual Account does not result in the corresponding licenses being transferred. You will have to transfer the licenses separately.

NOTE: From CSSM Cloud, you cannot transfer or remove Product Instances from Local Virtual Accounts associated with a SSM On-Prem Account.
When transferring a Product Instance between Local Virtual Accounts, all the reserved licenses for that Product Instance will move to the destination Local Virtual Account.

Complete these steps to transfer a Product Instance.

Step	Action	
Step 1	In the Smart Licensing, click the **link to a Local Virtual Account**.	
Step 2	Select the **Inventory tab,** and then click the **Product Instances** tab.	
Step 3	In the Product Instances table, locate the **Product Instance** that you want to transfer.	
Step 4	In the Actions column, select **Actions > Transfer...** for the Product Instance you want to transfer.	
Step 5	In the Transfer Product Instance dialog box, enter the required information for this field:	
	Name	**Description**
	Transfer To drop-down list	Choose the virtual account that you want to transfer the Product Instance to.
Step 6	Click **Transfer** the Product Instance. **NOTE**: If you are using SL Using Policy, see Collect Usage for managing Usage Reports.	

NOTE: You can also access the Transfer Product Instance dialog box, by clicking on the Product Instance name and clicking **Transfer...** from the Product Instance details dialog.

Removing a Product Instance

When you remove a product instance from SSM On-Prem, you are disassociating it from its licenses and deregistering it from SSM-On-Prem. The licenses that the product instance was using are still available and can be used by other products. Following removal, if you wish to use this product with SSM On-Prem and associate it with licenses, you must re-register the product instance with SSM On-Prem and re-synchronize so that CSSM and SSM-On-Prem can communicate with the product again. Note that it is not necessary to resynchronize, since this will automatically happen on the default synchronization schedule, every 30 days, but if you wish CSSM to become aware of this product instance immediately, it is necessary to invoke synchronization (see Synchronization Widget).

Complete these steps to remove a Product Instance

Step	Action
Step 1	In the Smart Licensing, click **Inventory tab** and then select the Local Virtual Account that you need from the pull-down list.
Step 2	Still in the Inventory table, click the **Product Instances** tab.

Step 3	In the Product Instances table, **locate the product instance** that you want to remove.
Step 4	In the Actions column, click the **Remove** link for the product instance that you want to remove.
Step 5	In the Confirm Remove Product Instance dialog box, click **Remove Product Instance**.

SL Using Policy Tab

(Added for On-Prem 202102)

The SL Using Policy tab represents the On-Prem interface for managing Product Instances. Listed here are the functional capabilities utilized in this tab.

The functional buttons enable you to perform the following tasks:

- **Add Single Product**: This button opens the **Add Product** screen so that you can add a single device.

NOTE: There are multiple ways devices can be added to On-Prem CSSM. If a customer is connected to CSSM Cloud), they need to configure the **Tenant URL** available by selecting the **Default Virtual Account > General Tab** and clicking the **CSLU Transport URL** link. Usage reports can then be sent from that device(s) without any trust establishment or registration. (See Validating Devices.)

- **Actions for Selected...**: This button provides a list of menu options for the following:
  - **Remove** selected Product Instance(s) from a Local Virtual Account.
  - **Edit** one or more parameters for selected Product Instance(s).
  - **Collect Usage** from selected Product Instances on any selected Product Instance.
  - **Request authorization codes** by downloading an authorization request file for the selected Product Instance(s). This option is used when you are obtaining information from devices that need an authorization code as an extra security measure.
  - **Export a list of Product Instances** to a .csv file. This is a means of manually exporting usage information from multiple devices to CSSM Cloud. This feature is especially useful when you are working with many devices and reports.
- **Export/Import All...**: This button allows you to perform the following operations:
  - **Export All Product Instances List**: This menu option globally downloads a full Product Instance list as a `*.csv` file. The `*.csv` file can then be used for obtaining reports for managing Product Instances.
  - **Import Product Instances List**: When On-Prem is connected to CSSM Cloud this menu option globally uploads Product Instances to On-Prem using the Import Product Instance List feature. The information is uploaded in the `*.csv` format and all validated Product Instances are added to the device list.
  - **Export Usage To Cisco**: This option is a manual process used when not connected to CSSM Cloud (offline mode).

- **Import Usage From Cisco**: This menu option provides a manual process used to import usage report, acknowledgement, and other information to On-Prem.

- **SL Using Policy Table**: This table provides these informational columns:
  - **Product Instance Name**: Shows the Host name or IP Address of the Product Instance (this field can be filtered).

NOTE: For SLP device having Smart Agent version less than 5.5 then UID details will be displayed in the name field, if UID details are not available then IP address will be displayed. For SLP devices having Smart Agent version greater than or equal to 5.5 only Host name will be displayed.
For SLP device having Smart Agent version greater than or equal to 5.5 the host name cannot be created by using any special characters and spaces.

  - **Product Type**: The category of product that is listed.
  - **Last Contact**: Shows the date that there was communication with the Product Instance.
  - **Alerts**: Provides latest status of this Product Instance, for example: Successful, Downloaded, Failed to Connect. (See Appendix 7 for full list of alerts.)

- **Search Field**: Located on the right side of the screen above the Policy Actions table is a search field where you can search by: Name or Product Type.

NOTE: From CSSM Cloud, you cannot transfer or remove Product Instances from Local Virtual Accounts associated with an SSM On-Prem Account.

Adding a Single Product

Using the SL Using Policy tab, you can manually add a single product.

NOTE: For the complete procedure of adding a device and obtaining usage data, see obtaining usage information directly from devices (pull mode), or obtaining usage information from CSSM Cloud (push mode).

Complete these steps to add a Single Product.

Step	Action
Step 1	Return to SL Using Policy tab, click **Add Single Product**.
Step 2	From the Add Product column, enter the **Host** (IP Address of the Host) and select the **Connect Method**.
Step 3	In the right panel, click **Product Instance Login Credentials**. The left panel of the screen changes to show the User Name and Password fields.
Step 4	Enter the Product **User Name** and **Password**.
Step 5	Click **Save**. The information is saved to the system and the device is listed in the Product Instances with the Last Contact listed with the date. You can now collect usage (RUM) reports directly from the Product Instance when not connected to CSSM Cloud.

Remove a Device (Product Instance)

In On-Prem, you can remove one or multiple Product Instance (PIs) from your system using the **Actions for Selected** button.

Step	Action
Step 1	From the Inventory tab, select **one** or **more devices**.
Step 2	From the SL Using Policy screen, select **Actions for Selected... > Remove.** **NOTE**: If the device is removed or upgraded, the data associated with the device (for example reports) will not be removed.

Editing a Device (Product Instance)

CSLU allows you to edit a Product Instance (PI) in your system from the Available Actions menu.

Complete these steps to edit a Product Instance (bulk operations).

Step	Action
Step 1	Select **one** or **more Product Instances**. **NOTE**: If you select multiple devices, you can only modify the **User Name**, **Password**, and **Connect Method**. The Host, and all UDI fields can only be modified one Product Instance at a time. The Host Name and Product Version are not editable.
Step 2	From the SL Using Policy screen, select **Actions for Selected > Edit**.
Step 3	Log into the **device**. Using the **User Name** and **Password**.
Step 4	(Required) Modify the **appropriate fields** (see note in Step 1). **NOTE**: You can also modify the general parameters such as: • Host Identifier • MAC Address • SUVI • PID • Serial Number • VID • UUID
Step 5	Click **Save**. The modifications are listed in the Product Instances.

NOTE: You can also modify a single device by clicking on the **Product Instance Name** in the Product Instances table. From On-Prem 202206 Host name are added to the product Instance details.

Collect Usage

On-Prem also allows you to manually trigger the gathering of usage reports from devices without being connected to CSSM Cloud.

NOTE: By default, On-Prem is scheduled to collect usage information at 5-minute intervals.

After configuring and selecting a Product Instance (selecting **Add Single Product Instance**, filling in the **Host** name and selecting the appropriate connect method), then select **Actions for Selected > Collect Usage**. On-Prem connects to the selected Product Instance(s) and collects

the usage reports. These usage reports are then stored in On-Prem's local library. These reports can then be transferred to Cisco if On-Prem is connected to Cisco, or (if you are not connected to Cisco) you can manually trigger usage collection by selecting **Export/Import All.. > Export Usage to Cisco**.

Complete these steps to collect Product Instance usage reports.

Step	Action
Step 1	Select the SL Using Policy tab and select **one** or **more Product Instances**.
Step 2	From the SL Using Policy main screen, select **Actions for Selected > Collect Usage**. RUM reports are retrieved from each selected device and stored in the On-Prem local library. The Last Contacted column is updated to show the time the report was received, and the Alerts column shows the status. **NOTE**: If On-Prem is currently logged into Cisco the reports will be automatically sent to the associated Smart Account and Virtual Account in Cisco and Cisco will send an acknowledgement to On-Prem as well as to the Product Instance. The acknowledgement will be listed in the alerts column of the Product Instance table. **NOTE**: To manually transfer Usage Reports to Cisco, select **Export Usage to Cisco** from the Product Instances Menu. (For detailed steps, see Export Usage Data from Cisco Cloud.
Step 3	From the Export Usage to Cisco modal, select the **local directory** where the reports are stored. At this point, the usage reports are saved in your local directory (library). To export these usage reports to Cisco, Follow the steps described in Export Usage Reports to Cisco.

NOTE: The Windows operating system can change the behavior of a usage report file properties by dropping the extension when that file is re-named. The behavior change happens when you re-name the downloaded file and the re-named file **drops the extension**. For example, the downloaded default file named **UD_xxx.tar** is re-named to **UD_yyy**. The file loses its TAR extension and cannot function. To enable the usage file to function normally, after re-naming a usage report file, you must also **add the TAR** extension back to the file name, for example **UD_yyy.tar**.

Importing Usage Data from Cisco Cloud

Step 1	Click **Import from Cisco** and then wait for the acknowledgement file to be generated.
Step 2	Log into CSSM Cloud and navigate to **Reports > Usage Data Files**. The Acknowledgement (*.tar) file is listed in the table with a **Download** status showing for the Product Instance (Acknowledgement column.)
Step 3	Select the Product Instance record and click **Download**.
Step 4	To import the file back to On-Prem, return to **device list** in On-Prem, select the device, and from the Export/Import All tab, select **Import from Cisco**.
Step 5	The Import From Cisco pop-up opens where you can either **browse** for the file (in the download directory) or **drag & drop** the file from the library list.

	NOTE: If you use browse, select the file, and click **Open**. The file will be imported and a "successfully imported data" notice opens at the bottom of the screen which means that you have successfully obtained usage data from CSSM Cloud.

Exporting Usage Data to CSSM Cloud

Step 1	Navigate to the On-Prem UI and navigate to **SL Using Policy** tab to begin the export process from On-Prem to CSSM Cloud. a. Select a **device(s) (PI)** from the list. b. Select **Export/Import All > Export Usage to Cisco**. c. A pop-up window opens to list the ack file (***.tar**) that has been generated. d. Click **OK** to save the file. Now the ack file is ready to export to Cisco.
Step 2	To export, log into **CSSM Cloud** and navigate to **Smart Software Licensing > Reports > Usage Data File** tab. **NOTE**: The Usage Data Files are listed in the Reporting Status column and also in the Acknowledgement column as **download**.
Step 3	To download the ack file (*.tar), click on the **download link** in the Acknowledgement column. The file is downloaded to On-Prem and is listed in the download directory.
Step 4	To import the file back to On-Prem, return to **device list** in On-Prem, select the device, and from the Export/Import All tab, select **Import from Cisco**.
Step 5	The Import From Cisco pop-up opens where you can either **browse** for the file (in the download directory) or **drag & drop** the file from the library list. **NOTE**: If you use browse, select the file, and then click **Open**. The file will be imported and a "successfully imported data" notice opens at the bottom of the screen which means that you have successfully obtained usage data from CSSM Cloud.

Authorization Code Request

The Authorization Code Request menu option is specifically used to manually request authorization codes from Cisco. This option can be used for one or more selected Product Instances.

Complete these steps if you are not connected to Cisco to request authorization codes from Cisco.

Step	Action
Step 1	From the SL Using Policy table, select the **Devices** for authorization code request.
Step 2	With one or more Devices selected, select the **Authorization Code Request** option from the Actions for Selected... menu.
Step 3	In the modal that describes the steps to take, click **Accept**. The upload modal opens to select a *.CSV file for uploading. (local)
Step 4	Next, follow these steps. a. Upload the file to Cisco by following this directory path: **software.cisco.com > Smart Software Licensing > Inventory > Product Instances > Authorize License Enforced Features**.

Step	Action
	b. Follow the steps shown on the wizard to select licenses and then download the authorization codes to SL Using Policy in On-Prem. c. **NOTE**: You will need the Host Name (IP Address), UDI, and Serial Number.
Step 5	You then can apply the authorization codes by clicking **Import From Cisco**. (For uploading procedure, go to Import From Cisco). If SL Using Policy is In Product-Initiated mode: The imported codes are now applied to the Product Instances the next time the Product Instance contacts On-Prem. • If SL Using Policy is in another initiated mode: The uploaded codes are now applied to the Devices the next time the On-Prem runs an update.

Event Log Tab

The Event Log tab displays information for all the events in a Local Virtual Account. Events are actions that you have taken using CSSM Cloud such as Specific License Reservations, adding and removing licenses and products, adding, and renaming Local Virtual Accounts, and so on. From the Event Log tab, you can do the following:

- View a detailed list of all events in the selected Local Virtual Account.
- Export the list as a .csv file.

***** The following Specific License Reservation events are displayed in the Event Log:

Event Description
When a license is reserved.
When a product instance is present where reserved licenses are transferred between Local Virtual Accounts.
Anytime a user enters the confirmation code to update (increase/decrease) the quantity of licenses reserved.

NOTE: To view information on all the events at the Local Account level, including events for all Local Virtual Accounts associated with your Local Account, use the Activity link on the Smart Licensing screen, and then click on the Event Log tab in the Activity screen. To view information on the licensing events specific to a Local Virtual Account, use the Inventory link on the Smart Licensing screen, select a Local Virtual Account from the drop-down list, and then click on the Event Log tab to display event messages for that Local Virtual Account.

Convert to Smart Licensing Tab

Smart licensing enables you to say goodbye to product activation keys (PAKs). As you upgrade from a version of a product using Traditional Licensing to a version using Smart Licensing, the device or product instance will need to have Entitlements to Smart Licenses available in a CSSM Cloud Smart Account. There are three ways to make entitlements available:

- Order Smart enabled SKUs that deliver Smart License Entitlements (licenses) to a CSSM Cloud Smart Account.
- Migrate existing Traditional Licensing using the License Registration Portal (LRP) or Smart Software Manager workspace at software.cisco.com.
- The device can initiate the conversion.

In some cases, conversion of a license is not possible within the CSSM Cloud Licensing workspace and must have the conversion initiated by the device (product instance). Examples would be Right to User (RTU) licenses, Paper Licenses, or PAK files which are not listed in LRP or CSSM Cloud workspaces. To accommodate these license types, you can migrate from Traditional Licensing to Smart Licensing via SSM On-Prem and Device Led Conversion (DLC).

DLC allows the device/product instance to initiate the conversion of Traditional Licensing to Smart Licensing Licenses so that the entitlement can be reflected in CSSM Cloud. Products must be upgraded to a DLC-enabled version of software, connected directly to CSSM Cloud, or SSM On-Prem for this conversion to work.

DLC can only convert Traditional Licensing once if successful. That is, once a license has been converted and deposited in the Virtual Account (where the device registers) as a Smart-enabled license, CSSM Cloud will invalidate the corresponding Traditional License and will not allow the device to initiate the conversion again. If an attempt is made to convert an already converted license, the device will receive a “License Already Converted” status. The device itself remembers the status of the conversion across reboots and registrations and will only do one automatic conversion.

Prior to a conversion request from the device, the SSM On-Prem administrator needs to configure which Local Virtual Accounts are allowed or not allowed for license conversion.

Using SSM On-Prem, complete these steps to specify which Local Virtual Accounts are allowed for license conversion.

Step	Action
Step 1	Log into **SSM On-Prem**.
Step 2	Click the **link** to the **Smart Licensing** workspace.
Step 3	Click the **Convert to Smart Licensing tab**.
Step 4	Click the **Conversion Settings** tab.
Step 5	**Enable Device Led Conversion for all Local Virtual Accounts**, or the **Enable Device Led Conversion only on selected Local Virtual Accounts** associated with the SSM On-Prem Local Account.
Step 6	Click **Apply**.

Conversion Workflow

For devices registered to SSM On-Prem, the following list is a high-level workflow:

1. The device either automatically or manually initiates a migration after a successful registration.
   - Automatically initiated as part of registration via the command license smart conversion.

- Manually initiated by entering a license smart conversion start command on the device to start the conversion.

2. SSM On-Prem receives one or multiple migration requests from one or multiple devices. It validates that the request comes from a registered device.
3. SSM On-Prem displays an alert that the user should initiate a synchronization due to one or more DLC requests.
4. SSM On-Prem responds to the device and tells it to poll back in 1 hour (3600 seconds).
5. SSM On-Prem saves the conversion data so it can send it to CSSM Cloud on the next synchronization.
6. SSM On-Prem passes the encoded conversion data to CSSM Cloud in the next sync (network, scheduled, or manual).
7. SSM On-Prem waits for a response from CSSM Cloud via the next sync (success or failure with a reason).

NOTE: For the device led conversion process to complete, allow up to four hours for the synchronization to complete.

8. When the device polls SSM On-Prem for status, it will respond with the appropriate response (poll-me-later, agent-not-registered, migrate-success, migrate-failed, invalid message type).
9. SSM On-Prem keeps track of device conversion results and provides a report within its UI so users can view the status of the DLC requests/results.

Viewing a Conversion Report

Complete these steps to view a report of the conversion.

Step	Action
Step 1	From the Licensing workspace, click the **Convert to Smart Licensing** tab.
Step 2	Click the **Conversion History** tab. The report displays the: • Product Instance Name • Product Family • Conversion Status • Time of Conversion **NOTE**: You can filter the report by Device Identifier or Product Family.

As the status changes (for example, from pending to success or failure), the report is updated.

Backing Up and Restoring Conversion Results

Listed here are the high-level steps used for backing up/restoring conversion results.

1. When a conversion request is initiated by the device and the license conversion data from the device has been sent to SSM On-Prem. However, the user performs an SSM On-Prem database restore to a time before the SSM On-Prem received the information. When the device tries to poll again for status, SSM On-Prem will return an error since it has no

knowledge of the license conversion due to the restore operation. The device automatically retries the conversion.

2. If the device initiates a conversion and it is no longer registered (either as a direct result of a de-registration or an SSM On-Prem database restore operation before the result comes back. Depending on when SSM On-Prem was restored:
   a. If the SSM On-Prem is restored before the DLC request, then it wouldn't have knowledge of this request and the device needs to retry the DLC request.
   b. If the SSM On-Prem is restored before the device registration, it has no knowledge of the device, so the device needs to re-register and retry the DLC request.
   3. The device initiates a conversion. SSM On-Prem sends the conversion data to CSSM Cloud, which receives the conversion successful results, and notifies the device. If the SSM On-Prem is restored to a point before the sync was started but after SSM On-Prem receives the conversion data from the device, which means it thinks the request is pending, SSM On-Prem will send the DLC request and license data in the next synchronization with CSSM Cloud (network, scheduled, or manual). When it receives an ALREADY CONVERTED response, it will update the UI report accordingly. The device doesn't have to do anything because it has already received its successful status.

Reports Tab

The **Reports** tab allows you to run reports as well as run Usage Schedules (RUM Reports). The Reports tab has two subtabs:

- Reports: That allows you to run reports on all your Local Virtual Accounts and all your licenses within your Local Account. (See Running Reports)
- Usage Schedules: That allows you to run usage reports at specific times via the synchronization schedule fields.

Running Reports

You can run reports on devices such as Licenses, License Subscriptions, and Product Instances.

Complete these steps to run a report.

Step	Action
Step 1	In the Smart Licensing workspace, click the **Reports tab**.
Step 2	In the Reports window, click one of the following options to create the desired report: • **Licenses** • **License Subscriptions** • **Product Instance Report**
Step 3	Complete the following information in the **Run License Report dialog**. **NOTE**: **Show license transactions in report** checklist is applicable only for **Licenses** and **License Subscriptions** reports**.**
Step 4	Click the **button** for the type of report you want to generate: • Run Report • Export to Excel (XLS) • Export to CSV Clicking **Run Report** opens the report within the Reports tab. You can exit the report by clicking the **back arrow** located at the left of the export buttons.

	Clicking **Export to Excel** or **Export to CSV** opens a **File Save** dialog box where you can save the report to a specific location.

Licenses and License Subscriptions Reports

Name	Description
Name field	Enter the name that you want to assign to the report.
Description field	(Optional) Enter the description that you want to use for the report.
Local Virtual Accounts drop-down menu	Choose **All Local Virtual Accounts** to run the report against all your Local Virtual Accounts. Choose **Selected Local Virtual Accounts** or **Accounts with ALL of these Tags** to let you search by **Name** or **Tag** to select one or more Local Virtual Accounts.
Licenses drop-down menu	Choose one or more licenses from the drop-down menu. Choose between All Licenses, Licenses with ALL these License Tags, or Licenses with NO License Tags.
Subscription Status	If a subscriptions report is selected, then this field is shown where you can select All Subscriptions, Active Only, or Expired-or-Cancelled. **NOTE**: **Subscription Status** is applicable only for **License Subscriptions** report**.**
Show license transactions in report	Click this checklist if you want to get transaction details in reports.

Product Instances Reports

Name	Description
Name field	Enter the **name** for the report.
Description field	(Optional) Enter a description for the report.
local Virtual Accounts drop-down menu	Choose **All Local Virtual Accounts** to run the report against all your local Virtual Accounts. Choose **Selected Local Virtual Accounts** or **Accounts with ALL of these Tags** to let you search by **Name** or **Tag** to select one or more Local Virtual Accounts.
Product Type field	The product type that you want to run the report against. You can select **one** or **more product families**.

Setting Usage Schedules from Cisco and from Devices (PI)

The Usage Schedules subtab allows you to schedule usage (RUM) reports by synchronizing with Cisco Cloud or pulling directly from devices stored on On-Prem. These reports provide real-time information on the activity occurring on a device(s). You can obtain usage reports through the synchronization schedule function on the Usage Schedules subtab.

There are two ways to schedule usage reports. By synchronizing with Cisco Cloud (CSSM) or by pulling directly from devices (Product Instances) located on On-Prem. In both modes, you can either schedule synchronization or by using the **Synchronize Now** option which immediately sets up the ability to obtain usage reports.

Complete these steps to schedule usage reports when you are connected to CSSM Cloud.

Synchronizing with Cisco to Obtain Usage Reports

Step	Action
Step 1	In the Smart Licensing workspace, select **Reports tab > Usage Schedule > Synchronization schedule with Cisco**. **NOTE**: To immediately synchronize with Cisco, click **Synchronize now with Cisco**.
Step 2	Enter the **Frequency** (number of days) that you want the report to run (the constraints are...)
Step 3	In the **Time of Day** section enter the **Hour** and **Minutes** when the report is run (the constraints are...)
Step 4	After entering the required information, click **Save**, the synchronization schedule is set for running (downloading??) usage reports from CSSM Cloud.

Synchronizing with Devices to Obtain Usage Reports (Pull schedule)

Step	Action
Step 1	In the Smart Licensing workspace, select **Reports tab > Usage Schedule > Synchronization pull schedule with the devices**. **NOTE**: To immediately synchronize to obtain usage reports from the device, click **Synchronize now with the devices**.
Step 2	Enter the **Frequency** (number of days) that you want the report to run (the constraints are...)
Step 3	In the **Time of Day** section enter the **Hour** and **Minutes** when the report is run (the constraints are...)
Step 4	After entering the required information, click **Save**, the synchronization schedule is set for pulling usage information directly from devices. running.

Preferences Tab

The Preference tab allows you to enable license configuration in order to view License Transaction Details (located in the Inventory table). When this setting is enabled, a checkbox becomes visible in the License table where you can enable the license transaction details to be viewed. See Licenses sub tab under Inventory. Complete these steps to set this preference.

Name	Description
Step 1	From the pull-down list, select either **Disabled** or **Enabled** (Disabled is the default).
Step 2	Click **Save**. The preference is saved.

From this screen you can also view the change log (click the link: **View Change Log**). The dialog shows the:

- Date/Time of the change to the preference.
- Type of Event that occurred.
- The identity of the User who instigated the change.

- Any Notes that have been written by the user about the event/change.

Activity Tab

An activity in SSM On-Prem is defined to include license transactions and a variety of event messages.
As with Alerts, Activities in SSM On-Prem are organized into Local Account and Local Virtual Account levels.
In the Smart Licensing workspace, click the **Activity tab** to display the Activity screen. The screen has two tabs:

- License Transactions
- Event Log Occurrences

License Transactions Tab

Your view of the License Transactions tab depends upon your role as either a Cisco Administrator, Smart Licensing Administrator, System Operator, System User, or Local Virtual Account Administrator. The System Operator, and Local Virtual Account Administrator, for example, have access to Local Account information provided under the Transaction History and Event Log but the System User does not.

The parameters listed in the License Transaction tab are:

- Transaction Date: Date of the transaction
- License SKU: The Stock Keeping Unit number belonging to the license
- License: Name of the License
- Quantity: Quantity of licenses used
- License Expiration: Date the license expires
- License Type: Perpetual or Term
- Local Virtual Account: The name of the Local Virtual Account
- Source: The entity that created the license

In the Administration workstation, under the License Transactions tab, the Cisco Administrator also has the option to: (See Manage an Account)

- Add licenses by clicking **Add License**.
- Remove licenses by using the **Remove Licenses** option found under the Action heading in the License Transactions table.

Event Log

The Event Log shows the event message, the time of the event, and the userid (if any) associated with the event. The following types of events are captured on the Local Account Event Log:

- Changes to Local Account level attributes/properties

- Events for acceptance of legal agreements at the Local Account level
- Events for generation of tokens (Restricted or Un-restricted)
- Events for SSM On-Prem: Listings include account or local virtual account created, renamed, or deleted. SSM On-Prem account failed to sync SSM On-Prem synchronized via network, SSM On-Prem file synchronization (this last listing is for manual synchronization).
- Events for Licenses added or removed

Complete these steps to work in the Event Log tab.

Step	Action
Step 1	In Smart Licensing, click the **Inventory** tab.
Step 2	Select the **Local Virtual Account** from the drop-down list.
Step 3	Navigate to the **Activity** tab.
Step 4	From the Smart Licensing screen click the **Event Log** tab in the Activity table. **NOTE**: You can filter the event log to display either by license type or product instance. Enter a **value** in the Filter combo box and click **Filter** to limit the number of entries that are displayed.
Step 5	(Optional) You can export the event list to a *.csv file from this pane.

Using Smart Software Manager On-Prem APIs

Previously there were 21 REST APIs available on CSSM Cloud. More detailed information on these CSSM Cloud APIs can be found at:

https://anypoint.mulesoft.com/apiplatform/apx/#/portals/organizations/1c92147b-332d-4f44-8c0e-ad3997b5e06d/apis/5418104/versions/102456

Of the 21APIs, the below mentioned APIs are available on Cisco SSM On-Prem as of today.

NOTE: For those requested URLs below that include a Virtual Account name, it is necessary to use the default name “Default” unless this name has been changed in the License Workspace under Manage Accounts under Local Virtual Accounts. The Default account is the **‘*’** account shown in the License Workspace.

NOTE: For all request URLs, the following header fields must be provided:

```
Authorization:      Bearer be8f19829410c501fab265b70814ca39abe254
                    d05fc3c1adc1b39f5c8ddafd08
Content-Type:       application/json
```

NOTE: The bearer token can be generated by following the instructions in section Calling Access Tokens via the API Toolkit widget. Replace the above bearer token with the token you have generated. The client id and client secret used to generate the bearer token should have been generated from a resource owner grant if you plan on testing with a REST client.

This is a list of SSM On-Prem APIs:

NOTE: Few of the SSM On-Prem APIs will not support SLP enabled devices.

1. Virtual Account
    a. **Create a Virtual Account**: Allow users to create Local Virtual Accounts under the given Local Account domain.
    b. **List Local Virtual Accounts**: List all the Local Virtual Accounts in the specified Local Account domain where the requesting user has access.
    c. **Delete a Virtual Account**: Allow users to delete a Virtual Account under the given Local Account domain.
    2. Tokens
    a. **Create a new token**: Generate a new token within a specified Local Account/Virtual Account user for product registration. User needs to have necessary Admin or User access privileges either at the Local Account level or at the specified Virtual Account level.
    b. **List tokens**: Get existing active tokens within a specified Local Account/Virtual Account.
    c. **Revoke tokens**: Revoke the valid tokens available for the given Local Account domain and the Virtual Account. The User can pass an array of the Tokens that they want to revoke.
    3. Licenses
        a. **Smart License Usage**: Give the licenses usage in the specified Local Account Domain and the optional Local Virtual Accounts.
        b. **License Subscriptions Usage**: Return the License Subscriptions on the specified Local Account Domain and the optional Local Virtual Accounts.
        c. **Transfer Licenses**: Transfer the available licenses from one virtual account to another virtual account with in the same Local Account Domain.
        d. **Reserve Licenses**: Allows you to reserve Universal and Specific licenses. The API accepts an array of both Universal and Specific reservation requests in combination. Once the reservations are done, the response will be the Authorization codes for each of the submitted requests. If any reservation didn't go through, an appropriate error message will be given.

NOTE: Not applicable on SSM On-Prem.

        e. **Update SLR Reservation**: Update the license quantity for the reservation already done for a given Virtual Account and License. This API accepts device details along with the license details to be updated. With this API, you can only update the quantity for the reservations done on a license in the given Virtual Account. The response is an authorization code for the license request.

NOTE: Not applicable on SSM On-Prem.

f. **License Summary:** The API endpoint will require authentication and vManage will use the authorization token returned from the authentication process to fetch the license summary. The license summary resource is used to get the license summary of the Virtual Account.

NOTE: The License summary is limited to the SSM On-Prem "Default" virtual account. Will support local virtual account in the future.

g. **License Account Details:** The API endpoint will return account details that the user has access to base on the authorization token. vManage will fetch SSM On-Prem account details to setup usage reporting.

4. Devices/Product Instances

a. **Product Instance Usage**: List the device usage on the specified Local Account Domain and the optional Local Virtual Accounts specified. Based on access you have on the Local Account, the available devices will be fetched and returned.

b. **Product Instance Search**: List the available devices and their specific details (udiPid, serial number, product tag ID, etc.) on the specified Local Account Domain and Virtual account so that these details can be passed in the Product Instance Removal API.

c. **Product Instance Transfer**: This API is used to transfer the available product instances from one virtual account to another virtual account with in the same Local Account Domain.

d. **Product Instance Removal**: Users can invoke this method to remove devices that are registered in their Local Account. This will enable the users to automate device removal as part of their network operations. The User needs to have the necessary admin access privilege within the Local Account/virtual account to perform this request.

5. Alerts

- Alerts: Allow users to view the Alerts that are available for the Smart Entitlements. There are 13 alerts associated with APIs.
  - Update License Agreement (not applicable on SSM On-Prem)
  - Insufficient Licenses
  - Licenses Expired
  - Licenses Expiring
  - Licenses Not Converted
  - Licenses Converted
  - Product Instance Failed to Renew
  - Product Instance Failed to Connect
  - SSM On-Prem Unregistered and Removed
  - Synchronization Overdue
  - Authorization Pending
  - Authorization File Ready
  - Synchronization Failed

Once authentication has been setup, the application can call the API endpoints above.

Local Virtual Account

Creating a Local Virtual Account

Request Parameters

- smartAccountName: The SSM On-Prem Account

Example Method Call:

- HTTP Method: POST
- Request: https://<ip address>:8443/api/v1/accounts/{account name}/virtual-accounts

Request Body:

```
{ "name": "Test VA", "description": "Test VA Creation" }
```

Response:

- The created Local Virtual Account

Response Code: 200 OK

```
{
 "status": “SUCCESS",
 "statusMessage":"Virtual Account 'Test VA' created successfully"
}
```

Response Code: 422

```
{
 "status":"ERROR",
 "statusMessage":" The specified name 'Test VA' for the virtual account is already in use."
}
```

Response Code: 403

```
 {
 "status":"ERROR",
 "statusMessage":"Not Authorized to access Local Virtual Accounts in Local Account"
}
```

Listing Local Virtual Accounts

Request Parameters:

- smartAccountName: The SSM On-Prem Account

Response:

- The Local Virtual Accounts list which the user has access to

Example Method Call:

- HTTP Method: GET
- Request: https://<ip address>:8443/api/v1/accounts/{account name}/virtual-accounts

Response Code: 200 OK


```
{
 "status":"SUCCESS",
 "statusMessage":"",
 "virtualAccounts":[
  {
   "name":"Default",
   "description":"Default virtual Account",
   "isDefault":"Yes"
  },
  {
   "name":"Test Virtual Account",
   "description":"Test VA",
   "isDefault":"No"
  }
 ]
}
```



```
{
 "status":"ERROR",
 "statusMessage":"Not Authorized to create Local Virtual Accounts within
Local Account '{SA Domain Name}'"
```


Deleting a Local Virtual Account

Request Parameters:

- smartAccountName: The SSM On-Prem Account Name where the user wants to search the devices
- virtualAccountName: The name of the Local Virtual Account that you would like to remove

Response:

- The status of the delete virtual account request

Example Method Call:

- HTTP Method: POST
- Request: https://<ip address>:8443/api/v1/accounts/{smartAccountName}/virtual-accounts/{virtualAccountName}/delete

Response Code: 200 OK

```
{
 "status": "SUCCESS",
 "statusMessage": "Virtual Account '{virtual account name}' deleted successfully"
}
```

Tokens API

Creating a Token

Request Parameters:

- smartAccountName: The SSM On-Prem Account Name. example:
- virtualAccountName: The name of the Local Virtual Account.
- description: Description of the token.
- expiresAfterDays: The number of days that the token can be used for, after which it will expire.
- numberofUses: The number of times the token can be used, before the expiration date.

Response:

- The Token list that the user has access to.

Example Method Call:

- HTTP Method: POST
- Request: https://<ip address>:8443/backend/api/v1/accounts/{account name}/virtual-accounts/{virtual account name}/tokens

Request Body:

```
{
"expiresAfterDays": 100,
"description": "Test VA Creation",
"exportControlled": ["Allowed"|"Not Allowed"],
"numberofUses”: “3"
 }
```

Response Code: 200 OK

```
{
 "status":"SUCCESS",
 "statusMessage":"A valid, active token was generated.",
 "tokenInfo":{

"token":"OGVjMDk4YjktNGUwNS00OTc0LTk0YjQtNWZkZTI5ZTU2ZjFjLTE0Nzc1Mjc2%0ANTA
2NTZ8M0wvcmdBWmJnbVR1akdaa0xjTU9ldDRFbXVFQjh3L3k1aHAzdTBD%0ANzlYbz0%3D%
0A",
  "expirationDate":"2016-10-26T20:20:50",
```

```
 "description":"this is Ben September 23",
 "createdBy":"bvoogd",
 "exportControlled": "Not Allowed"
 }
}
```

NOTE: Choose either "Allowed" or "Not Allowed" without the brackets depending upon the export-controlled setting in Cisco SSM. If the Cisco SSM setting is set to “Allowed”, you can use either “Allowed” or “Not Allowed”. If the Cisco SSM setting is set to “Not Allowed”, sending Allowed or Not Allowed will always return “Not Allowed” for the token.

Listing all Tokens

This API will list all existing active tokens within a specified Account/Local Virtual Account. The tokens successfully read can be used for other Product Registration needs.

NOTE: You need to have the necessary access privileges either at the Account level or at the specified Local Virtual Account level.

Request Parameters:

- smartAccountName: The SSM On-Prem Account name.
- virtualAccountName: The name of the Local Virtual Account.

Response:

- List of all the active Tokens within the specified Local Virtual Account. For every active token tokenString, tokenExpirationDate, tokenDescription, createdBy will also be listed.

Example Method Call:

- HTTP Method: GET
- Request: https:// <ip-address>:8443/api/v1/accounts/{smartAccountName}/virtual-accounts/{virtualAccountName}/tokens

Response Code: 200 OK

```
{
 "status":"SUCCESS",
 "statusMessage":"Successfully read active tokens.",
 "tokens":[
  {

"token":"OWI2YmE2ZDgtYTBhZi00MGQyLWE1NDYtZThkMWZjMDUzYzM1LTE0NzcyNj
A1%0AMjI2NTh8cUhjaEtiaGlXalRLeFNseHFqQXpMUnpiZXVvZ0VybkNacU91L1Vq%0A
bDc0ST0%3D%0A",
```

```
    "expirationDate":"2016-10-23T22:08:42",
    "description":"this is Ben September 23",
    "createdBy":"bvoogd"
    "exportControl":"Not Allowed",
   },
   {

"token":"YWQwZjE2MmUtMWI4NS00YmM4LWIyZTAtYjA1OGJjMGI1MTkzLTE0NzcyND
My%0AMTgyMTF8K0djaEJOZWg2S3NIMHhURUI2aWFKOEgxQ0w0Wm41MXZIZHRsb
Vp3%0AOUFZOD0%3D%0A",
    "expirationDate":"2016-10-23T17:20:18",
    "description":"this is Ben September 23",
    "createdBy":"bvoogd"
    "exportControl":"Not Allowed",
   },
   {

"token":"OTI2M2I5YmYtYjRjMy00ZjcyLWE1OTEtOTUwZDY5ZWY3NWRlLTE0NzcyNDM
w%0ANDA0NTZ8U1pRVEJKNFh5a1VTWFprb2FMclh0bjBEVDNrVnNoUzVOdjdmZTJJ%
0AZklZYz0%3D%0A",
    "expirationDate":"2016-10-23T17:17:20",
    "description":"test ben",
    "createdBy":"bvoogd"
    "exportControl”: Allowed",
   }
  ]
}
```


Response Code: 403


```
{
 "status":"ERROR",
 "statusMessage":"Not Authorized to view the Tokens"
}
```


Revoking a Token

Users can use this method to revoke the valid tokens available for the given SSM On-Prem Account and the Local Virtual Account. The user can pass an array of the tokens they want to revoke.

Request Parameters:

- smartAccountName: The SSM On-Prem Account where you want to revoke the token.
- virtualAccountName: The Local Virtual Account of the SSM On-Prem Account where you want to revoke the token.

Response:

- The revoke token status for each of the requested tokens.

Call-outs:

- The maximum tokens you can revoke per request are 10.

Example Method Call:

- HTTP Method: POST
- Request: https://<ip address address>:8443/api/v1/accounts/{smartAccountName}/virtual-accounts/{virtualAccountName}/tokens/revoke

Request Body:


```
{
"tokens":[
"OGVjMDk4YjktNGUwNS00OTc0LTk0YjQtNWZkZTI5ZTU2ZjFjLTE0Nzc1Mjc2%0ANTA2NTZ8M0wvcmdBWmJnbVR1akdaa0xjTU9ldDRFbXVFQjh3L3k1aHAzdTBD%0ANzlYbz0%3D%0A",
"ZGQ1ZmQ2ZWQtNjE4YS00NjA5LThhODMtN2JmNzgyMTU2OTc5LTE0OTU3OTQ4%0ANzE5MTJ8UitTTXIzUGRwb3d5QXB5WExoM01RU1grU1hzYWNjTEo3MzhjOHRt%0AK3dPaz0%3D%0A"
]
}
```


Response Code: 200 OK


```
{
"status": "SUCCESS",
"statusMessage": "{count} tokens revoked successfully"
“tokenRevokeStatus”:[
{
 "status": "SUCCESS",
 "statusMessage": "Token-'ZTBkYjkzOGMtOWY3Yi00ZThjLThkOTAtYTljZmIwZTA5ZWFjLTE1MDU0MTcw%0AMzE2NzJ8Y1dZMkRGUWF1QVQzK3VuNVNSN3hNTDNUUG5XMkJiTS9jMGxMVzNq%0AZVV2TT0%3D%0A' revoked successfully"},
  {
   "status": "SUCCESS",
   "statusMessage": "Token-'ZTBkYjkzOGMtOWY3Yi00ZThjLThkOTAtYTljZmIwZTA5ZWFjLTE1MDU0MTcw%0AMzE2NzJ8Y1dZMkRGUWF1QVQzK3VuNVNSN3hNTDNUUG5XMkJiTS9jMGxMVzNq%0AZVV2TT0%3D%0A' revoked successfully"}
  ]
}
```


Response Code: 200 OK


```
{
 "status": "WARNING",
 "statusMessage": "2 tokens successfully revoked.",
 "tokensRevokeStatus": [
  {
   "status": "ERROR",
   "statusMessage": "The token MmFkMzgyNmMtMDQ2Zi00NjU2LThiZmMtMTk4YWZkNDVhNGU5LTE1MDU0MTcw%0AMjI0ODF8
```

Wjdu”NW5ObVd0L1BGZmFvOWZYenJiaGJyRVE4T0R5NFJheW90V2hq%0AQkRSND0%3D%0A has already been revoked."
},
{
"status": "SUCCESS",
"statusMessage": "Token-'ZTBkYjkzOGMtOWY3Yi00ZThjLThkOTAtYTljZmIwZTA5ZWFjLTE1MDU0MTcw%0AMzE2NzJ8Y1dZMkRGUWF1QVQzK3VuNVNSN3hNTDNUUG5XMkJiTS9jMGxMVzNq%0AZVV2TT0%3D%0A' revoked successfully"
}
]
}

Response Code:422 Unprocessable Entity

{
"tokens":[
{
"status": "ERROR",
"statusMessage": "Failed to find token OGVjMDk4YjktNGUwNS00OTc0LTk0YjQtNWZkZTI5ZTU2ZjFjLTE0Nzc1Mjc2%0ANTA2NTZ8M0wvcmdBWmJnbVR1akdaa0xjTU9ldDRFbXVFQjh3L3k1aHAzdTBD%0ANzlYbz0%3D%0A."
},
{
"status": "ERROR",
"statusMessage": "Failed to find token ZGQ1ZmQ2ZWQtNjE4YS00NjA5LThhODMtN2JmNzgyMTU2OTc5LTE0OTU3OTQ4%0ANzE5MTJ8UitTTXIzUGRwb3d5QXB5WExoM01RU1grU1hzYWNjTEo3MzhjOHRt%0AK3dPaz0%3D%0A."
}
],
"statusMessage": "Token(s) could not be revoked.",
"status": "ERROR"
}

Response Code: 403

{
"status":"ERROR",
"statusMessage": "Not Authorized to revoke tokens for Virtual Account ‘{virtualAccountName}’ ."
}

Licenses

License Usage

Request Parameters:

- smartAccountName: The SSM On-Prem Account being searched.

Response:

- The license usage for the requested domain and optional request parameters.

Example Method Call:

- HTTP Method: POST
- Request: https:// <ip address>:8443/api/v1/accounts/{SmartAccountName}/licenses

Request Payload:

- **virtualAccounts**: An optional list of Local Virtual Accounts where users can obtain the available licenses. If not specified, all the licenses from the smart account, where the user has access to, will be returned.
- **limit**: Number of records to return. Represents the page size for pagination. If all the data is required without pagination the limit can be set to -1. Default limit is 50.
- **offset**: The start offset to fetch data from for pagination. To retrieve data for the first page with a limit of 50, the offset will be 0, for the second page the offset will be 50 and for the third page the offset will be 100 and so on.

```
{
 "virtualAccounts": ["Physics", "Zoology"],
 "limit": 50,
 "offset": 0
}
```

Response Code: 200 OK

```
{
  "status": "SUCCESS",
  "statusMessage": "",
  "totalRecords": 7,
  "licenses": [
   {
    "license": "UC Manager Essential License (12.x)",
    "virtualAccount": "Physics",
    "quantity": 4,
    "inUse": 6,
    "available": 0,
    "status": "In Compliance",
    "ahaApps": false,
    "pendingQuantity": 0,
    "reserved": 0,
    "isPortable": false,

    "licenseDetails": [
    {
     "licenseType": "Term",
     “charge_type”: “Prepaid”
     "quantity": 4,
     "startDate": "2017-05-18",
     "endDate": "2018-05-17",
```

```
  "subscriptionId": "Sub905308"
 }
 ],
 "licenseSubstitutions": [
 {
  "license": " UC Manager Essential License (12.x)",
  "substitutedLicense": "UC Manager Enhanced License (12.x)",
  "substitutedQuantity": 2,
  "substitutionType": "Substitution From Higher Tier"
 }
 ]
},
{
 "license": "UC Manager Basic License (12.x)",
 "virtualAccount": "Physics",
 "quantity": 14,
 "inUse": 16,
 "available": 0,
 "status": "In Compliance",

 "ahaApps": false,
 "pendingQuantity": 0,
 "reserved": 0,
 "isPortable": false,
 "licenseDetails": [
 {
  "licenseType": "Term",
  "quantity": 10,
  "startDate": "2017-05-18",
  "endDate": "2017-11-14",
  "subscriptionId": ""
 },
 {
  "licenseType": "Perpetual",
  "quantity": 4,
  "startDate": "",
  "endDate": "",
  "subscriptionId": ""
 }
 ],
 "licenseSubstitutions": [
 {
  "license": " UC Manager Basic License (12.x)",
  "substitutedLicense": "UC Manager Enhanced License (12.x)",
  "substitutedQuantity": 2,
  "substitutionType": "Substitution From Higher Tier"
 }
 ]
},
{
 "license": "UC Manager Enhanced License (12.x)",
```

```
  "virtualAccount": "Physics",
  "quantity": 10,
  "inUse": 0,
  "available": 6,
  "status": "In Compliance",
     "ahaApps": false,
  "pendingQuantity": 0,
  "reserved": 0,
  "isPortable": false,

  "licenseDetails": [
  {
   "licenseType": "Term",
   "quantity": 10,
   "startDate": "2017-05-18",
   "endDate": "2017-11-14",
   "subscriptionId": ""
  }
  ],
  "licenseSubstitutions": [
  {
   "license": " UC Manager Basic License (12.x)",
   "substitutedLicense": "UC Manager Enhanced License (12.x)",
   "substitutedQuantity": 2,
   "substitutionType": "Substitution To Lower Tier"
  },
  {
   "license": " UC Manager Essential License (12.x)",
   "substitutedLicense": "UC Manager Enhanced License (12.x)",
   "substitutedQuantity": 2,
   "substitutionType": "Substitution To Lower Tier"
  }
  ]
 },
 {
  "license": "UC Manager Enhanced Plus License (12.x)",
  "virtualAccount": "Physics",
  "quantity": 10,
  "inUse": 21,
  "available": -1,
  "status": "Out Of Compliance",
  "licenseDetails": [
  {
   "licenseType": "Term",
   "quantity": 10,
   "startDate": "2017-05-18",
   "endDate": "2017-11-14",
   "subscriptionId": ""
  }
  ],
  "licenseSubstitutions": [
```

```
 {
  "license": "UC Manager Enhanced Plus License (12.x)",
  "substitutedLicense": "UC Manager CUWL License (12.x)",
  "substitutedQuantity": 10,
  "substitutionType": "Substitution From Higher Tier"
 }
 ]
},
{
 "license": "UC Manager CUWL License (12.x)",
 "virtualAccount": "Physics",
 "quantity": 10,
 "inUse": 0,
 "available": 0,
 "status": "In Compliance",
    "ahaApps": false,
 "pendingQuantity": 0,
 "reserved": 0,
 "isPortable": false,

 "licenseDetails": [
 {
  "licenseType": "Perpetual",
  "quantity": 10,
  "startDate": "",
  "endDate": "",
  "subscriptionId": ""
 }
 ],
 "licenseSubstitutions": [
 {
  "license": "UC Manager Enhanced Plus License (12.x)",
  "substitutedLicense": "UC Manager CUWL License (12.x)",
  "substitutedQuantity": 10,
  "substitutionType": "Substitution To Lower Tier"
 }
 ]
},
{
 "license": "CSR 1KV AX 100M",
 "virtualAccount": "Zoology",
 "quantity": 11,
 "inUse": 0,
 "available": 11,
 "status": "In Compliance",
    "ahaApps": false,
 "pendingQuantity": 0,
 "reserved": 0,
 "isPortable": false,

 "licenseDetails": [
```

```
    {
     "licenseType": "Term",
     "quantity": 1,
     "startDate": "2017-05-24",
     "endDate": "2020-05-23",
     "subscriptionId": ""
    },
    {
     "licenseType": "Demo",
     "quantity": 10,
     "startDate": "2017-05-22",
     "endDate": "2017-07-21",
     "subscriptionId": ""
    }
    ],
    "licenseSubstitutions": []
   },
   {
    "license": "CSR 1KV SECURITY 1G",
    "virtualAccount": "Zoology",
    "quantity": 5,
    "inUse": 7,
    "available": -2,
    "status": "Out Of Compliance",
       "ahaApps": false,
    "pendingQuantity": 0,
    "reserved": 0,
    "isPortable": false,

    "licenseDetails": [
    {
     "licenseType": "Perpetual",
     "quantity": 5,
     "startDate": "",
     "endDate": "",
     "subscriptionId": ""
    }
    ],
    "licenseSubstitutions": []
   }
  ]
}
```


Response Code:200 OK


```
{
  "status": "SUCCESS",
  "statusMessage": "The requested virtual account '<VA name1, va name 2>' doesn't belong to the account
'<Account Name>'. Hence returning the response for eligible Local Virtual Accounts.",
  "totalRecords": 1,
```

```
 "licenses": [
  {
   "license": "150 Mbps vNAM Software Release 6.2",
   "virtualAccount": "July10_VA2",
   "quantity": 18,
   "inUse": 9,
   "available": 18,
   "status": "In Compliance",
   "licenseDetails": [
    {
     "licenseType": "PERPETUAL",
     "quantity": 18,
     "startDate": null,
     "endDate": null,
     "subscriptionId": null
    }
   ],
   "licenseSubstitutions": [
    {
     "license": "150 Mbps vNAM Software Release 6.2",
     "substitutedLicense": "A9K 2x100G MPA Consumption Model LC license",
     "substitutedQuantity": 9,
     "substitutionType": "Substitution From Lower Tier"
    }
   ]
  ]
}
```


Response Code:403


```
{
 "status":"ERROR",
 "statusMessage": "Not Authorized to access licenses for specified Local Virtual Accounts"
}
```


Response Code:422


```
{
 "status":"ERROR",
 "statusMessage": "Invalid limit or offset value"
}
```


Response Code: 200 OK


```
{
 "status": "SUCCESS",
 "statusMessage": "",
 "totalRecords": 7,
 "licenses": [
```

```
{
 "license": "UC Manager Essential License (12.x)",
 "virtualAccount": "Physics",
 "quantity": 4,
 "inUse": 6,
 "available": 0,
 "status": "In Compliance",
 "ahaApps": false,
 "pendingQuantity": 0,
 "reserved": 0,
 "isPortable": false,

 "licenseDetails": [
 {
  "licenseType": "Term",
  "quantity": 4,
  "startDate": "2017-05-18",
  "endDate": "2018-05-17",
  "subscriptionId": "Sub905308"
 }
 ],
 "licenseSubstitutions": [
 {
  "license": " UC Manager Essential License (12.x)",
  "substitutedLicense": "UC Manager Enhanced License (12.x)",
  "substitutedQuantity": 2,
  "substitutionType": "Substitution From Higher Tier"
 }
 ]
},
{
 "license": "UC Manager Basic License (12.x)",
 "virtualAccount": "Physics",
 "quantity": 14,
 "inUse": 16,
 "available": 0,
 "status": "In Compliance",

 "ahaApps": false,
 "pendingQuantity": 0,
 "reserved": 0,
 "isPortable": false,
 "licenseDetails": [
 {
  "licenseType": "Term",
  "quantity": 10,
  "startDate": "2017-05-18",
  "endDate": "2017-11-14",
  "subscriptionId": ""
 },
 {
```

```
"licenseType": "Perpetual",
"quantity": 4,
"startDate": "",
"endDate": "",
"subscriptionId": ""
}
```


License Subscription Usage

Request Parameters:

- smartAccountName: The SSM On-Prem Account being searched.

Response:

- The available License Subscriptions usage for the request submitted.

Example Method Call:

- HTTP Method: POST
- Request: https://<ip-address>:8443/api/v1/accounts/{smartAccountName}/license-subscriptions

Request Body

- **virtualAccounts**: An optional list of Local Virtual Accounts for where users can obtain the available licenses. If not specified, all the licenses from the domain, where the user has access to, will be returned.
- **status**: The status of the subscriptions to be obtained. Valid values are Active, Canceled, Expired.
- **limit**: Number of records to return; represents the page size for pagination. If all the data is required without pagination the limit can be set to -1. Default limit is 50.
- **offset**: The start offset to fetch data from for pagination. To retrieve data for the first page with a limit of 50, the offset will be 0, for the second page the offset will be 50 and for the third page the offset will be 100 and so on.


```
{
"virtualAccounts": ["Physics", "Zoology"],
"status": ["Active", "Expired", "Canceled"],
"limit": 50,
"offset": 0
}
```


Response Code: 200 OK


```
{
 "status":"SUCCESS",
 "statusMessage":"",
 "totalRecords":3,
 "licenseSubscriptions":[
```

```
 {
 "virtualAccount":"Physics",
 "license":"CSR 1KV UCSD VIRTUAL CONTAINER",
 "quantity":"500",
 "startDate":"2016-12-04",
 "endDate":"2019-12-03",
 "status":"Active",
 "subscriptionId":"Sub905825"
 },
 {
 "virtualAccount":"Physics",
 "license":"ASR 9000 4-port 100GE Advanced IP Lic for SE LC",
 "quantity":"50",
 "startDate":null,
 "endDate":null,
 "status":"Canceled",
 "subscriptionId":"Sub905308"
 },
 {
 "virtualAccount":"Zoology",
 "license":"CSR 1KV UCSD VIRTUAL CONTAINER",
 "quantity":"10",
 "startDate":"2016-11-29",
 "endDate":"2019-11-28",
 "status":"Active",
 "subscriptionId":"Sub905309"
 }
]
}
```


Response Code: 403


```
{
 "status":"ERROR",
 "statusMessage": "Not Authorized to access license subscriptions for specified Local Virtual Accounts"
}
```


Response Code: 403


```
{
 "status":"ERROR",
 "statusMessage": "Not Authorized to access license subscriptions for Local Account {SA Domain}"
}
```


Response Code:422


```
{
 "status":"ERROR",
 "statusMessage": "Invalid limit or offset value"
```

```
}
```

License Transfers

Request Parameters:

- smartAccountName: The SSM On-Prem Account where the user intends to conduct the license transfer
- virtualAccountName: The name of the Local Virtual Account from which the user intends to perform the License transfer.

Response: A list of transfer responses for each of the list of transfer requests submitted.

Call-outs:

- There is a threshold of 10 licenses transfer which the user can transfer in a single request.

Example Method Call:

- HTTP Method: POST
- Request: https://<ip address>:8443/api/v1/accounts/{smartAccountName}/virtual-accounts/{virtualAccountName}/licenses/transfer

Request Payload

- TargetVirtualAccount: The target Local Virtual Account to which you wish to transfer the License to.
- Quantity: The quantity to transfer. This quantity should always be less than the available quantity for the specified license in the Local Virtual Account the licenses are being transferred from.
- Precedence: Optional attribute specifying the precedence order in which transfers will take place in the case of term-based licenses. Valid values are LONGEST_TERM_FIRST and LONGEST_TERM_LAST. By default, if this attribute is not specified, it will default to LONGEST_TERM_FIRST. As an example, assume there are 2 term-based licenses for CSR 1KV SECURITY 10M in Local Virtual Account Chemistry and the first term-based license has a term of 90 days and the second has a term of 60 days. If the precedence is LONGEST_TERM_FIRST, then the 90 days license will be processed first for the transfer followed by the 60 days license.
- LicenseType: The type of license the user wishes to transfer. Valid values are 'TERM' and 'PERPETUAL'. Please note that all the non 'PERPETUAL' licenses like 'DEMO', 'SUBSCRIPTION' will be treated as 'TERM'.
- ChargeType: The type of charge the user wishes to use. Valid values are ‘USAGE’ and ‘PREPAID’

NOTE: If you try to transfer licenses “ERROR”, “statusMessage”: “The license being transferred is a utility license and cannot be transferred to another virtual account.”

- License: The name of the license which the user wants to transfer.

```
{“licenses”:[
{
 "license": "CSR 10KV SECURITY 10M",
```

```
 "licenseType": "PERPETUAL",
 "quantity": 50,
 "targetVirtualAccount": "Physics",
“charge_type”: “USAGE”
},{
 "license": "CSR 1KV SECURITY 10M",
 "licenseType": "TERM",
 "precedence": "LONGEST_TERM_FIRST",
 "quantity": 50,
 "targetVirtualAccount": "VA2"
“charge_type”; “PREPAID”
},{
 "license": "CSR 1KV SECURITY 10M",
 "licenseType": "PERPETUAL",
 "quantity": 10,
 "targetVirtualAccount": "Physics"
}]
}
```


Response Code: 200 OK


```
{
 "status":"WARNING",
 "statusMessage":"{license count} licenses transferred successfully. ",
 "licensesTransferStatus":[
  {
  "status":"SUCCESS",
  "statusMessage":"50 ‘CSR 1KV SECURITY 10M’ licenses were transferred to Virtual Account ‘Physics’
from Virtual Account ‘VA1’."
  },
  {
  "status":"ERROR",
  "statusMessage":"Failed to find “CSR 1KV SECURITY 10M” license in Virtual Account “VA1."
  },
  {
  "status":"ERROR",
  "statusMessage":"You do not have access to ‘VA9’."
  }
 ]
}
```


Response Code: 200 OK


```
{
 "status":"SUCCESS",
 "statusMessage":"{license count} licenses transferred successfully.",
 "licensesTransferStatus":[
  {
  "status":"SUCCESS",
```

```
 "statusMessage":"50 ‘CSR 1KV SECURITY 10M’ licenses successfully transferred from Virtual Account ‘VA1’ to Virtual Account ‘Physics’."
 },
 {
 "status":"SUCCESS",
 "statusMessage":"50 ‘CSR 10 KV SECURITY 10M’ licenses successfully transferred from Virtual Account ‘VA1’ to Virtual Account ‘va2’."
 }
]
}
```


Response Code: 422


```
{
 "status":"ERROR",
 "statusMessage":"All licenses failed to transfer.",
 "licensesTransferStatus":[
 {
 "status":"ERROR",
 "statusMessage":"Failed to find Virtual Account '{vaName}'."
 }
]
}
```


Response Code: 422


```
{
 “status”: “ERROR”,
 “statusMessage”: ”All licenses failed to transfer.”
 “licensesTransferStatus”:[
{
 "status": "ERROR",
 "statusMessage": "Invalid ‘licenseType’ or ‘precedence’ value."
}]
}
```


Response Code: 422


```
{
 “status”: “ERROR”,
 “statusMessage”: ”All licenses failed to transfer.”
 “licensesTransferStatus”:[
 "status": "ERROR",
 "statusMessage": "Quantity to transfer is greater than the available quantity for license ‘CSR 1KV SECURITY 10M’ license in Virtual Account ‘{vaName}’."
}]
}
```

Response Code: 403

```
{
 “status”: “ERROR”,
 “statusMessage”: ”All licenses failed to transfer.”
 “licensesTransferStatus”:[
{
 "status": "ERROR",
 "statusMessage": "Not Authorized to access Local Virtual Accounts ‘{vaName}’ or ‘Physics’."
}]
}
```

Response Code: 403

```
{
 “status”: “ERROR”,
 “statusMessage”: ” Not Authorized to access Virtual Account ‘{Source VA Name}’.”
}
```

VManage License Summary

Response

- The available license summary of the SSM On-prem account responses for the request submitted.

Example Method Call

- HTTP Method: POST
- Request: https://<ip-address>:8443/api/v1/upstream_satellites/{account_name}/licenses_summary

Request Body

- Empty

Response Body: 200 OK

```
"summary": [
      {
         "tag": "regid.2017-11.com.cisco.advanced_features,12.4_81e0d1a9-0481-4236-9f3b-422019ba96a1",
         "compliance_status": "In Compliance",
         "display_name": "Advanced Features",
         "enforced": false,
         "export_restricted": false,
         "license_details": [
            {
               "billing_type": "PREPAID",
               "quantity": 6,
               "postpaid_usage": 0,
```

```
            "start_date": null,
            "end_date": null,
            "subscription_id": null,
            "status": "ACTIVE",
            "billing_model": null,
            "license_type": "PERPETUAL"
         }
      ],
      "prepaid_entitled": 6,
      "prepaid_inuse": 0,
      "prepaid_reserved": 0
   },
```


VManage Account Details

Response

- The list of available account details responses for the request submitted.

Example Method Call

- HTTP Method: POST
- Request: https://<ip-address>:8443/api/v1/upstream_satellites/accounts

Request Body

- Empty

Response Body: 200 OK


```
accounts": [
   {
      "account_id": "1",
      "domain": "delphi.cisco.com",
      "name": "My_acc1",
      "cslu_tenant_url": "https://10.83.111.80/cslu/v1/pi/My_acc1-1",
      "cssm_smart_account_id": 106851,
      "cssm_smart_account_name": "DLO Test Account",
      "cssm_virtual_account_id": 616352,
      "cssm_virtual_account_name": "My_acc1",
      "virtual_accounts": [
         {
            "virtual_account_id": "1",
            "name": "Default",
            "default": true
         }
      ]
   },
   {
      "account_id": "2",
```

```
        "domain": "delphi.cisco.com",
        "name": "Local_acc",
        "cslu_tenant_url": "https://10.83.111.80/cslu/v1/pi/Local_acc-2",
        "cssm_smart_account_id": 106851,
        "cssm_smart_account_name": "DLO Test Account",
        "cssm_virtual_account_id": 616703,
        "cssm_virtual_account_name": "Local_acc",
        "virtual_accounts": [
          {
            "virtual_account_id": "3",
            "name": "Default",
            "default": true
          }
        ]
      }
  ]
}
```


Device/Product Instances

Product Instance Usage

Lists the available information on the Product Instances in the specified Account and Local Virtual Account so that this information can be easily included in the PI Remove API.

Request Parameters:

- smartAccountName: The SSM Account where the user will search for devices.

Request Body:

- SSM On-Prem Accounts: An optional list of Local Virtual Accounts where users intend to obtain the available licenses. If not specified, all the licenses from the domain where the user has access will be returned.
- limit: Number of records to return; Represents the page size for pagination. If all the data is required without pagination the limit can be set to -1. Default limit will be 50.
- offset: The start offset to fetch data from for pagination. To retrieve data for the first page with a limit of 50, the offset will be 0, for the second page the offset will be 50 and for the third page the offset will be 100 and so on.


```
{
  "virtualAccounts": ["Physics", "Zoology"],
  "limit": 50,
  "offset": 0
}
```


Response:

- The available Product Instances for the submitted request.

Example Method Call:

- HTTP Method: POST
- Request: https://<ip-address>:8443/api/v1/accounts/{account name}/devices

Response Code: 200 OK


```
{
  "status": "SUCCESS",
  "statusMessage": "",
  "totalRecords": 2,
  devices: [{
    "virtualAccount": "Physics",
    "hostName": "ucbu-aricent-vm107",
    "sudi": {
      "suvi": "",
      "uuid": "062f582e30844ed2b8d005c14c425b06",
      "hostIdentifier": "",
      "udiPid": "Cisco Unity Connection",
      "udiSerialNumber": "062f582e30844ed2b8d005c14c4",
      "udiVid": "",
      "macAddress": ""
    },
    "productName": "Cisco Unity Connection (12.0)",
    "productDescription": "Cisco Unity Connection",
    "productTagName": "regid.2014-04.com.cisco.ASR_9000,1.0_577f0b47-7ba4-4cae-
a86e-77b64604d808",
    "productType": "UNICONN",
    "status": "In Compliance",
    "registrationDate": "2017-05-23T12:34:35Z",
    "lastContactDate": "2017-05-23T12:54:22Z",
    "licenseUsage": [{
       "license": "Unity Connection Enhanced Messaging User Licenses (12.x)",
       "quantity": 7
      }, {
       "license": "Unity Connection Basic Messaging User Licenses (12.x)",
       "quantity": 2
      }
    ]
   }, {
    "virtualAccount": "Zoology",
    "hostName": "infy-lm05-lnx",
    "sudi": {
      "suvi": "",
      "uuid": "ba8892ae89bf45688ce00302d1db8a35",
      "hostIdentifier": "",
      "udiPid": "UCM",
```

```
      "udiSerialNumber": "b8a35",
      "udiVid": "",
      "macAddress": ""
    },
    "productName": "Unified Communication Manager (12.0)",
    "productDescription": "Unified Communication Manager",
    "productTagName": "regid.2014-04.com.cisco.ASR_9000,1.0_577f0b47-7ba4-4cae-
a86e-77b64604d808",
    "productType": "UCL",
    "status": "Out Of Compliance",
    "registrationDate": "2017-05-18T12:34:35Z",
    "lastContactDate": "2017-06-02T12:54:22Z",
    "licenseUsage": [{
      "license": "UC Manager Basic License (12.x)",
      "quantity": 4
     }, {
      "license": "UC Manager Enhanced License (12.x)",
      "quantity": 10
     }
    ]
   }
  ]
}
```


Product Instance Transfer

Request Parameters:

- smartAccountName: The SSM On-Prem Account where the user wants to transfer the Product Instances.
- virtualAccountName: The name of the Local Virtual Account where the user intends to perform the device transfer.

Response:

- A list of transfer responses for each of the list of submitted transfer requests.

Call-outs: There is a threshold of 10 devices transfer that the user can conduct in a single request.

Example Method Call:

- HTTP Method: POST
- Request: http://<ip address>:8443/api/v1/accounts/{smartAccountName}/virtual-accounts/{virtualAccountName}/devices/transfer

Request Body


```
{
"productInstances":[{
 "sudi": {
  "suvi": null,
```

```
 "uuid": null,
 "hostIdentifier": null,
 "udiPid": "N77-C7710",
 "udiSerialNumber": "JPG3032006T",
 "udiVid": null,
 "macAddress": null
 },
 "productTagName": "regid.2015-09.com.cisco.Nexus_7000,1.0_6e2b6ed8-fe9b-48e0-a71f-74eaf1bcc991",
 "targetVirtualAccount": "Physics"
},
{
 "sudi": {
  "suvi": null,
  "uuid": null,
  "hostIdentifier": null,
  "udiPid": "N77-C7711",
  "udiSerialNumber": "JPG3032004T",
  "udiVid": null,
  "macAddress": null
 },
 "productTagName": "regid.2015-39.com.cisco.Nexus_7000,1.0_6e2b6ed8-fe9b-48e0-a71f-74eaf1bcc991" ,
 "targetVirtualAccount": "Maths"
}]
}
```


Response Code: 200 OK


```
{
“status”: “WARNING”,
“statusMessage”: ”{device count} product instances transferred successfully.”
“productsTransferStatus”: [
{
 {
 "status": "SUCCESS",
 "statusMessage" : "Device ‘N77-C7711’ successfully transferred from Virtual Account ‘{vaName}’ to Virtual
Account ‘Physics’."
},
 {
 "status" : "ERROR",
 "statusMessage" : "Failed to find device ‘N897-C0987’ in Virtual Account ‘{vaName}’."
}]
}
```


Response Code: 200 OK


```
{
“status”: “SUCCESS”,
 “statusMessage”: ”{device count} product instances transferred successfully.”
 “productsTransferStatus”: [
```

```
{
"status": "SUCCESS",
"statusMessage" : "Device ‘N77-C7711’ successfully transferred from Virtual Account ‘{source VA Name}’ to Virtual Account ‘{target VA Name}’."
},
{"status": "SUCCESS",
 "statusMessage" : "Device ‘N77-c5644’ successfully transferred from Virtual Account ‘{source VA Name}’ to Virtual Account ‘{target VA Name}’."
}]
}
```


Response Code: 422


```
{"status": "ERROR",
 "statusMessage": "all the product instances failed to transfer"
 "productsTransferStatus": [
{
 "status" : "ERROR",
 "statusMessage" : "Failed to find device with specified information in Virtual Account  ‘{target VA Name}’."
}]
}
```


Response Code: 422


```
{
"status": "ERROR",
"statusMessage": "all the devices failed to transfer"
"productsTransferStatus": [
{
 "status": "ERROR",
 "statusMessage" : "Failed to find Virtual Account ‘{target VA Name}’."
}]
}
```


Response Code: 422


```
{
"status": "ERROR",
"statusMessage": "Failed to find Virtual Account ‘Physics’."
}
```


Response Code: 403


```
{
"status": "ERROR",
"statusMessage": " Not Authorized to access Virtual Account ‘{Source VA Name}’."
```

```
}
```

Product Instance Search

Lists the available information of Product Instances within the specified SSM On-Prem Account and Local Virtual Account, the response of this API, can be used in Product Instance Removal API as well.

Request Parameters:

- smartAccountName: The SSM On-Prem Account where the user wants to search for the devices.
- virtualAccountName: The name of the Local Virtual Account where the user wants to search for the devices.

Request Parameters (*Optional*):

- Instance Name: The instance name from the order- Hostname, UDI Serial Number, Host Identifier, Mac Address, IP Address, SUVI, UUID, whichever is available, add to the suffix of request URL.
  For example: ?udiSerialNumber=123456Albert45678901.
- Limit: Number of records to return; Represents the page size for pagination. If all the data is required without pagination the limit can be set to -1. Default limit will be 50.
- Offset: The start offset to fetch data from for pagination. To retrieve data for the first page with a limit of 50, the offset will be 0, for the second page the offset will be 50 and for the third page the offset will be 100 and so on.

Response:

- The available Product Instances for the request submitted.

Example Method Call:

- HTTP Method: GET
- Request: https://<ip address>:8443/backend/api/v1/accounts/{smartAccountName}/virtual-accounts/{virtualAccountName}/devices

Response Code: 200 OK

```
"devices": [
    {
      "instanceName": "firepower",
      "sudi": {
        "suvi": null,
        "uuid": "a91dba0a-af1a-11ea-90bf-57292abdab7c",
        "hostIdentifier": null,
        "udiPid": "FS-VMW-SW-K9",
        "udiSerialNumber": "3",
        "udiVid": null,
        "macAddress": null
      },
```

```
        "productTagName": "regid.2015-06.com.cisco.FPR-TD,v1_f782c685-80e4-45ac-8d5b-
a080457146c2"
      },
      {
        "instanceName": "UDI_PID:ISR4321/K9;UDI_SN:FDO22011HP1;UDI_VID:;",
        "sudi": {
          "suvi": "",
          "uuid": "",
          "hostIdentifier": "",
          "udiPid": "ISR4321/K9",
          "udiSerialNumber": "FDO22011HP1",
          "udiVid": "",
          "macAddress": ""
        },
        "productTagName": "regid.2014-12.com.cisco.ISR_4321,1.0_fe94a4a6-84c7-4f71-9118-
018541b9c358"
      },
      {
        "instanceName": "UDI_PID:ISR4321/K9;UDI_SN:FDO22011HP1;UDI_VID:;",
        "sudi": {
          "suvi": "",
          "uuid": "",
          "hostIdentifier": "",
          "udiPid": "ISR4321/K9",
          "udiSerialNumber": "FDO22011HP1",
          "udiVid": "",
          "macAddress": ""
        },
        "productTagName": "regid.2014-12.com.cisco.ISR_4321,1.0_fe94a4a6-84c7-4f71-9118-
018541b9c358"
      }
    ],
    "totalRecords": 3,
    "statusMessage": "",
    "status": "SUCCESS"
}
```


NOTE: From Version 8-202212 SSM On-Prem Supports both SL And SLP devices in Product Instance Search API.

Product Instance Removal

This API enables user to programmatically, remove devices that are registered to the SSM On-Prem Account. This method enables user to automate device removal as part of network

operations. User should have the necessary **admin access privileges** within the SSM On-Prem Account/Local Virtual Account to perform this request.

Request Parameters:

- smartAccountName: The SSM On-Prem Account where the user wants to perform device removal.
- virtualAccountName: The name of the Local Virtual Account where the user wants to perform device removal**.**

Payload Parameters:

- SUDI of Device: The SUDI is a certificate and an associated key-pair. The SUDI provides an immutable identity for the router that is used to verify that the device is a genuine Cisco product, and to ensure that the router is well-known to the customer's inventory system.
- Software/Product Tag Identifier: Identifier that helps the Smart Licensing system to identify the software product family. The product Tag Identifier can be found by logging into device, running 'show license tech-support', and using the value of the 'Software ID' key.

Response:

The Local Virtual Account lists the admin privilege users.

Call-outs:

- The provided SUDI details must match a product instance in the provided virtual account.

Example Method Call:

- HTTP Method: POST
- Request: https://<ip-address>:8443/backend/api/v1/accounts/{smartAccountName}/virtual-accounts/{virtualAccountName}/devices/remove

Request Payload

```
{
 "productInstanceRemoveRequests": [
   {
     "sudi": {
      "udiPid": "CSR1000V",
      "udiSerialNumber": "97N1PAGTEOZ",
      "uuid": "",
      "suvi":"",
      "hostIdentifier": "",
      "udiVid": "",
      "macAddress": ""
      },
     "productTagName": "regid.2013-08.com.cisco.CSR1000V,1.0_1562da96-9176-
4f99-a6cb-14b4dd0fa135"
   },
   {
```

```
     "sudi": {
      "udiPid": "C8000V",
      "udiSerialNumber": "9ENUB66G5PT",
      "uuid": "",
      "suvi":"",
      "hostIdentifier": "",
      "udiVid": "",
      "macAddress": ""
      },
      "productTagName": "regid.2019-10.com.cisco.C8000V,1.0_e361c3dc-27c2-
4084-b4a4-cae639cff335"
    }
 ]
}
```


Response Code: 200 OK


```
{
  "status": "SUCCESS",
  "statusMessage": {
    "statusMessage": "1 Product Instance(s) removed successfully.",
    "removeProductInstancesStatus": [
      {
        "statusMessage": "The Product Instance local.lab was successfully
removed.",
        "status": "SUCCESS",
        "device": "udiPid:CSR1000V udiSerialNumber:97N1PAGTEOZ
hostName:local.lab"
      },
      {
        "statusMessage": "The Product Instance UDI_PID: C8000V;UDI_SN:
9ENUB66G5PT;UDI_VID:; was successfully removed.",
        "status": "SUCCESS",
        "device": "udiPid:C8000V udiSerialNumber:9ENUB66G5PT hostName:"
      }
    ]
  }
```


NOTE: From Version 8-202212 SSM On-Prem Supports both SL And SLP devices in Product Instance Removal API.

Account Policy

(Added for SSM On-Prem 8 Release 202212)

This API allows user to view the account policy details.

NOTE: The Policy defined on CSSM, shall be obtained during the acknowledgement response.

Response:

- The available Policy details of the account.

Example Method Call:

- HTTP Method: GET
- Request: https://<ip address>:8443/backend/api/v1/account/policy

Headers:

- X-CSL-LOGICAL-ACCOUNT-ID: Account id represents an account on which the policy details are requested.

Response Code: 200 OK


```
{
   "status": "COMPLETE",
   "message_code": "",
   "message": "",
   "timestamp": 1667783004078,
   "policy": "PHNtYXJ0TGljZW5zZVBvbGljeT48cG9saWN5Q29kZT48bmFtZT5ETE8gVGVzdDwvbmFtZT
48dmVyc2lvbj4yMzwvdmVyc2lvbj48ZmxhZz48L2ZsYWc+PGRhdGVzdGFtcD4yMDIxLTEyLTA4VDE0Oj
A0OjExPC9kYXRlc3RhbXA+PGFja1JlcXVpcmVkPnllczwvYWNrUmVxdWlyZWQ+PHN1YnNjcmlwdGlvbj
48Zmlyc3RUaW1lUmVwb3J0PjA8L2ZpcnN0VGltZVJlcG9ydD48b25Hb2luZ1JlcG9ydGluZz4wPC9vbkdva
W5nUmVwb3J0aW5nPjxyZXBvcnRPbk1BQ0Q+MDwvcmVwb3J0T25NQUNEPjwvc3Vic2NyaXB0aW9uPjx
wZXJwZXR1YWw+PGZpcnN0VGltZVJlcG9ydD41MTwvZmlyc3RUaW1lUmVwb3J0PjxvbkdvaW5nUmVw
b3J0aW5nPjM8L29uR29pbmdSZXBvcnRpbmc+PHJlcG9ydE9uTUFDRD4yPC9yZXBvcnRPbk1BQ0Q+PC9
wZXJwZXR1YWw+PGVuZm9yY2VkPjxvbkdvaW5nUmVwb3J0aW5nPjA8L29uR29pbmdSZXBvcnRpbmc+
PHJlcG9ydE9uTUFDRD4zPC9yZXBvcnRPbk1BQ0Q+PC9lbmZvcmNlZD48ZXhwb3J0PjxvbkdvaW5nUmV
wb3J0aW5nPjA8L29uR29pbmdSZXBvcnRpbmc+PHJlcG9ydE9uTUFDRD4zPC9yZXBvcnRPbk1BQ0Q+PC9
leHBvcnQ+PGdlbmVyaWM+PGZpcnN0VGltZVJlcG9ydD4wPC9maXJzdFRpbWVSZXBvcnQ+PG9uR29pb
mdSZXBvcnRpbmc+MDwvb25Hb2luZ1JlcG9ydGluZz48cmVwb3J0T25NQUNEPjA8L3JlcG9ydE9uTUFDR
D48L2dlbmVyaWM+PC9wb2xpY3lDb2RlPjxzaWduYXR1cmU+TUVZQ0lRQ0dMekdXWWJGeWQxUStsQl
BnMGN3WnNFNWRsRVJsbW1ZVFRjYVFIc2NqaHdJaEFMSkd6YklNOE81WHJtSUhhYnArQndvSjdDN09
Ha3Voek53aVFMMnIrcW8yPC9zaWduYXR1cmU+PC9zbWFydExpY2Vuc2VQb2xpY3k+"
}
```


Response Code: 403


```
{
   "error": "base",
   "error_message": "Cannot find account with the provided id:'3'."
```

```
}
```

Alerts

This API will allow you to view the Alerts that are available for the Smart entitlements.

Request Parameters:

- smartAccountName: The SSM On-Prem Account where the user wants to fetch the alerts.

Response:

- The available Alerts for the submitted request.

Example Method Call:

- HTTP Method: POST
- Request: https://<ip address>:8443/api/v1/accounts/{Account}/alerts

Request Payload

- virtualAccounts: An optional list of Local Virtual Accounts for which users intend to fetch the available licenses. If not specified, all the alerts from the domain for which the user has access to will be returned.
- severity: Optional list of numeric values for severity of the alerts. If not specified defaults to both Major and Minor alerts.
- limit: Number of records to return: Represents the page size for pagination. If all the data is required without pagination the limit can be set to -1. If the limit is set to -1, the first 1000 alerts matching the request criteria will be fetched. If the limit is not specified, the default limit will be 50.
- offset: The start offset to fetch data from for pagination. To retrieve data for the first page with a limit of 50, the offset will be 0, for the second page the offset will be 50 and for the third page the offset will be 100 and so on.

```
{
"virtualAccounts": ["Physics", "Zoology"],
"severity": ["Major","Minor"],
"limit": 50,
"offset": 0
}
```

Response Code: 200 OK

```
{

  "status": "SUCCESS",
  "statusMessage":"",
  "totalRecords": 13,
  "alerts": [
   {
```

```
    "virtualAccount": "",
    "message": "Please review and indicate acceptance of the updated Cisco Smart Software Licensing
Agreement's terms and conditions.",
    "severity": "Major",
    "messageType": "Updated Smart Software Licensing Agreement",
    "actionDue": "Now",
    "source": "",
    "sourceType": "Account Agreement"
   },
   {
    "virtualAccount": "Physics",
    "message": "The Virtual Account \"Physics\" has a shortage of \"CSR 1KV SECURITY 10M\" licenses. 1
license is required to return to compliance.",
    "severity": "Major",
    "license": "CSR 1KV SECURITY 10M",
    "messageType": "Insufficient Licenses",
    "actionDue": "Now",
    "source": "Physics",
    "sourceType": "Virtual Account"
   },
   {
    "virtualAccount": "Physics",
    "message": "10 \"CSR 1KV ADVANCED 50M\" demo licenses in the Virtual Account \"Physics\" expired
on May 24, 2017",
    "severity": "Minor",
    "license": "CSR 1KV ADVANCED 50M",
    "messageType": "Licenses Expired",
    "actionDue": "Now",
    "source": "Physics",
    "sourceType": "Virtual Account"
   },
   {
    "virtualAccount": "Physics",
    "message": "10 \"CSR 1KV STANDARD 50M\" demo licenses in the Virtual Account \"Physics\" are set to
expire in 43 days on Jul 15, 2017",
    "severity": "Minor",
    "license": "CSR 1KV STANDARD 50M ",
    "messageType": "Licenses Expiring",
    "actionDue": "43 days",
    "source": "Physics",
    "sourceType": "Virtual Account"
   },
   {
    "virtualAccount": "Physics",
    "message": "The product instance \"1491321888000\" was successfully registered to the Virtual Account
\"Physics\" however an eligible Smart Software License could not be identified to for the conversion of one or
more licenses. Please contact Cisco Support for conversion assistance",
    "severity": "Minor",
    "productInstanceHostName": "1491321888000",
    "messageType": "Licenses Not Converted",
    "actionDue": "None",
```

```
    "source": "Physics",
    "sourceType": "Virtual Account"
   },
   {
    "virtualAccount": "Physics",
    "message": "The product instance \"hiDLCShe3\" was successfully registered to the Virtual Account \"Physics\" but one or more traditional licenses that were installed on it failed to be converted to Smart Software Licenses.",
    "severity": "Minor",
    "productInstanceHostName": "hiDLCShe3",
    "messageType": "Licenses Converted",
    "actionDue": "None",
    "source": "Physics",
    "sourceType": "Virtual Account"
   },
   {
    "virtualAccount": "Physics",
    "message": "The product instance \" ucbu-aricent-vm107\" in the Local Virtual Account \"Physics\" failed to connect during its renewal period and may be running in a degraded state. The licenses it was consuming have been released for use by other product instances.",
    "severity": "Major",
    "productInstanceHostName": "ucbu-aricent-vm107",
    "messageType": "Product Instance Failed to Renew",
    "actionDue": "Now",
    "source": "Physics",
    "sourceType": "Virtual Account"
   },
   {
    "virtualAccount": "Physics",
    "message": "The product instance \" ucbu-aricent-vm108\" in the Virtual Account \"Physics\" has not connected for its renewal period. The product instance may run in a degraded state if it does not connect within the next 2 days. If the product instance is not going to connect, you can remove it to immediately release the licenses it is consuming.",
    "severity": "Minor",
    "productInstanceHostName": "ucbu-aricent-vm108",
    "messageType": "Product Instance Failed to Connect",
    "actionDue": "2 days",
    "source": "Physics",
    "sourceType": "Virtual Account"
   },
   {
    "virtualAccount": "Zoology",
    "message": "The Smart Software Manager On-Prem \"TestOn-Prem\" failed to synchronize within 90 days and was removed from Smart Software Manager. All of the product instances registered through the On-Prem were also removed from the associated Local Virtual Accounts and may be running in a degraded state.",
    "severity": "Major",
    "On-PremName": "TestOn-Prem",
    "messageType": "On-Prem Unregistered and Removed",
    "actionDue": "Now",
    "source": "TestOn-Prem",
    "sourceType": "On-Prem"
```

```
  },
  {
   "virtualAccount": "Zoology",
   "message": "The Smart Software Manager On-Prem \"test-may5\" has not synchronized for 28 days. If it is not synchronized within 62 days, this On-Prem will be removed from Smart Software Manager and all of the product instances registered through the On-Prem may run in a degraded state.",
   "severity": "Major",
   "On-PremName": "test-may5",
   "messageType": "Synchronization Overdue",
   "actionDue": "Now",
   "source": "test-may5",
   "sourceType": "On-Prem"
  },
  {
   "virtualAccount": "Zoology",
   "message": "The Smart Software Manager On-Prem \"TestSat\" has been created but requires an On-Prem Authorization File to complete the registration process. An email notification will be sent to \"att-admin@att.com\" when the file has been generated and is ready to be downloaded.",
   "severity": "Minor",
   "On-PremName": "TestSat",
   "messageType": "Authorization Pending",
   "actionDue": "Now",
   "source": "TestSat",
   "sourceType": "On-Prem"
  },
  {
   "virtualAccount": "Zoology",
   "message": "The Authorization File for Smart Software Manager On-Prem \"TestSat123\" has been generated and is ready to be downloaded. To complete the registration process, save this file and upload it to Smart Software Manager On-Prem using the On-Prem setup utility.",
   "severity": "Minor",
   "On-PremName": " TestSat123",
   "messageType": "Authorization File Ready",
   "actionDue": "Now",
   "source": "TestSat123",
   "sourceType": "On-Prem"
  },
  {
   "virtualAccount": "Zoology",
   "message": "An error occurred while processing the Synchronization File for the On-Prem. Try generating a new Synchronization File from your On-Prem and synchronizing again. If the problem persists, contact Cisco Support.",
   "severity": "Major",
   "On-PremName": " Thera",
   "messageType": "Synchronization Failed",
   "actionDue": "Now",
   "source": "Thera",
   "sourceType": "On-Prem"
  }
 ]
}
```

Response Code: 403

```
{
 "status":"ERROR",
 "statusMessage": "Not Authorized to access alerts for specified Local Virtual Accounts"
}
{
 "status":"ERROR",
 "statusMessage": "Not Authorized to access alerts for Local Account '{Local Account Domain}'"
}
```

Response Code: 422

```
{
 "status":"ERROR",
 "statusMessage": "Invalid limit, offset or severity value"
}
```

Using Smart Software Manager On-Prem SYSLOG

Overview of SYSLOG Message Variables

The following variables are used in syslog alert messages. Each variable must begin with a percent sign and be enclosed in curly braces as, for example, %{VariableName}.

Variable	Description
%{count}	Number of licenses
%{end_date}	Expiry Date
%{ha_list}	HA Software Unique Device Identifier
%{identifier}	Product Instance name
%{new_pool_name}	New Virtual Account
%{old_pool_name}	Old Virtual Account
%{pak_name}	migration_name
%{pool_name}	Local Virtual Account
%{On-Prem_name}	On-Prem
%{sub_ref_id}	Subscription ID
%{tag}	Entitlement_tag
%{type}	License type

Device-Led Conversion

Device Led Conversion Requested	
Severity:	MINOR(1)

Message Text:	Synchronization Required: Device Led Conversion requests are pending. Conversion results will be displayed when synchronization with CSSM is completed.

Device Led Conversion Complete	
Severity:	MINOR(1)
Message Text:	Conversion Successful

Device Led Conversion Failed	
Severity:	MINOR(1)
Message Text:	Conversion Failed error for product “%{product}

Export Control

Export Keys Returned	
Severity:	MINOR(1)
Message Text:	"Export restricted licenses were removed from product instance “%{pi_display_name}” in Virtual Account “%{pool_name}” and were released back to the inventory for use by other product instances. Licenses: 1 “%{entitlement_tag_name}” perpetual."

Export Keys Consumed	
Severity:	MINOR(1)
Message Text:	"Export restricted licenses were assigned to product instance “%{display_name}” in Virtual Account “%{pool_name}”."

Export Control Authorization Pending	
Severity:	MINOR(1)
Message Text:	"The product instance “%{device_name}” in the Virtual Account “%{pool_name}” requested a license with restricted encryption technology which is pending authorization via synchronization with CSSM Cloud."

Export Control Authorization Return Pending	
Severity:	MINOR(1)
Message Text:	"The product instance “%{device_name}” in the Virtual Account “%{pool_name}” requested a return of a license with restricted encryption technology which is pending authorization via synchronization with CSSM Cloud."

Export Keys Returned	
Severity:	MINOR(1)

Message Text:	"Export restricted licenses were removed from product instance “%{pi_display_name}” in Virtual Account “%{pool_name}” and were released back to the inventory for use by other product instances. Licenses: 1 “%{entitlement_tag_name}” perpetual."

Export Keys Consumed	
Severity:	MINOR(1)
Message Text:	"Export restricted licenses were assigned to product instance “%{display_name}” in Virtual Account “%{pool_name}”

License Not Available	
Severity:	MINOR(1)
Message Text:	• "The product instance “%{display_name}” has requested licenses that enable restricted encryption technology. These licenses are not available within the virtual account “%{pool_name}”. You must add the licenses to the virtual account or transfer the product instance to a virtual account that contains the licenses." • "The product instance “%{display_name}” in Virtual Account “%{pool_name}” has requested export restricted licenses that are not available. You must add these licenses to this Virtual Account or transfer the product instance to a Virtual Account that contains these licenses. Licenses: %{licenses}." • "The product instance “%{display_name}” has requested licenses that enable restricted encryption technology. These licenses are not available within the virtual account “%{pool_name}”. You must add the licenses to the virtual account or transfer the product instance to a virtual account that contains the licenses." "The product instance “%{display_name}” in Virtual Account “%{pool_name}” has requested export restricted licenses that are not available. You must add these licenses to this Virtual Account or transfer the product instance to a Virtual Account that contains these licenses. Licenses: %{licenses}."

Get Third Party Key

Get Third Party Key	
Severity:	MINOR(1)
Message Text:	“The product instance “%{identifier}” in the Virtual Account “%{pool_name}” connected and received third party keys”

Licenses

Insufficient Licenses	
Severity:	MAJOR(2)
Message Text:	• "The Virtual Account “%{pool_name}” reported a shortage of 1 “%{tag}” license.

	• "The Virtual Account “%{pool_name}” reported a shortage of %{count} “%{tag}” licenses.

Insufficient Expired	
Severity:	MINOR(1)
Message Text:	• "1 “%{tag}” %{type} license associated with Subscription ID “%{sub_ref_id}” in the Virtual Account %{pool_name}” expired on %{end_date}" • "%{count} “%{tag}” %{type} licenses associated with Subscription ID “%{sub_ref_id}” in the Virtual Account “%{pool_name}” expired on %{end_date}"

Licenses Removed	
Severity:	MINOR(1)
Message Text:	• "1 “%{tag}” %{type} license was removed from the Virtual Account “%{pool_name}”" • "%{count} “%{tag}” %{type} licenses were %{remove} from the Virtual Account “%{pool_name}”"

New Licenses	
Severity:	MINOR(1)
Message Text:	• "one: "1 new “%{tag}” %{type} license was added to the Virtual Account “%{pool_name}” via Smart License Conversion (PAK:%{pak_name})" • "%{count} new “%{tag}” %{type} licenses were added to the Virtual Account “%{pool_name}” via Smart License Conversion (PAK:%{pak_name})" • "1 new “%{tag}” %{type} license was added to the Virtual Account “%{pool_name}” via Smart License Conversion (%{device_name})" • "%{count} new “%{tag}” %{type} licenses were added to the Virtual Account “%{pool_name}” via Smart License Conversion (%{device_name})" • "1 new “%{tag}” %{type} license was added to the Virtual Account “%{pool_name}” from the Customer Suite Name “%{suite_name}” (TRAN ID:%{migration_id})" • :%{migration_id}: migration id • “%{suite_name}” : migration_name • "%{count} new “%{tag}” %{type} licenses were added to the Virtual Account “%{pool_name}” from the Customer Suite Name “%{suite_name}” (TRAN ID:%{migration_id})" • "1 new “%{tag}” %{type} license associated with Subscription ID “%{sub_ref_id}” was added to the Virtual Account “%{pool_name}”" • "%{count} new “%{tag}” %{type} licenses associated with Subscription ID “%{sub_ref_id}” were added to the Virtual Account “%{pool_name}”" • "1 new “%{tag}” perpetual license was automatically added to the Virtual Account “%{pool_name}”." • "%{count} new “%{tag}” perpetual licenses were automatically added to the Virtual Account “%{pool_name}”." • "1 new “%{tag}” %{type} license was added to the Virtual Account “%{pool_name}”"

New Licenses	
	• "%{count} new “%{tag}” %{type} licenses were added to the Virtual Account “%{pool_name}”"

Licenses Expiring	
Severity:	MINOR(1)
Message Text:	• "1 %{tag} %{type} license associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” is set to expire today on %{end_date}" • "%{count} %{tag} %{type} licenses associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” are set to expire today on %{end_date}" • "1 “%{tag}” %{type} license in the Virtual Account “%{pool_name}” is set to expire today on %{end_date}" • "%{count} “%{tag}” %{type} licenses in the Virtual Account “%{pool_name}” are set to expire today on %{end_date}" • "1 %{tag} %{type} license associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” is set to expire in 1 day on %{end_date}" • "%{count} %{tag} %{type} licenses associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” are set to expire in 1 day on %{end_date}" • "1 “%{tag}” %{type} license in the Virtual Account “%{pool_name}” is set to expire in 1 day on %{end_date}" • "%{count} “%{tag}” %{type} licenses in the Virtual Account “%{pool_name}” are set to expire in 1 day on %{end_date}" • "1 %{tag} %{type} license associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” is set to expire in %{days} days on %{end_date}" • "%{count} %{tag} %{type} licenses associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” are set to expire in %{days} days on %{end_date}" • "1 “%{tag}” %{type} license in the Virtual Account “%{pool_name}” is set to expire in %{days} days on %{end_date}" • "%{count} “%{tag}” %{type} licenses in the Virtual Account “%{pool_name}” are set to expire in %{days} days on %{end_date}"

Insufficient Licenses	
Severity:	MINOR(1)
Message Text:	• "The Virtual Account “%{pool_name}” has a shortage of “%{tag}” licenses. 1 license is required to return to compliance." • "The Virtual Account “%{pool_name}” has a shortage of “%{tag}” licenses. %{count} licenses are required to return to compliance."

Licenses Transferred	
Severity:	MINOR(1)
Message Text:	• "1 “%{tag}” %{type} license associated with Subscription ID “%{sub_ref_id}” was transferred from the Virtual Account “%{old_pool_name}” to the Virtual Account “%{new_pool_name}”."

Licenses Transferred	
	• "%{count} “%{tag}” %{type} licenses associated with Subscription ID “%{sub_ref_id}” were transferred from the Virtual Account “%{old_pool_name}” to the Virtual Account “%{new_pool_name}”." • "1 “%{tag}” %{type} license associated with Subscription ID “%{sub_ref_id}” was transferred to the Virtual Account “%{new_pool_name}” from the Virtual Account “%{old_pool_name}”." • "%{count} “%{tag}” %{type} licenses associated with Subscription ID “%{sub_ref_id}” were transferred to the Virtual Account “%{new_pool_name}” from the Virtual Account “%{old_pool_name}”." • "1 “%{tag}” %{type} license was transferred from the Virtual Account “%{old_pool_name}” to the Virtual Account “%{new_pool_name}”." • "%{count} “%{tag}” %{type} licenses were transferred from the Virtual Account “%{old_pool_name}” to the Virtual Account “%{new_pool_name}”." • "1 “%{tag}” %{type} license associated with Subscription ID “%{sub_ref_id}” was transferred to the Virtual Account “%{new_pool_name}” from the Virtual Account “%{old_pool_name}”." • "%{count} “%{tag}” %{type} licenses associated with Subscription ID “%{sub_ref_id}” were transferred to the Virtual Account “%{new_pool_name}” from the Virtual Account “%{old_pool_name}”." • "1 “%{tag}” %{type} license was transferred from the Virtual Account “%{old_pool_name}” to the Virtual Account “%{new_pool_name}”." • "%{count} “%{tag}” %{type} licenses were transferred from the Virtual Account “%{old_pool_name}” to the Virtual Account “%{new_pool_name}”." • "1 “%{tag}” %{type} license was transferred to the Virtual Account “%{new_pool_name}” from the Virtual Account “%{old_pool_name}”." • "%{count} “%{tag}” %{type} licenses were transferred to the Virtual Account “%{new_pool_name}” from the Virtual Account “%{old_pool_name}”."

Licenses Expired	
Severity:	MINOR(1)
Message Text:	• "1 %{tag} %{type} license associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” is set to expire today on %{end_date}" • "%{count} %{tag} %{type} licenses associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” are set to expire today on %{end_date}" • "1 “%{tag}” %{type} license in the Virtual Account “%{pool_name}” is set to expire today on %{end_date}" • "%{count} “%{tag}” %{type} licenses in the Virtual Account “%{pool_name}” are set to expire today on %{end_date}" • "1 %{tag} %{type} license associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” is set to expire in 1 day on %{end_date}" • "%{count} %{tag} %{type} licenses associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” are set to expire in 1 day on %{end_date}" • "1 “%{tag}” %{type} license in the Virtual Account “%{pool_name}” is set to expire in 1 day on %{end_date}"

Licenses Expired	
	• "%{count} “%{tag}” %{type} licenses in the Virtual Account “%{pool_name}” are set to expire in 1 day on %{end_date}" • "1 %{tag} %{type} license associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” is set to expire in %{days} days on %{end_date}" • "%{count} %{tag} %{type} licenses associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” are set to expire in %{days} days on %{end_date}" • "1 “%{tag}” %{type} license in the Virtual Account “%{pool_name}” is set to expire in %{days} days on %{end_date}" • "%{count} “%{tag}” %{type} licenses in the Virtual Account “%{pool_name}” are set to expire in %{days} days on %{end_date}" • "1 “%{tag}” %{type} license associated with Subscription ID “%{sub_ref_id}” in the Virtual Account “%{pool_name}” expired on %{end_date}" • "%{count} “%{tag}” %{type} licenses associated with Subscription ID “%{sub_ref_id}” in the Virtual Account “%{pool_name}” expired on %{end_date}" • "1 “%{tag}” %{type} license in the Virtual Account “%{pool_name}” expired on %{end_date}" • "%{count} “%{tag}” %{type} licenses in the Virtual Account “%{pool_name}” expired on %{end_date}"

Insufficient Licenses	
Severity:	MAJOR(2)
Message Text:	• "The Virtual Account “%{pool_name}” has a shortage of “%{tag}” licenses. 1 license is required to return to compliance." • "The Virtual Account “%{pool_name}” has a shortage of “%{tag}” licenses. %{count} licenses are required to return to compliance." • “The Virtual Account “%{pool_name}” reported a shortage of 1 “%{tag}” license." • “The Virtual Account “%{pool_name}” reported a shortage of %{count} “%{tag}” licenses."

Licenses Corrected	
Severity:	MINOR(1)
Message Text:	• "The shortage of 1 “%{tag}” license in the Virtual Account “%{pool_name}” has been corrected." • "The shortage of %{count} “%{tag}” licenses in the Virtual Account “%{pool_name}” has been corrected."

Licenses Expiring	
Severity:	MINOR(1)
Message Text:	• "%{type} license associated with Subscription ID %{sub_ref_id} in the Virtual Account %{pool_id} is set to expire today on %{end_date}" • "%{type} licenses associated with Subscription ID %{sub_ref_id} in the Virtual Account %{pool_id} are set to expire today on %{end_date}"

Licenses Expiring	
	• "1 %{tag} %{type} license associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” is set to expire today on %{end_date}" • "%{count} %{tag} %{type} licenses associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” are set to expire today on %{end_date}" • "%{type} license in the Virtual Account “%{pool_name}” is set to expire today on %{end_date}" • "%{type} licenses in the Virtual Account “%{pool_name}” are set to expire today on %{end_date}" • "1 “%{tag}” %{type} license in the Virtual Account “%{pool_name}” is set to expire today on %{end_date}" • "%{count} “%{tag}” %{type} licenses in the Virtual Account “%{pool_name}” are set to expire today on %{end_date}" • "%{type} license associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” is set to expire in 1 day on %{end_date}" • "%{type} licenses associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” are set to expire in 1 day on %{end_date}" • "1 %{tag} %{type} license associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” is set to expire in 1 day on %{end_date}" • "%{count} %{tag} %{type} licenses associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” are set to expire in 1 day on %{end_date}" • "%{type} license in the Virtual Account “%{pool_name}” is set to expire in 1 day on %{end_date}" • "%{type} licenses in the Virtual Account “%{pool_name}” are set to expire in 1 day on %{end_date}" • "1 “%{tag}” %{type} license in the Virtual Account “%{pool_name}” is set to expire in 1 day on %{end_date}" • "%{count} “%{tag}” %{type} licenses in the Virtual Account “%{pool_name}” are set to expire in 1 day on %{end_date}" • "%{type} license associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” is set to expire in %{days} days on %{end_date}" • "%{type} licenses associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” are set to expire in %{days} days on %{end_date}" • "1 %{tag} %{type} license associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” is set to expire in %{days} days on %{end_date}" • "%{count} %{tag} %{type} licenses associated with Subscription ID %{sub_ref_id} in the Virtual Account “%{pool_name}” are set to expire in %{days} days on %{end_date}" • "%{type} license in the Virtual Account “%{pool_name}” is set to expire in %{days} days on %{end_date}" • "%{type} licenses in the Virtual Account “%{pool_name}” are set to expire in %{days} days on %{end_date}"

Licenses Expiring	
	• "1 “%{tag}” %{type} license in the Virtual Account “%{pool_name}” is set to expire in %{days} days on %{end_date}" • "%{count} “%{tag}” %{type} licenses in the Virtual Account “%{pool_name}” are set to expire in %{days} days on %{end_date}" • "%{type} license associated with Subscription ID “%{sub_ref_id}” in the Virtual Account “%{pool_name}” expired on %{end_date}" • "%{type} licenses associated with Subscription ID “%{sub_ref_id}” in the Virtual Account “%{pool_name}” expired on %{end_date}" • "1 “%{tag}” %{type} license associated with Subscription ID “%{sub_ref_id}” in the Virtual Account “%{pool_name}” expired on %{end_date}" • "%{count} “%{tag}” %{type} licenses associated with Subscription ID “%{sub_ref_id}” in the Virtual Account “%{pool_name}” expired on %{end_date}" • "%{type} license in the Virtual Account “%{pool_name}” expired on %{end_date}" • "%{type} licenses in the Virtual Account “%{pool_name}” expired on %{end_date}" • "1 “%{tag}” %{type} license in the Virtual Account “%{pool_name}” expired on %{end_date}" • "%{count} “%{tag}” %{type} licenses in the Virtual Account “%{pool_name}” expired on %{end_date}"

Fail to Connect	
Severity:	MINOR(1)
Message Text:	• "in the Virtual Account “#{ref.license_pool.name}” has not connected for its renewal period. The product instance may run in a degraded state if it does not connect today. If the product instance is not going to connect, you can remove it to immediately release the licenses it is consuming." : "in the Virtual Account “#{ref.license_pool.name}” has not connected for its renewal period. The product instance may run in a degraded state if it does not connect within the next #{remain_days} days. If the product instance is not going to connect, you can remove it to immediately release the licenses it is consuming."

License Not Available	
Severity:	MINOR(1)
Message Text:	• "The product instance “%{display_name}” has requested licenses that enable restricted encryption technology. These licenses are not available within the virtual account “%{pool_name}”. You must add the licenses to the virtual account or transfer the product instance to a virtual account that contains the licenses."

Product Instances

New Product Instance	
Severity:	MINOR(1)

Message Text:	• "The product instance “%{identifier}” was added to the Virtual Account “%{pool_name}” and configured for redundancy with the following Standbys “%{ha_list}””

Product Instance Transferred	
Severity:	MINOR(1)
Message Text:	• " The product instance “%{identifier}” was transferred from the Virtual Account “%{old_pool_name}” to the Virtual Account “%{new_pool_name}”." • The product instance “%{identifier}” was transferred to the Virtual Account “%{new_pool_name}” from the Virtual Account “%{old_pool_name}”."

Product Instance Removed	
Severity:	MINOR(1)
Message Text:	• " The product instance “%{identifier}” was removed from the Virtual Account “%{pool_name}” via synchronization with the On-Prem “%{On-Prem_name}” • “The product instance “%{identifier}” was removed from Smart Software Manager. "

Product Instance Failed to Connect	
Severity:	MINOR(1)
Message Text:	• "The product instance “%{identifier}” in the Virtual Account “%{pool_name}” has not connected for its renewal period. The product instance may run in a degraded state if it does not connect today. If the product instance is not going to connect, you can remove it to immediately release the non-restricted licenses it is consuming. Please have the product instance connect to Smart Software Manager or open a support case to have it removed." • "The product instance “%{identifier}” in the Virtual Account “%{pool_name}” has not connected for its renewal period. The product instance may run in a degraded state if it does not connect within the next 1 day. If the product instance is not going to connect, you can remove it to immediately release the non-restricted licenses it is consuming. Please have the product instance connect to Smart Software Manager or open a support case to have it removed." • "The product instance “%{identifier}” in the Virtual Account “%{pool_name}” has not connected for its renewal period. The product instance may run in a degraded state if it does not connect within the next %{count} days. If the product instance is not going to connect, you can remove it to immediately release the non-restricted licenses it is consuming. Please have the product instance connect to Smart Software Manager or open a support case to have it removed."

Product Instance Failed to Renew	
Severity:	MINOR(1)
Message Text:	• “The product instance “%{identifier}” in the Virtual Account “%{pool_name}” failed to connect during its renewal period and may be

	running in a degraded state. The non-restricted licenses it was consuming have been released for use by other product instances. Please have the product instance connect to Smart Software Manager or open a support case to have it removed."

Product Instance Connected	
Severity:	MINOR(1)
Message Text:	• "The product instance "%{identifier}" in the Virtual Account "%{pool_name}" connected and successfully renewed."

Product Instance Renew	
Severity:	MINOR(1)
Message Text:	• "The product instance "%{identifier}" in the Virtual Account "%{pool_name}" connected and successfully renewed its identity certificate."

SSM On-Prem

SSM On-Prem Registered	
Severity:	MINOR(1)
Message Text:	• "The On-Prem "%{On-Prem_name}" was registered to Smart Account "%{smart_account_name}" and Virtual Account "%{virtual_account_name}" by User "%{user_name}" at %{time}"

SSM On-Prem Removed	
Severity:	MINOR(1)
Message Text:	• "The On-Prem "%{On-Prem_name}" was removed."

SSM On-Prem Renamed	
Severity:	MINOR(1)
Message Text:	• "The On-Prem “%{old_On-Prem_name}” was renamed to “%{new_On-Prem_name}”"

Synchronization Overdue	
Severity:	MINOR(1)
Message Text:	• "The Smart Software Manager On-Prem “%{On-Prem_name}” has not synchronized for %{not_sync_days}. If it is not synchronized within %{remain_sync_days}, this On-Prem will be removed from Smart Software Manager and all of the product instances registered through the On-Prem may run in a degraded state."

SSM On-Prem Unregistered and Removed	
Severity:	MINOR(1)
Message Text:	• "The Smart Software Manager On-Prem “%{On-Prem_name}” failed to synchronize within 90 days and was removed from Smart Software Manager. All of the product instances registered through the On-Prem were also removed from the associated Local Virtual Accounts and may be running in a degraded state."

Authorization Pending	
Severity:	MINOR(1)
Message Text:	• "The Smart Software Manager On-Prem “%{On-Prem_name}” has been created but requires an On-Prem Authorization File to complete the registration process. An email notification will be sent to “%{email}” when the file has been generated and is ready to be downloaded."

Authorization File Ready	
Severity:	MINOR(1)
Message Text:	• "The Authorization File for Smart Software Manager On-Prem “%{On-Prem_name}” has been generated and is ready to be downloaded. To complete the registration process, save this file and upload it to Smart Software Manager On-Prem using the On-Prem setup utility."

SSM On-Prem Registered	
Severity:	MINOR(1)
Message Text:	• "The On-Prem “%{On-Prem_name}” was registered."

Synchronization Overdue	
Severity:	MINOR(1)
Message Text:	• "The Smart Software Manager On-Prem “%{On-Prem_name}” has not synchronized for %{not_sync_days}. If it is not synchronized within %{remain_sync_days}, this On-Prem will be removed from Smart Software Manager and all of the product instances registered through the On-Prem may run in a degraded state."

SSM On-Prem Unregistered and Removed	
Severity:	MINOR(1)
Message Text:	• "The Smart Software Manager On-Prem “%{On-Prem_name}” failed to synchronize within 90 days and was removed from Smart Software Manager. All of the product instances registered through the On-Prem were also removed from the associated local Virtual Accounts and may be running in a degraded state."

Authorization Pending	
Severity:	MINOR(1)
Message Text:	• "The Smart Software Manager On-Prem “%{On-Prem_name}” has been created but requires an On-Prem Authorization File to complete the registration process. An email notification will be sent to “%{email}” when the file has been generated and is ready to be downloaded."

Authorization File Ready	
Severity:	MINOR(1)
Message Text:	• "The Authorization File for Smart Software Manager On-Prem “%{On-Prem_name}” has been generated and is ready to be downloaded. To complete the registration process, save this file and upload it to Smart Software Manager On-Prem using the On-Prem setup utility."

Synchronization Required	
Severity:	MINOR(1)
Message Text:	• "Synchronization Required: An Export Controlled license request from a product instance needs authorization from CSSM Cloud."

Synchronization Required	
Severity:	MINOR(1)
Message Text:	• "Synchronization Required: Device Led Conversion requests are pending. Conversion results will be displayed when synchronization with CSSM is completed."

Synchronization Failed	
Severity:	MAJOR(2)
Message Text:	• "Synchronization Failed: The Smart Software Manager On-Prem account “%{display_name}” synchronization to Cisco has failed. Please go to the synchronization log for more details."

Synchronization Successful	
Severity:	MINOR(1)
Message Text:	• "Synchronization Successful"

Synchronization Required	
Severity:	MINOR(1)
Message Text:	• "Synchronization Required: An Export Controlled license request from a product instance needs authorization from CSSM Cloud."

Synchronization Overdue	
Severity:	MINOR(1)
Message Text:	• “On-Prem has not synchronized in #{@On-Prem.days_from_last_sync} days.”

Re-registration Required	
Severity:	MINOR(1)
Message Text:	• "On-Prem was not synchronized for 365 days and must be re-registered with CSSM Cloud."

Synchronization Failed (Network Synchronization)	
Severity:	MAJOR(2)
Message Text:	• "The file being processed for this On-Prem is invalid." • "Invalid Certificate timestamp. Please ensure the On-Prem is synchronized with the NTP server." • "Invalid ID Certificate. The file being processed has an invalid certificate." • "Invalid Signing Certificate. The file being processed has an invalid certificate." • "Invalid Certificate. The file being processed during synchronization has an invalid certificate. Please do a full synchronization to get a new certificate."

Synchronization Failed (Manual Synchronization)	
Severity:	MAJOR(2)
Message Text:	• "Please ensure the file being uploaded corresponds to this On-Prem." • "The file you selected is not a valid synchronization response file. It must be in YAML format with the file extension ".yml". Ensure the correct file was selected and try again." • "The file you selected is not a valid synchronization response file. It might be corrupted or was modified after being downloaded from Smart Software Manager. Redownload the synchronization response file and try again." • "The file you selected is not a valid synchronization response file. It appears to have been modified after it was downloaded from Smart Software Manager. Redownload the synchronization response file and try again." • "Invalid Certificate timestamp. Please ensure the On-Prem is synchronized with the NTP server." • "Invalid ID Certificate. The file you uploaded has an invalid certificate. Ensure the file you uploaded corresponds to this On-Prem and it has not been modified." • "Invalid Signing Certificate. The file you uploaded has an invalid certificate. Ensure the file you uploaded corresponds to this On-Prem and it has not been modified." • "The synchronization response file you selected has already been processed by this On-Prem. Ensure that you are selecting the most recent file." • "The file you selected is not a valid synchronization response file. Certificates are missing in the response file which you have uploaded. Redownload the synchronization response file and try again." • "Invalid Certificate. The file uploaded during synchronization has an invalid certificate. Please do a full synchronization to get a new certificate."

One or More Entitlements Failed to Synchronize	
Severity:	MINOR(1)
Message Text:	• "One or more entitlements failed to synchronize with CSSM"

One or more products failed to synchronize	
Severity:	MINOR(1)
Message Text:	• "One or more products failed to synchronize with CSSM"

SSM On-Prem Re-Registration	
Severity:	MAJOR(2)
Message Text:	• "Re-registration file generated for account %{logical_account_name}" • "The On-Prem "%{logical_account_name}" was Re-Registered to Smart Account "%{smart_account_name}" and Virtual Account "%{virtual_account_name}" by User "%{user_name}" at "%{time}""

Version Compatibility Note

Severity:	MINOR(1)
Message Text:	• "Temporarily, this SSM On-Prem will only be able to register Product Instances that are using the multi-level certificate hierarchy feature (use show license on the Product Instance to ensure that the agent version is 1.5+). To enable registration of Product Instances using older versions of the agent, wait ten business days after the On-Prem's initial registration and then synchronize."

Token ID

Token Revoked	
Severity:	MINOR(1)
Message Text:	• "The Token “%{token_string}” in the Virtual Account “%{pool_name}” was revoked."

Token Removed	
Severity:	MINOR(1)
Message Text:	• "The Token “%{token_string}” in the Virtual Account “%{pool_name}” was removed."

Restricted Token	
Severity:	MINOR(1)
Message Text:	• "A new Token “%{token_string}” allowing export-controlled functionality was generated for the Virtual Account “%{pool_name}”."

Non-Restricted Token	
Severity:	MINOR(1)
Message Text:	• "A new Token “%{token_string}” not allowing export-controlled functionality was generated for the Virtual Account “%{pool_name}”."

User

User Added	
Severity:	MINOR(1)
Message Text:	• "A new user “%{user_name}” was added."

User Roles Added	
Severity:	MINOR(1)
Message Text:	• "The user “%{user_name}” was assigned the role “%{role_name}”."

User Roles Removed	
Severity:	MINOR(1)
Message Text:	• "User “%{user_ccoid}” was removed as virtual account admin when “%{pool_name}” was deleted."

User Groups

User Group Added	
Severity:	MINOR(1)
Message Text:	• "User group “%{user_group_name}” was created."

User Group Updated	
Severity:	MINOR(1)
Message Text:	• "User group “%{user_group_name}” was updated."

User Group Removed	
Severity:	MINOR(1)
Message Text:	• "User group “%{user_group_name}” was removed."

User Group User Removed	
Severity:	MINOR(1)
Message Text:	• "User “%{uid}” was removed from group “%{user_group_name}”."

User Group User Added	
Severity:	MINOR(1)
Message Text:	• "User “%{uid}” was added to user group “%{user_group_name}”."

Local Virtual Account

New Virtual Account	
Severity:	MINOR(1)
Message Text:	• "The Virtual Account “%{pool_name}” was created"

Virtual Account Renamed	
Severity:	MINOR(1)
Message Text:	• "The Virtual Account “%{old_pool_name}” was renamed to “%{new_pool_name}”"

Virtual Account Removed	
Severity:	MINOR(1)
Message Text:	• "The Virtual Account “%{pool_name}” has been deleted"

Virtual Account Disassociated from a SSM On-Prem	
Severity:	MINOR(1)
Message Text:	• "The Virtual Account “%{pool_name}” was disassociated from the On-Prem “%{On-Prem_name}”."

Virtual Account Associated to a Satellite	
Severity:	MINOR(1)
Message Text:	• "The Virtual Account “%{pool_name}” was associated with the On-Prem “%{On-Prem_name}”."

Troubleshooting Smart Software Manager On-Prem

Account Registration Issues

The following is a list of registration issues that can occur in SSM On-Prem with the steps to correct the issue.

1. The Smart Licensing and Manage Local Account options are grayed out on the Licensing workspace.

- You need to request a new account or request access to an existing Account.
- Register it to CSSM Cloud.
- Log back into the Licensing workspace and your Local Account will show up on the upper right-hand side.
- Once a Local Account is created and registered, these options are enabled.

2. I cannot add a user

- Verify that you have the appropriate authentication method configured in the Administration workspace
- If you are using LDAP, the user must log into SSM On-Prem Licensing workspace first before they can be found in the “Add User” screen

3. I cannot register a product

- Verify that you have a token which has not expired
- Verify the URL on the product points to the proper common name or IP address for SSM On-Prem (For details, see Filling the Common Name)

4. When a user logs into the Licensing workspace, they cannot see their SSM On-Prem Local Account

- Ensure the user has been assigned a role for (access to) the Local Account. The available roles are Local Account Administrator, Local Account User, Local Virtual Account Administrator, Local Virtual Account User

5. What ports are used in SSM On-Prem?

- User Interface: HTTPS (Port 8443)
- Product Registration: HTTPS (Port 443), HTTP (Port 80)
- CSSM Cloud: Ensure port 443 (HTTPS) is allowed through your firewall and ensure the following are accessible:
  - cloudsso.cisco.com
    - 173.37.144.211
    - 72.163.4.74
  - api.cisco.com (Prior to 6.2.0)
    - 173.37.145.221
    - 72.163.8.72
  - swapi.cisco.com (6.2.0 and later)

Product Registration Issues

NOTE: A product registration time must fall within the 24-hour window of the SSM On-Prem time. If the registration time is anywhere outside of that time limit. The registration will fail.

If you experience issues with the product registration process, take the following actions:

- Ensure that the On-Prem configuration is correct.
- Verify the Network settings are properly configured.
- Verify the time on the On-Prem is correct.
- Verify that the Call-Home configuration on the client points to the On-Prem.
- Verify the token has been generated from the On-Prem used in the call-home configuration.
- Your firewall settings should allow traffic to and from On-Prem for the following:
  - Product interaction with SSM On-Prem IP address uses ports 443 and 80
    - 443 if using HTTPS
    - 80 if using HTTP
  - User browser to SSM On-Prem IP address uses port 8443

NOTE: Products which support Strict SSL Cert Checking require the hostname for SSM On-Prem to match the “destination http” URL address configured for the product.

Manual Synchronization Issues

If you experience issues with the manual synchronization process, take the following actions:

- Verify the time on the On-Prem is correct.
- Verify the licenses in the associated Local Virtual Account.
- Make sure that you are uploading and downloading the YAML (request and response) files from the correct On-Prem Local Account. You can do this by verifying that the file names include the name of the On-Prem that you are synchronizing.
- You may be requested to re-perform a full manual synchronization after a standard manual synchronization as explained previously.

Network Synchronization Issues

If you experience issues with the network synchronization process, take the following actions:

- Verify that the On-Prem can reach cisco.com.
- Ensure port 443 (HTTPS) is allowed through your firewall and ensure the following are accessible:
  - cloudsso.cisco.com
  - api.cisco.com (Prior to 6.2.0)
  - swapi.cisco.com (6.2.0 and later)
- Verify that the On-Prem can reach the configured DNS server.
- Verify that the time on the On-Prem is correct.

Firewall Warnings on On-Prem Installation and Startup

Docker-related firewall warning messages are the result of internal Docker startup sanity checks. As Docker adjusts the firewall to enable container communication through the firewall, Docker tries to make sure that there are no existing rules before setting up a container. If a rule does not exist, Docker adds the rule and generates a warning message.

These firewall warnings basically show that rules have been added where none existed and do not affect the installation or startup of the application and should be ignored. No action is required.

Getting Support with Global Licensing Operations (GLO)

Cisco provides around-the-clock, award-winning technical support services, online and over the phone to all customers, partners, resellers, and distributors who hold valid Cisco service contracts. To best meet customer's needs, TAC offers a wide variety of support options.

Opening a Case about a Product and Service

Follow these steps these steps to open a support ticket for products and services.

NOTE: Please have your Cisco.com User ID, Contract and Serial number(s) ready when you contact Cisco Support to prevent any delays with your support request.

Step	Action
Step 1	Go to: https://mycase.cloudapps.cisco.com/case
Step 2	Once in the Support Case Manager webpage, keep all the default settings and scroll down the left side of the page and click **Open New Case**. The Service Options pop-up opens on the left side of the screen.
Step 3	Select **Products and Services**.
Step 4	On the right section of the tab screen, click **Open Case**.
Step 5	Make sure the Request Type is set to **Diagnose and Fix**, and then scroll down the screen to the **Bypass Entitlement** field.
Step 6	In the Bypass Entitlement field, select **Software Licensing Issue** from the drop-down list.
Step 7	Click **Next**.
Step 8	In the Describe Problem screen, select the **Ask a Question** for the Severity level.
Step 9	Enter the **Title** and **Description** and all **pertinent information**.
Step 10	Review the information you entered, and then click **Submit Case**. You query has been submitted.

Opening a Case about a Software Licensing Issue

To open a case for software licensing, follow these steps.

NOTE: Please have your Cisco.com User ID, Contract and Serial number(s) ready when you contact Cisco Support to prevent any delays with your support request.

Step	Action
Step 1	Go to: https://mycase.cloudapps.cisco.com/case
Step 2	Once in the Support Case Manager webpage, keep all the default settings and scroll down the left side of the page and click **Open New Case**. The Service Options pop-up opens on the left side of the screen.
Step 3	Select **Software Licensing**.
Step 4	Scroll down and select the **Category** that fits your needs.
Step 5	Click **Open Case**.
Step 7	Enter the **Title** and **Description** and all **pertinent information** in the optional fields. **NOTE**: You can also begin a **chat** using the chat screen on the right side of the screen.

Step 8	Review the information you entered, and then click **Submit Case**. You license query has been submitted.

Smart Software Licensing (software.cisco.com)

Go to Smart Software Manager to track and manage your Smart Licenses.

- Under **"Convert to Smart Licensing"**, you can convert PAK-based licenses to Smart Licenses (if applicable)

Smart Accounts

Go to the **Administration** section of Cisco Software Central to manage existing Smart Accounts or to request a new account from the choices.

- Go to Request Access to an Existing Smart Account for access to your company's account.
- For training and documentation click here.

Enterprise License Agreements (ELA)

Go to the ELA Workspace to manage licenses from ELA.
Other self-serve licensing functions are available. Please go to our Help page for how-to videos and other resources.
For urgent requests, please contact us by phone.
To update your case, either send attachments or updates to attach@cisco.com and include the **case number** in the Subject line of your email. Please **do not** include licensing@cisco.com in your email with the engineer.

Appendix

A1. Manually Backing Up and Restoring SSM On-Prem

CAUTION: When SSM On-Prem is associated with High Availability (HA), you must backup and restore both the databases on the **active node**.

SSM On-Prem supports on-demand backup and restore operations. These operations allow you to backup and later restore the On-Prem to a prior operational state or migrate data from one system to a new deployment.

Backing Up SSM On-Prem Release 6.x

You can initiate an on-demand Backup at any time by performing the following procedure.

Step	Action
Step 1	From the CLI, login in to SSM On-Prem via shell.
Step 2	Elevate your permissions using the command: `sudo -s`

Step 3	Next, run this command: `docker exec -it db /bin/bash`
Step 4	Inside the container, run this command: `pg_dumpall -c -U postgres > /var/lib/postgresql/data/atlantis_complete_backup`
Step 5	Exit the container and verify the backup with this command: `ls -l /var/data/atlantis_complete_backup`

Step 6	Backup the certificates on the host using this command:
	`cd /home/deployer/ssl`
	`tar -zcvf atlantis_certificates_backup.tar.gz *`

NOTE: While it's possible to leave the backup files:

`atlantis_complete_backup and`
`atlantis_certificates_backup.tar.gz;`

on the SSM On-Prem it is recommended they be copied from SSM On-Prem and moved to a secure storage location of your choosing.

Restoring SSM On-Prem Release 6.x

CAUTION: When SSM On-Prem is associated with HA, you must both backup and restore the database on the active node.

The Restore action allows you to return an On-Prem to a previous operational state or migrate data from one system to a new one system running the same version. The Restore operation requires you to use a previously downloaded backup file. (See Backing Up SSM On-Prem 6.x)

NOTE: A system restart and synchronize is required when the Restore is complete.

Before you begin a Restore, you must **copy** prior backup files onto the SSM On-Prem, if they were copied off as part of the Backup process above. (See Backing Up SSM On-Prem 6.x) Complete these steps to restore SSM On-Prem 6.x.

Step	Action
Step 1	Login to SSM On-Prem via shell in the admin role.

Step 2	Elevate your permissions using the command: `sudo -s`
Step 3	Stop All containers and make sure that backend, frontend, redis, ipv6nat, db, and gobackend containers are stopped by using this command: `DOCKER_ORG=atlantis-docker BUILD_ENV=prod TMP=/var/tmp /usr/local/bin/docker-compose -f /home/deployer/atlantis/docker-compose-up.yml stop backend frontend gobackend redis ipv6nat`
Step 4	Verify only the database container is running and verify the name of the database container: `docker ps`
Step 5	Then run this command as sudo: `docker exec -it <container name> /bin/bash`
Step 6	In the container, run the following command: `psql -f /var/lib/postgresql/data/atlantis_complete_backup -U postgres`
Step 7	After completion, exit the container.
Step 8	Stop the db container: `DOCKER_ORG=atlantis-docker BUILD_ENV=prod TMP=/var/tmp /usr/local/bin/docker-compose -f /home/deployer/atlantis/docker-compose-up.yml stop db`
Step 9	Verify the DB container has stopped by running this command:
Step	**Action**
	`docker ps`

Step 10	Restore the certificates from the backup process:
	`cd /home/deployer/ssl`
	`tar -xvf atlantis_certificates_backup.tar.gz`

Step 11	Run this command on the host: `chown -R deployer:deployer /home/deployer/ssl` Then verify ownership.
Step 12	Start the application by running this command: `systemctl start On-Prem`

Backing Up the SSM On-Prem Release 8

You can initiate an on-demand backup and restore to the same version at any time by performing the following manual procedure (Available in Version 7-201907 or later releases).

Step	Action

Step 1	From the CLI, login in to SSM On-Prem via shell with this command. `$ onprem-console`

Step 2	Next, select the destination for the backup and type this command to begin the backup:
	`database_backup`
	The format should look similar to this:
	`Database_backup`
	`[sudo] password for admin:`
	`Get confirmation:`
	`Database successfully backed up to [destination directory]:`
	`/var/files/backups/oneprem-8-202004-2020032016822.sql.gz`

Step 3	Select the **destination** for the backup file (gzip) and copy the file to that destination (see note below).
Step 4	Exit the application.

NOTE: While it's possible to leave the backup files:

```
atlantis_complete_backup and
atlantis_certificates_backup.tar.gz;
```

on the SSM On-Prem it is recommended they be copied from SSM On-Prem and moved to a secure storage location of your choosing

Restoring the SSM On-Prem 7-201907 Release

NOTE: If the backup file is remote, you will need to first copy the backup file into the On-Prem Console backups directory.

CAUTION: The 7-201907 version was built with partitions that do not allow SSM On-Prem essential processes to work properly. Therefore, if you have deployed a fresh 7-201907 version you need to install on a new On-Prem Server from the 8-201908 version, then use the back-up/restore procedure for Release 8-201908.
Because you cannot change partitions on a running server, the upgrade script cannot fix this incompatibility issue. If you don't use the procedure shown here, you will continue to have issues with installing future versions.

Backup and Restore Procedure for only Release 8-201908

Step	Action
Step 1	Backup **current system** as precaution.
Step 2	Patch the system to the new release.
Step 3	Create a **backup** of the new release database.
Step 4	Redeploy a **fresh new release** (redeploying the release fixes the partition size incompatibility).
Step 5	Restoring the **database backup created in Step 3** to the fresh installation.

Restoring the SSM On-Prem Release 8

NOTE: Do not use this backup/restore procedure using 8-201908. Release 8-201908 has a specific procedure described in Backup and Restore Procedure Release 8-201908.

NOTE: If the backup file is remote, you will need to first copy the backup file into the On-Prem Console backups directory.

Backup and Restore Procedure

Step	Action
Step 1	From the CLI, login in to SSM On-Prem via shell with this command. `$ onprem-console`
Step 2	Copy the remote backup file to the On-Prem server and enter the administrator password when prompted as well as the user password on the remote server. `>> $ copy username@remote.server.com:/path_to_file backups:oneprem-8-202004-2020032016822.sql.gz`
Step 3	List the files in the On-Prem Console backups directory using this command: `>> dir backups: /var/files/backups/oneprem-8-202004-2020032016822.sql.gz`
Step 4	Restore database from a backup file using this command: `>> database_restore backups:oneprem-8-202004-2020032016822.sql.gz`
Step 5	Exit the application.

NOTE: Once registered and restored, an SSM On-Prem must be synchronized with Cisco Smart Software Manager.

A2. Product Compatibility Notice

Before the SSM On-Prem can accept registrations from product instances, it must register with CSSM Cloud. Previously, SSM On-Prem to CSSM Cloud registration required a 10-day wait because someone had to manually sign the Certificate Signing Request (CSR) from On-Prem to CSSM Cloud. This meant that if products wanted to connect to On-Prem, they had to wait 10 days for SSM On-Prem to be fully registered and functional.

The manual signing of the CSR has been automated so that the CSR from SSM On-Prem to CSSM Cloud is now signed immediately. However, there are changes that must be made to the product smart agents, SSM On-Prem and CSSM Cloud, for this trust chain to work in an automated way. The previous trust chain consisted of 3 levels of certificates (3-tier) from the device to SSM On-Prem to CSSM Cloud. In the new implementation to automate the trust chain validation, additional certificates were added, and you have 4-levels of certificates (4-tier). These changes must also be backward compatible so that older devices that do not have this updated level of smart agent, SSM On-Prem, and CSSM Cloud code would continue to function.

In the new implementation, smart agents, SSM On-Prem, and CSSM Cloud must exchange a new message type to know if it supports a 3-tier or 4-tier certificate. Products that have not implemented the latest smart agent code (1.4+) for registering with SSM On-Prem must wait 10 days as SSM On-Prem needs to get the 3-tier certificate from CSSM Cloud before it can register the product. Product teams can decide to implement Smart Agent code 1.4+ at their own schedules, so you don't always know what version of Smart Agent they embed. At the time of this writing, these 3-tier products are listed below. To know what version of the Smart Agent you have, issue the command:

```
"license smart status".
```

These are the following cases:

- **Devices with new Smart Agent registering to the latest On-Prem release**
  Devices that have implemented the latest Smart Agent code register successfully with latest SSM On-Prem using multi-tier certificate hierarchy.
- **Devices with new Smart Agent registering to a back-level On-Prem**
  Devices that have implemented the latest Smart Agent code dynamically validate the certificate chain (from device to On-Prem to Cisco Admin).
- **Devices with old Smart Agent registering to the latest On-Prem release**
  When you install the latest SSM On-Prem release, its registration with CSSM Cloud is instantaneous. During this process, the SSM On-Prem also requests a previous 3-tier certificate. When devices with older Smart Agent register with the SSM On-Prem, you get a registration failure message that informs you to wait 10 business days and perform a network or manual synchronization to get the backward compatible (3-tier) certificate and re-register. Afterwards, these devices can successfully register to the SSM On-Prem.

In this case, as HTTPS is used for device-to-SSM On-Prem communication, you need to complete the following steps:

Step	Action
Step 1	Ensure that the Smart Call-Home profile uses HTTPS as the transport.
Step 2	After the SSM On-Prem (with the multi-level certificate hierarchy function) registers successfully to CSSM Cloud, the product instance (with back-level smart agent) which tries to register with On-Prem fails with the following error message: "Compatibility Error: The On-Prem is not currently compatible with the Smart Licensing Agent version on this product. If it has been 10 days since the On-Prem was registered, synchronize the On-Prem with Cisco's licensing servers to enable compatibility with older agent versions and then try the registration again."
Step 3	Wait for **10 business** days.
Step 4	Run an **on-demand network** or **manual sync** between On-Prem and CSSM Cloud.
Step 5	Re-register **the product instance** to SSM On-Prem.

If you perform a fresh 3.1.x SSM On-Prem installation, after registration and upon logging, you will see the following message:

> **Version Compatibility Note**: Temporarily, this On-Prem will only be able to register Product Instances that are using the Smart Licensing Agent version 1.5 or later (use the "show license" commands on the Product Instance to see the agent version). To enable registration of Product Instances using older versions of the agent, wait two business days after the On-Prem's initial registration and then synchronize the On-Prem.

This version compatibility note means that a cert request can take 2 to 10 business days to be processed. The three-tier certificate will be obtained by On-Prem from CSSM Cloud during the sync to support three-tier smart agents.

Following are the current 3-tier agents:

Smart Agent C			
Product	**Product Version**	**Agent Version Supported**	**POC**
ASAv	9.9.1	1.6.14_rel/129	Hidde Beumer (hibeumer)
FMC	6.2.2	1.6.14	Vineet Jain (vinjain)
CBR8	IOS XE 3.15	1.5	Scott Raaf (raafs)
Cisco 5921 (ESR)	15.6(3)M1	1.6.10_rel/106	Ahmed Abu Sharkh (ahmabush)
Smart Agent Java			
Product	**Product Version**	**Agent Version Supported**	**POC**
vCUSP	9.1.7	1.3	John Vickroy (jvickroy)

A3. Product Registration Example: Cisco Cloud Service Router (CSR)

For complete instructions for configuring the **Cisco Cloud Service Router (CSR)** product instance to communicate with SSM On-Prem, see the CSR Smart Licensing configuration: http://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/csr1000Vswcfg/licensing.html

For a specific product, please use this URL:

https://www.cisco.com/go/smartlicensing

NOTE: A product registration time must fall within 24-hours of the current SSM On-Prem server time either ahead or behind. If the registration time is anywhere outside of that time limit, the registration will fail.

Then, select the product you need from the drop-down list from the **View Smart License document by product** section of the screen.

To get your transport gateway:

In the Smart Licensing Workspace go to **Inventory >General** and then within the Product Usage Registration Tokens section, click either the **Smart Transport Registration URL**, **CSLU Transport URL**, or **Smart Call-Home Registration URL** (see the Product Instance Registration Tokens section located under the Inventory Tab for more information).

For products that use CSLU as transport, click the **CSLU Transport URL**

Copy the **URL** to your browser.

Ensure you have the following commands configured in the respective router platforms:

- For IOS-XR platforms:

```
Crl optional
```

- For IOS/XE platforms:

```
use revocation-check none
```

Sample Smart Transport to Use SSM On-Prem on the Cloud Service Router

These are the steps you would complete to configure a CSR.

Step	Command	Action
Step 1	Enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	Configure terminal	Enters global configuration mode.
Step 3	License smart utility	no device(config)# license smart utility
Step 4	License smart transport URL	device(config)# license smart transport smart.
Step 5	License smart registration	no device(config)# license smart url https://server/path

Step	Command	Action
Step 6	Exit	Saves and exits the current configuration mode and returns to privileged EXEC mode.
Step 7	End	Returns to privileged EXEC mode.
Step 8	wr	Saves the configuration.

Sample Smart Call-Home Profile to Use SSM On-Prem on the Cloud Service Router

Sample Procedure

Step	Command	Action
Step 1	enable	Enables privileged EXEC mode. Enter your **password** if prompted.
Step 2	configure terminal	Enters global configuration mode.
Step 3	call-home	Enters call-home configuration mode.
Step 4	contact-email-addr (email address)	Enters the contact email address.
Step 5	Profile_Cisco TAC-1	Specify the profile name **Cisco TAC-1** is the default profile.
Step 6	Destination transport http Or Destination transport https	Sets the **transport** to HTTP or HTTPS. Additionally, depending on your choice, use either **example a** (for HTTP) or **example b** (for HTTPS) below. a. For destination address http use http from TG to access the SCH the Transport Gateway URL. **NOTE**: The destination URL is: http://<ip-address>:80/Transportgateway/services/DeviceRequestHandler. b. For destination address https use https from TG to access the Transport Gateway URL. **NOTE**: The destination URL is: https://<ip-address>:443/Transportgateway/services/DeviceRequestHandler
Step 7	Destination command	no destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
Step 8	active	Activates the **profile** specified in step 5
Step 9	Exit	Saves and exits the **current configuration mode** and returns to privileged EXEC mode.
Step 10	End	Returns to **privileged EXEC mode**.
Step 11	wr	Saves the **configuration**.

The following configuration is only a sample for CSR for HTTP. Please see platform specific configurations for the call-home profile config.

Example:

```
Router#configure terminal
Router(config)#call-home
Router(cfg-call-home)#profile CiscoTAC-1
Router(cfg-call-home-profile)#destination address http
https://172.19.76.177:80/Transportgateway/services/DeviceRequestHandler
Router(cfg-call-home-profile)#no destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

The following configuration is only a sample for CSR for HTTPS. Please see platform specific configurations for the call-home profile config. Starting with CSSM On-Prem 3.0.x port # and URL are not needed.

Example:

```
Router#configure terminal
Router(config)#call-home
Router(cfg-call-home)#profile CiscoTAC-1
Router(cfg-call-home-profile)#destination address http
https://172.19.76.177:443/Transportgateway/services/DeviceRequestHandler
Router(cfg-call-home-profile)# no destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

For ASR9K and CSR, ensure you remove the URL for CSSM Cloud as follows:

no destination address http: https://tools.cisco.com/its/service/oddce/services/DDCEService

Add the URL for On-Prem and the following command:

```
Destination address https://<host common name>:
443/Transportgateway/services/DeviceRequestHandler
```

A4. Setting up ADFS and Active Directory (AD) Groups and Claims

The following procedures are specifically for setting up AD and ADFS for SSM On-Prem.

To configure AD groups and claims for Microsoft Windows Server 2019 and 2012, follow the procedures described in the Windows 2019 and 2012 sections.

Configuring ADFS and Active Directory (AD) Groups and Claims for Windows 2019 Server

For specific constraints to enable ADFS and generate bearer tokens, see Generating Bearer Tokens.

Prerequisites

NOTE: You must make sure that On-Prem is synchronized with the NTP server. See configuring the Time Settings Tab under the Administration Workspace Setting Widget.

- Before you begin to configure the Windows 2019 server, make sure you have the Service Provider Redirect URI, located in the ADFS Configuration Tab.

Step	Action
Step 1	Log into the Windows 2019 server on your system. Navigate to **Service Manager > Tools**. (The Tools menu is located on the right side of the screen.)
Step 2	From the Tools menu, select **AD FS Management**. The AD FS screen opens.
Step 3	In the left panel, select **Application Groups**.
Step 4	In the right panel click **Add Application Group...** The Add Application Group Wizard opens.
Step 5	In the Wizard, enter a **Name** in the Name field.
Step 6	(Optional) Enter a **Description** of the application group.
Step 7	In the Template Window under the Client-Server application section, select the **Server application accessing a web API** option and then click **Next**.
Step 8	Use the default **Client Identifier value** to be used for the client_id. (**Hint:** The Client ID value that you documented in the OAuth2 ADFS Configuration screen in the Access Management Widget.)
Step 9	Enter the **Redirect URI** (obtained from the Service Provider Redirect URI field in ADFS Configuration Tab in On-Prem shown in the next line). https://<fqdn/ip>:8443/backend/auth/adfs/callback **NOTE**: After successful login to On-Prem, the ADFS will redirect to the URL you just entered.
Step 10	Click **Add** (the URL is added to the list field), and then click **Next**. The Configure Application Credentials screen opens.
Step 11	**Select** the **Generate a shared secret** option and then click **Next**. **NOTE**: You do not have to enter a secret, just make sure that the section is selected.
Step 12	Enter a **String** into the Identifier field, and then click **Add**. Then click **Next**. The Choose Access Control Policy screen opens. **NOTE**: This Identifier string is located in the OAuth2 ADFS Configuration field in the Access Management Widget. It will be used for the **resource name**.
Step 13	Select the **Access Control Policy** that you want to use. **NOTE**: Use the **Default** policy (to permit everyone) if you don't know what policy to use, and then click **Next**. The Configure Application Permissions screen opens.
Step 15	In the Configure Application Permissions screen, select the following check boxes: • **allatclaims** • **email** • **openid** Click **Next**. The Summary screen opens. Review the screen, and then click **Next**, and then click **Close**.

Mapping Claims to Roles in On-Prem

NOTE: On-Prem cannot accommodate role differentiation across multiple groups. For example, if there are two groups such as, Group A and Group B, and if a user belongs to both groups, but has different role designations, such as SYSADMIN and SYSUSEDR, the system will only designate SYSUSER privileges when the user logs into the system. See Step 11 in Mapping Claims to Roles.

Once you have set up an AD Group, the next step in the configuration process is to map claims to On-Prem. Complete these steps to map claims to On-Prem Roles.

Step 1	Navigate to **Server Manager Tools > AD FS Management**.
Step 2	Click **Application Groups**, and then select the newly configured **application group**.
Step 3	In the right-hand section, click **Properties**. The Application Group Properties screen opens.
Step 4	Click the **Web API** for the application group and click **Edit**.
Step 5	Select the **Issuance Transform Rules** tab.
Step 6	Click **Add Rule...**
Step 7	Select **Send Group Membership as a Claim**, and then click **Next**.
Step 8	Enter a **Name** in the Claim Rule Name field.
Step 9	Click **Browse...** and then select an **AD Group Name**.
Step 10	Select **Role** for the Outgoing claim type.
Step 11	Enter **one of the claims** listed here into the **Outgoing Claim Value** field (such as ONPREM-SYSUSER). For example: • ONPREM-SYSADMIN: Maps to System Admin Role • ONPREM-SYSOP: Maps to System Operator Role • ONPREM-SYSUSER: Maps to System User Role **NOTE**: Once you have mapped ONPREM-SYSADMIN role, repeat steps 6-11 to map the other roles.
Step 12	Click **Finish** and then click **OK**. The application group configuration is complete. Follow the steps in Assigning a User with a Claim.

Assigning a User with a Claim

Follow these steps to associate a user with a claim.

Step 1	Select **Server Manager Tools**.
Step 2	Select **Active Directory User** and **Computer**.
Step 3	In the left panel, select **Users**.
Step 4	In the right panel, select the desired **User** and click **Properties**.
Step 5	Select the **Member Of** tab to open the Select Groups screen.
Step 6	Click **Add** and click **Check Names** and search for the **ONPREM role** want.
Step 7	Select the **Role** you want. **NOTE**: Only one role can be supported.
Step 8	Once you have selected the role, click **OK**. The role is added to your ADFS configuration.
Step 9	Next, follow the steps outlined in **Next Steps in Configuring the Windows 2019 Server**.

Next Steps in Configuring the Windows 2019 Server

The next stage in configuring the Windows 2019 server is to:

1. Log into **On-Prem**.
2. Navigate to the **Administration Workspace**.
3. Navigate to the ADFS Configuration Tab and enter the appropriate information into the ADFS using these steps. (See Step 13 for the resource name.)

NOTE: Make sure that you select the **v4** for Windows 2019 option.

NOTE: To get an explanation of the field, hover your cursor over the field which opens a tooltip that explains the function of the field. All the fields that have an [*] are required fields.	
Step 1	Select **Access Management > OAuth2 ADFS Configuration**.
Step 2	At the top left corner of the pane, enable **OAuth2 ADFS Secondary Authentication**. (Default setting is Disabled) **NOTE**: Once OAuth2 ADFS is enabled, a prompt opens under the field stating that OAuth2 ADFS is enabled and to use any other LDAP authentication process OAuth2 ADFS authentication must be disabled. As soon as the OAuth2 ADFS setting is enabled, all other tabs (LDAP Config, SSO Client, etc.) are disabled.
Step 3	(Optional) If you are establishing TLS connections to your server, select **Verify Server Certificate** to verify that the verification of the server's certificate was signed by a trusted CA or by a custom CA that was uploaded. By enabling this option, communication to the remote server will go over TLS which requires that the certificate is trusted. Go to Adding a CA Certificate for more information. This **NOTE**: This is a default setting for all new installations but needs to be activated for all existing customers.
Step 4	Enter the **ADFS Server URL**. (Host Name, FQDN, IPv4, or IPv6 must begin with https:// or http://)
Step 5	Select the **mode** of ADFS mode you are using: • ADFS V4 Mode: Allows ADFS on Microsoft Server 2019 • Import Claims: When enabled this option allows ADFS user claims to be mapped to SSM On-Prem user claims.
Step 6	Enter the **ADFS Resource Name**. (A unique name in your organization that is used to identify the ADFS server.) Copy this **value** from your ADFS server's Relying party identifier field. (Add step)
Step 7	Enter the **Client ID**. (Copy the unique ID that you configured in your ADFS server into this field.)
Step 8	Copy the **Service Provider Redirect URI** (read-only field) to your ADFS server's Redirect URI field. **NOTE**: This URI is generated by assuming that you are logged into the same SSM On-Prem URL used by your users.
Step 9	Click **Save**.

4. Once you have configured for OAuth2 ADFS, **logout of On-Prem**.
5. Open **On-Prem** and in the authentication page, click **Login Using OAuth2 ADFS** on either Workspace (License or Administration). You are redirected to On-Prem using ADFS configuration.
6. Log into On-Prem by entering your **User Name** and **Password**.

Configuring ADFS and Active Directory (AD) Groups and Mapping Claims for Windows 2012 Server

For specific constraints for enabling ADFS and generating bearer tokens, see Generating Bearer Tokens.

Prerequisites

NOTE: You must make sure that On-Prem is synchronized with the NTP server. See configuring the Time Settings Tab under the Administration Workspace Setting Widget.

When you are configuring the Windows 2012 server, make sure that the **Service Provider Redirect URI** is accessible. It is located in the ADFS Configuration Tab under the field.

NOTE: Windows 2012 Server supports only letters, numbers, and underscores, **no spaces**.

Step	Action
Step 1	Open your **Windows 2012 server**.
Step 2	Open the **Powershell terminal**.
Step 3	Enter the following: **Add-AdfsClient -ClientId "clientId"** -Name "**name**" -RedirectUri "**Error! Hyperlink reference not valid.**" -Description "description"
Step 4	Open the **Server Manager Application** and from the toolbar, select **Tools > AD FS Management**. The Wizard window opens.
Step 5	In the left panel, expand **Trust Relationships** (by clicking the little triangle to the left of the heading) and select **Relying Party Trusts**.
Step 6	In the right panel, click **Add Relying Party Trust...** the Add Relying Party Trust Wizard opens at the Welcome screen.
Step 7	Click **Start**.
Step 8	Select the option entitled: **Enter data about relying party manually**, and then click **Next**.
Step 9	Enter the **Display Name** and then click **Next**. **NOTE**: This name must be the same as the name you entered in the Powershell ClientId. The Choose Profile screen opens.
Step 10	Select the "**AD FS profile**" option and then click **Next**.
Step 11	Skip the next screen by clicking **Next**.
Step 12	Leave all check boxes **blank** (default setting) in the next screen and click **Next**.
Step 13	In the Relying party trust identifier field enter the **ADFS resource identifier** name click **Add**. The resource identifier is added to the list section.

Step	Action
	NOTE: The resource identifier name will be your **ADFS Resource Name** in the On-Prem ADFS Configuration Screen. See OAuth2 ADFS Configuration Tab for details. **NOTE**: On-Prem has field restrictions, so when creating the resource identifier name, make sure they contain only letters, numbers, and underscores. If the two names are not the same, you will receive a login error when you try to log using the ADFS mode. Click **Next**.
Step 14	Select the **I do not want to configure multi-factor authentication...** option. Click **Next**.
Step 15	Make sure the **Permit all users to access this relying party** option is selected and then click **Next**.
Step 16	Leave all the options/tabs in the Metadata screen blank (default). Click **Next**.
Step 17	Confirm that the **Open the Edit Claims Rules dialog...** option is **selected**.
Step 18	Click **Close**. The Edit Claim Rules for Roles screen opens, and you can begin to enter roles for mapping claims.

Mapping Claims to Roles in On-Prem

NOTE: On-Prem cannot accommodate role differentiation across multiple groups. For example, if there are two groups such as, Group A and Group B, and if a user belongs to both groups, but has different role designations, such as SYSADMIN and SYSUSEDR, the system will only designate SYSUSER privileges when the user logs into the system. See Step 3 in in Mapping Claims.

Once you have set up an AD Group, the next step in the configuration process is to map claims to On-Prem. Complete these steps to map claims to On-Prem Roles

Step 1	**Entering First Claim Rule** From the Edit Claim Rules for Roles screen, begin the procedure to enter the first claim rule: a. In the Issuance Transform rules tab, click **Add Rule** to add a claim rule. The Add Claim Rule screen opens. b. Confirm that the Rule template is: **Send LDAP Attributes as Claims** c. Enter a **Claim Rule Name**. d. In the Attribute store field, select **Active Directory** from the drop-down menu. e. In the Mapping table LDAP Attribute field select **User-Principal-Name** option. f. In the Outgoing Claim Type field select **UPN**.
Step 2	Click **Finish**. The Edit Rules screen opens again.
Step 3	**Entering Second Claim Rule for On-Prem role** To enter the second claim rule: a. Click **Add Rule...** to add a second claim rule. b. Select the **Send Group Membership** as a Claim option. Click **Next**.

	c. Enter another **Claim rule name**. d. In the User's Group field, click **Browse**... and select an appropriate **AD Group** for the ONPREM Role. e. From the Outgoing Claim Type, select the **Role** option from the drop-down menu. f. In the Outgoing Claim Value field, enter an **appropriate Claim Value** listed in Sub step g). g. Enter **one of the claims** listed here into the **Outgoing Claim Value** field (such as ONPREM-SYSUSER). • ONPREM-SYSADMIN: Maps to System Admin Role • ONPREM-SYSOP: Maps to System Operator Role • ONPREM-SYSUSER: Maps to System User Role
Step 4	Click **Finish**. **NOTE**: Repeat all the sub steps in step 3 to map more roles.
Step 5	Return to the Powershell command line and enter the following: Set -AdfsRelyingPartyTrust-TargetName "**name**"-EnableJWT $true

Next Steps in Configuring the Windows 2012 Server

The next stage in configuring the Windows 2012 server is to:

1. Log into **On-Prem** and open **Administration Workspace**.
2. Navigate to the ADFS Configuration Tab and enter the appropriate information into the ADFS using these steps.

NOTE: Make sure that you select the v3 for Windows 2012 option.

NOTE: To get an explanation of the field, hover your cursor over the field which opens a tooltip that explains the function of the field. All the fields that have an [*] are required fields.	
Step 1	Select **Access Management > OAuth2 ADFS Configuration**.
Step 2	At the top left corner of the pane, enable **OAuth2 ADFS Secondary Authentication**. (Default setting is Disabled) **NOTE**: Once OAuth2 ADFS is enabled, a prompt opens under the field stating that OAuth2 ADFS is enabled and to use any other LDAP authentication process OAuth2 ADFS authentication must be disabled. As soon as the OAuth2 ADFS setting is enabled, all other tabs (LDAP Config, SSO Client, etc.) are disabled.
Step 3	(Optional) (Optional) If you are establishing TLS connections to your server, select **Verify Server Certificate** to verify that the verification of the server's certificate was signed by a trusted CA or by a custom CA that was uploaded. By enabling this option, communication to the remote server will go over TLS which requires that the certificate is trusted. Go to Adding a CA Certificate for more information. **NOTE**: Selecting Verify Server Certificate automatically checks the verification authenticity of the peer's certificate.

	NOTE: If you disable certificate verification compromises the security of the communication. Just having encryption on a transfer does not ensure that you are communicating with the correct endpoint.
Step 4	Enter the **ADFS Server URL**. (Host Name, FQDN, IPv4, or IPv6 must begin with https:// or http://)
Step 5	Select the **mode** of ADFS mode you are using: • ADFS V3 Mode: Allows ADFS on Microsoft Server 2012 • Import Claims: When enabled this option allows ADFS user claims to be mapped to SSM On-Prem user claims.
Step 6	Enter the **ADFS Resource Name**. The is the name entered in Step 13 of the Windows 2012 configuration procedure.
Step 7	Enter the **Client ID**. (Copy the unique ID that you configured in your ADFS server into this field.)
Step 8	Click **Save**.

3. Once you have configured for OAuth2 ADFS, **logout of On-Prem**.
4. Open **On-Prem** and in the authentication page, click **Login Using OAuth2 ADFS** on either Workspace (License or Administration). You are redirected to On-Prem using ADFS configuration.
5. Log into On-Prem by entering your **User Name** and **Password**.

Implementing ADFS and Generating Bearer Tokens

When implementing ADFS (using Microsoft Windows Server 2012 or 2019) all bearer tokens must be created by a user with a System Administrator role. If any other user role trying to generate a bearer token, an error occurs with the following statement:

```
We're sorry, but something went wrong (500).
```

A5. Events that Trigger Email Notifications

The following is a list of events that would trigger an email notification.

- User Group Created
- User Group Deleted
- User Group Member Added
- User Group Member Removed
- User Group Send Message
- License Pool removed
- Account Deactivated
- Account Reactivated
- Account Request Pending
- Account Request Accepted
- Account Request Rejected

- User Role Modified
- User Password Expiration Notification
- Activation of the code for resetting a password
- Notification of password update

A6. SL Using Policy Initiated Collect Method Descriptions

The table below provides the protocol, reference documentation, and transport information for each of the SL Using Policy-initiated collect methods used.

Network Management Protocol	Reference	Additional information
NETCONF	rfc6241	Transport: SSH. Requires configuring SSH and Netconf.
RESTCONF	rfc8040	Transport: HTTP, HTTPS. Requires configuring HHTP/HTTPS server, Restconf.
Native REST	Cisco Proprietary	Transport: HTTP, HTTPS. Requires configuring HHTP/HTTPS server. Some devices may enable HTTP server by default.

A7. Default Data Transfer Intervals

By default, SL Using Policy is scheduled to transfer usage data with Cisco or Product Instance(s) at specific intervals. Listed here are the usage data intervals:

- Retrieve Usage Data from Product Instances: 60-day intervals
- Importing Usage Data to Product Instances: 5-minute intervals

NOTE: On-Prem provides an additional method of manual synchronization. To set synchronization schedules or manually trigger a synchronization for getting Usage Reports, see Usage Schedules

A8. Configuring TACACS+ Through CLI

Complete these steps to configure your On-Prem server for TACACS+ authentication using the CLI.

NOTE: The tacacs_config command requires administrator (sudo) privilege to invoke it.

Step	Action
Step 1	Log into the CLI by typing the Linux administrator's command **ssh**. Then use the On-Prem-console command.
Step 2	Once in the On-Prem console to configure the TACACS+ server, type the command **tacacs_config**. and then, when prompted, enter in the **password**.
Step 4	Select option **#1** (server details) to configure the primary TACACS server. **NOTE**: To configure a secondary server, select **option #2** and complete steps 5-9 a second time. **NOTE**: Option **#5** (Enable/Disable TACACS provides a means of disabling a configured server (primary or secondary) without deleting the configuration. You can enable a disabled server by selecting **Option #5**. The server is enabled without having to reconfigure it. (Option #5 changes functionality according to the state of the server. If a server is disabled using Option #5, you can enable it by selecting Option #5 again.)
Step 5	Enter the **ip/hostname** (IP Address or Hostname) for the primary server.
Step 6	Enter the **shared secret** for connecting to the TACACS primary server. **NOTE**: When you create the shared secret, you cannot use these three characters. The system will give you an error message. • Space: " " • Hash sign: "#" • Backslash: "\"
Step 7	Select the authentication method (PAP, CHAP, ASCII) for connecting to the TACACS primary server. Enter **yes** to proceed with the configuration process. **NOTE**: Once the configuration is confirmed, the configuration saved is successful. **NOTE**: At this point, you can select option **#3** to display the configuration parameters for the server.
Step 8	Next, select option **#4** (User management) for user management. **NOTE**: When you select option #4, a banner opens on the screen that Linux requires a local linux user account that matches the tacacs+ username for all required users.
Step 9	Next, select **option #1** (Add local TACACS users). You can add multiple users by separating each user with a **comma** (**,**). After entering all the users, press **Enter** to complete the user management process. To return to the main menu, select **option #4** (back).
Step 10	When the configuration process has completed, select **option #6** to quit the on-prem console. Then you can logout of the On-Prem server. **NOTE**: At this point, you can log into the server as a TACACS user and access the functionality of On-Prem based on your authorization level, configured on TACACS server.
Step 11	If you are configured as a TACACS admin (privilege level 15) in the TACACS server, you can utilize all the functionality of on-prem. However, if you are configured as a normal TACACS user (privilege level < 15) in TACACS server, you can utilize the on-prem console functionality that does not require sudo permission.

A9. SL Using Policy Table Alerts and Errors

Alert	Description
error_discovery_delete	Error deleting information from discovery
error_discovery_invalid_host	Host is empty or invalid
error_cssmconn_get	Error downloading data with CSSM connector API
invalid_sa_va_cssm	Connection to CSSM failed: Invalid SA/VA
error_discovery_get_host	Error getting information from discovery - host parameter is missing
error_core_notification_api	Error handling notification API
error_cssmconn_accounts	Error getting accounts with CSSM connector API. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
error_cssmconn_summary	Error downloading account summary with CSSM connector API. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
error_storage_add	Failed to add to storage
usage_report_cssm	Usage report uploaded to CSSM
pi_not_https	Unable to connect. Please configure HTTPS on the product instance
error_core_listener_api	Error handling listener API
error_cssmconn_poll	Error handling CSSM connector Poll. Please make sure provided POLL ID is correct if querying for a specific POLL ID
error_export	Error exporting data to offline file. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
policy_request_cssm	Policy request sent to CSSM
error_discovery_load	Error loading information in discovery
error_start_scheduler	ailed to start scheduler
usage_report_ack_pi	Usage report acknowledgement to product instance
policy_request_pi	Policy requested by product instance
error_cssmconn_auth_return	Error returning authorization code with CSSM connector API. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
error_cssmconn_auth_request_post	Error downloading authorization code with CSSM connector API. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
error_oauth_token	Error getting new OAuth access token. Previous token is invalid. Login with credentials needed
dlc_request_pi	DLC requested by product instance

Alert	Description
error_cssmconn_auth_confirm	Error confirming authorization code with CSSM connector API. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
error_oauth_post	Error generating OAuth access token, CCO credential needed
error_oauth_login	Error login with CCO credential
usage_report_pi	Usage report from product instance
error_core_tenant_conf_get	Error getting tenant configuration
error_cssmconn_error_polling	Error occurred during polling for a response from CSSM. Either received status failed or reached 60 seconds time limit. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
error_oauth_delete	Error revoking OAuth access token
error_stop_scheduler	Failed to stop scheduler
piconn_comm_err	Device operation failed
error_core_conf_api	Error handling configuration API
error_core_tenant_conf_empty_sa_va	Configuration Error: Smart Account Name and Virtual Account Name must be specified
rror_rum_ack_read	Failed to read rum acknowledgement
piconn_pull_data	Failed to fetch data from the product instance
error_cssmconn_auth_code	Error requesting/polling authorization code with CSSM connector API. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
va_not_found	Virtual Account is not found
error_piconn_pull	Error pulling data from product instance
host_not_found	Device Host is not found
error_export_empty	No data pending for exporting data to offline file
usage_report_ack_cssm	Acknowledgement received from CSSM
dlc_ack_pi	DLC acknowledgement to product instance
error_core_conf_get	Error getting configuration
login_again	User session with CSSM is unauthorized. OAuth token is invalid. Please login again
error_discovery_get	Error getting information from discovery
method_not_allowed	Method not allowed
error_core_compose_auth_request_post	Error handling cssmconn auth-request API with CSSM connector API. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
error_piconn_api	Error handling PI connector API

Alert	Description
error_import_auth	Error importing authorization code. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
data_not_found	Data Not Found - no data found for the request
error_cssmconn_pi_delete	Error deleting product instance with CSSM connector API. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
error_discovery_store	Error storing information in discovery
udi_missing	UDI information is required for the operation but is missing or invalid
error_core_tenant_conf_add	Error adding tenant configuration
error_data_type	Invalid data type
error_policy_write	Failed to write policy
error_cssmconn_rum_report	Error uploading usage report with CSSM connector API. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
cisco_connection_offline	Unable to connect to Cisco
error_auth_code_read	Failed to read authorization code
error_json_decode	Failed to decode or unmarshal JSON payload. Please verify JSON payload
pi_login_failed	Unable to connect. Provide correct username and password for product instance login
error_core_validation_fail	Data is invalid
error_rum_report_write	Failed to write rum report
error_dlc_write	Failed to write DLC
bad_request	Bad request
error_import	Error importing data from offline file. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
cssm_account_access_denied	Smart Account access denied, user has no permission
error_poll_id_missing	Poll ID Missing
error_core_conf_add	Error adding configuration
pi_host_not_found	Unable to connect. Provide correct Host/IP of the product instance and make sure HTTPS is configured
auth_code_cssm	Authorization message received from CSSM
error_core_tenant_conf_put	Error updating tenant configuration
error_cssmconn_api	CSSM connector API failed
error_cssmconn_ping_err	CSLU could not connect to the Cisco network. Please check your network settings
cssm_offline_mode	cssm_offline_mode

Alert	Description
warning_unknown_pi_added	Unknown product instance added to discovery
error_core_validation_api	Error validating the data
error_core_listener_add	Error adding listener information
error_cssmconn_policy	Error downloading policy with CSSM connector API. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
dlc_request_cssm	DLC request sent to CSSM
error_core_tenant_conf_exists	Configuration Error: Unique pair of Smart Account Name and Virtual Account Name required
error_cssmconn_add	Error uploading data with CSSM connector API
error_discovery_update	Error updating information in discovery
error_storage_get	Failed to get from storage
udi_not_allowed	Device is not authorized to request the service
error_cssmconn_delete	Error deleting data with CSSM connector API
error_storage_api	Error handling storage API
error_core_tenant_conf_api	Error handling tenant configuration API
error_core_notification_add	Error adding notification
dlc_ack_cssm	DLC acknowledgement received from CSSM
pi_not_found	Product Instance is not found
auth_code_pi	Authorization message sent by product instance
error_piconn_send	Error sending data to product instance
error_storage_delete	Failed to delete from storage
limit_exceeded	The request has exceeded the limit of number
error_discovery_add	Error adding information to discovery
error_discovery_api	Error handling discovery API
error_auth_code_write	Failed to write authorization code
piconn_send_import_data	Failed to send data to product instance
error_core_tenant_conf_validate	Configuration Error: Check settings of Smart Account Name and Virtual Account Name and try again
error_cssmconn_dlc	Error uploading dlc with CSSM connector API. See logs (CSLU_WORKING_DIRECTORY/var/logs/) for more details
error_acc_info_missing	Smart Account information is missing for the request
login_required	Login with CCO credential required
error_scheduler_api	Error handling scheduler API
tenant_not_found	Tenant ID is not found
error_core_listener_get	Error getting listener information

Acronyms

Acronym	Definition
CCW	Cisco Commerce Workspace
CSLU	Cisco Smart License Utility
CSSM Cloud	Cisco Smart Software Manager Cloud
CSR	Certificate Signing Request
DLC	Device Led Conversion
DNS	Domain Name Server
FQDN	Fully Qualified Domain Name
LCS	License Crypto-Module Support
LDAP	Lightweight Directory Access Protocol
LVA	Local Virtual Account
MSLA	Managed Service License Agreement
OOC	Out of Compliance
PI	Product Instances
PIDs	Product IDs
PLR	Permanent License Reservation
RBAC	Role Based Access Control
SA	Smart Account
SBP	Subscription Billing Platform
SCH	Smart Call-Home
SKU	Stock Keeping Units
SLR	Specific License Reservation
SSM On-Prem	Smart Software Manager On-Prem
SUDI	The Secure Unique Device Identifier
TPL	Third (3rd) Party Licensing
TLS	Transport Layer Security
UUID	Universally Unique Identifier