Smart Software Manager On-Prem User Guide

Version 7 Release 202001

First Published: 01/16/2016
Last Modified: 1/24/2020

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS

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 important 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 On-Prem Quick Start Guide
- Cisco Smart Software On-Prem Installation Guide
- Cisco Smart Software On-Prem Console Reference Guide
- Cisco Smart Software On-Prem Release Notes (Version 7 Release 202001)

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. RSS feeds are a free service.

Introduction to Cisco Smart Software Manager On-Prem

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 an Administration 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 50,000 product instances with a maximum capacity of 25,000 PI per account using 1 license each.
- Provides online or offline connectivity to Cisco.

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.

Hardware-based Deployment Requirements

The SSM On-Prem can be deployed on physical servers, such as the Cisco UCS C220 M3 Rack Server, or on Virtual servers which meet the following requirements:

Minimum	Recommended
100 GB Hard Disk	200 GB Hard Disk
8 GB RAM	8 GB RAM
x86 Dual Core	x86 Quad Core
1 Ethernet NIC	2 Ethernet NIC

Virtual Machine-based Deployment Requirements

The SSM On-Prem supports the following versions of VMware vSphere Web Client are:

- VMware vSphere Web Client 6.0
- VMware vSphere Web Client 5.5

When creating the Virtual Machine for deployment, ensure the Guest-OS is set to “Linux CentOS 7 64 bit” or “Linux Other 64 bit” and has the following configuration:

Minimum	Recommended
100 GB Hard Disk	200 GB Hard Disk
8 GB RAM	8 GB RAM
2 vCPUs	4 vCPUs
1 vNICs - VMXNET3 or vertio.	2 vNICs - VMXNET3 or vertio.

System Limits and Scalability

- Up to 500 local Accounts
- Up to 1,000 Local Virtual Accounts
- Up to 25,000 product instances

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.

About Cisco Smart Software Manager On-Prem

Smart Software Manager On-Prem is linked to Cisco through a single management workspace and allows customers to support multiple Local Accounts, each linked to a unique Virtual Account within their Cisco. Smart Account/Cisco Virtual Account pair.

Cisco Smart Software Manager 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 Cisco Smart Software Manager, it gets a new ID certificate (364 day duration) allowing uninterrupted functioning.

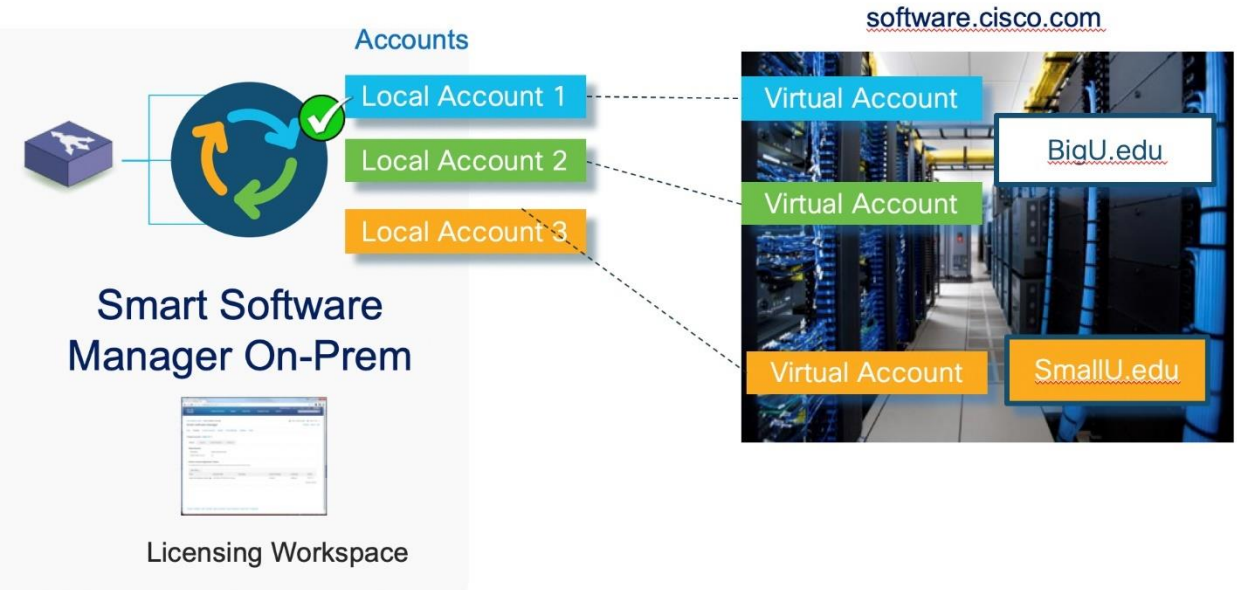

Figure 1 - Today's SSM On-Prem structure

SSM On-Prem has a new architecture and updated user interface. It also has containerized packaging (see About Accounts and local Virtual Accounts) with separate Licensing and Administration workspaces, multi-tenancy capability, new registration and synchronization procedures, new system roles and RBAC (Role Based Access Control) for license management, external authentication, syslog, proxy, and other functions. Therefore, it is important to understand how the new system setup and operations have changed.

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: system user creation, local Account creation, registration, synchronization, network, system and security settings, and more. The License Administration Workspace is accessed via:

https://<ip-address>:8443/admin

NOTE: See your 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 has similar functionality to CSSM (located on software.cisco.com) where users can manage their local accounts, users, product instances, licenses, etc. The Licensing Workspace is accessed via:

https://<ip-address>:8443

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

Feature	Description
Multi-tenancy	Manage multiple customer local Accounts in a single management workspace.
System Security Enhancements	SSM On-Prem is packaged as a deployable ISO with a CentOS 7 Security Harden Kernel and is Nessus Scanned with Critical and Major (CVE) issues addressed.
LDAP Authentication	A System Administrator can set the authentication method to be LDAP and OAuth2. If not specified, it will be using local authentication.
LDAP Groups	Group LDAP users so 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	Group users so 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	Allows users to configure multiple interfaces for traffic separation between management and product instance registrations. Some restrictions apply.
Syslog Support	Local Account events can be configured to be sent to a syslog server.
Proxy Support	Allows for On-Prem to have a proxy between itself and Cisco Smart Software Manager for traffic separation.
API Support	Allows applications to call On-Prem APIs for virtual account, token, license, product instance, reporting, alerts and other operations.
Virtual Account Tagging	Allows local Virtual Accounts to be tagged for easy virtual account classification, grouping, locating and/or role assignment.
License Tagging	Users can define and assign tags to licenses. Tags are useful for classifying, locating, and grouping licenses.

About 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 logon 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 logon page. From this page, you can continue to work in ADFS applications by:

- Clicking the **Login Using OAuth2 ADFS** link located on the right side of the login screen.

After clicking the ADFS link, since 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.

About Pop-up Modal Behavior

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

SSM On-Prem uses two types of pop-up modals. One type of pop-up modal has an "**X**" located on the top-right corner. The second type of pop-up modal has no such **X**.

Therefore, to close the first type of pop-up modal:

- Click the "**X**"

To close the second type of pop-up modal:

- Click anywhere **off the screen**

Logging into 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 SSL Certificate.

Initial Login Procedure

You initially log into SSM On-Prem with your username and password. After you have logged into the application, a 4-step Wizard screen opens asking you to:

- Set the default language
- Reset your password
- Check your SSL Certificate
- 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, Japanese, Chinese, Korean.
Step 3	Enter your **new password**.
Step 4	Confirm your **new password**.
Step 5	Confirm your **SSL Certificate**.
Step 6	Review your **changes**. If they are correct, click **Next**. The Wizard returns you to the Logon screen. Where you can log into SSM On-Prem using your new password. If they are incorrect, click **Back**, you are returned to the previous screen.

Cisco Smart Software Manager On-Prem: Basic Components

About 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 (see BigU/LittleU edu callout in Figure 1) and two are found in the SSM On-Prem. For Cisco Smart Software Manager, we have **Cisco Smart Accounts** and **Cisco Virtual Accounts**. For SSM On-Prem we have **local Accounts** and **local Virtual Accounts**.

Accounts Located in Cisco Smart Software Manager

Accounts that reside in CSSM are **Cisco Smart Accounts** and **Cisco Virtual Accounts**. Each Cisco Smart Account, in turn, contains **one** or **more 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** and so it is not possible to directly transfer information between Cisco Smart Accounts.

Accounts Located in SSM On-Prem

Each SSM On-Prem local Account 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 and an SSM On-Prem application instance. All other local Virtual Accounts associated with a local Account besides the Default Local Virtual Account can only be populated with product instances and licenses by the customer deciding to transfer those items from the Default Local Virtual Account to the other local Virtual Accounts within the same local Account. **This type of transfer has the effect of hiding network information from Cisco** when the other local Virtual Accounts are used to contain product instances and licenses.

About the Relationship between Cisco Smart Software Manager and SSM On-Prem Accounts

Outlined here are two examples describing the relationship between CSSM and SSM On-Prem Accounts

This example shows the strict one-to-one relationship where one Cisco Virtual Account is directly related to one On-Prem Local Account. In this relationship, product instance and license information

is synchronized between these two accounts for the Cisco Smart Software Manager (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 Local Default Virtual Account associated with that On-Prem Local Account. Conversely, a license removed from the Cisco Virtual Account, it will also be removed first from the Local Default 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 Cisco Smart Software Manager (Cloud).

NOTE: While the relationship between CSSM 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.

Outlined here is another example of Account integrity between Cisco Smart Software Manager and SSM On-Prem. In this example, if two local Accounts (localAcctA and localAcctB) are created, each local Account **must** be associated with a unique Cisco Virtual Account in CSSM (as stated in the note). This scenario allows you to have local Virtual Accounts associated with one local Account and other local Virtual Accounts associated with second local Account. In this example, it would **not** be possible to transfer product instances or licenses between local Virtual Accounts of localAcctA to those of localAcctB, because this transfer would cross local Account container boundaries. However, it is possible to transfer product instances or licenses at the CSSM end, since the Cisco Virtual Accounts associated with local Accounts localA and localB are within the single container of the Cisco Smart Account. After the transfer, the customer forces a synchronization to occur to propagate the transfer from CSSM to the SSM On-Prem instance.

About Licenses

Licenses are required for all Cisco products. The following types of product licenses vary depending on the Cisco product:

- **Term Licenses**: Licenses that automatically expire after a set amount of time: one year, three years, or whatever term was purchased.
- **Perpetual Licenses**: Licenses that do not expire.
- **Demo Licenses**: Licenses that expire after 60 days. Demo licenses are not intended for production use.
- **Reporting only licenses**: Licenses that are zero-dollar base and bundled with the hardware. Once a device registers and reports the use of these reporting only licenses, Cisco Smart Software Manager will begin to show consumption of such licenses in the SA/VA to which the device is registered. Please note: Cisco Smart Software Manager 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.

NOTE: Perpetual, Demo, and Term Licenses are valid for a different period. Perpetual licenses do not expire, 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.

About Product Instances

A product instance is an individual device (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.)

About Product Instance Registration

Once the SSM On-Prem is operational, smart-enabled product instances can register to the SSM On-Prem and report license consumption. This registration is between the product instances to the SSM On-Prem and is different from the registration between the SSM On-Prem and Cisco Smart Software Manager.

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 the SSM On-Prem:

- **SSM ON-PREM-URL**: The SSM ON-PREM-URL is the Host Common Name (CN). The Host Common Name (CN is set in the System Administration within the Security Widget, on the Certificates tab, and is entered in the form of a Fully Qualified Domain Name (FQDN), hostname, or IP address of the 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 URL in the Smart Transport configuration section of product configuration. The URL should be set to:
  https://<SSM ON-PREM-URL>:/SmartTransport
  http://<SSM ON-PREM-URL>:/SmartTransport
- **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;
  https://<SSM ON-PREM-URL>:/Transportgateway/services/DeviceRequestHandler
  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 the SSM On-Prem.
- **Configuration Guide**: Smart-enabled product instances vary in how they register to SSM On-Prem via CLI or GUI depending on the product. For complete instructions for configuring a

product instance to communicate with the SSM On-Prem, see the documentation for your product.

NOTE: Products which support Strict SSL Cert Checking require the **SSM ON-PREM-URL** to match the SSM On-Prem Common Name. The common name is provided as the hostname in the Networking Widget.

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

About 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. Once 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 365 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.)

Cisco License Features

Overview

Cisco Smart Software Manger On-Prem is tailored to maximize Cisco's licensing features. This section describes, in detail, the four 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 the SSM On-Prem to generate restricted tokens for 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 LRP or CSSM portals based on information available in the SWIFT database. DLC allows the device/product instance to initiate a conversion of classic licenses (such as RTU) to Smart licenses that are not on the SWIFT database. Upon conversion, these Smart Licenses are deposited into Cisco Smart Software Manager. Products must be upgraded to a DLC-enabled version, connected to a DLC-enabled Cisco Smart Software Manager or SSM On-Prem for this feature to work.
- **Third-Party Software Support (TPL)**: TPL, such as Speech View in Unity Connection and Apple Push Notification (APNs) in Unified Communication Manager, is used to authorize Smart License enabled Cisco products to use their services.

About 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 High Availability (HA) cluster. In this model, the 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 Cisco Smart Software Manager or SSM On-Prem can match up multiple usages of the same license

With this additional information, Cisco Smart Software Manager 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 Cisco Smart Software Manager 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.
    - Show which licenses in-use are shared on a device.

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, [DeviceA, TagA, ApplicationA, ID1, Active], reports using 1 license and has peer of [DeviceB, TagB, ApplicationB , ID2, Standby].
    - 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 has the information on Application Redundant peers, it would show in the Product instance High Availability tab that 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 specifically reconfigure (via a set of product specific commands) and declare itself an Active application (without a peer) so that Cisco Smart Software Manager 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 Cisco Smart Software Manager to ensure that Cisco Smart Software Manager has the same peer information. This way, the Cisco Smart Software Manager's Product and License tabs match SSM On-Prem. An example of the Application Redundancy is shown below:

```
:ha_attributes
      :application_name: User_A
      :app_role: ACTIVE
      :app_id: '1'
      :peer:
      - :name: User A1
        :role: STANDBY
        :id: '2'
        :product_instance_identifier: 250cafe6-a06d-48fd-8b5f-8a58806fbacd
```

Reporting for Application Redundant Enabled Products

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

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 (approx. 14% 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 an 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 Cisco Smart Software Manager.
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.
4. SSM On-Prem updates its GUI under the Products Instance 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 Cisco Smart Software Manager.
    a. If the SSM On-Prem is in manual mode, there is a dismissible alert in the Administration workspace to remind the user to perform a manual synchronization so that the Cisco Smart Software Manager authorization can come down to SSM On-Prem.
    b. If the SSM On-Prem is in network mode, the next synchronization request to Cisco Smart Software Manager will contain the export control restricted license authorization response.
6. When SSM On-Prem receives the response from Cisco Smart Software Manager, it processes the request and updates the alerts accordingly with the success or failure message and the associated reason(s).
    a. If authorized, SSM On-Prem updates its Product Instance tab indicating the correct reserved export license count.
    b. If not authorized due to the license not being available, a status is reflected on the SSM On-Prem 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 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 the 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 Cisco Smart Software Manager.

New Export Control Alerts

There are several new alerts in the 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 Cisco Smart Software Manager.
- **License Return Pending**: When a product requests a cancellation of an Export Control license and is waiting for an authorization from Cisco Smart Software Manager.
- **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 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 VA and synchs.

Product Instance and License Transfer Behaviors

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

NOTE: This behavior is only for local Virtual Accounts on SSM On-Prem.

About Product Instance (PI) Transfer

SSM On-Prem PI transfer between local Virtual Accounts is like Cisco Smart Software Manager.

- Non-restricted licenses being consumed by 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 VA 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 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 VA because the PI would not have been able to consume a controlled license in the first place if it didn't have available licenses. So, the destination VA will never go Out of Compliance.

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

About License Transfers

Recall that Cisco SSM is the “single source of truth” for all license entitlements and Cisco 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 Cisco Smart Software Manager. However, on Cisco SSM On-Prem, since all licenses in the local Virtual Accounts are not visible to Cisco SSM, the license transfer behavior between local VAs in Cisco SSM On-Prem is like Cisco Smart Software Manager. During a synchronization of Cisco SSM On-Prem to Cisco Smart Software Manager, all product instances and licenses are aggregated across all Cisco SSM On-Prem local Virtual Accounts and updated in Cisco Smart Software Manager and vice versa.

Cisco Smart Software Manager 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 Licenses Tab. 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" OOC.
    - You cannot transfer licenses if the VA 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, Cisco Smart Software Manager/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, Cisco Smart Software Manager/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, Cisco Software Manager/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.

About License Hierarchy

When using a smart licensing product, the product instance reports back to Smart Software Manager the licenses that are being used. If a license being used is not available for consumption in Smart Software Manager, rather than letting the requested license go out of compliance, some products will allow other licenses to satisfy that request if the higher tier licenses exist in the Virtual Account. For example, if a Network Advantage license (parent) exists, it can be used (borrowed) to satisfy a request for a Network Essentials license (child) if no licenses are available. SSM On-Prem supports license hierarchies that support multiple parents or multiple children.

To see if a license hierarchy is being used, navigate to the **Smart Licensing** workspace, select **Inventory > Licenses**. The licenses table provides these information categories:

- **License**: Lists the name of the license.
- **Billing**: Lists what status the license in such as, Prepaid.
- **Purchased**: Total number of licenses that have been purchased (shows as a positive number) any borrowed licenses will be in parenthesis as a negative number. If there is any borrowing/lending in 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.
- **Balance**: Lists the difference between the total number of licenses minus the licenses that are being used.
- **Alerts**: Lists any alerts that can affect the license (as if 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 window opens showing the Virtual Account Usage in a Pie Graph.

Cisco Smart Software Manager On-Prem Roles

About User Role-Based Access (RBAC)

Cisco SSM On-Prem offers role-based access control (RBAC) to restrict system access to authorized users. RBAC allows you to limit system access according to responsibility.

About System Roles

The available system roles and responsibilities are:

- **System Admin** (Full Access)
  - Full System access
  - Access to all Account(s)
- **System Operator** (Limited Access)
  - No ability to change system configurations
  - Access to all Account(s)
- **System User** (Restricted Access)
  - Limited to License Workspace Only
  - Access to Account(s) defined by Account RBAC

About Local Account Roles

In addition to system roles which are set in the Administration Workspace, support for Account Roles can be setup for individual accounts in the License Workspace to provide finer grained access over virtual and smart accounts.. 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 Virtual Accounts or manage user access.
  - Add Administrator role to specific Virtual Accounts for other System Users
- **Virtual Account Administrator can:**
  - Allow User or Administrator access only to specific Virtual Accounts.
  - Add Administrator role to specific Virtual Accounts for other System Users
- **Virtual Account User can:**
  - Can allow User or Administrator access only to specific Virtual Accounts

Cisco Smart Software Manager On-Prem: System Administration

The System Administration portal 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 portal has a collection of Widgets. 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 logon page. For more details on this feature, see Cisco SSM On-Prem Idle Timeout Feature.

- **Users Widget**: Allows the Administrator (or System Operator) to create local users and configure advanced parameters such as setting passwords, expiration rules, and password auto-lock features.
- **Access Management Widget**: Allows the Administrator to manage the configuration for LDAP, LDAP Users, LDAP Groups, OAuth2 ADFS, as well as SSO Clients.
- **System Settings Widget**: Allows the Administrator to manage settings needed by SSM On-Prem such as: Messaging, Syslog, Language, Email, Time Settings, NTP Server, and Message of the Day.
- **Network Widget**: Allows the Administrator to manage network IP, NTP, 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), as well as synchronization schedules for each account.
- **API Toolkit Widget**: Allows the Administrator to create client and resource authentication credentials for accessing the On-Prem public API.
- **Security Widget**: Allows the Administrator to manage certificates, password strength and expiration. 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.) Allows the Administrator to view the basic cluster information with a simulated illustration.

- **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 is how long the server has been running
  - The Interface parameter monitors the traffic load being used by that interface
- Resource Monitor Percentage: This parameter shows the 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.

User Widget

The User widget allows the System Administrator or System Operator to create local users and configure advanced parameters such as setting passwords and 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 logon page. For more details on this feature, see Cisco SSM On-Prem Idle Timeout Feature.

When you create a user on the Administration workspace portal, 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 can 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**. a. (Optional) Enter the user's **First Name**. b. (Optional) Enter the user's **Last Name**. c. (Optional) Enter a brief description of the user for example, user role, position, responsibilities in using SSM On-Prem). d. (Required) Enter a **User Name** for the user. e. (Optional but strongly recommended) Enter a valid **Email** for the user. f. (Required) Enter a **Password** for the user. g. (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	Navigate to the System Role column and select one of the following roles: • User • System Operator • System Admin See SSM ON-Prem Roles for more information on role privileges.

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, SSO Client, ADFS) are secondary forms of authentication and are only active when the Access Management methods are used.

Actions 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.

- **Disabled User**: The user still exists in the database but is not able to login until re-enabled again. However, you can only remove a user after you disable that user.
- **Removed User**: This option is activated **after** a user has been disabled.

NOTE: You must first disable a user before you can remove them.

NOTE: A System Administrator or System Operator cannot remove themselves. You must first disable a user before you can remove them.

Access Management Widget

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

- **None**: 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.
- **LDAP Users tab**: As LDAP Users log into SSM On-Prem and are authenticated for the first time, they are added to the LDAP Users tab. Use this tab to see which LDAP users have access to SSM On-Prem Accounts and local Virtual Accounts. Once these LDAP users log into SSM On-Prem, they can be assigned RBAC to the SSM On-Prem Accounts/local Virtual Accounts according to their 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.
- **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.

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:
    - **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 specific examples):
        - **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 Authentication** (Optional): 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=John Smith, ou=San Diego.
    - **Password**: The password for this LDAP server Bind DN.
- **LDAP Group Import Settings** (Optional): This designation enables you to automatically import LDAP groups. You will need to specify both these attributes:
    - **Group Base DN**: 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

When you have filled in the required information, click **Save**.

LDAP Users Tab

When an LDAP user logs into the Licensing Workspace with LDAP authentication configured, the LDAP Users tab is populated with that LDAP user. In this example, once **testUser1** is logged into the Licensing workspace, **testUser1** is added under the LDAP Users tab. LDAP users that are added to

the SSM On-Prem can be assigned RBAC (Account Administrator, Account User, local Virtual Account Administrator, local Virtual Account User) via the User option in the Licensing workspace.

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

NOTE: You can only add up to 1000 LDAP Groups for each SSM On-Prem.

LDAP Groups Tab

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

Each group defines one or more members. SSM On-Prem uses the `memberuid` attribute for the uid of each member in the group.

Click **Update LDAP Data** to get the users and user groups information from the LDAP server to populate in the SSM On-Prem.

Each LDAP group can be assigned access to the various resources (Account or local Virtual Account).

Complete these steps to give universal access to accounts as either an Account Admin or Account User role.

Step	Action
Step 1	In the Administration Workspace, open the **Access Management Widget**.
Step 2	Select **LDAP Groups**.
Step 3	Select the **Group Name** that need to be updated/modified.
Step 4	Select the local **Account** for access to those resources.
Step 5	Select either **Account Admin** or **Account User** for the assigned role.
Step 6	Click **Save**. All the users in that group will have that role assigned for that account.

Complete these steps to assign access to your resources for local Virtual Accounts.

Step	Action
Step 1	In the Administration Workspace, open the **Access Management Widget**.
Step 2	Select **LDAP Groups**.
Step 3	Select the **Group Name** that need to be updated/modified.
Step 4	Select the local **Account** for access to those resources.
Step 5	Select **Per Virtual Account** for the assigned role.

Step 6	Click **Add**. A (**+**) sign in front of the Account Name designates the list of local Virtual Accounts.
Step 7	Click the (**+**) sign to open the list of Accounts.
Step 8	Select the **Account** that needs to be modified.
Step 9	Select the **Role** for that Account.
Step 10	Click **Save**. All the users in that group will have that role assigned for that account.

OAuth2 ADFS Configuration Tab

(Added for SSM On-Prem 7 Release 201910)

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 and a tooltip opens defining 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	Enter the **ADFS Server URL**. (Host Name, FODN, IPv4, or IPv6 must begin with https:// or http://)
Step 4	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 5	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 6	Enter the **Client ID**. (Copy the unique ID that you configured in your ADFS server into this field.)
Step 7	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 8	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. See Appendix A4. Setting up ADFS Server and Active Directory Groups and Claims for guidelines.

Logging into SSM On-Prem using OAuth2 ADFS

(Added for SSM On-Prem 7 Release 201910)

Once you have enabled OAuth2 ADFS Secondary Authentication, clicked **Save** and configured 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.
- **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 login.

SSO Client Tab

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

To utilize an SSO Client, complete these steps.

Step	Action
NOTE: All the fields that have an [*] are required fields.	
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	Enter the name of the **Authentication Server**.
Step 4	Enter the **Application ID**.
Step 5	Enter the **Application Secret**.
Step 6	Click **Save**.

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

Settings Widget

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

About the 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) Enter **Banner Text**.
Step 2	(Optional) Click **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 the events based on the following severities:

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

Language Tab

Currently, SSM On-Prem supports English, 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**.
Step 4	(Required) Enter the **Email From** address. **NOTE**: This must be a legitimate email address.
Step 5	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. h. (Required) Enter a **Username**. i. (Required) Enter a **Password**.
Step 6	Click **Save**. Your email settings are saved to the system.

Time Settings Tab

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	Configure the **Time Setting**. If you want to manually set the time, turn on **Manually Set Time**. a. Slide Manually Set Time to **On**. b. Select the **Date** (default to current date). c. Set the **Hour**, **Minutes**, **Seconds**. If you want to Synchronize with an NTP Server: d. Turn on **Synchronize with NTP Server**. e. (Required) Enter the **NTP Server Address**. f. Click **Synchronize Time Now**.
Step 3	Click **Apply**. **NOTE**: Click **Reset** if you need to reset the time settings.

Message of the Day Settings Tab

The options on this tab allow you to set the greeting message on the SSM On-Prem console.

- **Message of the Day**: Is the display 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**.

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 auto lock feature as well as set the time an account is locked.
- Password: Provides password 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.

Accounts Tab

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

The tab interface contains three sections:

- **Enable auto lock**: That 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**: Allows user with admin privileges to set the number of sessions that can be opened for a user. The range is 1-999.

Configuring Password Auto Lock and Lock Expiration Settings

Complete these steps to enable the password auto lock feature.

Step	Action
Step 1	In the Administration Workspace, click **Security Widget**. The Security Widget screen opens.
Step 2	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** in which the number of missed attempts can occur.
Step 5	Click **Apply**. **NOTE**: Click **Reset** if you need to reset the auto lock settings.
To configuring 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 8	Click **Apply** to save the settings to the system.

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 three main options and seven sub-selections.

- Toggle switch: (default Enabled) Enable login error message notification. 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: 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. Aneurysm

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
- 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	From the Administration Portal, navigate to **Security Widget > Certificates**.
Step 2	Enter the **Host Common Name**. **NOTE**: Please read the note in the table outlining the details for entering a Host Common Name.
Step 3	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 Cisco Smart Software Manager.
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.

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 Browser Certificate section of the Common Name tab, click **Generate CSR**. The Generate CSR screen opens.
Step 2	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. **Key Size**: Select from the drop-down list. • 2048 • 4096 e. **Subject Alternative Name**: Another possible designation for the certificate. For example, an IP Address.
Step 3	Click **Generate**. The certificate signing request is downloaded and appears on the bottom of the browser window.
Step 4	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 5	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	From the Security Widget Certificate tab, click **Add**. The Certificate Wizard opens.
Step 2	In the next screen, select **Add a new certificate**.
Step 3	Click **Import Certificate**.

Step	Action
	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	Enter the following: • Description: Enter the **description** for the certificate. • Certificate: Click **Browse** to find the certificate on your drive. • 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.
Step 5	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.

Deleting a Certificate

Each certificate has an expiration date. The Expiration Date pull down list is located on the left-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.

Step	Action
	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 that certificate.
- The .type of Event associated with that certificate.
- The Event message associated with that certificate.
- What user was associated with that certificate activity

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, netmask/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 Cisco Smart Software Manager. 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** 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.

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, Cisco, and ssh into the On-Prem Console/CLI.)
- Management Only (User: Access to SSM On-Prem is open just a browser and ssh into the On-Prem console/CLI.)
- Product is for product registration and authorization.(Product: Access open through the product.)
- Cisco Communication Only (DMZ: Restricted to outbound traffic only from Cisco.) Two NICs are needed for this configuration.

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

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:

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**.
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.

Step	Action
	Destination1: 72.163.0.0/16 Next Hop1: 204.75.212.2 Destination2:173.37.0.0/16 Next Hop2: 204.75.212.2 **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**.

Proxy Tab

The Proxy tab provides proxy services to SSM On-Prem. Basically, a proxy server is a device in the network which acts as an intermediary for requests from devices with-in 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. The 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). The 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 Cisco Smart Software Manager (**products > SSM On-Prem > HTTPS proxy > Cisco SSM**). This support enables customers to control or monitor traffic between SSM On-Prem and Cisco Servers.

Complete these steps to setup proxy support.

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.

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 Cisco Smart Software Manager before it can be active and usable. Both network and manual registrations are supported.

Accounts Tab

During the SSM On-Prem local Account registration, a Cisco. Smart Account/Virtual Account pair must be specified. If the Cisco Virtual Account does not exist, Cisco Smart Software Manager 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 **Accounts 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 • 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 de-activated the Account is not removed from the SSM On-Prem and no user permissions are changed.

Complete these steps to de-activate the local Account.

Step	Action
Step 1	Right click on the **Account Name 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 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	Right-click on the **Account Name 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 Cisco Smart Software Manager 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 Cisco Smart Software Manager 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 an SSM On-Prem account:

Step	Action
	a. Navigate to the **SSM On-Prems** pane. b. Select the **SSM On-Prem** corresponding to that local account. c. From the Actions menu, select **Remove**. d. Confirm **SSM On-Prem removal**.
Step 7	The 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 Cisco Smart Software Manager is to synchronize SSM On-Prem to Cisco Smart Software Manager 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 the SSM On-Prem in Cisco Smart Software Manager 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 had the SSM On-Prem instance removed from Cisco Smart Software Manager, 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 Cisco Smart Software Manager. 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 **Accounts 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**.

Step	Action
	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 Cisco Smart Software Manager. 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 **Accounts 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	Action
Step 6	Log into **Cisco Smart Software Manager**.
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 Cisco Smart Software Manager 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 Cisco Smart Software Manager.
Step 2	Click **Next.**
Step 3	To gain access to Cisco Account/Virtual Account Cisco Smart Software Manager, enter your **CCO ID credentials**.
Step 4	Click **Submit**. A status of the registration progress opens.

Step	Action
	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 the SSM On-Prem on Cisco Smart Software Manager **SSM On-Prems** 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 Cisco Smart Software Manager. 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 Cisco Smart Software Manager.

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 **Cisco Smart Software Manager**.
Step 4	Navigate to the **On-Prem** tab.
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	Action
Step 8	Upload the **Account Authorization File** from Cisco Smart Software Manager 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 Cisco Smart Software Manager.

Event Log Tab

There are also event log entries that gives statuses of the various synchronization activities, successes, failures and associated reasons.

You can search for specific events using the search field or you can download a .csv file to a local drive.

Synchronization Widget

Cisco Smart Software Manager 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 Cisco Smart Software Manager, 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.

There are two types of synchronization: Standard and Full. Both types are described here.

Standard Synchronization

Under standard synchronization, SSM On-Prem and Cisco Smart Software Manager 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 Cisco Smart Software Manager detects that it needs the SSM On-Prem to compile and send a complete list of its data, regardless of when it was created. In return, Cisco Smart Software Manager also gathers a complete list of its current “source of truth” elements and passes that list along to the SSM On-Prem.

Synchronization Alerts

Below are the synchronization alerts for local Account non-synchronization with Cisco Smart Software Manager:

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 Cisco Smart Software Manager

After 364 days of non-synchronization, the SSM On-Prem local Account is still present (not deleted) on the Cisco Smart Software Manager; 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 Cisco Smart Software Manager 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 Cisco Smart Software Manager, 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 Cisco Smart Software Manager periodically to ensure the licensing information between the SSM On-Prem and Cisco Smart Software Manager is not out-of-sync. Scheduling is accomplished by setting up a scheduled synchronization. (For more information on scheduling synchronizations, see Scheduling Tab.

On-Demand Online Synchronization

Online synchronization assumes there is an Internet connection to Cisco Smart Software Manager from SSM On-Prem. On each local Account, you can choose to perform either a **Standard Synchronization Now...** action or **Full Synchronization Now...** action for synchronization.

NOTE: If it's the first time or if your session has expired and you need to be re-authenticated to Cisco Smart Software Manager, you are presented with a login screen to the Cisco Virtual Account in the SSM On-Prem Administration Workspace.

Complete these steps to make an online synchronization.

Step	Action
Step 1	Click the **Synchronization Widget** to open it.
Step 2	On the local Account, under Actions**,** 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.

NOTE: The SSM On-Prem Name (the SSM On-Prem Name in the table) is the name of the account on Cisco Smart Software Manager and the Account Name (the name column in the table) is the local Account Name on the SSM On-Prem. They are typically the same. (Giving these accounts the same name prevents confusion when dealing with multiple accounts.)
In the case where a user changes the SSM On-Prem Name to something else on Cisco Smart Software Manager, SSM On-Prem will reflect that new name in the SSM On-Prem Name field after it detects in a synchronization response.

If you click the **Name** of the local Account, the following information is listed under the General tab:

- Account Name: The name of the account on SSM On-Prem.
- Cisco Smart Account Name: The name of the account on the Cisco Smart Software Manager.
- Cisco Virtual Account Name: Same as the Account Name.
- Cisco SSM On-Prem 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.

NOTE: Event log entries are created that give the status of the various synchronization activities, successes, failures and associated reasons.

On-Demand 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 Cisco Smart Software Manager and SSM On-Prem.

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 Cisco Smart Software Manager. Once the file is received, a synchronization response file is sent to SSM On-Prem to reflect the same license information.

When you select **Manual Synchronization,** you are offered the additional options for **Standard Synchronization** or **Full Synchronization**.

Complete these steps to initiate 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	Depending on your need, 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 **Cisco Smart Software Manager** and click the **On-Prem** tab.
Step 6	In the SSM On-Prems 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 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	Action
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 **Browse** 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 Cisco Smart Software Manager 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 Cisco Smart Software Manager.

Schedules Tab

SSM On-Prem provides the ability to Schedule all local Accounts to be checked to determine if they need to be synchronized with Cisco SSM On-Prem on a specified interval. The default schedule is once per 30 days, but the scheduled to check for accounts which need to be synchronized can be done daily, weekly, or monthly, and, depending on the frequency, the data on the SSM On-Prem can be as current as the workspace on a daily basis.

NOTE: A local Account not synchronized with Cisco Smart Software Manager for 1 year (365 days) is no longer operational and will need to be deleted (both on Cisco Smart Software Manager and SSM On-Prem) and then registered again. This means that all the product instances and licensing information about that SSM On-Prem is lost.

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

By default, 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**.

NOTE: Currently, it is not possible to change the default 30-day synchronization due notice.

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 the Synchronizations Schedule

Currently, there is no a 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.

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. We embedded an internal OAuth2 server embedded within the SSM On-Prem software (https://gihub.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, a System 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.

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 Portal, 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 Portal, 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 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

Step	Action
	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.

shown here.

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 a HTTP POST (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
```

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.

High Availability Status Widget

NOTE: This Widget is visible only if a functioning High Availability cluster is configured on your system.

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 and Installing a High Availability Cluster for more information on installing and configuring HA.

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

About the 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 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.

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:

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

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

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

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

- **Software 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 cluster:

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

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 consist

Feature	Functionality
	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.

Cisco Smart Software Manager On-Prem Licensing Workspace: Administration Section

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.

Requesting an Account

If a local Account does not exist on Cisco Software Manager, then only a Virtual Account can be created until an account is requested and approved. 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. Enter a **Message to Creator** (text).
Step 4	In the Account Information section enter this information: a. (Required) **Local Account Name** b. (Required) **Cisco Smart Account** c. (Required) **Cisco Virtual Account** **NOTE**: For more information, see creating a local virtual 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).

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

Managing an 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.)

Creating a Local Virtual Account

You can create local Virtual Accounts using the local 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 **local Virtual Accounts tab**.
Step 3	In the local 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.

Modifying the Default Local Virtual Account Name

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.

Adding Users to a Local Virtual Account

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**, if correct click **Add User**. The User is added to the Virtual Account. **NOTE**: If the information incorrect, click **Back** to modify it.

Adding Custom Tags to a Local Virtual Account

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,** if correct click **Add Virtual Account Custom Tag**. **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.

Modifying or Deleting Custom Tags

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	Action
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	Action
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.

Smart Software Manager On-Prem: Smart Licensing Section

Overview

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

Log into SSM On-Prem and click **Smart Licensing** in the License section.

The License Workspace provides the following tabs to allow you to manage licenses:

- **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.
- **Preferences tab**: View or enable or disable (default) viewing license transaction details in the Inventory tab.
- **Activity tab**: Review license transactions.

Exporting as *.CSV Files

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

There are two levels of alert messages used in the SSM On-Prem:

- Local Account alerts
- Virtual Account alerts

Alert Icons

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.

In the local Account alerts screen, these icons provide a summary of the number of Major and Minor alerts listed.
In the local Virtual Account alerts screen, these icons are buttons to be used to toggle between displaying the Major or Minor alerts for that specific Virtual Account.

Hiding Alerts

In the Virtual Account alerts screen a **Hide Alerts** button allows you to collapse the details window for major and minor alerts.

NOTE: You will always be able to view the number of Major and Minor alerts for any Virtual Account by using the drop-down list in the Virtual Account screen under the Inventory Tab. From this tab you can see the Major and Minor Alert Summary window.

Alerts Tab

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

Name	Description
	• 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 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.

Alert	Action	Behavior
Updated Smart License Agreement: The Cisco Smart Licensing Agreement has been updated and this new 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.
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	The alert is removed when either action is performed.

Alert	Action	Behavior
	will be removed from the Virtual Account OR • Transfer the entitlement to another Virtual Account that should not already have the same entitlement.	
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 Cisco Smart Software Manager 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

Inventory: 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 365 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. Any violations are subjected 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. May be blank if no value was specified at token creation.
	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:** This field is visible for only for those local Accounts that are permitted to use this functionality. . The Cisco SSM export-controlled flag must be set to **Allowed** for this checkbox to be visible.
	Created By field	The userid of the person who created the token.

Step	Action	
	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.

Inventory: Licenses Tab

Overview

The Licenses tab displays information about all the licenses in your 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: You must first navigate to the Preferences Tab and set Show License Transaction Details in Inventory Tab to **Enable**.

  - 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
  - Add, edit, and remove license tags for licenses and local Virtual Accounts using the Available Actions and Manage License Tags tabs
  - Bulk assign/delete license tags at both the Summary Level and License Transaction Detail Level
- Specific Actions Reserve Licenses
  - Transfer Licenses (individual or bulk), Port, and Upgrade Virtual Account

NOTE: The Show License Transactions checkbox is only visible, if it is enabled under the **Preferences** tab. (See Preferences Tab)

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) See: Exporting to CSV Files
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 are associated with local Virtual Accounts or licenses.

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, 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 is 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 • 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)
Purchased	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 parenthesis () next to the available quantity. For example, if there are 10 regular entitlements and 5 pending upgrade entitlements in a Virtual Account, it would appear as 10 (+5 pending).

Column Heading	Description
	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, 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 parenthesis (). 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 in transition will be 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 reservation of reporting only licenses has been updated to reduce the quantity, they 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 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 Cisco Smart Software Manager, 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: A number of 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 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 displayed in a pop-up window with the following tabs:

Overview Tab

The Overview tab displays:

- local Virtual Account Usage
- Description of the licenses in a graphic illustration (pie chart) of local Virtual Account usage of the license
- Licenses that are duplicates or are pending upgrade are not included in these quantities
- License Types Table:
    - Count (as well as duplicate licenses)
      If there are any upgrade licenses, they will appear as (pending) in this column
    - Type (Perpetual/Term)
    - Number of licenses reserved
    - Start date
    - Expiration date
    - Subscription ID (if any)

Product Instances Tab

The Product Instances tab displays:

- Product instances
- Product types
- Number of licenses used for these Product Instances

Event Log Tab

The Event Log tab displays details on events specific to the license for the selected local Virtual Account:

- Messages describing events
- Times the events occurred
- Userids associated with the event (either the account owner's CCO ID or Cisco Support)

NOTE: To view information on the 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 Virtual Account, use the Inventory link on the Smart Licensing screen, select a Virtual Account from the drop-down list, and then click on the Event Log tab to display event messages for that Virtual Account.

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 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.

Transaction History Tab

The Transaction History tab displays license order history including:

- Transaction Date
- License SKU
- Quantity
- Expiration Date
- Order (Line) Number

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.

Manage License Tags 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.

Modifying and Deleting License Tags

When you modify or delete a license tag(s) in a local Virtual Account, you modify ALL the licenses in 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.

Available Actions Tab

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)

Adding License Tags

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	Action
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 ae 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 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.	

Removing License Tags

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 > General** tabs and then 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.	

Using the License Advanced Search Feature

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 > General tab**, and 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	
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	Action
Step 5	Click **Clear** to remove all search criteria and redisplay all unfiltered licenses.

Transferring a License

Licenses can be transferred between local Virtual Accounts within a local Account. You can choose one or more licenses from the licenses table either at the **Summary Level** or **License Transaction Detail Level**.

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.

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).

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 > General** tab, and then select the **virtual account** you want from the local Virtual Accounts drop-down list.

Step	Action	
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 **Virtual Account** to transfer the license(s) to/from.
	License	Shows the name of the license, the 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 • 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

Step	Action	
		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.	

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.

Searching Licenses by Name

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.

Searching Licenses by Tag

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 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	Action
Step 4	Click **inside the Search field**. A list of license tags available within the 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 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.

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 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 Virtual Account(s) has duplicate licenses or • The 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).

Product Instances Tab

Product Instances Tab Overview

The Product Instances tab displays information about all the product instances in your 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 between local Virtual Accounts.

NOTE: You cannot transfer or remove Product Instances from local Virtual Accounts associated with an SSM On-Prem.

- 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.

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. See Exporting as CSV Files.
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 Virtual Account.

Column Heading	Description
Name	Product ID plus Product Instance name
Product Type	Product Identification Number
Last Contact	Date
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 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.

Overview Tab

Name	Description
Overview	In the **Description** section a product description is provided. In the **General** section, the following product instance details are displayed: • Product Name • Product Identifier • Host Identifier • MAC Address • PID • Serial Number • Virtual Account • Registration Date • Last Contact 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 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 Cisco Smart Software Manager, 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.
Event Log	In the Event Tab, you can view the: • Message describing the event. • Times the event occurred. • The user who generated the message. (Either the account owner's CCO ID or "Cisco Support")

Product Instance Events

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>".
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>”.

Event	Message
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: You cannot transfer or remove Product Instances from local Virtual Accounts associated with an SSM On-Prem.

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: 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**.

Inventory: Event Log Tab

Local Virtual Account Event Log Tab

The Event Log tab displays information for all the events in a virtual account. Events are actions that you have taken using Cisco Smart Software Manager 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 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.

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 Smart License Entitlements available in a Cisco Smart Software Manager Smart Account. There are two ways to make entitlements available:

- Order Smart enabled SKUs that deliver Smart License Entitlements (licenses) to a Cisco Smart Software Manager Smart Account.
- Migrate existing Traditional Licensing using the License Registration Portal/workspace (LRP) or Smart Software Manager workspace.

In some cases, conversion of a license is not possible within the SSM On-Prem Smart Licensing workspace and must be converted at Cisco to be converted by the device. Examples would be Right to User (RTU) licenses, Paper Licenses, or PAK files which are not listed in LRP or Cisco Smart Software Manager 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 Cisco Smart Software Manager. Products must be upgraded to a DLC-enabled version of software, connected directly to or Cisco Smart Software Manager, 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, Cisco Smart Software Manager 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 **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 automatic.
   - Manually initiated license smart conversion start command needs to be entered 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 display an alert that the user should initiate a sync 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 Cisco Smart Software Manager on the next synchronization.
6. SSM On-Prem passes the encoded conversion data to Cisco Smart Software Manager in the next sync (network, scheduled, or manual).
7. SSM On-Prem waits for a response from Cisco Smart Software Manager via the next sync (success or failure with a reason).
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 on its UI so users can know 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, 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 to:
    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 Cisco Smart Software Manager, 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 Cisco Smart Software Manager. 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

Reports Overview

The **Reports** tab allows you to run reports on all your local Virtual Accounts and all your licenses within your local Account. The Reports table displays the following information for each supported report:

Name	Description
Name area	The name of the SSM On-Prem report. Click the link to view the specific report page.
Description area	The description of the Report.

Running Reports

You can run reports on Licenses, License Subscriptions, and Product Instances.

Complete these steps to run a report.

Step	Action
Step 1	In the Smart Licensing, 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	In the Run License Report dialog, complete the **appropriate information** (shown in the pertinent table below).
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.

Name	Description
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.

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**.

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

Activity Overview

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 had two tabs:

- License Transactions
- Event Log Occurrences

License Transactions Tab

Your view of the License Transactions tab depends upon your role as a Cisco Administrator, Smart Licensing Administrator, or local Virtual Account Administrators. The Smart Licensing Administrator and local Virtual Account Administrator, for example, have access to local Account information provided under the Transaction History and Event Log.

Event Log Tab

The messages listed in the Event Log of the **Activity** tab are a compilation of all local Account events, and all events associated with all local Virtual Accounts managed under the local Account. Event Log messages specific to each local Virtual Account are accessed from the **Inventory tab**.
A **Cisco Administrator** has access to information provided under a different set of tabs (see Administration workspace)
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 utilized
- License Expiration: Date the license expires
- License Type: Perpetual or Term
- local Virtual Account: 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 the **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 (New SSM On-Prem created, SSM On-Prem renamed, SSM On-Prem failed to sync and removed, SSM On-Prem removed, SSM On-Prem synchronized via network, SSM On-Prem file synchronization)

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. See Exporting to CSV Files.

Using Smart Software Manager On-Prem APIs

Previously there were 21 APIs available on Cisco Smart Software Manager. More detailed information on these Cisco Smart Software Manager APIs can be found at:

https://anypoint.mulesoft.com/apiplatform/cisco-stage/#/workspaces/organizations/a4479091-a60c-4c9c-97ab-068d54235cea/apis/4824776/versions/95443/pages/293810

Of these 21APIs, only 14 are available on Cisco SSM On-Prem because we do not support the local Account or SLR/PLR features.

NOTE: For those request 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 Portal under Manage Accounts under local Virtual Accounts. The Default account is the **‘*’** account shown in the License Portal.

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:

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.

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

Creating a Token

Request Parameters:

- smartAccountName: The SSM On-Prem Account Name
- virtualAccountName: The name of the local Virtual Account
- Description: Description of the token
- Expiration Days: Number of days before the token expires

Response:

- The Token list that the user has access to.

Example Method Call:

- HTTP Method: POST
- Request: https://<ip address>:8443/api/v1/accounts/{account name}/virtual-accounts/{virtual account name}/tokens

Request Body:

```
{ "expiresAfterDays": 100, "description": "Test VA Creation", "exportControlled": ["Allowed"|"Not Allowed"] }
```

Response Code: 200 OK

```
{
 "status":"SUCCESS",
 "statusMessage":"A valid, active token was generated.",
 "tokenInfo":{

"token":"OGVjMDk4YjktNGUwNS00OTc0LTk0YjQtNWZkZTI5ZTU2ZjFjLTE0Nzc1Mjc2%0ANTA2NT
```

```
Z8M0wvcmdBWmJnbVR1akdaa0xjTU9ldDRFbXVFQjh3L3k1aHAzdTBD%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 where the user can take the tokens

virtualAccountName: The local Virtual Account of the Account where tokens can be taken

Response:

- List of all the active Tokens within the specified local Virtual Account. For every active token, tokenString, tokenExpirationDate, tokenDescription, createdBy

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":"OWI2YmE2ZDgtYTBhZi00MGQyLWE1NDYtZThkMWZjMDUzYzM1LTE0NzcyNjA1
%0AMjI2NTh8cUhjaEtiaGlXalRLeFNseHFqQXpMUnpiZXVvZ0VybkNacU91L1Vq%0AbDc0S
T0%3D%0A",
  "expirationDate":"2016-10-23T22:08:42",
  "description":"this is Ben September 23",
  "createdBy":"bvoogd"
  "exportControl":"Not Allowed",
 },
 {

"token":"YWQwZjE2MmUtMWI4NS00YmM4LWIyZTAtYjA1OGJjMGI1MTkzLTE0NzcyNDMy
%0AMTgyMTF8K0djaEJOZWg2S3NIMHhURUI2aWFKOEgxQ0w0Wm41MXZlZHRsbVp3%0
AOUFZOD0%3D%0A",
  "expirationDate":"2016-10-23T17:20:18",
  "description":"this is Ben September 23",
  "createdBy":"bvoogd"
  "exportControl":"Not Allowed",
 },
 {

"token":"OTI2M2I5YmYtYjRjMy00ZjcyLWE1OTEtOTUwZDY5ZWY3NWRlLTE0NzcyNDMw%
0ANDA0NTZ8U1pRVEJKNFh5a1VTWFprb2FMclh0bjBEVDNrVnNoUzVOdjdmZTJJ%0AZklZ
Yz0%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%0AMjI0ODF8Wjdu
”NW5ObVd0L1BGZmFvOWZYenJiaGJyRVE4T0R5NFJheW90V2hq%0AQkRSND0%3D%0A has already been
revoked."
   },
   {
    "status": "SUCCESS",
    "statusMessage": "Token-
'ZTBkYjkzOGMtOWY3Yi00ZThjLThkOTAtYTljZmIwZTA5ZWFjLTE1MDU0MTcw%0AMzE2NzJ8Y1dZMkR
GUWF1QVQzK3VuNVNSN3hNTDNUUG5XMkJiTS9jMGxMVzNq%0AZVV2TT0%3D%0A' revoked
successfully"
   }
  ]
}
```


Response Code:422 Unprocessable Entity


```
{
  "tokens":[
    {
      "status": "ERROR",
      "statusMessage": "Failed to find token
OGVjMDk4YjktNGUwNS00OTc0LTk0YjQtNWZkZTI5ZTU2ZjFjLTE0Nzc1Mjc2%0ANTA2NTZ8M0wvcmdB
WmJnbVR1akdaa0xjTU9ldDRFbXVFQjh3L3k1aHAzdTBD%0ANzlYbz0%3D%0A."
    },
    {
      "status": "ERROR",
      "statusMessage": "Failed to find token
ZGQ1ZmQ2ZWQtNjE4YS00NjA5LThhODMtN2JmNzgyMTU2OTc5LTE0OTU3OTQ4%0ANzE5MTJ8UitTTXI
zUGRwb3d5QXB5WExoM01RU1grU1hzYWNjTEo3MzhjOHRt%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",
  "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"
}
```

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 where you want to transfer the License.
- 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'.
- License: The name of the license which the user wants to transfer.

```
{“licenses”:[
{
 "license": "CSR 10KV SECURITY 10M",
 "licenseType": "PERPETUAL",
 "quantity": 50,
 "targetVirtualAccount": "Physics"
},{
 "license": "CSR 1KV SECURITY 10M",
 "licenseType": "TERM",
 "precedence": "LONGEST_TERM_FIRST",
 "quantity": 50,
 "targetVirtualAccount": "VA2"
},{
 "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}’.”
}
```


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

List the available information on the Product Instances on the specified Account and local Virtual Account so that this information can be included easily in the Product Instance Removal API.

Request Parameters:

- smartAccountName: The SSM On-Prem Account where the user wants to search the devices.
- virtualAccountName: The Virtual Account Name where you would like to fetch the instance names.

- **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 first. For this parameter add, for example, ?udiSerialNumber=123456Albert45678901 to the end of the request URL below.
- 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/api/v1/accounts/ {smartAccountName}/virtual-accounts:/{virtualAccountName}/devices

Response Code: 200 OK


```
{
  "devices": [
    {
      "instanceName": "Albert-UCM3",
      "sudi": {
        "suvi": null,
        "uuid": null,
        "hostIdentifier": null,
        "udiPid": "UCM",
        "udiSerialNumber": "123456Albert45678901",
        "udiVid": null,
        "macAddress": null
      },
      "productTagName": "regid.2016-07.com.cisco.UCM,12.0_0511c508-37b4-45f0-ba73-bbbb402f44a4"
    },
    {
      "instanceName": "Albert-UCM1",
      "sudi": {
        "suvi": null,
        "uuid": null,
        "hostIdentifier": null,
        "udiPid": "UCM",
        "udiSerialNumber": "123456Albert456789",
        "udiVid": null,
        "macAddress": null
      },
      "productTagName": "regid.2016-07.com.cisco.UCM,12.0_0511c508-37b4-45f0-ba73-bbbb402f44a4"
    },
```

```
      {
         "instanceName": "local.lab",
         "sudi": {
            "suvi": null,
            "uuid": null,
            "hostIdentifier": null,
            "udiPid": "CSR1000V",
            "udiSerialNumber": "97N1PAGTEOZ",
            "udiVid": null,
            "macAddress": null
         },
         "productTagName": "regid.2013-08.com.cisco.CSR1000V,1.0_1562da96-9176-4f99-a6cb-
14b4dd0fa135"
      }
   ],
   "totalRecords": 3,
   "statusMessage": "",
   "status": "SUCCESS"
}
```


Product Instance Removal

You can invoke this method to programmatically remove devices that are registered in their SSM On-Prem Account. This method enables you to automate device removal as part of your network operations. You need to have the necessary **admin access privilege** within the SSM On-Prem Account/local Virtual Account to perform this request.

Request Parameters:

- smartAccountName: The SSM Account where the user wants to search the devices.
- virtualAccountName: The local Virtual Account Name from which you would like to fetch the instance names.
- **Payload Parameters**
- SUDI of Device
- Software/Product Tag Identifier

Response:

The local Virtual Accounts list for which the user is having access to.

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/api/v1/accounts/cisco.com/virtual-accounts/testVA/devices/remove

Request Payload

```
{
 "productInstanceRemoveRequests": [
   {
     "sudi": { "udiPid": "CSR1000V", "udiSerialNumber": "97N1PAGTEOZ" },
     "productTagName": "regid.2013-08.com.cisco.CSR1000V,1.0_1562da96-9176-
4f99-a6cb-14b4dd0fa135"
   }
 ]
}
```

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"
      }
    ]
  }
```

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

Related SYSLOG Message Text and Their Explanations

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 Cisco Smart Software Manager."

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 Cisco Smart Software Manager."

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}”" • "%{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}”." • "%{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}”."

Licenses Transferred	
	• "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}" • "%{count} “%{tag}” %{type} licenses in the Virtual Account “%{pool_name}” are set to expire in 1 day on %{end_date}"

Licenses Expired	
	• "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 Cisco Smart Software Manager."

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 Cisco Smart Software Manager."

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 Cisco Smart Software Manager."

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 an 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 an SSM On-Prem	
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 Cisco Smart Software Manager.
- 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)
- Cisco Smart Software Manager: 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

- swapi.cisco.com (6.3 and later)
  - IPv4: 146.112.59.25
  - IPv6: 2a04:e4c7:fffe::4

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.

Appendix

A1. Manually Backing Up and Restoring SSM On-Prem

CAUTION: When SSM On-Prem is associated with HA, you must backup and restore both the database 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: `docker ps`

Step	Action

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 7

You can initiate an on-demand backup and restore at any time by performing the following manual procedure (for Version 7 201907 to 202001 release).

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]:`
	`/backups/ssms-db-20201115160939.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 Release 7

NOTE: If the backup file is remote, you will need to first copy the backup file into the OnPrem Console backups directory.)

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/backup.sql.gz backups`

Step 3	List the files in the OnPrem Console backups directory using this command:
	`dir backups:`
	`FILESIZE FILENAME DATE`
	`894572b backups:backup.sql.gz 2020-01-08 18:23:49`

Step 4	Restore database from a backup file using this command: `$ database_restore backups:backup.sql.gz`
Step 4	Exit the application.

NOTE: Once registered and restored, an SSM On-Prem must be synchronized with Cisco Smart Software Manager to ensure the licensing information between the SSM On-Prem and Cisco Smart Software Manager is not out-of-sync.

CAUTION: This restore procedure can work on a backup generated using an earlier version (6x or later). Attempting to use a backup file created for a different software version, can generate unexpected results.

A.2 Product Compatibility Notice

Before the SSM On-Prem can accept registrations from product instances, it must register with Cisco Smart Software Manager. Previously, SSM On-Prem to Cisco Smart Software Manager registration required a 10-day wait because someone had to manually sign the Certificate Signing Request (CSR) from On-Prem to Cisco Smart Software Manager. This meant that if products wanted to connect to On-Prem, they must 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 Cisco Smart Software Manager is now signed immediately. However, there are changes that must be made to the product smart agents, SSM On-Prem and Cisco Smart Software Manager, 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 Cisco Smart Software Manager. In the new implementation to automate the trust chain validation, additional certificates were added, and we had 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 Cisco Smart Software Manager code would continue to function.

In the new implementation, smart agents, SSM On-Prem, and Cisco Smart Software Manager 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 Cisco Smart Software Manager before it can register the product. Product teams can decide to implement Smart Agent code 1.4+ at their own schedules, so we 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 Cisco Smart Software Manager 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 Cisco Smart Software Manager, 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 Cisco Smart Software Manager.
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 cert request can take from 2 to 10 days to be processed, the three-tier certificate will be obtained by On-Prem from Cisco Smart Software Manager during the sync to support three-tier smart agents.
Following are the current 3-tier products:

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)

A.3 Product Registration Example: Cisco Cloud Service Router (CSR)

For complete instructions for configuring the **Cisco Cloud Service Router (CSR)** product instance to communicate with the On-Prem, see the CSR Smart Licensing configuration, please refer to: http://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/csr1000Vswcfg/licensing.html

To 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 click **Smart Call Home Registration 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	Command	Action
Step 5	License smart registration	no device(config)# license smart url https://server/path
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	Command	Action
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 Cisco Smart Software Manager 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:

```
revocation-check none
```

A.4 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 2016 and 2019, complete these steps.

Step	Action
Step 1	On your system, navigate to **Service Manager > Active Directory Users and Computers**.
Step 2	Click **Create AD Group**.
Step 3	Enter an **AD Group Name**.
Step 4	Add **Members** to the group. **NOTE**: When you add an SSM On-Prem claim to this group, these users will have claims.
Step 5	(Recommended) Keep all other parameters with their default values.
Step 6	Next, navigate to **Server Manager Tools > AD FS Management**.
Step 7	Right-click **Application Group** and select **Add Application Group** from the drop-down list.
Step 8	Add an **Application Group Name**.
Step 9	Under standalone applications, select **Web API**.
Step 10	Click **Next >**.
Step 11	Copy the **Relying Party Identifier** to a safe place and click **Add**. **NOTE**: The Relying Party Identifier is used in the SSM On-Prem OAuth2 ADFS configuration.
Step 12	Click **Next>**.
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.
Step 14	Keep all the default values in each step clicking **Next** until you are done.
Step 15	Next, open the **Application Group** created in Step 8 and select **Add Application**.
Step 16	Select **Server Application** from the list and then click **Next**.
Step 17	Copy the **Client Identifier** to be able to add to the SSM On-Prem OAuth2 ADFS configuration
Step 18	Add the **Redirect URI** (found int the OAuth2 ADFS configuration) and then click **Next>**.
Step 19	Select **Generate a shared secret** and then click **Next>**. **NOTE**: The secret is unused.
Step 20	Open the **Application Group** you created and open the **API object** (double-click) you created in Step. You have now completed all the steps and can continue to associate the AD Group with SSM On-Prem RBAC claims.

Associating an AD Group with the SSM On-Prem RBAC Claims

Complete these steps to associate an AD group with the SSM On-Prem RBAC claims.

Step	Action
Step 1	Navigate to **Issuance Transform Rules > Add Rule...**
Step 2	For the claim, select **Send Group Membership** and then click **Next>**.
Step 3	Enter the **Claim Rule Name** and then browse and select the appropriate **AD User's Group**.
Step 4	Select a **Role for the outgoing claim type**.
Step 5	Enter **one of the claims** listed here into the **Outgoing Claim Value** field (such as ONPREM-SYSUSER). • ONPREM-SYSADMIN: (User's group: SLS-OAUTH\ONPREM-SYSADMIN, Outgoing claim type: Role, Outgoing claim value: ONPREM-SYSADMIN) • ONPREM-SYSOP: (User's group: SLS-OAUTH\ONPREM-SYSOP, Outgoing claim type: Role, Outgoing claim value: ONPREM-SYSOP) • ONPREM-SYSUSER: (User's group: SLS-OAUTH\ONPREM-SYSUSER, Outgoing claim type: Role, Outgoing claim value: ONPREM-SYSUSER)
Step 6	Click **Finish**. You are now ready to set client permissions.

Setting Client Permissions

Complete these steps to set client permissions for OAuth2 ADFS.

Step	Action
Step 1	Navigate to **Web API Properties > Client Permissions**.
Step 2	Click **Add...** to add a client.
Step 3	Select **client**(s) that will have permitted scopes such as: • allatclaimes • email • openid

You have now configured OAuth2 ADFS and AD Groups with an SSM On-Prem RBAC claim. Users in a configured AD group will have the access within SSM On-Prem specific to their assigned role such as administrator, system operator, or system user after they log into the SSM On-Prem via OAuth2 ADFS.

A.5 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

Acronyms

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

Getting Support

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 provides the following types of support:

Follow these steps these steps to open a support ticket:

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 Products & Services tab screen opens.
Step 3	On the right section of the tab screen, click **Open Case**.
Step 4	Make sure the Request Type is set to **Diagnose and Fix**, and then scroll down the screen to the **Bypass Entitlement** field.
Step 5	In the Bypass Entitlement field, select **Software Licensing Issue** from the drop-down list.
Step 6	Click **Next**.
Step 7	In the Describe Problem screen, select the **Ask a Question** for the Severity level.
Step 8	Enter the **Title** and **Description** and all **pertinent information**.
Step 9	Review the information you entered, and then click **Submit**. You license query has been submitted.

Opening a Case with Global Licensing Operations (GLO)

Traditional Licensing

To open a case for traditional licensing, go to the License Registration Portal to either generate, resend, or re-host your existing PAK-based licenses.

- Once in the License Registration Portal, click **Help** (top right corner of the screen).

Smart Software Licensing

Go to Smart Software Manager to track and manage your Smart Licenses.

Option 1:

- Once in the Cisco Software Central page, click **Help** (located on the right-hand side of the page). The Smart Software Manager help documentation opens. Use the search field to find the subject you need.
- In the Contents column on the left-hand side, scroll down and click **Feedback and Support**.
- Select **Smart Account Manager Support** and follow the steps (see option #2).

Option 2:

- From the Cisco Software Central page, click **Support** (located on the right-hand side of the page next to **Help**).
    - Enter the **details** about the issue
    - Fill in the **contact method**
    - Enter the **contact phone number**
    - Select the **Time Zone**
    - Click **Send**

Option 3:

- Send an email to **licensing@cisco.com**

Smart Accounts

Navigate to the “Administration” section of Cisco Software Central to either manage existing Smart Accounts or request a new one.

- Go to Request Access to an Existing Smart Account for getting access to your company’s account.
- Training and documentation are available here.
- To contact support, use **licensing@cisco.com**

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 because the licensing@cisco.com is only used to auto-create cases.