



Cisco Smart Software Manager satellite Enhanced Edition User Guide

First Published: 02/16/2015
Last Modified: 11/4/2018

Copyright © 2015 Cisco Systems, Inc.

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. All rights reserved. Copyright © 1981, Regents of the University of California.

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 NON-INFRINGEMENT 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)



The Java logo is a trademark or registered trademark of Sun Microsystems, Inc. in the U.S. or other countries.

Contents

Preface	v
Audience	v
Document Conventions.....	v
Obtaining Documentation and Submitting a Service Request.....	vi
Cisco Smart Software Manager satellite Overview	7
About Cisco Smart Software Manager satellite.....	7
Features.....	9
Feature Gaps from Previous Releases.....	12
System Requirements.....	12
Supported Web Browsers	12
Ports Used	12
Smart Software Manager satellite EE Overview	14
Multi-tenancy Account Management	14
SSM satellite EE System Roles	17
SSM satellite EE License Management Roles.....	17
SSM satellite EE User Workflow.....	18
Getting Started	19
SSM satellite EE Administration Portal	20
Users	21
Accounts.....	22
API Toolkit.....	25
Satellite APIs.....	28
Access Management	30
Network.....	34
System Settings.....	36
Synchronization.....	38
Software Download	42
SSM satellite EE Licensing Portal	44
Registering a satellite Account	44
Export Control Support.....	45
Application Redundancy Support.....	47
User Groups.....	49
Bulk Operations.....	51
Custom Virtual Account (VA) Tags.....	52
Search/Filter Virtual Accounts By Name or By Tag.....	54
License Tags.....	54

Adding License Tags.....	55
Search by License Tags.....	58
Advanced License Search/Advanced License View.....	59
Other SSM satellite EE Licensing Portal Functions.....	61
Backward Compatibility	62
Migration to SSM satellite Enhanced Edition	64
Troubleshooting	66
Satellite EE Issues.....	66
Client Registration Issues.....	66
Manual Synchronization Issues	67
Network Synchronization Issues.....	69
Appendix	70
Registering Product Instances to satellite.....	70
Invoking API Endpoints.....	71

Preface

[Audience](#) on page v

[Document Conventions](#) on page v

[Obtaining Documentation and Submitting a Service Request](#) on page vi

Audience

This guide is intended for site administrators who will manage Cisco Smart-enabled software installation and licensing.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
<i>Italic</i>	Italic text indicates arguments for which the user supplies the values.
[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 values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
screen font	Terminal sessions and information the switch displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
<i>italic screen font</i>	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note: Means *reader take note*. 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.



Cisco Smart Software Manager satellite Overview

[About Cisco Smart Software Manager satellite](#)

[Features](#)

[System Requirements](#)

[Supported Web Browsers](#)

[Ports Uses](#)

About Cisco Smart Software Manager satellite

[Cisco Smart Software Manager satellite](#) (SSM satellite) is a Smart Licensing solution that enables customers to administer products and licenses on their premises, instead of having to directly connect Smart Licensed enabled product instances to [Cisco Smart Software Manager](#) (Cisco SSM) hosted on cisco.com.

[Smart Software Manager satellite](#) has multiple deployment models:

Smart Software Manager satellite Classic:

- Targeted for small enterprises
- Operates at the Local Virtual Account level, supporting a single Virtual Account on Cisco Smart Software Manager (single tenant)
- Scales to 4,000 product instances
- Online or offline connectivity to Cisco

Smart Software Manager satellite Enhanced Edition (EE):

- SSM satellite EE is targeted for service providers and/or partners who need to manage their customer's account.
- New architecture and infrastructure with higher scalability and usability
- Supports multiple Local Accounts (multi-tenant)
- Scales to 10,000 product instances
- Online or offline connectivity to Cisco
- Allows downstream satellites to register to it, forming a hierarchical satellite structure (future) with the SSM satellite Lite Edition (LE)

*Smart Software Manager satellite Lite Edition (LE) (** Future):*

- SSM satellite LE is targeted for small enterprises

- Supports a single Local Virtual Account on SSM satellite Enhanced Edition (EE)
- Scales to 4,000 product instances
- Online or offline connectivity to SSM satellite Enhanced Edition

Today, SSM satellite Classic operates at the *Virtual Account* level within a customer’s *Smart Account* managed by Cisco Smart Software Manager. Thus, one customer can have many satellites but one SSM satellite Classic cannot be used to manage multiple customers. Furthermore, for customers with many Virtual Accounts, managing many satellites can be overwhelming as shown in Figure 1.

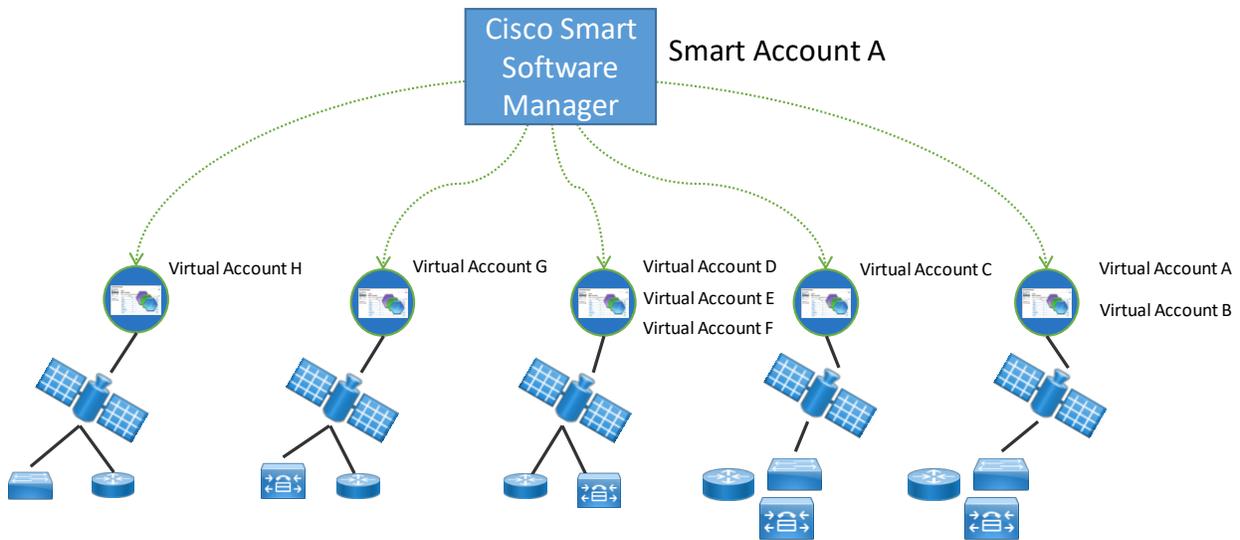


Figure 1 - Today's satellite structure (satellite Classic)

With the introduction of SSM satellite Enhanced Edition, though a single management portal, customers are now able to support multiple local Accounts, each linked to a Cisco Smart Account/Cisco Virtual Account pair. This is shown in Figure 2 below.

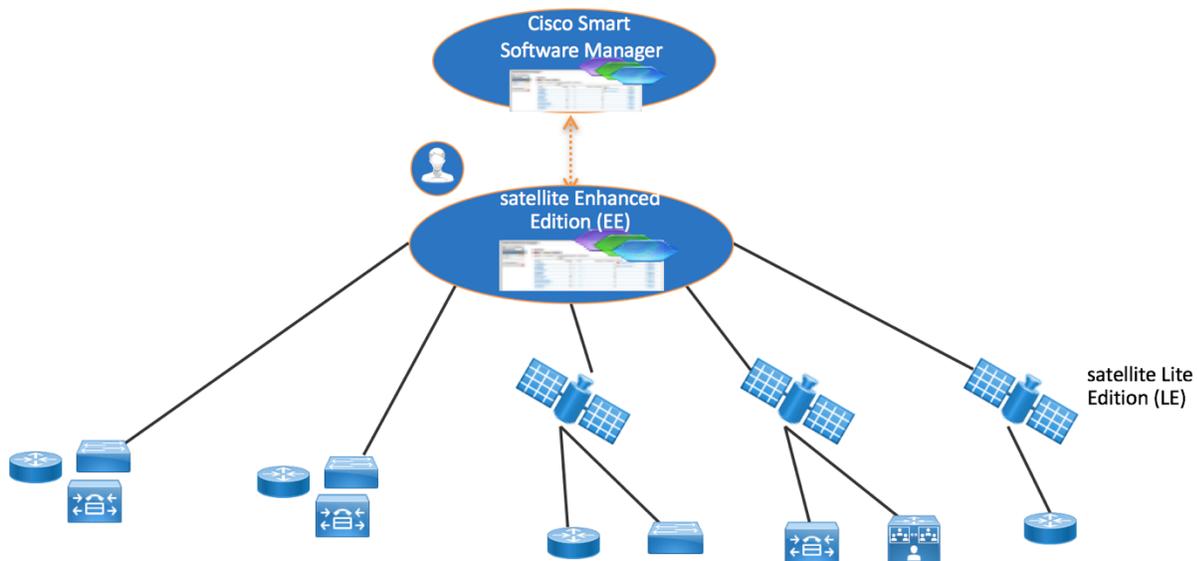


Figure 2- SSM satellite Enhanced Edition

Note: The SSM satellite Lite Edition (LE) is not yet available at the time of this writing, but it will function similarly to today's Smart Software Manager satellite Classic.

Features

The SSM satellite EE has a Licensing portal with similar functionality as software.cisco.com where users can manage their local Accounts, users, product instances, licenses, etc.

The SSM satellite EE has an Administration portal separately from the Licensing portal that allows for internal administrative functions such as system user creation, local Account creation, registration/synchronization, network, system and security settings, etc. This administration portal is restricted to only authorized users.

The Licensing portal is accessed via <https://<ip-address>:8443>

The Administration portal is accessed via <https://<ip-address>:8443/admin>

Key features of SSM satellite EE include the following:

Multi-tenancy - manage multiple customer Local Accounts in a single management portal

Separate Licensing and Administration portals



SSM satellite EE has two different portals for licensing management and system administration. SSM satellite Administration portal functions separately from the Licensing portal and allows for internal administrative functions such as user control, local Account creation, registration, synchronization, along with network, system and security settings, etc. This administration portal is restricted to only authorized users.

ISO Packaging

Satellite EE is packaged as a universal ISO which allows it to be exported to various image types as shown below:

- *OVA image* - An Open Virtualization Archive that contains a compressed, "installable" version of a virtual machine.
- *Hyper-V image* - Allows customers to install on a Hyper-V virtualized host of Microsoft Windows Server 2012.
- *KVM (Kernel-based Virtual Machine) image* - Allows customers to install on a virtualized Linux environment supporting Ubuntu and CentOS.

Note: Exporting of the ISO image to other image types is the responsibility of the customers and is not supported by Cisco.

System Security Enhancements

SSM satellite EE is packaged as a deployable ISO with a CentOS 7 Security Harden Kernel **and** Nessus Scans with Critical and Major (CVE) issues addressed.

User Authentication Control (LDAP & OAuth2)

A *System Administrator* can set the authentication method to be LDAP and OAuth2. If not specified, it will be using local authentication.

License Hierarchy

Enable borrowing of a higher-tier license to be fulfilled when a lower tier license is not available.

Local Account Administration and Licensing Management

Combined local Account administration and licensing management in a single portal 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



Allow for satellite to have a proxy between itself and Cisco Smart Software Manager for traffic separation.

Application Redundancy support - For application redundancy enabled products, to prevent double counting of licenses on active/active or active/standby or fail-over scenarios.

Export Control support - Allow customers located outside EULF/ENC to which US Export restriction apply to request specific export control licenses and associated quantity.

API Toolkit – Allow applications to call satellite APIs for virtual account, token, license, product instance, reporting, and alert operations.

User Groups - Group users so operations such as role assignment can be applied to multiple users within the group instead of individual users.

LDAP Groups – Group LDAP users so operations such as role assignment can be applied to multiple LDAP users within the group.

Custom Virtual Account Tagging – Allow local Virtual Accounts to be tagged for easy virtual account classification, grouping, locating and/or role assignment.

License Tagging - User-defined tags that can be created and tagged to licenses. They are useful for classifying, locating, and grouping licenses.

Virtual Account Search – Search local Virtual Accounts by Name or by Tag

Advanced License Search – Search Licenses based on detailed information such as SKU, Product Family, Expiration Date, or PAK (PAK # of a classic license that has been converted to Smart)

Bulk Operations - Enable transfer of multiple licenses between local virtual accounts

Configurable Banners and Login Information

Headers and footers and user login page on the satellite portal are configurable enabling them to be customized with meaningful classifications and information.

Scalability

- Up to 500 Local Accounts
- Up to 10K product instances

SSM satellite EE is designed to mirror Cisco Smart Software Manager's and Local Account Administration's experience through a common user interface and similar features. But instead of being hosted on cisco.com, it is available as an on-prem version. It has two separate portals: Administration and Licensing:

- The Licensing portal functions similarly to Cisco Smart Software Manager and Local Account administration.
- The Administration portal is used for system management functions mentioned above (network configuration, user creation, registration, synchronization, authentication setting, etc.). It also has other features not available on Cisco Smart Software



Manager such as syslog and proxy support. In the future, we will also be adding other features such as backup/restore, upgrade, security, high availability, and usage-based billing.

Feature Gaps from Previous Releases

Please note that existing features in satellite Classic 5.0.1 below are NOT available in this release and will be made available in future EE releases:

- DLC (Device-Led Conversion),
- 3rd party integration (Apple Push Notification and Text-To-Speech),
- Utility billing,
- Backup/Restore,
- High Availability

System Requirements

Note: Ensure that you are assigned to a Smart Account before you proceed with the tasks mentioned in this section.

Ensure that the software image supplied for the installation of Cisco Smart Software Manager satellite EE has the following configuration:

Minimum	Recommended
200 GB Hard disk	200 GB Hard disk
8GB Memory	8GB Memory
2 vCPUs	4 vCPUs

Your installation package of the universal ISO for Cisco Smart Software Manager satellite consists of the following components:

- **CentOS 7**
- **Smart Software Manager satellite Enhanced Edition**

For details on installing and setting up the satellite, see *Cisco Smart Software Manager satellite EE Installation Guide*.

Supported Web Browsers

The following web browsers are supported for Cisco Smart Software Manager satellite EE:

- Chrome 32.0 and later versions
- Firefox 25.0 and later versions
- Safari 6.0.5

Note: JavaScript 1.5 or later must be enabled in your browser.

Ports Used

Smart Software Manager satellite EE uses the following ports for various communication. Please ensure you have the following port numbers configured in your firewall rules:



- User Interface: HTTPS (port 8443)
- Product Registration: HTTPS (port 443), HTTP (port 80)
- Communication to CSSM: HTTPS (tools.cisco.com, api.cisco.com, clouso.cisco.com), port 443.

Smart Software Manager satellite EE Overview

[Multi-tenancy Account Management](#)

[Satellite EE System Roles](#)

[Satellite EE License Management](#)

[Satellite EE Workflow](#)

Smart Software Manager satellite EE has a new architecture and completely user interface from previous versions. It has containerized packaging with separate Licensing and Administration portals, multi-tenancy capability, new registration and synchronization procedures, new system roles and RBAC 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.

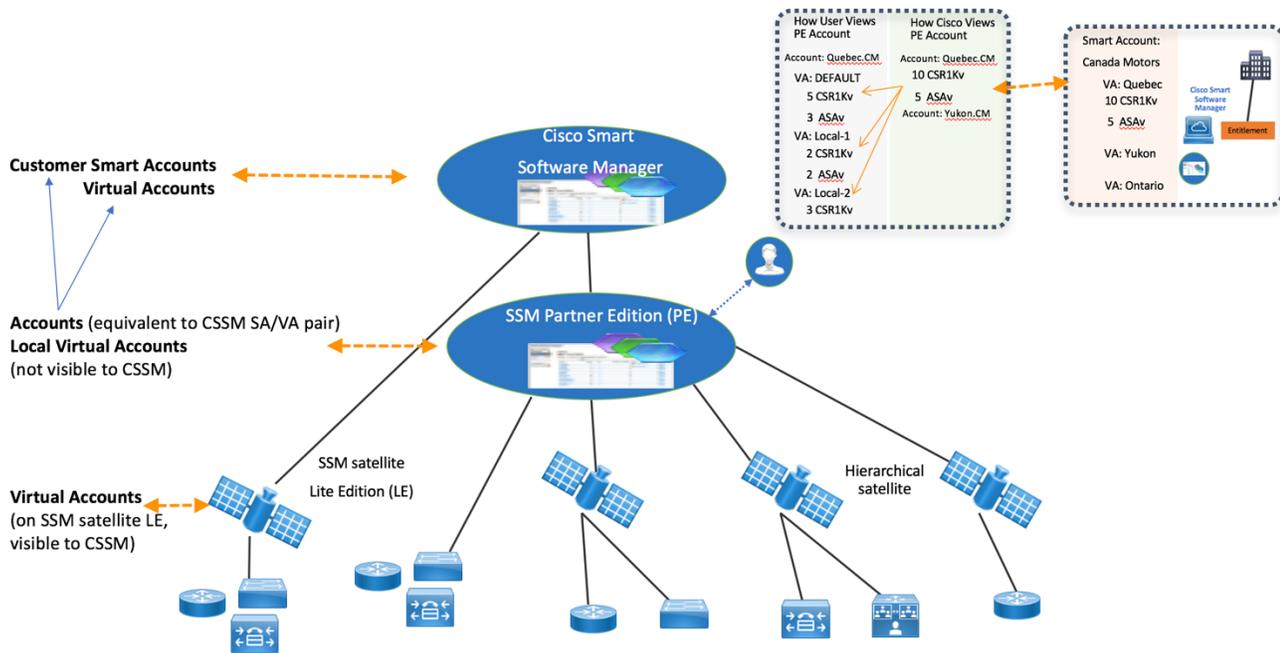
Multi-tenancy Account Management

On Cisco Smart Software Manager (CSSM), all licenses and product instances owned by a customer are managed in the customer's *Smart Accounts* and *Virtual Accounts* (collections of licenses and product instances organized by entities within the customer Virtual Account).

On SSM satellite EE, we represent a customer by a local Account (or simply Account), each corresponding to a Cisco Virtual Account within the Smart Account. License contained in the Cisco Virtual Account will be synchronized to the local Account and show up in the "DEFAULT" local Virtual Account. Local Virtual Accounts are created on SSM satellite EE are not visible on CSSM.

In summary, we have the following Account types and their relationship is depicted in the following diagram.

- *Smart Account, Virtual Accounts* on CSSM
- *Local Accounts* and *local Virtual Accounts* on SSM satellite EE
- *Local Virtual Accounts* on SSM satellite Lite Edition (not yet available)

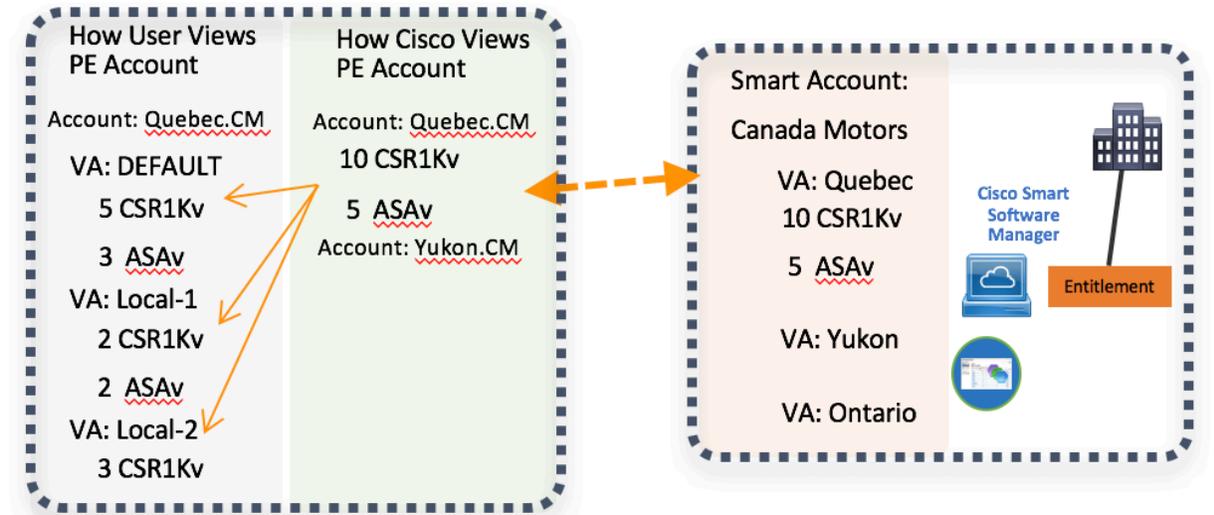


In the example above, Cisco Smart Account and SSM satellite EE local Accounts are further related as follows:

- The local Account *Quebec.CM* is created, it is associated with a Cisco Smart Account/Virtual Account pair, in this case *Canada Motors* and *Quebec* respectively.
- Cisco Smart Software Manager only sees satellite *Quebec.CM* with all the licenses in the *Quebec* VA; it does not know how the licenses are divided within the SSM satellite EE “DEFAULT” and any local Virtual Accounts that may have been created.
- An SSM satellite EE user can see and manage (create, delete, transfer) licenses in the Local *DEFAULT* Virtual Account and all the local Virtual Accounts (*Local-1*, *Local-2*) under SSM satellite EE Account *Quebec.CM*.
- What is visible to Cisco Smart Software Manager is the total count in *Quebec* VA of *Quebec.CM* satellite.
- During a synchronization to CSSM, SSM satellite EE aggregates the license counts from the *DEFAULT* Virtual Account and all local Virtual Accounts associated with *Quebec.CM* local Account and represents its entire count to CSSM.

In summary,

- Cisco Smart Software Manager user sees;
 - Smart Account *Canada Motors*
 - Virtual Account *Quebec*
 - satellite *Quebec.CM*,
- SSM satellite EE user sees;
 - Local Account *Quebec.CM*
 - Local Virtual Account “*DEFAULT*”
 - Local Virtual Accounts “*Local-1*”, “*Local-2*”



- In this example, the license counts on CSSM and SSM satellite EE should look like below:

Satellite EE		CSSM	
		Smart Account: Canada Motors	
Account: Quebec.CM		satellite: Quebec.CM	
Default VA		Quebec VA	
	5 CSR1Kv		10 CSR1Kv
	3 ASAv		5 ASAv
Local-1 VA			
	2 CSR1Kv		
	2 ASAv		
Local-2 VA			
	3 CSR1Kv		

Each local Account name must be unique on SSM satellite EE, and normally the Cisco Virtual Account associated with the satellite EE would be the same as the local Account name to make management easier. This choice can lead to issues if the SSM satellite EE is registered to different Cisco Smart Accounts (different customers) each having Virtual Accounts with the same names.

In our example, the chosen local Account name is *Quebec.CM* for Canada Motors, and if the SSM satellite EE was also registered to another customer, say American Card, which had a Cisco Virtual account named “Quebec”, a different local Account name would need to be assigned, for example *Quebec.AC*, on the SSM satellite EE.

SSM satellite EE System Roles

SSM satellite EE has different roles: System and Licensing roles. System roles apply to the entire SSM satellite EE system. It allows the user to configure and operate satellite EE, such as configuring the IP address, approving new local Accounts, changing banner texts, performing synchronizations to CSSM, upgrading satellite, etc. These operations are performed on the SSM satellite EE Administration Portal based on the following roles:

- *System Administrator*
 - Full administrator access to all local Accounts
 - Approve new local Accounts
 - Delete all local Accounts
 - Perform registration and synchronization which are only available on the Administration portal
 - Configure IP addresses, NTP, Authentication, Syslog, Proxy
- *System Operator*
 - Full administrator access to all local Accounts.
 - Perform registration and synchronization which are only available on the Administration portal
 - View IP addresses, NTP, Authentication, Syslog, Proxy
- *System User*
 - No access to Administration Portal
 - Restricted to RBAC on the local Accounts off Licensing portal. That is, a System User has specific account access such as local Account Administrator, local Account User, Virtual Account Administrator, and Virtual Account User

SSM satellite EE License Management Roles

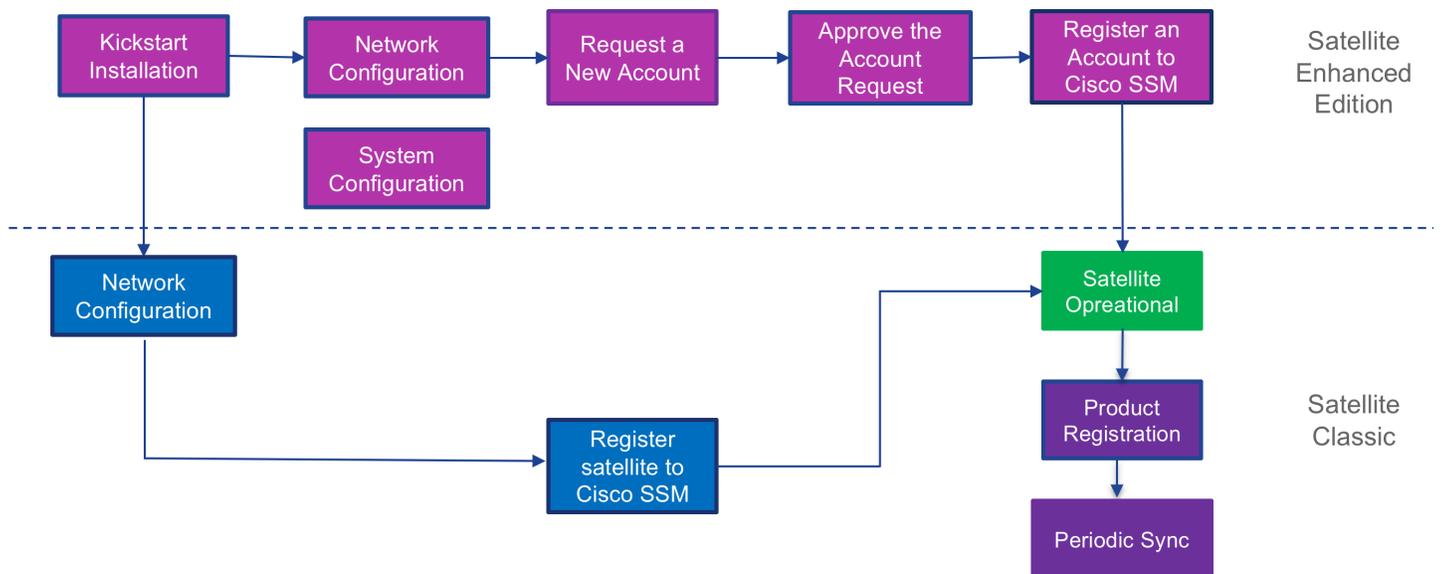
For the satellite *System User* role, the following Role Based Access Control (RBAC) applies to their local Accounts on the Licensing portal. These controls are provided at the Local Account and Local Virtual Account level to provide grainer access. Each of these roles, while independent from Cisco Smart Software Manager, function similarly to it.

- *Local Account User*
 - Generate a token with the local Virtual Accounts within the local Account
 - View local Virtual Accounts within the local Account
 - View events for the local Virtual Accounts within the local Account
- *Local Account Administrator*—Has rights to set up and manage all local Accounts.
 - All the access of the local Account user
 - Create a new user
 - Create/delete local Virtual Accounts within the local Account
 - Transfer product instances between local Virtual Accounts within the local Account

- Manage (create, delete) satellites
- Cannot edit satellite EE Local Account properties (*this is different from CSSM Smart Account Administrator role*)
- *Local Virtual Account User*
 - Generate token within the assigned local Virtual Accounts
 - View & add a satellite with the assigned local Virtual Accounts
 - View events for the assigned local Virtual Accounts
- *Local Virtual Account Administrator*
 - All the access of the local Virtual Account user
 - Create a user

SSM satellite EE User Workflow

Once SSM satellite EE is installed, the system needs to be configured in order to login to its user interface. In addition, each SSM satellite EE local Account needs to register with Cisco Smart Manager in order to manage licenses in it. Following is a typical workflow for SSM satellite EE:



Getting Started

Following are the steps to get your satellite operational and access Smart Licensing functions:

1. **Kickstart Installation** – User follows the installation guide to deploy the satellite via the **Kickstart** procedure.
2. **Network Configuration** – User configures the IPv4 address(es) of the satellite using the **Network** option from the Administration portal. Up to 2 interfaces can be configured.
3. **System Configuration** – User configures login message and banner, authentication method (LDAP, OAuth2, local).
 - After completing these steps, the SSM satellite EE system is operational locally.
 - To access **Accounts** within the Licensing portal, a user must request a new local Account or access to an existing local Account. For greenfield deployments, the user needs to request a new local Account.
 - For new local Account requests, the local Account must be registered to a Cisco Smart Account/Cisco Virtual Account pair (using CCO credentials). When the registration is complete, the Account can be used by the user to manage their licenses.
4. **Requesting a New Account** - User requests a new local Account after logging into the Licensing portal at <https://<ip-address>> or <https://<ip-address>:8443>. Once this is done, the request shows up under **Account Request** tab in the **Account** widget of the satellite Administration portal. Another way to request a new local Account is by using **Accounts, New Account** options in the Administration portal.
5. **Approve a new local Account** – The Administrator logs into the Administration portal at <https://<ip-address>:8443/admin>, under **Accounts, Account Requests** to approve the request in #4. When the **Approve** action is completed, it is registered to Cisco Smart Software Manager and the satellite Licensing portal is fully functional. The user can now use **Smart Licensing** option.
6. **Request Access to an Existing Account**
 - a. User requests an access to an existing local Account after logging into the Licensing portal at <https://<ip-address>>.
 - b. Approve access to an existing local Account – The Administrator logs into the Licensing portal, select **Manage Account, Accounts Requests**, and see the **Pending** local Accounts waiting to be approved. Note that this workflow is different from a new local Account request in that it is performed in the Licensing portal and does not go through the account registration process (the existing account is already registered to CSSM).

The user can now use Smart Licensing features such as register the product(s), create local Virtual Accounts or users, view/transfer product and license status, etc.



SSM satellite EE Administration Portal

[Users](#)

[Accounts](#)

[API Toolkit](#)

[Access Management](#)

[Network](#)

[Settings](#)

[Synchronization](#)

[Software Download](#)

The Administration Portal is used to setup the satellite system before it can be operational. It is shown below and accessed via at <https://<ip-address>:8443/admin>.

Note: The System Health display is automatically displayed and cannot be turned off at this time.

Smart Software Manager satellite Enhanced Edition

System Health
Good
Your machine is working well

Server Name: CentOS
Version: 6.1.0
Uptime: 6:32 hours

Resource Monitor Percentage
CPU
RAM
DISK

Interface: ens32 ↑ 6340.4 ↓ 10020.2

Recent Alerts

- ⊘ Synchronization Error
- ⊘ This is a Logical Account Alert
- ⊘ Insufficient Licenses
- ⊘ Insufficient Licenses
- ⊘ Insufficient Licenses

Connected Users

User	Time
admin	02:59:38
admin	03:13:00
admin	03:08:37
admin	03:09:32
admin	02:03:27

The SSM satellite EE Administration portal allows for system level functions such as:

- **Users** - Manage users such as creating system users with sysadmin, sysops, or user roles.
- **Accounts** – Create or Approve request for SSM satellite EE Local Accounts
- **Network** - Configure or change network IP, NTP, DNS server, default gateway addresses, proxy parameters, syslog configuration
- **API Toolkit** – enable creation of client and resource authentication credentials for accessing satellite API
- **Access Management** – configure authentication method and LDAP groups
- **Settings** – Configure banner text, authentication method, and syslog parameters
- **Synchronization** – Synchronize Accounts with Cisco Smart Software Manager
- **Software Download** – An (optional) local software repository available to SSM satellite EE users. The Admin uploads software images to this repository allowing users to download them from the Licensing portal if they are entitled.

Users

The User widget allows the System Administrator or System Operator to create local users (in the local authentication database) and configure advanced parameters such as password rules and auto lock features for the users to be created.

When you create a user on the Administration portal, it is added to the local authentication database (not LDAP, SSO, or another authentication server) with a default system role of System User (the lowest authority). An LDAP or SSO user is created within that authentication server and can login to the Licensing Portal as long as the authentication method is configured accordingly. This user can request access to an existing local Account or a new local Account before he/she can use the satellite Licensing portal for Smart Licensing functions.

To create a new user, use the following procedures:

- Click on **Users** from the Administration portal.
- Click on **Create**.
- Fill in the information requested on the screen. The required fields (identified with *) such as **User Name, Email, Password, Language**.
- Click **Add User**.

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

A User can be disabled and removed by the System Administrator or System Operator role.

“Disable” - User still exist 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.

“Remove” - Option shows after the “Disable” action has been performed.

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

Accounts

A new or existing SSM satellite EE local Account must be available before Smart Licensing functions can be performed in the licensing portal. Until this is completed, all other Smart Licensing options are grayed out.

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.

During the SSM satellite EE local Account registration, a Cisco Smart Account/Virtual Account pair has to 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.

Account Request via Licensing portal

The SSM satellite EE local Account can be requested from the Licensing portal via the following options:

- **Request an Account** or
- **Request Access to an Existing Account**

To request a new local Account on the Licensing Portal, perform the following steps:

- Click on **Request an Account**.
- Fill in the information such as Email, Message to Creator, local Account Name, Cisco Smart Account, Cisco Virtual Account. The required information is labeled with *.
- A correct Cisco Smart Account/Virtual Account pair must be specified for registration to succeed. Note that the Smart Account must have existed on CSSM. A Cisco Virtual Account is created if it does not exist on CSSM.
- Click “**Continue**”.

Once this is submitted, the System Administrator can approve it in the Administration Portal.

Account Request via Administration portal

A new local Account can (optionally) be created by a System Administrator or System Operator via the **Accounts** widget on the Administration portal. Use the following procedure:

- Open the **Account** widget
- Click on **Accounts**
- Click on **New Account**
- Type in the information such as Account Name, Cisco Smart Account, Cisco Virtual Account, and Email for Notification. The required fields are labeled with *.
- Click **Submit**.

- Enter the Cisco Smart Software Manager Smart Account and Virtual Account pair you wish the local Account to be registered to. Note that the Smart Account must have existed on CSSM. A Cisco Virtual Account is created if it does not exist on CSSM.
- A message that a new Account request has been created, and ready to be registered to Cisco is displayed.
- The Account request then appears on the **Account Requests** tab in the **Accounts** widget.

Account Request Approval (Account Registration in Network Mode)

The local Account request shows up in **Account Requests** in the Administration portal, awaiting the System Administrator to approve and register.

- The System Administrator clicks on **Approve** under **Actions** to register to the local Account to CSSM.
- Click **Next**.
- The System Administrator enters his/her CCO ID credentials when prompted for Cisco Smart Account/Virtual Account access on CSSM.
- Click **Submit**.
- Satellite EE provides a status of the registration progress.
- Upon successful registration, a message will show “Account was created successfully”.
- And the local Account shows up as **Active** under **Accounts** tab.
- The local Account is shown as a satellite registered on Cisco Smart Software Manager **Satellites** pane. Note that the local *Account* name is the *satellite name* on the “**General**” tab, and the local Account name shows up under the “**Virtual Accounts**” tab.

Note: Only one single Cisco Virtual Account is supported per SSM satellite EE local Account.

If you add another Cisco Virtual Account to the SSM satellite EE on CSSM under **Satellites** pane, only the Cisco Virtual Account originally registered is used to exchange license information during the synchronization. Additional Cisco Virtual Accounts will be ignored.

Account Approval (Account Registration in Manual Mode)

You can select the **Manual Registration** instead of **Approve** to manually register the local Account to Cisco Smart Software Manager. While manual registration is supported, it’s not recommended as you have to keep track of the specific registration request/authorization file(s) for each registration.

Use the following steps to manually register a local Account to Cisco Smart Software Manager:

- Select “**Manual Registration**” from the local Account name.



- Generate a local Account Registration File.
- Log into Cisco Smart Software Manager.
- Navigate to “**Satellites**”.
- Click on “**New satellite**”
- Fill in satellite information.
- On “**Choose File**”, select the file you created in the 2nd step above.
- Generate and Download the Authorization File.
- Upload the local Account Authorization File from CSSM onto the satellite by “**Choose File**” option.
- Click **Register Account**.

Account Request Reject

The System Administrator can also “Reject” the local Account and provide a reason, which is included in the email to be sent to the requestor.

To Reject a local Account,

- Under **Actions**.
- Select “**Reject**”
- Enter a message or reason so it can be included in the email to be sent to the requestor.
- The local Account is not registered to CSSM.

Account Deactivation

A local Account can be deactivated, activated or deleted once it’s been registered with Cisco. The “Deactivate” option will disable access to the local Account in the Licensing portal. The account is not removed from the SSM satellite EE, and no User permissions are changed.

To Deactivate a local Account,

- Navigate to the local Account
- Under **Actions**, select **Deactivate**
- Enter a message or reason so it can be included in the email to be sent to the requestor.
- Select **Deactivate** or **Cancel**

Account Deletion

In the case where the satellite local Account is registered to an incorrect Cisco Smart Account/Virtual Account pair, it can be deleted.



The following procedure on the Administration portal must be followed exactly for it to work:

1. Remove all PIs on all local virtual accounts in the satellite local Account.
2. Synchronize with CSSM so that CSSM reflects that the PIs are longer on satellite. Note that the only way to remove PIs on satellite and have them reflected on CSSM is to synchronize satellite to CSSM after removing them from satellite because satellite is the source of truth for all PIs registered to it.
3. **Deactivate** the local Account.
 - a. Navigate to the local Account and click **Deactivate**.
 - b. The local Account shows as **Inactive**.
4. **Delete** the local Account
 - a. Under **Actions**, select **Delete** the local Account. Note the **Delete** option is only visible after the local Account has been deactivated.
 - b. Click **OK** to confirm Delete local Account or **Cancel**.
 - c. All registered product instances and local Virtual Accounts are removed from this local Account.
5. Go to CSSM and remove the satellite representing this local Account. At this point, the VAs associated with this satellite are empty because the PIs were removed in step 1.
 - a. Navigate to **Satellites** pane
 - b. Select the satellite corresponding to this local Account
 - c. Select **Remove** from “**Actions**”
 - d. Confirm satellite removal.
6. After this action, the satellite is removed from CSSM and the local Account can be re-registered again to the correct Cisco Smart Account/Virtual Account pair.

Account Activation

The Activate option is available for any account which has been deactivated. When set back to active, the account will again show up on the Licensing portal and will be available to any user which has authorization.

- To **Activate** and account, right click on Account Name
- Select “**Activate**”
- Enter a reason for activation
- Select **Activate** or **Cancel**

API Toolkit

As an application, you need to authenticate prior to using the satellite APIs. This is done via the API Toolkit widget.

You first 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 satellite Enhanced Edition. If this is not done, your application will receive “403 Access Restricted” error. We embedded an internal OAuth2 with the satellite software (<https://github.com/oauth-xx/oauth2>).

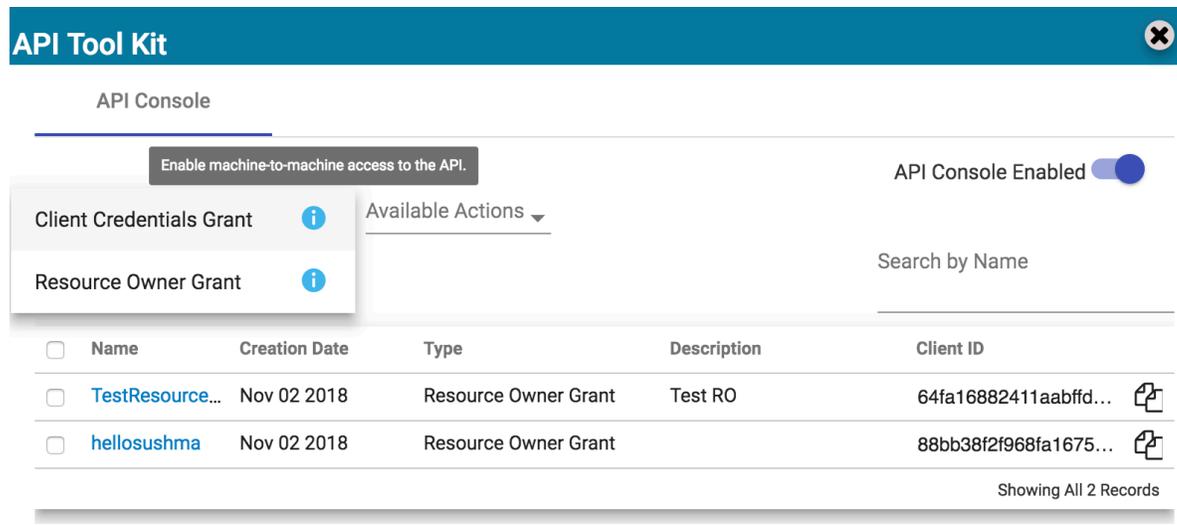
API Console Access must be enabled by the System Administrator. Once this is enabled, a System or SysOps user can create Client or Resource credentials to get the Access Token (from the embedded OAuth2 server) to invoke the APIs. There are two types of credentials: Client and Resource grants.

- Client Credentials Grant: Enable machine-to-machine access to the API so that it can issue the API call.
- Resource Owner Grant: Enable the 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 have been generated, they need to be used by the application to request the OAuth2 server to generate the Access Token that is used as the header of the HTTP request(s) for the API endpoints.

Enable API Console

The “API Console Enable” toggle must be turned on by the System Administrator.



API Tool Kit

API Console

Enable machine-to-machine access to the API.

API Console Enabled

Client Credentials Grant *i*

Resource Owner Grant *i*

Available Actions ▾

Search by Name

<input type="checkbox"/>	Name	Creation Date	Type	Description	Client ID
<input type="checkbox"/>	TestResource...	Nov 02 2018	Resource Owner Grant	Test RO	64fa16882411aabffd...
<input type="checkbox"/>	hellosushma	Nov 02 2018	Resource Owner Grant		88bb38f2f968fa1675...

Showing All 2 Records

Create OAuth2 Grants

The Client Credentials or Resource Owner Grants need to be generated to obtain the Access Tokens from the embedded OAuth2 server.

Client Credentials Grant

Name *
CC2

Description
|

Expiration Date *
10/5/2018

Client ID *
a3b8dc4aa84032c36252b5d945e6f1ce7afb7133de927a5969eab50d23210d7e

Client Secret *
.....

[Click here to set API Access Control](#) [Regenerate Client Secret](#)

Key Restrictions
The key is unrestricted. To prevent unauthorized use of SSM satellite, restrict your key.

Set API Access Control

Within the API Console, enable the Account and local Virtual Account access for the application that use the Client Credentials by selecting “Click here to set API Access Control”

Procedure:

1. Click on Accounts
2. Select Roles (Account Admin, Account User, Per Virtual Account) and click Add

Client Credentials Grant

Accounts Role Add

Search by Name

Account Name	Role	Actions
APITK1004	Account Admin	Remove...

Showing All 1 Records

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



Get Access Tokens

Both Client Credentials Grant and Resource Owner Grant use the same URL to call the satellite: **POST "/backend/oauth/token"**.

Example:

```
Chloes-MacBook-Pro:oauth2 ccorrigan$ ./gen_token.sh
Enter 1 for a Client Credentials Grant, or 2 for Resource Owner Grant.1
Enter the Client IDa3b8dc4aa84032c36252b5d945e6f1ce7afb7133de927a5969eab50d23210d7e
Enter the Client Secretf3e35a2e0c7380b4e4c50642742087d7900ae4f6c877699155035321e404e971
Enter the IP Address of the ISO/QA Server. Ex: 172.18.77.90172.20.222.254

{"access_token":"72d6f18ad55e49f8cf8acde2e9f917e462ba75f908ce611ad1221160a19c9ebc","token_type":"Bearer","expires_in":3600,"created_at":1538676798}Chloes-MacBook-Pro:oauth2
ccorrigan$
```

Call APIs

After receiving an access token in the previous step, the remote systems use that access token to call the satellite APIs. In the case of Client Credentials Grant, the executions of the API functions are authorized by roles granted to the OAuth Client Credential Grants (shown above in API Access Control). In the case of Resource Owner Grant, the executions of the API functions are authorized by the user's roles in the system.

Satellite APIs

There are 21 APIs that have been available on Cisco SSM previously. More detailed information on these Cisco SSM APIs can be found at:

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

Of these APIs, only 14 are available on satellite as we do not support Smart Account or SLR/PLR feature.

Cisco SSM APIs are as follows:

1. Smart Account
 - a. Smart Account Search - Provide the available smart accounts for the search criteria provided. Irrespective of what Smart Accounts you have access to, this API will provide all the Smart Accounts matching the search criteria to the users who have access to the APIs. **Not applicable to satellite.**
 - b. Validate User Access – V1 enables a user to validate the access privilege held by them within their company's smart account **Not applicable to satellite.**
 - c. Validate User Access – V2 - This is an enhancement to V1 which makes the domain query parameter optional. If the Smart Account domain is not specified, then this API should return all the Smart Accounts that the user is associated with along with their roles in each of those Smart Accounts. **Not applicable to satellite.**
2. Virtual Account
 - a. Create a Virtual Account - allow users to create Virtual Accounts under the given Smart Account domain
 - b. List Virtual Accounts - list all the Virtual accounts in the specified Smart Account domain for which the requesting user has access to.
 - c. Delete a Virtual Account - allow users to delete a Virtual Account under the given Smart Account domain.
3. Tokens

- a. Create a new token - Generate a new token within a specified Smart Account/Virtual Account user for product registration. User needs to have necessary Admin or User access privileges either at the Smart Account level or at the specified Virtual Account level.
- b. List tokens – Get existing active tokens within a specified Smart Account/Virtual Account.
- c. Revoke tokens - Revoke the valid tokens available for the given Smart Account domain and the Virtual Account. The User can pass an array of the Tokens that they want to revoke.

4. Licenses

- a. Smart License Usage - Give the licenses usage in the specified Smart Account Domain and the optional Virtual Accounts.
- b. License Subscriptions Usage - Return the License Subscriptions on the specified Smart Account Domain and the optional Virtual Accounts.
- c. Transfer Licenses - Transfer the available licenses from one virtual account to another virtual account with in the same Smart Account Domain.
- d. Reserve Licenses - Allow 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 request. If any reservation didn't go through, appropriate error message will be given. **Not applicable on satellite.**
- 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. **Not applicable on satellite.**
- f. Confirm SLR Update - Allow the user to confirm the previously updated license reservations. Without confirming the previous update, the user will not be able to submit another update reservation request. **Not applicable on satellite.**

5. Devices/Product Instances

- a. Product Instance Usage - List the device usage on the specified Smart Account Domain and the optional Virtual Accounts specified. Based on access you have on the Smart 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 Smart 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 Smart Account Domain.
- d. Product Instance Removal - Users can invoke this method to remove devices that are registered in their Smart 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 smart account/virtual account to perform this request.
- e. Product Instance Remove V2 (PLR/SLR) - This is an enhancement API to the existing product instance removal API to remove the Product instances of a Universal or Specific license reservation. Not available on satellite.

6. Alerts –allow users to view the Alerts that are available for the Smart Entitlements. There are 13 alerts as follows.

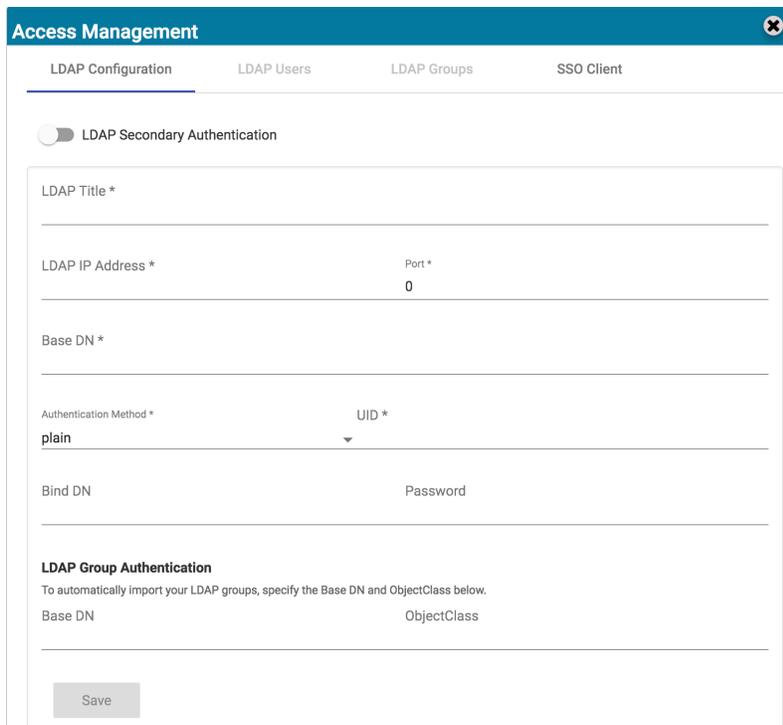
- a. Update License Agreement (not applicable on satellite)
- b. Insufficient Licenses
- c. Licenses Expired
- d. Licenses Expiring
- e. Licenses Not Converted
- f. Licenses Converted

- g. Product Instance Failed to Renew
- h. Product Instance Failed to Connect
- i. Satellite Unregistered and Removed
- j. Synchronization Overdue
- k. Authorization Pending
- l. Authorization File Ready
- m. Synchronization Failed

Access Management

The Access Management widget in the satellite Administration portal provides the following access management functionality:

- LDAP Configuration – configure LDAP server for satellite to use as an external authentication mechanism.
- LDAP Users – As the LDAP Users login to satellite and authenticated, they are populated to the LDAP Users tab. Use this tab to see which LDAP users have access to satellite Accounts and local Virtual Accounts. Once these LDAP users log into satellite they can be assigned RBAC to the satellite Accounts/local Virtual accounts as needed.
- LDAP Groups – LDAP user groups are defined on the LDAP server and consists of groups of LDAP users. Satellite integration with LDAP allows it to assign RBAC of the accounts and local Virtual Accounts to these LDAP groups. So instead of assigning individual user one at a time the access to the Account and local Virtual Accounts in satellite “Users” tab, you can use the LDAP Groups tab in this widget to assign these resources to the LDAP user groups.
- SSO Configuration – Not supported.



The screenshot shows the 'Access Management' widget with the 'LDAP Configuration' tab selected. The interface includes a toggle for 'LDAP Secondary Authentication' which is currently off. Below this are several input fields: 'LDAP Title *', 'LDAP IP Address *', 'Port *' (set to 0), 'Base DN *', 'Authentication Method *' (set to 'plain'), 'UID *', 'Bind DN', and 'Password'. There is also a section for 'LDAP Group Authentication' with fields for 'Base DN' and 'ObjectClass'. A 'Save' button is located at the bottom left of the form.

LDAP Configuration

To enable satellite to use an external LDAP server for external authentication, use LDAP Configuration option.

Recall that there are 3 options when configuring authentication methods:

- None –using a local authentication database (not using an external authentication server)
- LDAP – using Lightweight Directory Access Protocol
- SSO – using Single Sign-On (not currently supported)

Depending which method is selected, you have to enter the appropriate parameters.

- For local authentication, select **None**
- For LDAP authentication enter the information below:
 - LDAP Title: Any title
 - LDAP IP Address – the IP address or FQDN of the LDAP server
 - Port - port to access LDAP service
 - Base – LDAP DN (Distinguished Name)
 - Authentication Method – select the option below
 - Plain
 - SSL
 - TLS
 - UID – Name of User Identifier field
 - Username – user name to LDAP server
 - Password – password to the LDAP server
 - Click **Save**
- SSO is currently not supported.

Access Management ✕

LDAP Configuration LDAP Users **LDAP Groups** SSO Client

Update LDAP Data Search by Name

Group Name	Account Roles	Users
users	Account Admin: 0 Accounts Account User: 1 Accounts Virtual Account Admin: 1 Accounts Virtual Account User: 0 Accounts	0
Directory Operators	Account Admin: 0 Accounts Account User: 0 Accounts Virtual Account Admin: 0 Accounts Virtual Account User: 0 Accounts	0
Directory Clients	Account Admin: 0 Accounts Account User: 0 Accounts Virtual Account Admin: 0 Accounts Virtual Account User: 0 Accounts	0
Directory Consumers	Account Admin: 0 Accounts Account User: 0 Accounts Virtual Account Admin: 0 Accounts Virtual Account User: 0 Accounts	0
administrators	Account Admin: 0 Accounts Account User: 0 Accounts Virtual Account Admin: 0 Accounts Virtual Account User: 0 Accounts	0

Showing All 5 Records

Each LDAP group can be assigned RBAC to the various resources (Account or Virtual Accounts). Below is an example of an LDAP group “users” given access as a satellite Account User role.

Group Details: users

Accounts Role

Daves Test Account Account User **Add**

Search by Name

Account Name	Role	Actions
No Records Found		

Save Cancel

Below is an example of an LDAP group “users” given access as Virtual Account Admin access to a local Virtual Account.

Group Details: users

Accounts Role

Search by Name

Account Name	Role	Actions
<input type="checkbox"/> Daves Test Account	Per Virtual Account <input type="text"/>	Remove...

Virtual Accounts Role

Daves Test VA Virtual Account...

Virtual Accounts

Showing All 1 Records

Network

Satellite supports configuration of IPv4, dual stack IPv4 and IPv6 addressing schemes. The Network widget allows users to configure network parameters such as IP address, netmask/prefix, default gateways, and proxy settings used by SSM satellite EE.

On the **General** tab, enter the Satellite Name, Default Gateway IP address, and DNS Settings.

Network
✕

General

Network Interface

Proxy

General

Enter the server name, DNS server and default gateway information.

Satellite Name:

Default Gateway Settings:

<p>IPv4</p> <p><input type="text" value="172.18.77.1"/></p>	<p>IPv6</p> <p><input type="text" value="fe80::2d0:2ff:fe85:8000"/></p>
---	---

DNS Settings:

Primary DNS

Alternate DNS

Alternate DNS

Interface Support

SSM satellite EE adds support for multiple interfaces (up to 4) to be configured and used for User management, Product Registration, and communications with CSSM. However, only 2 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 eth0 and eth1 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.

Interface Status

In the **Network Interface** tab, the interfaces have the following status:

- Connected - Interface has a connection and is configured with an IP address.
- Connected (Unconfigured) - Interface has a connection but is NOT configured with an IP address.
- Disconnected (Unconfigured) - Interface does not have a connection and therefore not configured with an IP address.

Interface Zones

The firewall configuration provides for traffic separation and security control as needed:

- Product is for product registration.
- Management is for User Interface Management
- You can click on **Edit Interface** to modify specific configured parameters such as IP address, Subnet Mask, IP Gateway, Default Gateway, Firewall Ports Requirements.
- Click **Ok** to finish

Edit Network Interface

IPv4
IPv6

IPv6 Setup Is On

* IPv6 Address
2001:420:2170:200f:250:56ff:fe8f:6689

* IPv6 Prefix
64

IPv6 Gateway
fe80::2d0:2ff:fe85:8000

Default Gateway Is On

Firewall Ports Requirements

Product and Management (Public)

Management Only (User)

Product Only (Product)

Cisco Communication Only (DMZ)

Ok
Cancel

Proxy Support

Proxy support allows SSM satellite EE to configure an HTTPS proxy between it and Cisco Smart Software Manager (products => satellite => HTTPS proxy => Cisco SSM), enabling customers to easily control both inbound and outbound traffic from/to satellite according to their firewall rules.

Use the following procedure:

- Slide the **Use A Proxy Server** to **On**
- Enter the **Proxy Username** and **Proxy Password**.
- Click **Apply** or **Reset**

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

System Settings

The **Settings** widget allows the System Administrator to configure various settings needed by the SSM satellite EE, such as a system

banner, authentication method, syslog parameters, and language settings.

Messaging

Messaging tab allows the user to configure various messages

- Enter **Banner Text**.
- Click on **Display Message** and select Text/Background Colors.
- Type in **Login Page Message**.

Syslog

Satellite syslog support allows for SSM satellite EE Events to be sent to a remote syslog server.

To enable syslog support, use the following procedure:

- Select the **Enable Remote Logging** option for the events to be sent to the syslog server.
- Configure the **Syslog Server Address** and **UDP Port** number.

The software sends the events based on the following severities:

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

Language

Today, we support only English.

Email

You can configure the SMTP parameters to get email notifications from satellite.

- Enter SMTP Server URL, SMTP Port, and Hello Domain

Time Settings

Today, you can set the time manually or allow it to synchronize with NTP. The time zone for your SSM satellite EE 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 local time of the system.

Under Time Settings, enter the following information:

- Select **Time Zone** from the drop down.
- Slide **Manually Set Time** to **On** to set it manually, or
- Turn on **Synchronize with NTP Server** and enter the **NTP Server Address**. Click on **Synchronize Time Now**.
- Click **Apply**.

Console Message of The Day Settings

- This option allows the user to set the greeting message on the SSM satellite EE console.
- **Message of the Day** is the display after the user logs in.
- **Before-login-Message** is the console display or greeting before the user is prompted to login.
- Click **Save**.

Synchronization

Once registered, an SSM satellite EE local Account is recommended to be synchronized with Cisco Smart Software Manager periodically to ensure the licensing information between the SSM satellite EE and Cisco Smart Software Manager is not out-of-sync.

Satellite support on-demand, scheduled, and manual synchronizations. When you click on the “**Synchronization**” widget on the Administration portal, you can see a list of local Accounts and their status and available options.

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 satellite EE 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 (1-year duration) allowing it to continue functioning.

Note: A local satellite 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 satellite) and registered again. This means that all of the product instance and licensing information about that SSM satellite EE is lost.

Synchronization Types

In the past, SSM satellite Classic and Cisco Smart Software Manager operated on a delta synchronization model, which means that only incremental changes on product instances, license purchases and consumption would be sent and received. However, in the case where the SSM satellite EE 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 (versus delta or standard synchronization) is introduced when Cisco Smart Software Manager detects that it needs the SSM satellite Classic or EE 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 along to the satellite. The System Administrator can also initiate full or partial synchronizations.

Synchronization Alerts

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

- Synchronization Overdue (minor alert) - 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)

- Synchronization overdue (major alert) - synchronization hasn't happened for 90 to 364 days:

"Synchronization Overdue: Satellite has not synchronized in X days." (X will be between 90th – 364th day, depending on last synchronization date)

- Re-registration Required (major alert) – synchronization has not happened in 365 days:

"Re-registration Required: Satellite was not synchronized for 365 days and must be re-registered with Cisco Smart Software Manager."

After 1 year of non-synchronization, the SSM satellite EE local Account will still be present (not deleted) on the CSSM; however, the ID certificate would have expired and the satellite EE local Account can no longer synchronize. License counts on SSM satellite EE and CSSM may be out-of-sync, and neither network or manual synchronization can be performed. Existing products will not get valid responses from the satellite, and no new products can be registered. However, it only affects this local Account. The only recourse is to delete the satellite Account, re-register it to CSSM, and re-register all of the product instances to the local Account (see Account Deactivation and Account Deletion on page 21-22).

On-Demand Network Synchronization

Network synchronization assumes there is an Internet connection to CSSM from satellite. On each local Account, you can choose to perform either a **Standard Synchronization Now** or **Full Synchronization Now** for Network Synchronization.

When you click on the **Standard Synchronization Now** or **Full Synchronization Now**, you may be presented a login screen to the Cisco Virtual Account if it's the first time or if your session has expired and you need to be re-authenticated to Cisco Smart Software Manager.

Procedures to synchronize.

- Open the **Synchronization** widget.
- On the local Account, under **Actions**, select **Standard Synchronization Now** or **Full Synchronization Now**.

- Enter your **Cisco Smart Account** credentials
- Click **Ok**
- Afterwards, the spinner appears and the **Alerts** column gives the status of the synchronization as it progresses.

Synchronization ✕					
Accounts			Schedules		
0 Major 0 Minor		Search by Name			
Name	Satellite Name	Last Synchronization	Synchronization Due	Alerts	Actions
Red_Hat_Account	Red_Hat_Account	2018-Apr-26 20:48:31	2018-May-26 20:48:31	Synchronization Successful	Actions
Account_smart_license_init		2018-Apr-26 20:43:45	-	Synchronization In Progress	Actions

Note that **Satellite Name** is the name of the **satellite on CSSM** and **Account Name** is the local Account Name on the satellite. They are typically the same. In the case where a user changes the Satellite Name to something else on CSSM, satellite EE will reflect that new name in the Satellite Name field after it detects in a synchronization response.

If you click on the “Name” of the Local Account, you will see the information about it in the **General** tab such as local Account Name, Cisco Virtual Account, Cisco Virtual Account, Cisco Satellite Name, UID, Date Registered, Last Synchronization and Synchronization Due date.

There are also event log entries that gives statuses 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 Cisco Smart Software Manager and SSM satellite EE.

In this case, you can perform a manual synchronization which results in an SSM satellite EE synchronization request file to be created, uploaded to Cisco Smart Software Manager, and a synchronization response file to be received on SSM satellite EE to reflect the same license information.

You can click on “Manual Synchronization” and select Standard or Full Synchronization.

Manual Synchronization procedure:

1. Click the **Synchronization** widget from the Administration portal
2. Under **Accounts**, click on **Actions**
3. Select **Standard** or **Full Synchronization**

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 and opens the local file directory to save.
 - b) Choose a location where you want to save the data file.
5. Login to the Cisco Smart Software Manager and click the **Satellites** tab.
6. In the **Satellites** page, locate the satellite for which you want data synchronization or click on the **New Satellite** to add a new satellite
7. If you are adding a new satellite, a screen appears so you can:
 - a) Input the new satellite name in the **Satellite Name** box.
 - b) Click on **Choose File** to select a registration file.
 - c) Select from a list of existing satellites or **New Local Virtual Account**.
 - d) If new Local Virtual Account, type the name of the Local Virtual Account and click **Add**.
8. If you are selecting an existing satellite from the list, click **File Sync** link against the satellite in the **Actions** column of this page.
9. In the **Synchronize Satellite** dialog box, click **Choose File** to upload the data file that was generated in the satellite step 4.
10. Click **Generate Response File** to generate a response file that has the data synchronized.
 - a) The **Synchronization Response File Generated** dialog displays.
 - b) Click **OK** to continue.
11. Click **Download Response File** to download to your local hard disk.
12. Go back to SSM satellite EE in the **Synchronization** widget of the Administration portal
13. Click **Browse** to select the synchronization response file you just downloaded in step 11.
14. Click **Upload** dialog box to upload the response file and complete the manual synchronization process.

After this step completes, the license entitlement and usage on both Cisco Smart Software Manager and local Account are identical. All of the licenses in the DEFAULT and local Virtual Accounts associated with the satellite local Account added together equal the count in the Cisco Virtual Accounts of the said satellite on CSSM.

Scheduled Network Synchronization

In addition to manual synchronization per account, SSM satellite EE provides the ability to **Schedule** all Local Accounts to be synchronized with Cisco on a specified interval. The default schedule is once per 30 days, but the automatically scheduled synchronizations can be daily, weekly, or monthly, and, depending on the frequency, the data on the satellite can be as current as the

portal on a daily basis.

Global Synchronizations 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 the settings in the individual local Accounts:

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

Synchronizations Schedule

You can set schedule frequency (Daily, Weekly, Monthly) and Time of Day for the Local Accounts as shown below.

Note: This schedule applies to ALL the local Accounts. There is not a way to set individual schedule(s) for each account.

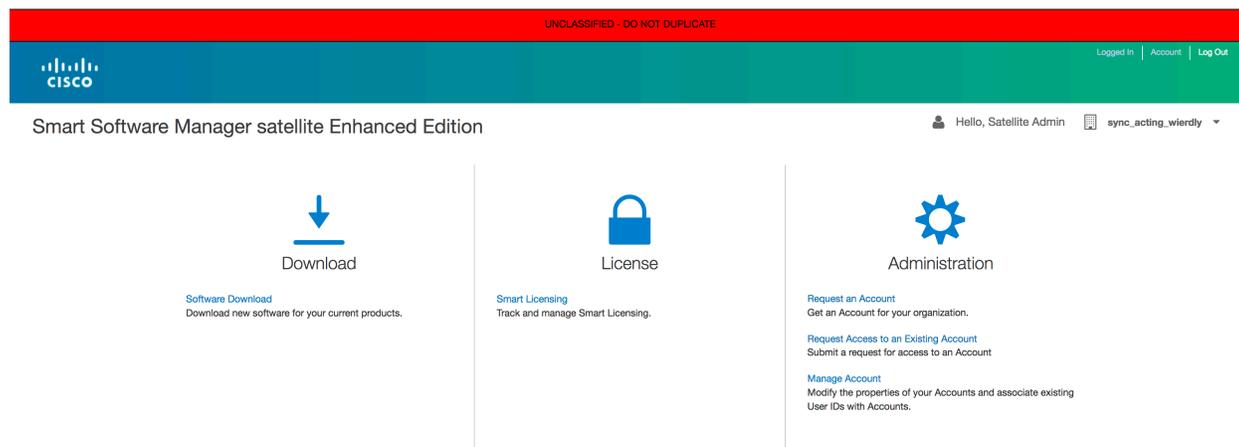
Currently, there is not a way to disable the scheduled synchronizations globally. To disable scheduled synchronization for individual local Accounts, use the following procedure:

- Select the **Account**
- Click on **Disable Scheduled Synchronization**.

This will cause the scheduled synchronization for that local Account to be skipped.

Software Download

The SSM satellite EE System Administrator can turn on **Show Software Downloads** in the **Software Download** widget. This action enables the **Software Download** menu (most left) to show up on the Licensing portal.



The screenshot shows the Cisco Smart Software Manager satellite Enhanced Edition interface. At the top, there is a red banner with the text "UNCLASSIFIED - DO NOT DUPLICATE". Below this is a green header bar with the Cisco logo on the left and "Logged In | Account | Log Out" on the right. The main content area is white and contains three widgets:

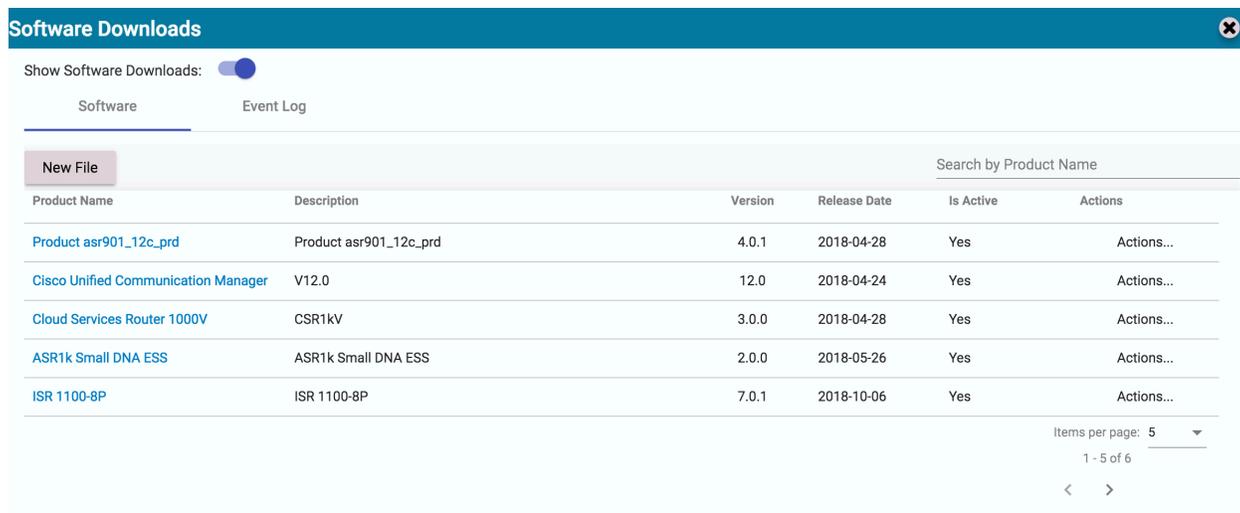
- Download:** Features a blue downward arrow icon. Below it, the text reads "Software Download" and "Download new software for your current products."
- License:** Features a blue padlock icon. Below it, the text reads "Smart Licensing" and "Track and manage Smart Licensing."
- Administration:** Features a blue gear icon. Below it, the text reads "Administration" and lists several actions: "Request an Account" (Get an Account for your organization), "Request Access to an Existing Account" (Submit a request for access to an Account), and "Manage Account" (Modify the properties of your Accounts and associate existing User IDs with Accounts).

At the bottom of the interface, there is a user profile section showing "Hello, Satellite Admin" and a user ID "sync_acting_wierdly" with a dropdown arrow.

From the Licensing portal, you can download the software that have been uploaded by the System Administrator for your local Account. The System Administrator can upload any software images available on CCO onto the Administration portal **Software Download** widget. But first, he/she needs to download them from CCO to his computer and upload them to the Administration portal as follows:

- Click on **New File**.
- Enter the Product information as it shows up on CCO download page.
- Browse the file from your computer
- Click **Save** to upload it to satellite Administration portal.

After uploading, the Administration portal Software Downloads looks like the following. You can click on the Product Name to get additional information about the specific uploaded image.



The screenshot shows the 'Software Downloads' interface. At the top, there is a toggle for 'Show Software Downloads:' which is turned on. Below this, there are two tabs: 'Software' (selected) and 'Event Log'. A 'New File' button is visible on the left. The main area contains a table with the following data:

Product Name	Description	Version	Release Date	Is Active	Actions
Product asr901_12c_prd	Product asr901_12c_prd	4.0.1	2018-04-28	Yes	Actions...
Cisco Unified Communication Manager	V12.0	12.0	2018-04-24	Yes	Actions...
Cloud Services Router 1000V	CSR1kV	3.0.0	2018-04-28	Yes	Actions...
ASR1k Small DNA ESS	ASR1k Small DNA ESS	2.0.0	2018-05-26	Yes	Actions...
ISR 1100-8P	ISR 1100-8P	7.0.1	2018-10-06	Yes	Actions...

At the bottom right of the table, there is a pagination control showing 'Items per page: 5' and '1 - 5 of 6'.

Once uploaded to the Administration portal, these software images show up under the Licensing portal for the local Account after the product successfully registers. That is, when each product is registered, the software ID of the registered product is checked against the images already loaded in the Administration portal and made available to the user for download on the Licensing portal.



SSM satellite EE Licensing Portal

[Registering a satellite Account](#)

[Export Control Support](#)

[Application Redundancy Support](#)

[User Groups](#)

[Bulk Operations](#)

[Custom Virtual Account Tags](#)

[Search/Filter Virtual Accounts By Name or By Tag](#)

[License Tags](#)

[Search By License Tags](#)

[Advanced License Search/Advanced License View](#)

[Other SSM satellite EE Licensing Portal Functions](#)

Registering a satellite Account

SSM satellite EE Licensing Portal has a similar user interface to Cisco Smart Software Manager, allowing customers to perform local Account Administration and Smart Licensing operations.

The Account Administration option allows a customer to create a new local Accounts, request access to an existing local Account, and manage the local Accounts (i.e., create local Virtual Account, add users to local Virtual Accounts, etc.).

Note that **Smart Licensing** and **Manage Account** options are grayed out when the user first login without a local Account. Therefore, you must request a local Account and register your local Account to Cisco Smart Software Manager as follows:

- **Request an Account** on Smart Licensing portal and tie it to a Cisco Smart Account/Virtual Account pair. If the Cisco Virtual Account does not exist on CSSM, it will be created during the registration process.
- Go into Administration Portal <https://<ip-address>:8443/admin>
- Approve the local Account request on **Account Requests** tab by selecting **Approve** under **Actions**
- Enter your CCO/SSO credentials for the Cisco Smart Account.
- You will get a successful registration message.
- SSM satellite EE local Account is now registered with CSSM and you can use Smart Licensing features.

Export Control Support

Overview

Previous export control support on satellite 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 Smart Account representing the customer is classified as to whether or not 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 to which US export restrictions apply. These customers are not allowed to generate export-control-allowed tokens today. However, they can apply and receive special permissions for Export Licenses and turn on specific restricted functionality authorized by those Export Licenses.

Updated Export Control Authorization Workflow

At a high level, the new Export Control support on satellite includes:

1. The Product generates a “Not-allowed” registration token from a local Virtual Account on satellite and registers to it. Note that this type of customers cannot generate an “Allowed” registration token (i.e., this option is not available on the Licensing portal for them).
2. The Product requests a restricted license and quantity from satellite via a command or Graphical User Interface (GUI) action, which need to be authorized from Cisco Smart Software Manager (Cisco SSM).
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. Satellite updates its GUI under the “Products Instance Tab” to indicate the status of the request (License Authorization Pending).
5. When a synchronization is done on satellite, it sends the restricted license request it receives from the product to Cisco SSM
 - a. If the satellite is in manual mode, there is a dismissible alert in the Administration portal to remind the user to perform a manual synchronization so that the Cisco SSM authorization can come down to satellite.
 - b. If the satellite is in network mode, the next synchronization request to Cisco SSM will contain the export control restricted license authorization response.
6. When satellite receives the response from CSSM, it processes the request, updates the alerts accordingly with the success or failure message and the associated reason(s).
 - a. If authorized, satellite updates its Product Instance tab indicating the correct reserved export license count.
 - b. If not authorized due to the license not available, a status is reflected on the satellite Product Instances tab. If there are other types of errors such as bad format, invalid export control tag, etc., these statuses are sent to the products only and not available on the satellite 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 satellite would get the cancellation request from the product, informs the product to check in later for the cancellation authorization status, and sends it along for authorization from Cisco SSM.

New Export Control Alerts

There are several new alerts in the “Product Instances” tab on the satellite 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 SSM.

- License Return Pending = when a product requests a cancellation of an Export Control license and is waiting for an authorization from Cisco SSM.
- 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 none is available in the local Virtual Account.
- Export License Not Sufficient = when an Export Control license has been requested by the product, but only some is available (not sufficient in quantity) in the local Virtual Account.

Product Instance and License Transfer Behaviors

Product Instance and License transfer behaviors are different when a license is export restricted. Note that this behavior is only for local Virtual Account on satellite. Recall the following product instance (PI) and license transfer.

PI Transfer

Satellite PI transfer between local virtual accounts works similarly as CSSM.

- Non-restricted licenses being consumed by PI.
 - 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'll get a warning "License Shortage" message.
 - The available license(s) (Purchased Qty) in "From local VA" are not transferred with the PI transfer. You have to 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 additional verbiage shown below:

Transfer Product Instance ? x

Name: UDI_PID:pid_pid_008; UDI_SN:sn_pid_008; UDI_VID:vid_pid_008;
(CSR1KV)

Transfer

i 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.

License	Description	Expires	Quantity
BAT_Export_test	BAT_Export_test	- never -	1

- 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 1st place if it didn't have available licenses. So, the destination VA will never go OOC.

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 OOC condition which is not allowed for Export Control.

License Transfer

Recall that Cisco SSM is the source of truth for all license entitlements and satellite is the source of truth for product instance registrations and license consumption. This dictates that licenses cannot transfer outside of CSSM. However, on satellite, since all licenses in the local Virtual Accounts are not visible to Cisco SSM, the license transfer behavior between local VAs in satellite is similar to CSSM. During a synchronization of satellite to Cisco SSM, all product instances and licenses are aggregated across all satellite local Virtual Accounts and updated in Cisco SSM and vice versa.

CSSM and satellite have following behaviors for license transfer:

- Non export-restricted license transfers
 - Only purchased quantity licenses is transferred (not in-use quantity) on Licenses Tab. If all licenses are in-use (e.g., 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 SSM/satellite allows the license transfer for 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 SSM/satellite allows the license transfer for available quantity (balance) WITH export control verbiage as shown:

 Because this license enables 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 SSM/satellite does NOT allow the license transfer because allowing that would render the "From VA" OOC and we do not allow OOC for Export Control. The Transfer/Preview is grayed out

Application Redundancy Support

Overview

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

Currently product High Availability 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, 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.

- An indicator that this is an application redundant configuration
- Role: Active or Standby
- Peer information

- An application unique identifier (UID) so Cisco SSM or satellite can match up multiple usages of the same license.

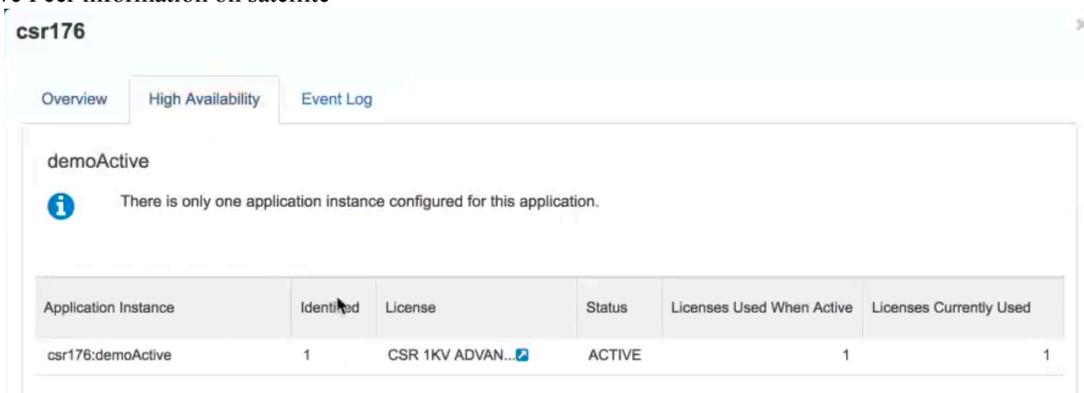
With this additional information, Cisco SSM and satellite will know a particular license in-use is being shared between two applications and it will know the Unique Device Identifier (UDI)s of the devices hosting those applications.

With this additional information Cisco SSM and satellite shows 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 would use the license count from the previous active to avoid double counting.
 - Show which licenses in-use on a device that is being shared.

Application Redundant Enabled Product Instance Workflow

1. Register product instances to satellite
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)
 - a. Configure the Active peer to point 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]
 - b. Configure the Active/Active peers with similar information.
3. Request licenses on both Active and Standby (or Active/Active) peers. Since Cisco SSM and satellite 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.
 - a. Active Peer information on satellite



csr176

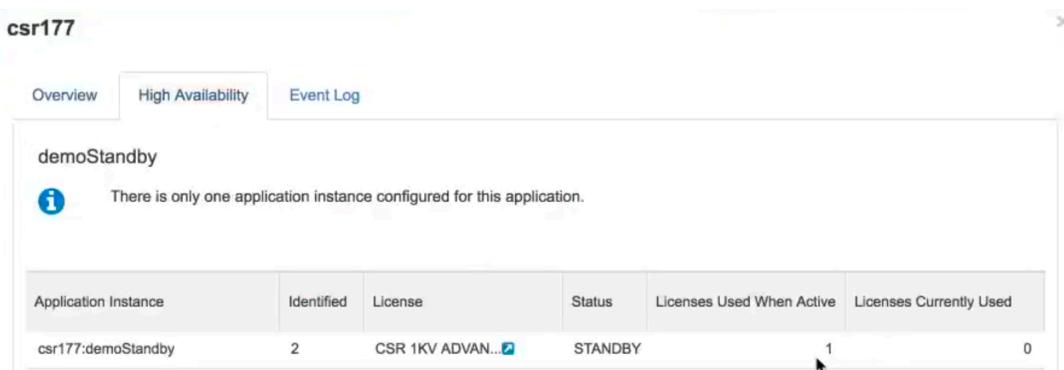
Overview High Availability Event Log

demoActive

i There is only one application instance configured for this application.

Application Instance	Identified	License	Status	Licenses Used When Active	Licenses Currently Used
csr176:demoActive	1	CSR 1KV ADVAN...	ACTIVE	1	1

- b. Standby Peer information on satellite



csr177

Overview High Availability Event Log

demoStandby

i There is only one application instance configured for this application.

Application Instance	Identified	License	Status	Licenses Used When Active	Licenses Currently Used
csr177:demoStandby	2	CSR 1KV ADVAN...	STANDBY	1	0

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 SSM or satellite would be able to show that the license is now consumed by the new Active (old Standby).

Synchronization File Changes for Application Redundancy

Satellite needs to add the Application Redundancy information to the synchronization request when it synchronizes with Cisco SSM ensure that Cisco SSM has the same peer information. This way, the Cisco SSM's Product and License tabs would match the satellite. An example of the Application Redundancy is shown below:

```
1 | :ha_attributes:
2 |     :application_name: Scott
3 |     :app_role: ACTIVE
4 |     :app_id: '1'
5 |     :peer:
6 |     - :name: Schrute
7 |       :role: STANDBY
8 |       :id: '2'
9 |       :product_instance_identifier: 250cafe6-a06d-48fd-8b5f-8a58806fbacd
```

UI 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.

User Groups

User Groups are a way to group users so operations can be applied to multiple users within the group more efficiently. Instead of having to assign access to satellite Accounts or local Virtual Accounts to each user multiple times, you create a user group of multiple users and apply the role assignment to that user group.

Note that users on satellite can consist of local users (created in the Administration portal under User widget), or imported from a federated authentication protocol (e.g., LDAP, OAuth2) via the Access Management configuration. In the latter case, only after the user logs into the satellite, is he/she added to the satellite User widget and you can perform RBAC for the satellite Account or local Virtual Accounts.

Add a User Group

When you create a User Group, you are automatically the group owner. A group owner can delete the user group and add members to the group.

To create a new User Group, use the following procedure:

- From the main satellite menu, click on Manage Account.
- Navigate to User Groups.
- Click on New User Group.
- Enter the User Group name and description (optional).
- Click Create.

- The user group is listed showing the User, Group Owner access, and whether he/she is an Account user.
- A successful creation message appears on the screen and a notification email to send to the user, provided that SMTP is properly configured on the satellite.

Edit a User Group

If you are the group owner, you can edit your User Group.

- Click on I Want To Manage Users off your User Group name.
- Click on the Edit button  next to the User Group Name to edit it.
- You can change the Group Name or Description and save it.

Delete a User Group

If you are the group owner, you can edit your User Group.

- Click on I Want To Manage Users off your User Group name.
- Click on Delete User Group.

Add member(s) to a User Group

You can add users to a User Group one at a time or in mass by uploading a csv file.

- To add members individually, click on I want to Manage Users.
- Enter the member email or user ID (local, LDAP, or OAuth2 user).
- Check or leave Group User unchecked if you don't want to make the added user the group owner.
- Click Add.
- To add multiple members by uploading a CSV file.
- Make sure the CSV conforms to the correct template. The csv has the following fields: First Name, Last Name, UserId, and isOwner
- Click on Upload Users.
- Browse the file or drag it from your computer.
- You see a message File Uploading 100%.
- Click X to close this modal.
- The users in your CSV files are added to the UI.
- If there are errors, they are displayed in red.

Delete member(s) in a User Group

- Navigate to the User Group and click on I want to Manage Users.
- Select the user(s) and click the Delete icon  Delete .

Assign local Virtual Account Access to a User Group

You can assign access to your local Virtual Account(s) so that all members of that User Group can have a particular RBAC (VA Admin or VA User) to those local Virtual Accounts. In the case that the members in the User Group already has individual access to these local Virtual Accounts, the highest roles win. For example, *User1* previously has VA Admin access to *VA-1* via individual assignment and you assign a User Group *Group1* (for which *User1* is a member of) access to *VA-1* as VA User, *User1* retains VA Admin access.

Assign VA Access to User Groups by VA Names

- On the main User Management screen, navigate to I want to Manage Virtual User Access
- You are presented with 4 quadrants.
- The top left quadrant you can select all or the individual VA by Name.
- Select the VAs and they are marked with checked boxes
- Click on Assign Roles to Selected Virtual Accounts.
- Select Virtual Account Admin or Virtual Account User and the selected VAs go to the top right quadrant.
- You can click X or Delete All to remove them from the right quadrant to start over again
- Once you have the roles you want, click Apply.
- Now, all your members in the selected User Group has the access for the role you selected above.

Assign VA Access to User Groups by VA Tags

- If you select By Name, the local Virtual Accounts are listed on the top left quadrant.
- If you select By Tag, the VA Tag(s) are listed on top left quadrant.
- Select the VA Tag from the top left quadrant and they get added to the bottom left quadrant.
- Select Assign Roles to Selected Virtual Accounts and the VAs affected By Tag show up on the bottom right quadrant.
- Click Apply as above.

Send message(s) to a User Group

You can send messages to a User Group by selecting I want to Send Message to User Group. Here, you can send as follows:

1. To all users of the User Group including group owners and group members.
2. To User Group owners only, or
3. To User Group members.

After selecting the recipient, type the message you want and click Send. A successful message appears and email is sent if your SMTP is set up correctly.

Download Users

- Navigate to I want to Manage Users.
- Click on the Download User icon 
- A file named “GroupName.csv” is downloaded with the following fields: First Name, Last Name, UserId, and isOwner.

Bulk Operations

Bulk Operations allows you to transfer multiple licenses between a pair of **local** virtual accounts as opposed to having to transfer individual licenses one at a time as in the past. This operation is only available for license transfer, not product instance transfer.

Procedure:

- Navigate to the local Virtual Account.
- Click on Licenses tab
- With “Show License Transactions” not checked, select multiple license entries
- The Available Action box becomes enabled. This is grayed out if multiple license entries are NOT selected. In this case the single transfer action is available on the license entry.

- Click on Transfer.
- You are presented with a modal to Transfer To or Transfer From.
- Select the toggle for Transfer To/Transfer From
- Select the Transfer To/Transfer From local Virtual Account accordingly.
- Put the quantity you want to transfer in the Transfer box.
- Note that you can only transfer the maximum value in the “Balance” column.
- Click Preview to see the value being added/subtracted.
- Click on Transfer.

Note that the single license transfer function is still available on the Actions off the license entry.

Custom Virtual Account (VA) Tags

All Virtual Account operations on satellite are *local*. That is, when a VA or License tag is created on the satellite or CSSM, they are local to each system and not federated across satellite and Cisco SSM.

There are two types of tags on satellite: Custom VA Tags and License Tags.

- Custom VA tags are those that can be associated with local Virtual Accounts
- License tags are those that can be associated with licenses

Custom VA tags are user-defined tags that can be created and tagged to local Virtual Accounts. They are useful in performing various operations to a group of local Virtual Accounts (classifying, grouping, locating, and role assignment). The following operations can be used with custom local VA tags:

1. Create a custom local VA tag
2. Tag it to a group of local VAs (on existing or new local VA creation workflow)
3. Search the tagged local VAs by these tags
4. Assign specific roles (VA Administrator or VA User) to a set of local VAs grouped by a tag

Create A Custom VA Tag

Procedure:

- Select the Manage Account option on satellite Licensing portal.
- Click Custom Tags.
- Click on New Virtual Account Custom Tag.
- Enter the required (*) fields: Tag Name, Required for All Virtual Accounts (*Mandatory/Optional*), Tag Value Assignment Options (*One Tag Value Only* or *Allow Multiple Tag Values*).
 - *Mandatory* means you must assign the local VAs to the tags being created. The workflow takes you to a list of Virtual Accounts to assign the custom VA tags.
 - *Optional* means you can choose to assign the local VAs to the tags being created
 - One Tag Value Only: You can assign multiple values to this tag. However, you can only assign one tag value to one local VA. For example, once you assign the VAs one tag, the VAs do not appear on the left quadrant on the GUI to be re-assigned another tag.
 - Allow Multiple Tag Values: You can assign multiple values to this tag. You can assign multiple tag values to one or more local VAs. For example, once you assign the VA a particular tag, the VAs can appear on the left quadrant in the GUI to be re-assigned another tag.
- Click Next.
- Click “Add Virtual Account Custom Tags”.

- If you selected *Mandatory*, you will be presented a list of local Virtual Accounts Impacted to add tags.
 - Select Tag Values for each local Virtual Account and click Save.
- If you selected *Optional*, you have the option to assign local VAs to the tags being added.
- The next steps allow you to assign the tags you are about to create to various local Virtual Accounts.
 - Click on the  to assign roles (VA Administration/VA User).
 - You are presented a table with Tag Values on the left and Tagged Virtual Accounts on the right.
 - From this screen, you can search for local VA by Name to narrow down the list.
 - Move from the left quadrant (Virtual Account (Not Tagged)) to the right quadrant (Virtual Accounts (Tagged)) and vice versa using the >> or << sign
 - Click OK to close this modal.
 - Click Next.
- Click Add Virtual Account Custom Tag.
- You get a “Custom Tags Added Successfully” message.

Delete A Custom VA Tag

- A custom local VA tag can be deleted via the Actions Delete under Custom Tags option.
- Navigate to the named Custom VA tag.
- Under Actions, click on Delete.
- Confirm the Delete operation.

Edit Custom VA Tag Values

Once you create a custom VA tag and you want to change its values, you can do so using the following procedure:

- Go to Manage Account.
- Navigate to the Custom Tag option.
- Your custom VA tag should be clickable. Click on it.
- Click on Tag Value Management tab.
- Under the General tab, change the values you want.
- Click Save or Cancel.

Manage Custom VA Tags

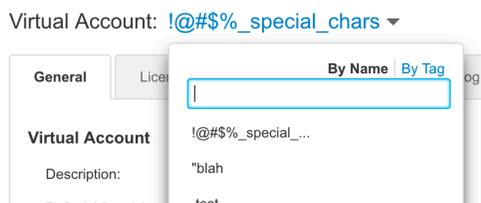
Use this option when you want to change the assignment of the tags to various local Virtual Accounts. To do this, use either step 4 or 5 below:

1. Navigate to Custom Tag option.
2. Click the Custom VA tag you want to manage.
3. Go to Tag Value Management.
4. Click All Manage Tag Values to manage all tag values (instead of individual ones)
 - a. You are presented a table with Tag Values on the left and Tagged Virtual Accounts on the right.
 - Select the tag(s) on the left. If they are *One Tag Value Only*, they show up as radio buttons which means you can only assign one tag value to one local Virtual Account. If they were created with *Allow Multiple Tag Values* option, they show up as check boxes which means you can assign multiple tag values to one or multiple local Virtual Accounts.
 - b. Click Add/Remove.
 - c. You are presented with a modal of two quadrants: left quadrant (Virtual Account (Not Tagged)), and right quadrant (Virtual Accounts (Tagged))
 - d. From this screen, you can search for local VAs by Name to narrow down the list of local Virtual Accounts

- e. Move the local Virtual Accounts from the left quadrant to the right quadrant and vice versa using the >> or << sign
 - f. Click OK to close this modal.
 - g. You can Add/Remove more local Virtual Accounts to assign tag values
 - h. Click OK
 - i. Click Save or Cancel
 - j. If correct, you get a “Properties of Virtual Accounts Custom Tag “XYX” updated successfully” message.
5. Click on  to on each tag value manage one tag value at a time.
- a. You are presented with a modal of two quadrants, left quadrant (Virtual Account (Not Tagged)), and right quadrant (Virtual Accounts (Tagged))
 - b. From this screen, you can search for local VAs by Name to narrow down the list of local Virtual Accounts
 - c. Move the Virtual Accounts from the left quadrant to the right quadrant and vice versa using the >> or << sign
 - d. Click OK to close this modal.
 - e. The UI show the local Virtual Accounts are assigned to the tag values
 - f. Click Save or Cancel
 - g. If correct, you get a “Properties of Virtual Accounts Custom Tag “XYX” updated successfully” message.

Search/Filter Virtual Accounts By Name or By Tag

Instead of scrolling through hundreds of local Virtual Accounts to locate the one you need to work on, satellite users can search or filter them By Name or By Custom VA Tags. In the Smart Licensing screen, select Inventory from the menu options, and then select the Virtual Accounts drop-down menu. 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. By Name is searching or filtering the local Virtual Accounts names, and By Tag is searching or filtering by Custom VA Tags that have been assigned to the various VAs.



Multiple VA Tag Values can be entered to be searched:



License Tags

License Tags are user-defined tags that can be created and tagged to licenses. They are useful for classifying, locating, and grouping licenses. Adding, editing, and deleting license can be done through the Licenses tab under Inventory within your local Virtual Account(s) at both the Summary Level and License Transaction Detail Level (Preference must be enabled). The License Tag

operations are:

- Add a Tag
- Remove a License Tag
- Manage License Tags
 - Edit a License Tag
 - Delete a License Tag

Remove a Tag vs. Delete a Tag

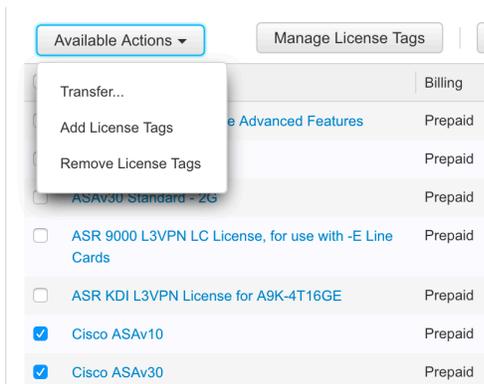
1. Removing a tag simply disassociates it with the selected license entry (Summary or Detailed level). It does not delete the tag itself.
2. Deleting a Tag disassociates it with all the licenses (Summary or Detailed level) and delete the tag itself.

You can perform the following functions in the License Tab.

Add License Tags

Tags can be added to the License Summary level or individual License Transaction Detail level. For example, a license can have multiple License Transaction Detailed levels (shipped to different countries, different order #, associated with different SKUs or PAKs), and different License Tags can be associated with these different levels. On satellite; however, we do not have Shipped To, Order # from Cisco SSM and only track Product Family, SKU, Expires By and PAK (PAK # of a classic license that has been converted to Smart).

To add a License Tag, you must select the license(s) either at the Summary level or Transaction Detail level to enable “Available Transactions”.



Summary Level

- In the Licenses table, select the checkbox(es) to choose one or more licenses.
- Click Available Actions above the table and choose Add License Tags.
- Once you add a License Tag to one License or more lines, you can add it to another license lines.

Virtual Account: **DEFAULT** ▾

General | **Licenses** | Product Instances | Events

Available Actions ▾ | Manage License Tags

Add Tags to the Selected Licenses

Currently available tags across selected lines:

Tags to be added on all selected lines:

11 Minor | Hide Alerts

By Name | By Tag

License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input type="checkbox"/> ASA5506 Threat Defense Advanced Features KTN Test Tag1	Prepaid	1894	0	+ 1894		Actions ▾
<input type="checkbox"/> ASAv10 Standard - 1G KTN Test Tag1	Prepaid	78073	0	+ 78073	4 Alerts	Actions ▾
<input checked="" type="checkbox"/> ASAv30 Standard - 2G KTN Test Tag1	Prepaid	804	0	+ 804		Actions ▾
<input checked="" type="checkbox"/> ASR 9000 L3VPN LC License, for use with -E Line Cards	Prepaid	7	0	+ 7		Actions ▾
<input checked="" type="checkbox"/> ASR KDI L3VPN License for A9K-4T16GE	Prepaid	931	0	+ 931		Actions ▾

Save | Cancel

License Transaction Detail Level

- Above the Licenses table, check the Show License Transactions check box and in the Licenses table, click the plus (+) icon next to the Licenses to choose the individual detailed transaction lines of each license.
- Click Available Actions above the table and choose Add License Tags.
- Click on Add License Tags, enter the Tag value, click Save, and OK.

Remove License Tags

Remove the license tags and unassign them from the selected licenses.

1. Summary Level
 - a. In the Licenses table, select the checkbox(es) to choose one or more licenses. Click Available Actions above the table and choose Remove License Tags.
 - b. Review the Tags selected for removal and click Save to remove the selected tag(s) from the licenses.

Virtual Account: **DEFAULT**

General | **Licenses** | License Reservation...

Available Actions ▾ | Manage License Tags | License Reservation...

Remove Tags from the Selected Licenses

The set of tags that are currently assigned to any of the selected licenses is shown below. Remove the tags that you want to be unassigned from the licenses.

Currently Assigned Tags:

Tags selected for removal:

11 Minor | Hide Alerts

By Name | By Tag

License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input type="checkbox"/> ASA5506 Threat Defense Advanced Features	Prepaid	1894	0	+ 1894		Actions ▾
<input checked="" type="checkbox"/> ASAv10 Standard - 1G KTN Test Tag1	Prepaid	78073	0	+ 78073	4 Alerts	Actions ▾
<input checked="" type="checkbox"/> ASAv30 Standard - 2G KTN Test Tag1	Prepaid	804	0	+ 804		Actions ▾

Remove | Cancel

Show License Transactions Search by License

2. License Transaction Detail Level

- a. Above the Licenses table, check the Show License Transactions check box and in the Licenses table, click the plus (+) icon to choose the individual lines of each license. Click Available Actions above the table and choose Remove License Tags.
- b. Review the Tags selected for removal and click Save to remove the selected tag(s) from the licenses.

Manage License Tags (Edit and Delete License Tags)

You can edit/delete your license tags across satellite local Virtual Account. The License tags are displayed alphabetically and show the number of licenses and license transactions that are associated with each tag.

Procedure:

- Click the Licenses tab.
- Click Manage License Tags.
- Each tag will be shown under the License Tag column and the details of the tag association are shown under the Assigned To column.
- Under the tag name, click Edit.
- Update the tag name and click Save. If the updated tag name already exists in the Virtual Account, an error message will display. To stop editing the tag, click Cancel.

Note: Clicking Save will update the tag name on all the associated licenses and license transactions in your Virtual Account.

- Once Saved, “Tag Updated Successfully” confirmation message will be displayed.

You can delete your license tags at both the Summary Level and License Transaction Detail Level. Recall that deleting a Tag disassociates it with all the licenses (Summary or Transaction Detail level) and delete the tag itself.

Procedure:

- Click the Licenses tab.
- Click Manage License Tags.
- Each tag will be shown under the License Tag column and the details of the tag association are shown under the Assigned To column.
- Under the tag name, click Delete to delete the tag. The following messages are displayed: “Are you sure you want to delete the tag?” and “Clicking on delete will delete the tag from all the associated summary lines and license transactions.”
- Click Yes, Delete It to delete the tag from all associated summary lines and license transactions or click Cancel to cancel its deletion. A “Tag Deleted Successful” confirmation message will display once the tag is deleted.

Before Tag Deletion Example

Virtual Account: **DEFAULT**

General Licenses Product Instances

Available Actions Manage License

License

ASA5506 Threat Defense Advanced Features

ASAv10 Standard - 1G
KTN Test Tag1

ASAv30 Standard - 2G
KTN Test Tag1

ASR 9000 L3VPN LC License, for use with -E Line Cards
KTN Test Tag1

ASR KDI L3VPN License for A9K-4T16GE
KTN Test Tag1

Prepaid 931 0 + 931

Manage License Tags

License Tags Assigned to

Filter by License Tags

100M	0 Licenses	0 License transaction details
250M	0 Licenses	0 License transaction details
Colton_Tag_Tag	0 Licenses	1 License transaction details
KTN Test Tag1	4 Licenses	0 License transaction details
KTN1	0 Licenses	0 License transaction details

Are you sure you want to delete the tag?
Yes, Delete It | Cancel

Clicking on delete will delete the tag from all the associated summary lines and license transactions.

You can search your licenses By Tag to see where the tags are assigned

11 Minor Hide Alerts

By Name By Tag

Search by License

Alerts Actions

4 Alerts Actions

Alerts Actions

Alerts Actions

After Tag Deletion Example (Delete Tag deletes the tag itself and all its associations with the licenses).

Virtual Account: **DEFAULT**

General Licenses Product Instances Event Log

Available Actions Manage License Tags License Reservation... Show License Transactions

By Name By Tag

Search by License

License	Billing	Purchased	In Use	Balance	Alerts	Actions
ASA5506 Threat Defense Advanced Features	Prepaid	1894	0	+ 1894		Actions
ASAv10 Standard - 1G	Prepaid	78073	0	+ 78073	4 Alerts	Actions
ASAv30 Standard - 2G	Prepaid	804	0	+ 804		Actions
ASR 9000 L3VPN LC License, for use with -E Line Cards	Prepaid	7	0	+ 7		Actions
ASR KDI L3VPN License for A9K-4T16GE	Prepaid	931	0	+ 931		Actions

Search by License Tags

You can limit the license entries by searching or filtering by License Tags as follows:

Virtual Account: Default

General Licenses Product Instances Event Log

Available Actions Manage License Tags... Show License Transactions

vpn-2 csr

By Name By Tag

Advanced Search

License	Billing	Purchased	In Use	Balance	Alerts	Actions
CSR 1KV AX 100M 100M csr	Prepaid	2	0	2		Actions
CSR 1KV APPX 250M 250M appx csr tag-2	Prepaid	3	0	3		Actions
ASR KDI L3VPN License for A9K-4T16GE vpn-2 csr	Prepaid	4	0	4		Actions

Showing All 3 Records

Procedure:

- From the Inventory tab of the satellite Enhanced Edition Smart Licensing, click on the local Virtual Account dropdown.
- Click By Name or By Tag.
- Enter a few letters in the Search Virtual Accounts field and hit Enter.
- The list of local Virtual Account matching the search criteria returns.

Advanced License Search/Advanced License View

The Advanced Search feature allows you to filter using additional criteria on the Licenses. Note that satellite does not have the same detailed license fields as CSSM. We only track Product Family, SKU, Expires, and PAK (PAK # of a classic license that has been converted to Smart). You can narrow the licenses by product family, expiration date, SKU, and/or PAK.

NOTE: satellite does not have the exact SKU which was part of the original order. As a result, satellite will display all possible SKUs which could have been used to purchase the license. Searching for the known SKU could generate license match's for SKUs which were not originally order as part of the searched for SKU.

You can perform an Advanced Search 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.

Preferences Tab Setting:

License Configuration

Show License Transaction Details in Inventory Tab: Enabled [View Change Log](#)

Click on Save and enter notes on the Change log.

Show License Transactions Setting:

When this option is checked, you can see the detailed transactions under the main transaction line.

Virtual Account: **DEFAULT** Minor Hide Alerts

General | **Licenses** | Product Instances | Event Log

Available Actions | Manage License Tags | License Reservation... | Show License Transactions | [By Name](#) | [By Tag](#)

Advanced Search

License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input checked="" type="checkbox"/> ASA5506 Threat Defense Advanced Features	Prepaid	1876	0	+ 1876		Actions
<input type="checkbox"/> Sku: L-ASA5506T-ADV= Family: ASA Low End	2				Expires: -never-	
<input type="checkbox"/> Sku: L-ASA5506T-ADV= Family: ASA Low End	1				Expires: -never-	
<input type="checkbox"/> Sku: L-ASA5506T-ADV= Family: ASA Low End	859				Expires: -never-	

If you set the preference to Enabled, but do not check the “Show License Transactions”, you do not see the detailed license entries.

Virtual Account: **DEFAULT** ▾

9 Minor | Hide Alerts

General | **Licenses** | Product Instances | Event Log

Available Actions ▾ | Manage License Tags | License Reservation... | | Show License Transactions | | [By Name](#) | [By Tag](#)

<input type="checkbox"/>	License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input type="checkbox"/>	ASA5506 Threat Defense Advanced Features	Prepaid	1876	0	+ 1876		Actions ▾
<input type="checkbox"/>	ASAv10 Standard - 1G	Prepaid	78092	0	+ 78092	4 Alerts	Actions ▾
<input type="checkbox"/>	ASAv30 Standard - 2G	Prepaid	813	0	+ 813		Actions ▾

To search for specific detailed License field, click on “Advanced Search”, enter the specific field(s) you want to search, and click Apply.

Virtual Account: **DEFAULT** ▾

9 Minor | Hide Alerts

General | **Licenses** | Product Instances | Event Log

Available Actions ▾ | Manage License Tags | License Reservation... | | Show License Transactions | | [By Name](#) | [By Tag](#)

Advanced Search ▾

Product Family: SKU:

Expires By: PAK:

[Apply](#) [Clear](#)

<input type="checkbox"/>	License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input checked="" type="checkbox"/>	ASA5506 Threat Defense Advanced Features	Prepaid	1876	0	+ 1876		Actions ▾
<input checked="" type="checkbox"/>	ASAv10 Standard - 1G	Prepaid	78092	0	+ 78092	4 Alerts	Actions ▾
<input checked="" type="checkbox"/>	ASAv30 Standard - 2G	Prepaid	813	0	+ 813		Actions ▾
<input checked="" type="checkbox"/>	Cisco ASAv10	Prepaid	756	0	+ 756		Actions ▾
<input checked="" type="checkbox"/>	Cisco ASAv30	Prepaid	4909	0	+ 4909		Actions ▾

Showing All 5 Records

The following search rule applies:

Field	Description	Type of Search	Type Ahead
Product Family	License Product Family	Contains	
SKU	License or Product SKU	Contains	
Expires By	End Date of Term-based License	Any license that has expiration date on or before specified date	No
PAK	PAK # of a classic license that has been converted to Smart	Exact Match	Yes

Other SSM satellite EE Licensing Portal Functions

SSM satellite EE Smart Licensing functions are similar to Smart Account Administration and Cisco Smart Software Manager as follows. However, all the Accounts and Virtual Accounts are *local* to the satellite EE.

- Request an Account
- Request Access to an Existing Account
- Manage Account
 - Local Account Properties
 - Local Virtual Accounts
 - Local Users
 - Local Account Requests
 - Event Logs
- Smart Licensing
 - Alerts
 - Inventory
 - Reports
 - Satellites
 - Activity

For more information about these functions, see the Help link on the Licensing portal or software.cisco.com.

Backward Compatibility

Before the satellite can accept registrations from product instances, it has to register with CSSM. Previously, satellite to CSSM registration requires a 10-day wait because someone has to manually sign the Certificate Signing Request (CSR) from satellite to CSSM. This means that if products want to connect to satellite, it has to wait 10 days for satellite to be fully registered and functional.

Over a year ago, this manual signing of the CSR was automated so that the CSR from satellite to CSSM is now signed immediately. However, there are changes that must be made to the product smart agents, satellite and CSSM for this trust chain to work in an automated way. The previous trust chain consisted of 3 levels of certificates (i.e., 3-tier) from the device to satellite to CSSM. In the new implementation to automate the trust chain validation, additional certificates were added and we had 4-levels of certificates (i.e., 4-tier). These changes also must be backward compatible so that older devices that do not have this updated level of smart agent, satellite, and CSSM code would continue to function.

In the new implementation, smart agents, satellite and CSSM 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+) needing to register with satellite will need to wait 10 days as satellite needs to get the 3-tier certificate from CSSM 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, simply issue the command `"license smart status"`.

We have the following cases:

Devices with new Smart Agent registering to the latest satellite release

Devices that have implemented the latest Smart Agent code register successfully with latest satellite using multi-tier certificate hierarchy.

Devices with new Smart Agent registering to a back-level satellite

Devices that have implemented the latest Smart Agent code dynamically validate the certificate chain (from device to satellite to Cisco Admin).

Devices with old Smart Agent registering to the latest satellite release

When you install the latest satellite release, its registration with Cisco Smart Software Manager is instantaneous. During this process, the satellite also requests a previous three-tier certificate. When devices with older Smart Agent registers with the satellite, 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 (three-tier) certificate and re-register. Afterwards, these devices can successfully register to the satellite.

In this case, as HTTPS is used for device to satellite communication, you need to ensure following steps:

- Smart Call Home profile uses HTTPS as the transport
- After the satellite (with the multi-level certificate hierarchy function) registers successfully to CSSM, the product instance (with back-level smart agent) which tries to register with satellite fails with the following error message:

```
Compatibility Error: The satellite is not currently compatible with the Smart Licensing Agent version on this product. If it has been 10 days since the satellite was registered, synchronize the satellite with Cisco's licensing servers to enable compatibility with older agent versions and then try the registration again.
```
- User waits for 10 business days
- User runs an on-demand network or manual sync between satellite and Cisco SSM.



- User re-registers the product instance to satellite.

If you perform a fresh 3.1.x satellite installation, after registration and upon logging, you will see the following message:

Version Compatibility Note – Temporarily, this satellite 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 satellite's initial registration and then synchronize the satellite.

This means that after 2 business days, the three-tier certificate will be obtained by satellite from Cisco SSM 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)

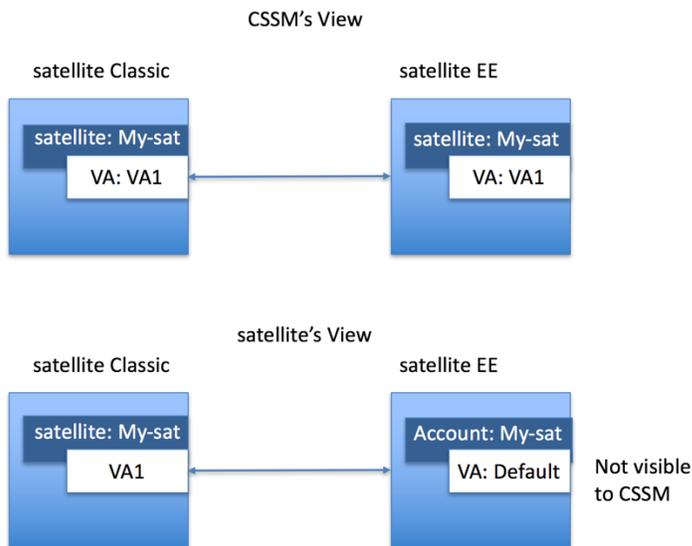
Migration to SSM satellite Enhanced Edition

For customers who wish to migrate from satellite Enhanced Edition 6.0.1 to this release, please use the 6.1.0 patch when it is posted.

There is no direct upgrade path from satellite Classic (3.x, 4.x, or 5.x) to satellite Enhanced Edition 6.1.0. However, you can use the following procedures to manually migrate from a previous satellite Classic release to satellite Enhanced Edition (EE).

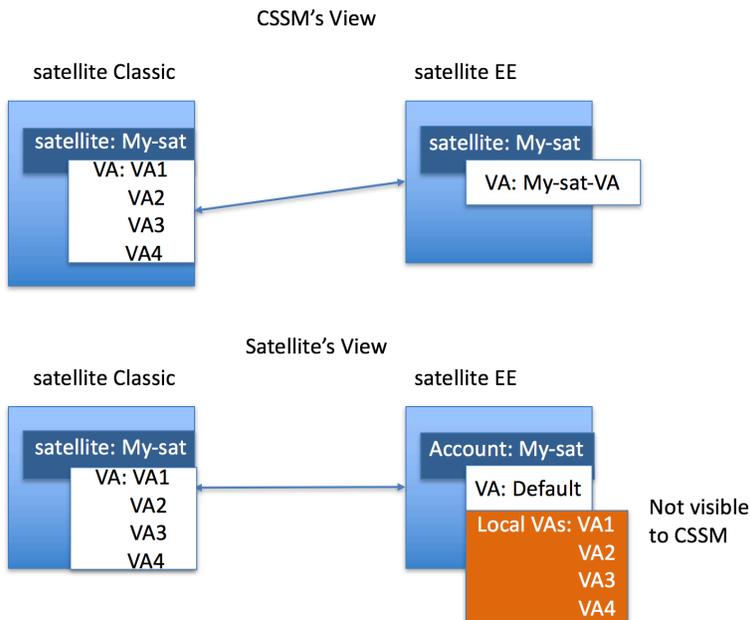
Procedures:

1. Backup your satellite Classic system.
2. Remove all the Product Instances (PIs) that are registered to the satellite Classic.
3. Synchronize the satellite Classic with Cisco SSM.
4. Remove the satellite Classic that is currently registered to Cisco SSM with the following steps. Note that a satellite can be removed only if there are no PIs registered to it. Satellite can be removed while containing licenses in it.
 - a. Login into CSSM.
 - b. Go to “Satellites” pane.
 - c. Under Action, select “Remove”.
 - d. Confirm the Removal message by selecting OK.
5. Deploy a satellite EE system.
6. Login to satellite EE Administration Portal.
 - a. Create a “New Account”. This account will have a local *Default* VA associated with it automatically on satellite EE.
 - b. This “New Account” workflow automatically registers the Account with Cisco Smart Software Manager Smart Account/Virtual Account pair.
7. Single VA satellite
 - a. Re-register all our PIs to the local *Default* Virtual Account on satellite EE.
 - b. Re-create users under the satellite EE Licensing Portal and re-assign their roles to the Default VA.
 - c. If the satellite Classic has one VA, here is what it looks like after the migration.



8. Multiple VA satellite
 - a. If satellite Classic has more than one VAs, then create additional local VAs under the satellite EE Licensing Portal to match that structure as shown in 8.d.
 - b. On CSSM, move the licenses from the virtual accounts linked to satellite Classic (*VA1, VA2, VA3, VA4*) to the virtual account (*My-sat-VA*) linked to satellite EE.

- c. Register satellite EE Account to CSSM Smart Account/Virtual Account pair. The virtual account on CSSM in this example is *My-sat-VA*. All of the entitlements from *My-sat-VA* are added to local *Default* VA on satellite EE after the registration.
- d. Create the local virtual accounts *VA1*, *VA2*, *VA3*, *VA4*.
- e. Register your PIs to the matching local VAs (*VA1*, *VA2*, *VA3*, *VA4*) on satellite EE.
- f. Transfer your licenses from the local *Default* VA to the local VAs created in 8.d (*VA1*, *VA2*, *VA3*, *VA4*) to replicate the same structure you had on satellite Classic before.
- g. Re-create users under the satellite EE Licensing Portal and re-assign their roles to the corresponding VAs.



Troubleshooting

[Satellite EE Issues](#)

[Client Registration Issues](#)

[Manual Synchronization Issues](#)

[Network Synchronization Issues](#)

Satellite EE Issues

1. The Smart Licensing and Manage Local Account options are grayed out on the Licensing portal
 - You need to request a new or access to an existing Local Account
 - Register it to CSSM
 - Log back into the Licensing portal 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 you have the appropriate authentication method configured in the Administration portal
 - If you are using LDAP, the user must log into SSM satellite EE Licensing portal first before they can be found in the “Add User” screen
3. I cannot register a product
 - Verify you have a token which has not expired
 - Verify the URL on the product points to the proper host name or IP address for SSM satellite EE
4. When a user logs in to the Licensing portal, they cannot see their SSM satellite EE 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 satellite EE?
 - User Interface: HTTPS (Port 8443)
 - Product Registration: HTTPS (Port 443), HTTP (Port 80)
 - CSSM: HTTPS (api.cisco.com, cloudsso.cisco.com) – no port needed because it’s outbound
 - CSSM opens port 443, same port for software.cisco.com

Client Registration Issues

If you experience issues with the client registration process, take the following actions:

- Ensure that the satellite configuration is correct.
Please refer to the **Network** is properly configured.

- Verify that the Call-Home configuration on the client points to the satellite.
Please refer to the section "*Registering Product Instances to satellite*" in the *Appendix*.
- Verify the token has been generated from the satellite.

Your firewall settings should allow traffic to and from satellite for the following:

- satellite IP address ports 443 and 80
 - 443 if using HTTPS
 - 80 if using HTTP to communicate with satellite
- satellite IP address port 8443 to get access to satellite portal

Manual Synchronization Issues

If you experience issues with the manual synchronization process, take the following actions:

- Verify the time on the satellite is correct.
Please refer to the section *Time Settings* on page 28.
- Ensure port 443 (HTTPS) is allowed through your firewall.
- Verify the licenses in the associated virtual account.
- Make sure that you are uploading and downloading the YAML (request and response) files from the correct satellite Account. You can do this by verifying that the file names include the name of the satellite 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:

- Ensure port 443 (HTTPS) is allowed through your firewall.
 - tools.cisco.com ports 443
 - api.cisco.com ports 443
- Verify that the satellite can reach the configured DNS server.
- Verify that the satellite can reach cisco.com.
- Verify that the time on the satellite is correct. Please refer the section "*Time Settings*" on page 28.

Appendix

Registering Product Instances to satellite

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

Smart-enabled product instances register to satellite via CLI or GUI depending on the product. For more information on this, refer to the specific platform Configuration Guide. For CSR Smart Licensing configuration, please refer to <http://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/csr1000Vswcfg/licensing.html>

Ensure you have the following commands configured in the respective router platforms:

- For IOS-XR platforms, `Cr1` optional
- For IOS/XE platforms, use `revocation-check none`.

Sample SCH Profile to Use Smart Software Manager satellite on the Cloud Service Router

Procedure

1. **enable**
Enables privileged EXEC mode. Enter your password if prompted.
2. **configure terminal**
Enters global configuration mode.
3. **call-home**
Enters call-home configuration mode.
4. **contact-email-addr** *email address*
Specify a valid email ID.
5. **profile** *name*
Specify the profile name.

Note: CiscoTAC-1 is the default profile.
6. Choose **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*.
Accesses the SCH Transport Gateway URL.

Note: The destination URL is `http://<ip-address>:80/Transportgateway/services/DeviceRequestHandler`.
 - b) For **destination address https** use *https from TG*.
Accesses the SCH Transport Gateway URL.

Note: The destination URL is `https://<ip-address>:443/Transportgateway/services/DeviceRequestHandler`.

7. **active**
Activates the profile specified in step 5.
8. **exit**
Saves and exits the current configuration mode and returns to privileged EXEC mode.
9. **end**
Returns to privileged EXEC mode.
10. **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) #contact-email-addr aaa@cisco.com
Router (cfg-call-home) #profile CiscoTAC-1
Router (cfg-call-home-profile) #active
Router (cfg-call-home-profile) #destination transport-method http
Router (cfg-call-home-profile) #no destination transport-method email
Router (cfg-call-home-profile) #destination address http
Router (cfg-call-home-profile) #http://172.19.76.177:80/Transportgateway/services/DeviceRequestHandler
```

The following configuration is only a sample for CSR for HTTPS. Please see platform specific configurations for the call-home profile config. Starting with satellite 3.0.x port # and URL are not needed.

Example:

```
Router# configure terminal
Router (config) #call-home
Router (cfg-call-home) #contact-email-addr aaa@cisco.com
Router (cfg-call-home) #profile CiscoTAC-1
Router (cfg-call-home-profile) #active
Router (cfg-call-home-profile) #destination transport-method http
Router (cfg-call-home-profile) #no destination transport-method email
Router (cfg-call-home-profile) #destination address https
Router (cfg-call-home-profile) #https://172.19.76.177:443/Transportgateway/services/DeviceRequestHandler
```

For ASR9K and CSR, ensure you remove the URL for Cisco SSM as follows:

```
no destination address https://tools.cisco.com/its/service/oddce/services/DDCEService
```

Add the URL for satellite and the following command:

```
revocation-check none
```

Invoking API Endpoints

Once authentication has been setup, the application can call the API endpoints above.

The specific input/response/method call parameters are as follows:

Create a local Virtual Account

Input Required:

- Satellite Account Name

Example Method Call:

- HTTP Method: POST
- Request <ip-address of satellite>:/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 Virtual Accounts in Smart Account"  
}
```

List local Virtual Accounts

Input Required:

- Satellite Account Name

Response:

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

Example Method Call:

- HTTP Method: GET
- Request <ip address of satellite>: /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 Virtual Accounts within Smart Account
  \'{SA Domain Name}\'"
}
```

Delete A local Virtual Account

Input Required:

- satellite Account Name: satellite Account for which the user wants to search the devices.
- Local Virtual Account Name: The local Virtual Account Name from which you would like to remove.

Response:

- The status of the delete virtual account request.

Example Method Call:

- HTTP Method: POST
- Request <ip-address of satellite>: `api/v1/accounts/{account name}/virtual-accounts/{virtual account name}/delete`

Response Code: 200 OK

```
{
  "status": "SUCCESS",
  "statusMessage": "Virtual Account '{virtual account name}' deleted successfully"
}
```

Create A Token

Input Required:

- Satellite Account Name
- Local Virtual Account Name
- Description
- Expiration Days

Response:

- The Token list for which the user has access to.

Example Method Call:

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

Request Body:

```
{ "expiresAfterDays": 100, "description": "Test VA Creation" }
```

Response Code: 200 OK

```
{
  "status": "SUCCESS",
  "statusMessage": "A valid, active token was generated.",
  "tokenInfo": {
    "token": "OGVjMDk4YjktNGUwNS00OTc0LTk0YjQtNWZkZTI5ZTU2ZjFjLTE0Nzc1Mjc2%0ANTA2NTZ8M0wvcmdBWMJnbVR1akdaa0xjTU9ldDRFbXVFQjh3L3k1aHAzdTBD%0ANzlYbz0%3D%0A",
    "expirationDate": "2016-10-26T20:20:50",
    "description": "this is Ben September 23",
    "createdBy": "bvoogd"
  }
}
```

List 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. User needs to have necessary access privileges either at the Account level or at the specified local Virtual Account level.

Input Required:

- Account: satelliteAccount from which the user wants to fetch the tokens.
- Virtual Account Name: The local Virtual Account of the Account from which tokens are to be fetched.

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 <ip-address of satellite>:/api/v1/accounts/{account name}/virtual-accounts/{virtual account name}/tokens

Response Code: 200 OK

```
{
  "status": "SUCCESS",
  "statusMessage": "Successfully read active tokens.",
  "tokens": [
    {
      "token": "OWI2YmE2ZDgtYTBhZi00MGQyLWE1NDYtZThkMWZjMDUzYzM1LTE0Nzc
yNjA1%0AMjI2NTh8cUhjaEtiaGlXalRLeFNseHFqQXpMUnpiZXVvZ0VybkNacU91L1Vq%0AbDc0ST0%3
D%0A",
      "expirationDate": "2016-10-23T22:08:42",
      "description": "this is Ben September 23",
      "exportControl": "Not Allowed",
      "createdBy": "bvoogd"
    },
    {
      "token": "YWQwZjE2MmUtMWI4NS00YmM4LWIyZTA1OGJjMG11MTkzLTE0Nzcy
NDMy%0AMTgyMTF8K0djaEJOZWg2S3NIMHhURUI2aWFKOEgxQ0w0Wm41MXZIZHRsbVp3%0AOU
FZOD0%3D%0A",
      "expirationDate": "2016-10-23T17:20:18",
      "description": "this is Ben September 23",
      "exportControl": "Not Allowed",
      "createdBy": "bvoogd"
    },
    {
      "token": "OTI2M2I5YmYtYjRjMy00ZjcyLWE1OTEtOTUwZDY5ZWY3NWRILTE0NzcyN
DMw%0ANDA0NTZ8U1pRVEJKNFh5a1VTWFprb2FMclh0bjBEVDNrVnNoUzVOdjdmZTJJ%0AZklZYz0
%3D%0A",
      "expirationDate": "2016-10-23T17:17:20",
      "description": "test ben",
      "exportControl": "Allowed",
      "createdBy": "bvoogd"
    }
  ]
}
```

Response Code: 403

```
{
  "status": "ERROR",
  "statusMessage": "Not Authorized to view the Tokens"
```

```
}
```

Revoke A Token

Users can invoke this method to revoke the valid tokens available for the given satellite Account and the local Virtual Account. The user can pass an array of the tokens they want to revoke.

Input Required:

- Account: The satellite Account from which user wants to revoke the token.
- virtualAccountName: The local Virtual account of the satellite Account which the user wants to revoke the token.

Response:

- The revoke token status for each of the requested tokens.

Call-outs:

- The maximum tokens user can revoke per request are 10.

Example Method Call:

- **HTTP Method:** POST
- **Request URL:** <ip address of satellite>:api/v1/accounts/{smartAccountDomain}/virtual-accounts/{virtualAccountName}/tokens/revoke

Request Body:

```
{
  "tokens": [
    "OGVjMDk4YjktNGUwNS00OTc0LTk0YjQtNWZkZTI1ZTU2ZjFjLTE0Nzc1Mjc2%0ANTA2NTZ8M0wvcmdBWmJnbVR1a
    kdaa0xjTU9ldDRFbXVFQjh3L3k1aHAzdTBD%0ANz1Ybz0%3D%0A",
    "ZGQ1ZmQ2ZWQtNjE4YS00NjA5LTlhODMtN2JmNzgyMTU2OTc5LTE0OTU3OTQ4%0ANzE5MTJ8UitTTXIZUGRwb3d5Q
    XB5WExoM01RU1grU1hzYWNjTEo3MzhjOHRt%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 s
      uccessfully",
      {
        "status": "SUCCESS",
        "statusMessage": "Token- 'ZTBkYjkzOGMtOWY3Yi00ZThjLThkOTAtYTljZmIwZTA5ZWFjLTE
      1MDU0MTcw%0AMzE2NzJ8Y1dZMkRGUWF1QVQzK3VuNVNSN3hNTDNUUG5XMkJiTS9jMGxMVzNq%0AZVV2TT0%3D%0A'
      revoked successfully"
      }
    }
  ]
}
```

```
}}}
```

Response Code: 200 OK

```
{
  "status": "WARNING",
  "statusMessage": "2 tokens succesfully revoked.",
  "tokensRevokeStatus": [
    {
      "status": "ERROR",
      "statusMessage": "The token MmFkMzgyNmMtMDQ2Zi00NjU2LThiZmMtMTk4YWZkNDVhNGU5L
TE1MDU0MTcw%0AMjI0ODF8WjduNW5ObVd0L1BGZmFvOWZYenJiaGJyRVE4T0R5NFJheW90V2hq%0AQkRSND0%3D%0
A has already been revoked."
    },
    {
      "status": "SUCCESS",
      "statusMessage": "Token- 'ZTBkYjkzOGMtOWY3Yi00ZThjLThkOTAtYTljZmIwZTA5ZWJjLTE
1MDU0MTcw%0AMzE2NzJ8Y1dZMkRGUWF1QVQzK3VuNVNSN3hNTDNUUG5XMkjiTS9jMGxMVzNq%0AZVV2TT0%3D%0A'
revoked successfully"
    }
  ]
}
```

Response Code: 403

```
{
  "status": "ERROR",
  "statusMessage": "Not Authorized to revoke tokens for Virtual Account '{virtualAccount
Name}' ."
}
```

License Usage

Request Parameters:

- **Satellite Account:** satellite Account being searched.

Response:

- The license usage for the requested domain and optional request parameters.

Example Method Call:

- **HTTP Method:** POST
- **Request** <ip address of satellite>:/api/v1/accounts/{Account}/licenses

Request Payload

- virtualAccounts: An optional list of local virtual accounts for which users intend to fetch the available licenses. If not specified, all the licenses from the domain for which 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 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 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 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 virtual accounts"
}

```

Response Code: 422

```

{
  "status": "ERROR",
  "statusMessage": "Invalid limit or offset value"
}

```

License Subscription Usage

Request Parameters:

- **Account:** satellite Account being searched.

Response:

- The available License Subscriptions usage for the request submitted.

Example Method Call:

HTTP Method: POST

Request URL: <ip-address of satellite>:api/v1/accounts/{smartAccountDomain}/license-subscriptions

Request Payload

- **virtualAccounts:** An optional list of virtual accounts for which users intend to fetch the available licenses. If not specified, all the licenses from the domain for which the user has access to will be returned.
- **status:** The status of the subscriptions to be fetched. 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 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"],
"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 virtual
accounts"
}
```

Response Code: 403

```
{
  "status": "ERROR",
  "statusMessage": "Not Authorized to access license subscriptions for Smart Account {SA
Domain}"
}
```

Response Code: 422

```
{
  "status": "ERROR",
  "statusMessage": "Invalid limit or offset value"
}
```

License Transfer

Request Parameters:

- **Account:** account from which the user intends to do 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 user can do in a single request.

Example Method Call:

- **HTTP Method:** POST
- **Request URL:** <ip address of satellite>:*api/v1/accounts/{smartAccountDomain}/virtual-accounts/{virtualAccountName}/licenses/transfer*

Request Payload

- **TargetVirtualAccount:** The target local Virtual Account to which you wish to transfer the License to.
- **Quantity:** The quantity to transfer. This quantity should always be less than the available quantity for the specified license in the local Virtual Account the licenses are being transferred from.
- **Precedence:** Optional attribute specifying the precedence order in which transfers will take place in the case of term based licenses. Valid values are `LONGEST_TERM_FIRST` and `LONGEST_TERM_LAST`. By default if this attribute is not specified it will default to `LONGEST_TERM_FIRST`. As an example, assume there are 2 term based licenses for CSR 1KV SECURITY 10M in local Virtual Account Chemistry and the first term-based license has a term of 90 days and the second has a term of 60 days. If the precedence is `LONGEST_TERM_FIRST` then the 90 days license will be processed first for the transfer followed by the 60 days license.
- **LicenseType:** The type of license the user wishes to transfer. Valid values are 'TERM' and 'PERPETUAL'. Please note that all the non 'PERPETUAL' licenses like 'DEMO', 'SUBSCRIPTION' will be treated as 'TERM'.
- **License:** The name of the license which the user wishes 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 successfully transferred from V
irtual Account 'VA1' to Virtual Account 'Physics'."
    },
    {
      "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 V
irtual 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 licen
se '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 Virtual Accounts '{vaName}' or 'Physics'."
    }
  ]
}
```

Response Code: 403

```
{
```

```
"status": "ERROR",
"statusMessage": " Not Authorized to access Virtual Account '#{Source VA Name}'."
}
```

Product Instance Usage

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 PI Remove API.

Input Required:

- Account Name: Account for which the user wants to search the devices.

Request Payload:

- Satellite Accounts: An optional list of local Virtual Accounts for which users intend to fetch the available licenses. If not specified, all the licenses from the domain for which 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 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 request submitted.

Example Method Call:

- HTTP Method: POST
- Request URL: <ip-address of satellite>: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 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.

Input Required:

- Satellite Account Name: Account for which the user wants to search the devices.
- Local Virtual Account Name: The Virtual Account Name from which you would like to fetch the instance names.
- Instance Name: The instance name from the order- Hostname, UDI Serial Number, Host Identifier, Mac Address, IP Address, SUVI, UUID, whichever is available first.

Input Optional:

- 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 URL: */api/v1/accounts/:logical_account_name/virtual-accounts/:license_pool_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:

- **satelliteAccount:** satellite Account from which the user wants to transfer the Product Instances.
- **VirtualAccountName:** The name of the local Virtual Account from which the user intends to perform the device transfer.

Response:

- A list of transfer responses for each of the list of transfer requests submitted.

Call-outs:

- There is a threshold of 10 devices transfer which user can do in a single request.

Example Method Call:

- **HTTP Method: POST**
- **Request URL:** <ip address of satellite>:api/v1/accounts/{smartAccountDomain}/virtual-accounts/{virtualAccountName}/devices/transfer

Request Payload

```
{
  "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-74ea1b991",
    "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-74ea1b991" ,
    "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 Removal

Users can invoke this method to programmatically remove devices that are registered in their satellite 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 satellite Account/local Virtual Account to perform this request.

Input Required:

- Account Name: Account for which the user wants to search the devices.
- Virtual Account Name: The local Virtual Account Name from which you would like to fetch the instance names.
- SUDI of Device
- Software/Product Tag Identifier

Response:

The 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 `<ip-address of satellite>:/api/v1/accounts/cisco.com/virtual-accounts/testVA/devices/remove`

Response Code: 200 OK

```
{
  "status": "SUCCESS",
  "statusMessage": "The Product Instance DHR_3000 was successfully removed."
}
```

Alerts

This API will allow users to view the Alerts that are available for the Smart entitlements.

Request Parameters:

- **Account:** satellite Account for which the user wants to fetch the alerts.

Response:

- The available Alerts for the submitted request.

Example Method Call:

- **HTTP Method: POST**
- **Request URL:** `<ip address of satellite>: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, first 1000 alerts matching the request criteria will be fetched. If limit is not specified, 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 Virtual Accountlocal 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 satellite \"TestSatellite\" failed to
synchronize within 90 days and was removed from Smart Software Manager. All of the
product instances registered through the satellite were also removed from the associated
virtual accounts and may be running in a degraded state.",
    "severity": "Major",
    "satelliteName": "TestSatellite",
    "messageType": "Satellite Unregistered and Removed",
    "actionDue": "Now",
    "source": "TestSatellite",
    "sourceType": "Satellite"
},
{
    "virtualAccount": "Zoology",
    "message": "The Smart Software Manager satellite \"test-may5\" has not
synchronized for 28 days. If it is not synchronized within 62 days, this satellite will
be removed from Smart Software Manager and all of the product instances registered
through the satellite may run in a degraded state.",
    "severity": "Major",
    "satelliteName": "test-may5",
    "messageType": "Synchronization Overdue",
    "actionDue": "Now",
    "source": "test-may5",
    "sourceType": "Satellite"
},
{
    "virtualAccount": "Zoology",
    "message": "The Smart Software Manager satellite \"TestSat\" has been created
but requires a satellite 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",
    "satelliteName": "TestSat",
    "messageType": "Authorization Pending",
    "actionDue": "Now",
    "source": "TestSat",
    "sourceType": "Satellite"
},
{
    "virtualAccount": "Zoology",
    "message": "The Authorization File for Smart Software Manager satellite
\"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 satellite
using the satellite setup utility.",
    "severity": "Minor",
    "satelliteName": " TestSat123",
    "messageType": "Authorization File Ready",
    "actionDue": "Now",
    "source": "TestSat123",
    "sourceType": "Satellite"
},
{
    "virtualAccount": "Zoology",
    "message": "An error occurred while processing the Synchronization File for the
satellite. Try generating a new Synchronization File from your satellite and
synchronizing again. If the problem persists, contact Cisco Support.",
    "severity": "Major",
    "satelliteName": " Thera",
    "messageType": "Synchronization Failed",
    "actionDue": "Now",
    "source": "Thera",
    "sourceType": "Satellite"
}

```

```
}
  ]
}
```

Response Code: 403

```
{
  "status":"ERROR",
  "statusMessage": "Not Authorized to access alerts for specified virtual accounts"
}
{
  "status":"ERROR",
  "statusMessage": "Not Authorized to access alerts for Smart Account '{Smart account Domain}'"
}
```

Response Code: 422

```
{
  "status":"ERROR",
  "statusMessage": "Invalid limit, offset or severity value"
}
```