Cisco Hosted Collaboration Solution Smart Licensing Operation Guide, Release 12.5

First Published: 2020-04-22

Last Modified: 2021-07-28

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

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

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

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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 NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

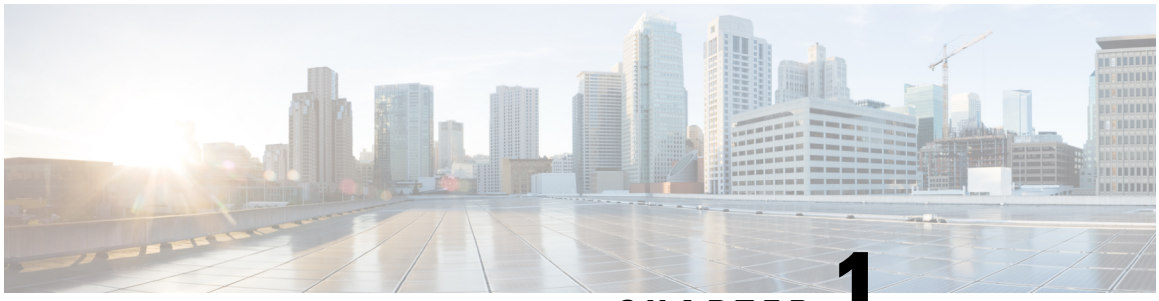
Change History

Change History

Date	Description
July 28, 2021	Updated the procedure to request access to operational licenses through smart sheet. See Task Flow of Operational License Without Satellite Account, on page 26 and Task Flow of Operational License With Satellite Account, on page 27 for details.
July 6, 2020	These are the updates to the guide: • Added procedure to onboard Expressway clusters in Smart licensing mode using the HCM-F interface. See Assign and Unassign a Cluster to Virtual Account, on page 24, View Cluster Summary, on page 28, and Edit Virtual Account, on page 31. • Supports changing the License Mode from Enterprise to Cisco HCS. See HCS Managed Services, on page 13 for details.
July 30, 2019	Initial version release

Change History

CONTENTS



CHAPTER 1

Overview

About the Guide

This guide describes steps to migrate an existing partner with Flex Hosted Calling and Cisco Hosted Collaboration Solution (HCS) Perpetual license Model to Smart Licensing Model.

Audience

This guide assumes that you are familiar with the traditional commercial model with HCS Perpetual licenses. Familiarize yourself with the knowledge and experience to deploy and manage the Smart Licensing for HCS.

Overview of Smart Licensing

Smart Licensing is a cloud-based, software license management solution that enables you to automate time-consuming, manual licensing tasks. The Smart Licensing solution allows you to easily track the status of your license and software usage trends.

It is a Cisco initiative to move all the licenses to the cloud. The purpose of this initiative is to simplify the license management for HCS partners and enable them to adopt Cisco's cloud-based license management system. Smart Licensing helps in overcoming most of the limitations with the traditional PAK-based licenses. Most of the Cisco products including routing, switching, security, collaboration, and so on supports smart licensing.

Smart Licensing in HCS depends on Cisco Smart Software Manager (CSSM), Satellite, and HCM-F. In CSSM and satellite you can activate and manage all Cisco licenses. HCM-F simplifies the complexities of registration or activation of UC Applications with CSSM or Satellite, management of Smart Licenses, generate licensing reports for inventory, and billing purposes. HCM-F also provides licensing dashboards for consumption details and compliance status.

PLM is not supported for UC applications cluster versions higher than 11.x. Register all the 12.x UC applications cluster to CSSM.

HCM-F currently supports registration of UC Applications to Prime License Manager (PLM) for consuming the traditional PAK-based licenses. UC application versions 11.x or earlier supports registration through PLM. For more information about PLM, see *Cisco Hosted Collaboration Solution License Management*.

Smart Licensing helps simplify three core functions:

- **Purchasing:** The software that you have installed in your network can automatically self-register themselves, without Product Activation Keys (PAKs).
- **Management:** You can automatically track activations against your license entitlements. Also, you do not need to install the license file on every node. You can create License Pools (logical grouping of licenses) to reflect your organization structure. Smart Licensing offers you Cisco Smart Software Manager, a centralized portal that enables you to manage all your Cisco software licenses from one centralized website.
- **Reporting:** Through the portal, Smart Licensing offers an integrated view of the licenses you purchased and the licenses that are deployed in your network. You can use this data to make better purchase decisions, based on your consumption.

Cisco Smart Software Licensing helps you to procure, deploy, and manage licenses easily, where devices register and report license consumption, removing the need for product activation keys (PAK). It Pools license entitlements in a single account and allow you to move licenses freely through the network, wherever you need them. It is enabled across Cisco products and managed by a direct cloud-based or mediated deployment model.

The Cisco Smart Software Licensing service registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager and/or Satellite.

HCM-F enables the user to perform multiple tasks, such as, change the license deployment to Hosted Collaboration Solution (HCS), setting the transport mode to UC Applications, create token in CSSM, register the UC applications and validate the same, and so on. If there is a failure while performing the tasks, HCM-F collects the error messages from the UC application or CSSM, and updates the HCM-F Job entry with the issue details.

CSSM reports at smart account-level and product level. However, user information is not available at these levels. HCM-F provides the Service Inventory report and the HLM report of license usage at customer-level and virtual account level. It also provides Licensing dashboards to display the usage.

You can use Smart Licensing to:

- See the license usage and count.
- See the status of each license type.
- See the product licenses registered on Cisco Smart Software Manager and/or Cisco Smart Software Manager satellite .
- Renew License Authorization with Cisco Smart Software Manager and/or Cisco Smart Software Manager satellite .
- Renew the License Registration.
- Deregister with Cisco Smart Software Manager and/or Cisco Smart Software Manager satellite.

The deployment option for Smart Licensing:

Cisco Smart Software Manager

The Cisco Smart Software Manager (CSSM) is a cloud-based service that handles system licensing. HCM-F can connect to CSSM either directly or through a proxy server. HCM-F and UC applications use the selected Transport Mode. We recommend using a proxy server to connect to CSSM instead of connecting directly. Cisco Smart Software Manager allows you to:

- Manage and track licenses.
- Move licenses across virtual account.
- Remove registered product instance.

To track smart account-related alerts, change the preference settings, and configure email notification. Navigate to **Smart Software Licensing** in **Cisco Smart Software Manager**.

For additional information, go to https://software.cisco.com.

Cisco Smart Software Manager Satellite

Cisco Smart Software Manager satellite is an on-premise deployment that can handle your licensing needs if HCM-F and UC applications cannot connect to CSSM directly, either for security or availability reasons. When this option is deployed, HCM-F registers and report license consumption to the satellite, which synchronizes its database regularly with the backend Cisco Smart Software Manager that is hosted on cisco.com.

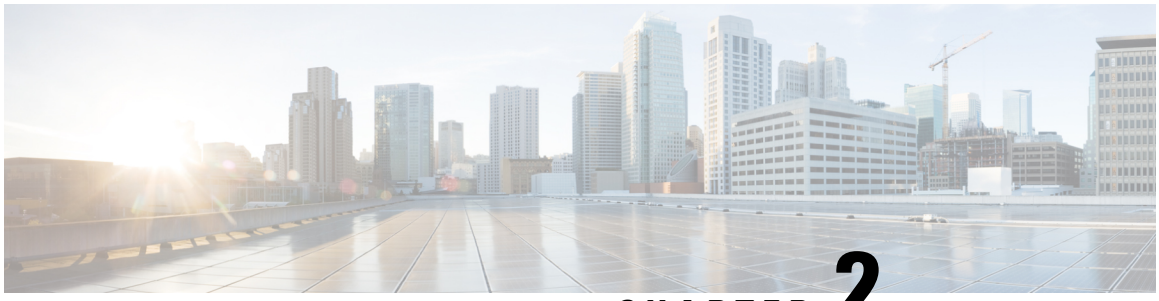
The Cisco Smart Software Manager satellite is deployed in either Connected or Disconnected mode, depending on whether the satellite can connect directly to CSSM on cisco.com.

- Connected—Used when there is connectivity to cisco.com directly from the Smart Software Manager satellite. Smart account synchronization occurs automatically.
- Disconnected—Used when there is no connectivity to cisco.com from the Satellite. Smart Account synchronization must be manually uploaded and downloaded. You can specify the sync schedule in CSSM. By default, the sync with CSSM should be within 30 days.

  For more information on CSSM to Satellite sync, see Certificates Used in Cisco SSM On-Prem Data Exchanges

For more information on Cisco Smart Software Manager satellite information, see https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html.

Note HCM-F does not support Smart Software Manager satellite Classic Edition (CE).



CHAPTER 2

Using Smart Licensing

Enabling Operational License

Complete these steps to enable Operational license:

Procedure

Step 1 The Partner must send an email to hcbu-a2q@external.cisco.com requesting to enable the HCS Operational License.

Ensure to include Cisco Account and Cisco Sales in the email for reference.

Step 2 The Partner uses a single VA (Ordered Virtual Account) to place the order for all the customers in Cisco Commerce (CCW).

These licenses are not used by the Unified Communication Applications

Step 3 Using HCM-F is mandatory.

Step 4 A single VA (Operational License Pool) is shared for both Flex Hosted (EA/NU) and HCS Perpetual Licenses.

Cisco deposits operational licenses into this VA. This Virtual Account is used by UC Applications for consumption.

Step 5 The Partner can avail auto registration features.

Cisco Smart Software Manager (CSSM)

Cisco Smart Software Manager allows product instances to register and report license consumption.

You can use Cisco Smart Software Manager to:

- Manage and track licenses
- Move licenses across virtual account
- Remove registered product instance

Note Enable Javascript 1.5 or a later version in your browser.

We recommend using `connected` mode for the satellite connection.

For details on Cisco Smart Software Manager (CSSM), see https://software.cisco.com/.

Initial One Time Setup in CSSM for Smart Licensing

Use this procedure to set up the CSSM for Smart Licensing.

Procedure

Step 1 Log in to Cisco Smart Software Manager (CSSM) portal (https://software.cisco.com).

Step 2 Create a Smart Account (if you do not have a smart account) in CSSM, or get access to an existing smart account.

Step 3 Send an email to *smart-operations@cisco.com*, requesting API access for your Cisco ID.

The support team provides access to your ID and responds with a confirmation email.

Step 4 Create a CSSM client application with the CCO ID which stores the client ID and client secret.

Note
- The CCO ID used must have a **`Smart Account User`** role for the specific Smart Account for HCM-F to manage it.
- To create the application, select the **`OAuth Grant type`** as **`Client Credentials Grant`**. HCM-F uses the Client Credentials Grant type to communicate with CSSM.

To create a new application with client credentials, click on **Request API Access** from the Cisco API Developer Portal and select the **Client Credentials Grant** option.

Step 5 Login to the Smart Account in CSSM, and create Virtual Accounts, as per your requirement.

Note The admin does not need to create any *product registration token* to register the product. HCM- F performs all the token management for product registration.

While assigning the clusters to VA, the export control cannot be set if HCM-F creates the product registration token. To set the export control value, you have to manually create the product registration token in CSSM and select the export control check-box. For more information about how to register the UC applications that are in mixed mode to the VA in CSSM, see Registering the UC Applications in Mixed Mode to VA in CSSM, on page 10.

We recommend you to get access to the operational licenses. If you have opted for operational licenses, then add the two virtual accounts: ordered virtual account (va-hcs-ordered), and operational virtual account (va-hcs-operational). For more information about operational licenses, see Configuring Operational Licenses, on page 25.

Step 6 Register your product with CSSM, using HCM-F.

For more information on how to register UC applications in HCM-F, see *Add Cluster Application* in *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide*.

Note Until you register, your product is still in Evaluation Mode.

Step 7 Log in to CCW, select a smart account and virtual account, and order HCS licenses.

Note HCS licenses get deposited to the smart account and virtual accounts.

Step 8 Configure Smart Software Licensing alerts in CSSM.

For more information to configure the alerts, see https://software.cisco.com

For more information about adding the On-prem local account to CSSM, see Smart Software Manager On-Prem User Guide.

Note If any of the virtual account has a cluster assigned to it and you need to delete the account, it is required to unassign the cluster from that account in HCM-F before you proceed to delete the account from CSSM server.

Generating Client Credentials in Smart Accounts and Licensing API

Use this procedure to set up the client credentials for Smart Licensing.

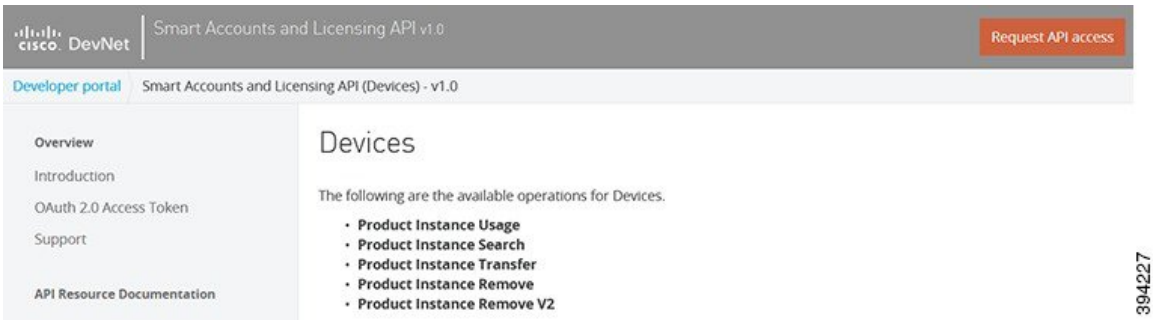
Before you begin

- To request API access for your Cisco ID, send an email to the support team at *smart-operations@cisco.com*. The support team takes the necessary steps to provide access to your ID and respond with a confirmation email within 24 hours.
- The CCO ID used must have a **`Smart Account User`** role for the specific Smart Account, for HCM-F to manage it.

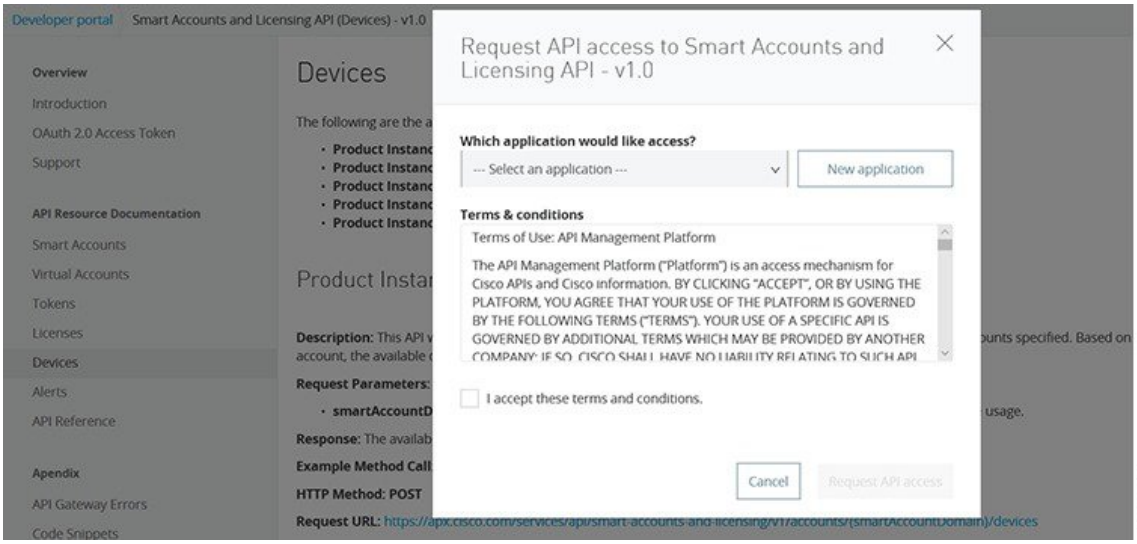
Procedure

Step 1 Log in to Smart Accounts and Licensing API.

Step 2 Click **Request API Access**.



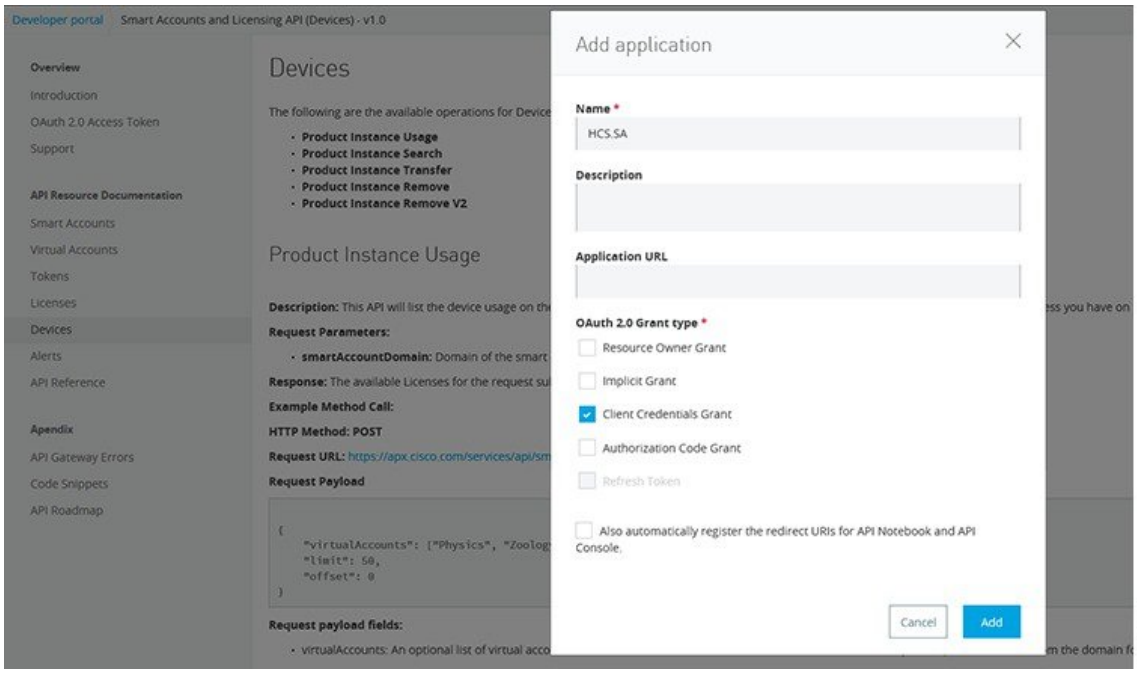
Step 3 Click **New Application**.



Step 4 Enter these details in the Add application window.

- Name: HCM-F instance
- Description: API access for HCM-F
- Select **`Client Credentials Grant`** from the **OAuth Grant Type** list
- Select automatically register the redirect URIs for AP Notebook and API

HCM-F uses the Client Credentials Grant type to communicate with CSSM.

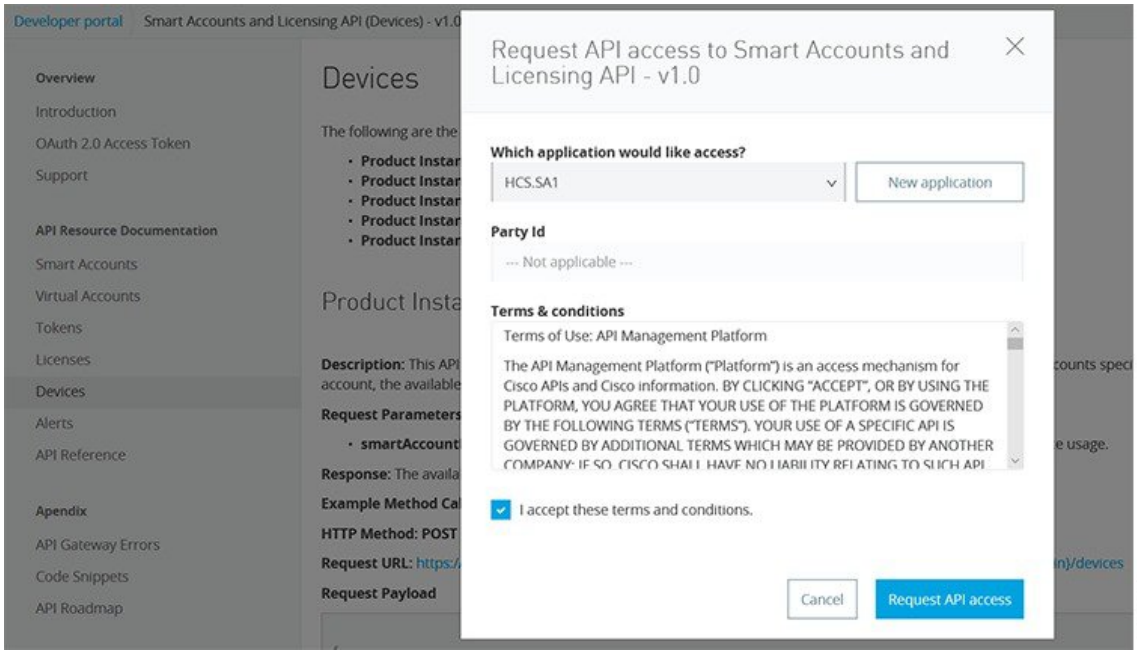


Step 5 Click **Add**.

The application is created and it redirects to the original URL.

Step 6 Select the application from the drop-down, accept the Terms and Conditions, and click **Request API Access**

It generates the Client ID and secret.



Note To get access to the smart account APIs, you must send mail to *smart-operations@cisco.com* with the CCO ID, smart account domain name, and the application created. Once mail is sent, you have to wait for few days to receive a confirmation message.

What to do next

From the Smart Accounts and Licensing API website. Click **Developer Portal**.

Click **My Applications** and select the Application name that is created for the HCMF instance.

You can view the Client ID and Client Secret.

Registering the UC Applications in Mixed Mode to VA in CSSM

You can create the tokens with export control functionality for the UC applications that are in mixed mode.

Before you begin

Remove all the tokens from the specific VA in CSSM.

Procedure

Step 1 Create a token in the VA and select export control functionality.

Step 2 Run a CSSM sync from HCMF.

Step 3 Ensure that only the manually created token is present in the VA.

Step 4 Perform cluster assignment.

Cisco Smart Software Manager On-Prem(Satellite)

Cisco Smart Software Manager on-prem (satellite) is similar to Cisco Smart Software Manager (CSSM). However, instead of being hosted on cisco.com, it is available as an *on-premise* version.

Cisco Smart Software Manager on-prem (satellite) is used to:

- Manage and track licenses of the on-premise users
- Support multiple local accounts (multi-tenant)
- Scale 10,000 product instances
- Connect to Cisco either online or offline

Note Enable Javascript 1.5 or a later version in your browser. Use Cisco Smart Software Manager satellite 7.2 or later version to use all the functionalities.

For details on Cisco Smart Software Manager on-prem (satellite), see Smart Licensing.

Initial One Time Setup in CSSM on-prem for Smart Licensing

Use this procedure to set up the Cisco Smart Software Manager (CSSM) on-prem server for Smart Licensing.

You can register the clusters to CSSM by using either the proxy or the on-prem server.

Pre-requisite for Registering Expressways clusters to the Cisco Smart Software Manager (CSSM) on-prem server for Smart Licensing

1. Configure the Expressway clusters with DNS and domain name of the on-prem Server to adhere to the FQDN requirements of the CSSM On-Prem Server to on-prem CSSM.
2. Expressway-E clusters are registered to CSSM via Proxy Mode, if Proxy is set at the Cluster level.
3. Expressway-E clusters are registered to CSSM via Direct Mode, if Proxy is set at Customer Level.
4. Expressway-C clusters are registered to CSSM via Proxy Mode, if Proxy is set at either Cluster level or Customer level.

Create a new or existing SSM on-prem local Account and register the account before using the Smart Licensing functions in the licensing workspace. Until you complete the registration process, all other Smart Licensing options are not available. Both network and manual registrations are supported.

For more information about CSSM on-prem configuration, see Smart Software Manager On-Prem User Guide.

Procedure

Step 1 Log in to Smart Software Manager on-prem portal.

Step 2 Create a Local Account or get access to an existing local account.

For more information about CSSM on-prem configuration, and creating local account, see Smart Software Manager On-Prem User Guide.

Step 3 Approve the account using the user name and password.

Step 4 Click **Network**, and ensure the hostname which is used in the registration URL is specified in the **SSM On-Prem Name**. Save the configuration.

Step 5 Click **Security**, and ensure the hostname which is used in the registration URL is specified in the **Host common name**. Save the configuration.

- For CSSM On-Prem version 6, use https://*satellite-server-ip*/Transportgateway/services/DeviceRequestHandler as the registration URL.
- For CSSM On-Prem version 7, use https://<*satellite-server-fqdn*>/SmartTransport as the hostname:8443.
- For CSSM On-Prem version 8, use https://<*satellite-server-fqdn*>/SmartTransport as the hostname:8443.

Update the registration URL in HCMF whenever you upgrade the Satellite Servers.

For example, if the registration url is: https://*hostname*/Transportgateway/services/DeviceRequestHandler, then the **SSM On-Prem Name** is *hostname* and **Host common name** is same as the CSSM On-Prem hostname. Example of a token url is: https://*hostname:8443*/backend/oauth/token.

Step 6 Click **Synchronisation** , and do a full synchronization.

Step 7 Enable the API tool kit and create the client ID and secret for the local account.

To create a product registration token in SSM on-prem, see Creating Product Instance Registration Tokens section in the Smart Software Manager On-Prem User Guide .

Note If any of the virtual account has a cluster assigned to it and you need to delete the account, it is required to unassign the cluster from that account in HCM-F before you proceed to delete the account from the CSSM on-prem server.

Smart Accounts and Virtual Accounts

Smart Account
Cisco Smart Account is an account where all products that are enabled for Smart Licensing are deposited. Cisco Smart Account allows you to manage and activate your licenses to devices, monitor license use, and track Cisco license purchases.

Virtual Account
Smart Licencing allows you to create multiple license Pools or virtual accounts within the Smart Software Manager portal or Cisco Smart Software Manager satellite. Using the Virtual Accounts option, you can aggregate licenses into discrete bundles that are associated with a cost center so that one section of an organization cannot use the licenses of another section of the organization. For example, if you segregate your company into different geographic regions, you can create a virtual account for each region to hold the licenses and product instances for that region.

For details on Cisco Smart Accounts and Virtual Accounts, see https://software.cisco.com/.

Smart Licensing Deployment Options

The following options are available for connecting to CSSM and Satellite:

Proxy (Cloud access through an HTTPs proxy)
In a proxy deployment method, Cisco products send usage information through a proxy server.

Note Proxy is the recommended transport mode.

Satellite (Cisco Smart Software Manager Satellite)
In the Satellite deployment method, UC applications register with a Satellite server. Based on the Satellite Server configuration (Offline or Online), Satellite syncs with CSSM.

Direct (Direct Cloud Access)
In a direct cloud-access deployment method, Cisco products send usage information directly.

HCS 12.5 release does not support Smart Licensing APIs.

License Conversion and Migration to Smart Licensing

You can convert Classic, PAK-based licenses (PLM licenses) to a Smart Entitlement (if a Smart License equivalent is available). The license conversion can be performed in the License Registration Portal (LRP) or in Cisco Smart Software Manager (CSSM). You can initiate the process by downloading and installing the Smart Licensing version of the software and registering the device to a Smart Account using a Registration Token. The migration of any entitlements tracked by Cisco, automatically migrates to the Customers Smart Account.

License conversion can be performed either on:

- LRP (License Registration Portal), go to the **PAKs/Tokens** tab, select **Actions** > **Convert to Smart Entitlement**, or
- CSSM (Cisco Smart Software Manager), go to the **License Conversion** tab to convert Classic Licenses to Smart Licenses.

For more information on converting classic licenses to smart licenses, see Migrating classic licenses to smart licenses with active SWSS in *Cisco Smart Software Licensing with Cisco Unified Communications Manager 12.0 Solution Overview*

HCS Managed Services

The UC applications and Prime License Manager (PLM) are available on premise. HCM-F does not have connectivity to the on-premise applications.

The change in Cisco Smart Software Manager (CSSM) helps customers migrating from Enterprise to cloud, to use HCS licenses that are Flex Hosted. The Flex Hosted licenses in version 12.x and later work for both on-premise UC (Enterprise mode) and HCS cloud (HCS mode) so it provides an easier migration from on-premise to HCS as there is no need to migrate licenses during the migration phase.

The CSSM accepts the license request from Enterprise UC applications in Enterprise mode and allocates the mapped HCS licenses if corresponding Enterprise licenses are not available. This is called dual parenting.

CSSM follows hierarchy in allocating the licenses. The higher level licences are utilized to fulfill the request for lower level licenses and avoid a shortage of the licenses.The licences are allocated in the following priority, higher to lower-order:

- Enterprise (when both Enterprise and HCS licences are available)
- HCS Foundation (when the Enterprise licences are all allocated or when there are only HCS licences)
- HCS Standard (when the Enterprise licences are all allocated or when there are only HCS licences)

Following is the HCS license mapping for Enterprise licenses:

Table 1: License Mapping

HCS License	Enterprise Licenses		
	Cisco Unified CM	Cisco Unity Connection	Cisco Emergency Responder
HCS Cisco UCM Foundation License	• Basic • Essential • Enhanced		
HCS Cisco UCM Standard License	• Cisco Unified Workspace Licensing (UWL) • Enhanced plus		
HCS Cisco UCM TelePresence Room License	Telepresence Room		
HCS Unity Connection Basic License		CUC_BasicMessaging	
HCS Unity Connection Standard License		CUC_EnhancedMessaging	
HCS Emergency Responder User License			CER_USER

Migration from On Premise to HCS

Use this procedure to change the license mode for the Unified Communication applications and PLM from enterprise license mode to HCS mode for cluster versions below 12.x and for versions 12.x and later. Use the `ciscocm.HCSMode_v4.cop.sgn` file to change the licensing from Enterprise Mode to HCS Mode. Install the cop file on the publisher node of all Cisco Unified CM, Cisco Emergency Responder, and Cisco Unity Connection clusters, and standalone PLM or co-resident PLM. The cop file is available at License Mode Change - Enterprise Mode to HCS Mode.

To change the licensing from HCS Mode to Enterprise Mode, install the `ciscocm.EnterpriseMode_v4.cop.sgn` file on the publisher node of all Cisco Unified CM, Cisco Emergency Responder, and Cisco Unity Connection clusters, and standalone PLM or co-resident PLM. The cop file is available at License Mode Change: HCS Mode to Enterprise Mode.

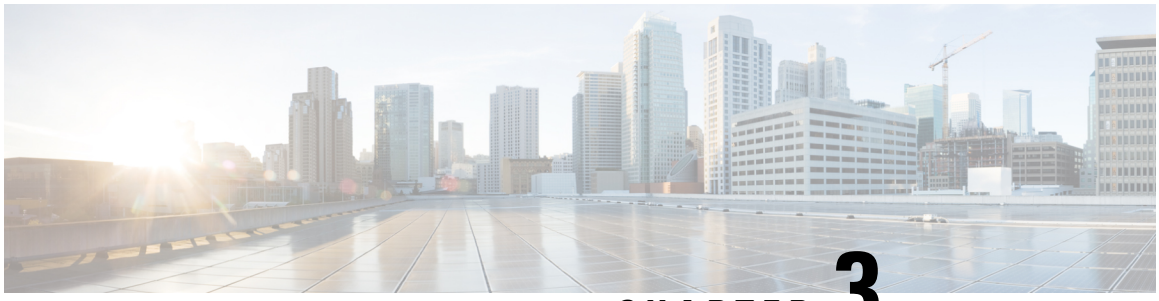
For detailed information on the COP files, see these links:

To change from enterprise mode to HCS mode: Readme for License Migration from On-prem to Hosted Collaboration Solution.

To change from HCS mode to enterprise mode: Readme for License Migration from Hosted Collaboration Solution to On-prem.

Smart Versus Traditional Licensing

Traditional (node locked) licensing	Smart (dynamic) licensing
You procure the license and manually install it on the PLM.	Your device requests the licenses that it needs from CSSM.
Node-locked licenses - license is associated with a specific device.	Pooled licenses - Smart accounts are the company account specific that can be used with any compatible device in your company.
No common install base location to view the licenses that are purchased or software usage trends.	Licenses are stored securely on Cisco servers that are accessible 24x7x365.
No easy means to transfer licenses from one device to another.	Licenses can be moved between product instances without a license transfer, which greatly simplifies the reassignment of a software license as part of the Return Material Authorization (RMA) process.
Limited visibility into all software licenses being used in the network. Licenses are tracked only on per node basis.	Complete view of all Smart Software Licenses used in the network using a consolidated usage report of software licenses and devices in one easy-to-use portal.



CHAPTER 3

Onboard Customer per Cluster

Provisioning Workflow for Smart Licensing

Before you begin

Complete the following:

- Read Cisco Smart Software Manager
- Configure CSSM as described in Initial One Time Setup in CSSM for Smart Licensing, on page 6
- Configure Satellite as described in Initial One Time Setup in CSSM on-prem for Smart Licensing, on page 11

Procedure

Step 1 View Smart Account Summary, on page 22

Step 2 Configure Smart Account Access

Step 3 Virtual Account Summary, on page 24

Step 4 Assign and Unassign a Cluster to Virtual Account

You can sync smart accounts and virtual accounts from HCM-F to CSSM and Satellite, either manually or automatically. For more information on manual sync, see *Perform Manual Sync* in *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide*.

Note HCM-F periodically syncs with CSSM and Satellite.

What to do next

Verify the **Status** column for the job status in the HCM-F interface. Navigate to (**Infrastructure Manager** > **Administration** > **Jobs**) and see the **Smart Account** in the **Job Entity** column. If a job fails, hover over the information icon and the **Job Details** window pops up. Check the status information and recommended action.

Create a Smart Account

Procedure

Step 1 Skip this section if you already have a Smart Account. Otherwise, you can continue to the next step.

Step 2 Log in to software.cisco.com using your Cisco.com ID (CCO ID).

Step 3 Select **Request a Smart Account** under the Administration section.

Step 4 Follow the steps to create a Smart Account for your organization.

Configure Smart Account Access

The Configure Smart Accounts page does not create a Smart Account in CSSM, but only saves the data locally in HCM-F to take care of other operations and reporting for Smart Accounts. You must create the Smart Account and client application directly in the CSSM portal.

Procedure

Step 1 From the side menu, select **Infrastructure Manager** > **Smart Licensing** > **Configure Smart Account**.

Step 2 Click **Add New**.

Step 3 Complete the fields in the **Configure Smart Account Access** page.

Fields	Description
Smart Account Domain Name	Domain name of smart account.
Client ID	ID of the smart account
Client Secret	Secret (password) of the smart account
Smart Account Name	Name of the smart account. This is an optional field.

Step 4 Complete the fields in the **Configure Smart Account Access** page.

a) In the **Transport Settings** enter the following fields:

Table 2: Transport Mode Settings

Fields	Description
Transport Mode	Select the transport mode to access CSSM. The options are: • Proxy: Cisco products send usage information through a proxy server. • Satellite: Cisco products are installed on premise and the connectivity to Cisco is online or offline. • Direct: Cisco products send usage information directly.

b) Configure the transport mode settings as follows:

Table 3: Direct Transport Mode Settings

Fields	Description
Authentication Gateway	Displays the authentication gateway.
CSSM Server	Displays the CSSM server.
Smart Account Domain Name	Domain name of smart account.
Client ID	ID of the smart account
Client Secret	Secret (password) of the smart account

Table 4: Proxy Transport Mode Settings

Fields	Description
Proxy Hostname/IP	Enter the proxy hostname or IP address. **Note** When you set the transport mode as proxy, the setting connects the HCM-F to the CSSM through proxy but does not register the customer and cluster with the CSSM. To register the cluster and customer to the CSSM, add the proxy values at the customer and cluster level to connect to the CSSM through proxy, otherwise it will connect through direct mode, by default. For more information about setting the proxy at customer and cluster level, see *Add Customer*, and *Add Cluster* at *Hosted Collaboration Mediation Fulfillment Install and Configure Guide*.
Proxy Port	Enter the proxy port.
Authentication Gateway	Displays the authentication gateway.
Enable Proxy Authentication	HCM-F uses the proxy authentication defined at the customer and cluster level to synchronize with CSSM. • Proxy Username- Enter the proxy username. • Proxy Password- Enter the proxy password.
CSSM Server	Displays the CSSM server.
Smart Account Domain Name	Domain name of smart account.
Client ID	ID of the smart account
Client Secret	Secret (password) of the smart account

Table 5: Satellite Transport Mode Settings

Fields	Description
Satellite Hostname	Enter the satellite hostname.
Satellite Port	Enter the satellite port.

Fields	Description

Registration URL	Enter the registration URL.
	Refer to the links below for the registration URLs for their respective satellite versions:
	• Satellite version 6.3.0 - https://<SATELLITE_IP_ADDRESS>/Transportgateway/services/DeviceRequestHandler
	• Satellite version 7.2.0 -
	  • HCM-F V12.5SU2 and above - https://<SATELLITE_FQDN>/SmartTransport
	  • below HCM-F V12.5SU2 - https://<SATELLITE_FQDN>/Transportgateway/services/DeviceRequestHandler
	• Satellite version 8.X - https://<SATELLITE_FQDN>/SmartTransport

Token URL	Enter the Token URL. Refer to the links below for the Token URLs for their respective satellite versions: • Satellite version 6.3.0 - https://<SATELLITE_IP_ADDRESS>:8443/backend/oauth/token • Satellite version 7.2.0 - https://<SATELLITE_FQDN>:8443/backend/oauth/token • Satellite version 8.X - https://<SATELLITE_FQDN>:8443/backend/oauth/token
Local Account Domain Name	Domain name of the satellite smart account. This field is displayed only when you select Satellite as the transport mode.
Client ID	ID of the smart account
Client Secret	Secret (password) of the smart account

If the cluster is already assigned to a virtual account, and you want to change the transport mode settings, the cluster has to be unassigned from the virtual account, change the transport mode settings, and then reassign the clusters to the virtual account.

Step 5 Enable the Operational Licenses to autoregister the clusters to the specified virtual account.

For more information about Operational Licenses and Auto Registration of clusters, see Auto-registration of Clusters Using Direct or Proxy Mode, on page 32

Step 6 Click **Save**.

Note For 12.5 release, HCM-F supports only one smart account. When the smart account is added in HCM-F, HCM-F performs a sync with CSSM to pull the Smart account and virtual account data. If the number of virtual accounts are high it might take more time to sync (approximately 1-2 hours).

Note From 12.5SU1 release, HCM-F supports multiple smart accounts with different client credentials, and multiple satellite accounts. When the smart account is added in HCM-F, HCM-F performs a sync with CSSM and satellite to retrieve the Smart account, virtual account, and local account data.

Related Topics

Auto-registration of Clusters Using Direct or Proxy Mode, on page 32

Set Transport Mode

Setting up the transport mode in HCM-F is required for connecting HCM-F and UC applications to CSSM.

HCM-F and UC application clusters support the following transport modes for license consumption and reporting:

- Proxy
- Direct

Procedure

Step 1 From the side menu, select **Infrastructure Manager** > **Smart Licensing** > **Transport Mode**.

Step 2 Select the mode from the **Transport Mode** drop-down list.

Note
- If transport mode is Direct, Authentication Gateway and CSSM Server information is displayed by default.

  When Smart account is provisioned with client credentials (Client ID and Client Secret) in HCM-F, the HCM-F authenticates with the Cisco Authentication Gateway with client credentials. HCM-F gets the access token from Cisco Authentication Gateway for communicating with CSSM.

- If transport mode is Proxy, enter the proxy server and the proxy server port details.

  Authentication Gateway and CSSM Server information is displayed by default.

  Note Proxy is the recommended option. Validate that HCMF and UC applications are connected to CSSM through the proxy.

View Smart Account Summary

The **Smart Account Summary page** displays the CSSM Smart Accounts, and Satellite Smart Accounts.

Procedure

Step 1 From the side menu, select **Infrastructure Manager** > **Smart Licensing** > **Smart Account Summary**.

Step 2 The **Smart Account Summary** page shows the following information on smart accounts:

Fields	Description
Name	Name of smart account
Domain	Domain name of smart account
Type	Type of smart account
Status	Status of smart account: active or inactive
VA#	Number of virtual account associated with the smart account
Last SyncUp	Last sync up time of smart account
Alerts	Shows the alerts

Note To see the virtual accounts associated with the smart account, click the smart account name from the list. The Virtual Accounts page shows the list of virtual accounts.

Note To see the virtual accounts associated with the smart account, click the virtual account name from the list. The Virtual Accounts page shows the list of virtual accounts.

Step 3 Click **Add New** to configure a new smart account.

Click the Smart Account Name to edit the existing Smart Account.

Related Topics

Configure Smart Account Access, on page 18

Create Virtual Account

Procedure

Step 1 Login to software.cisco.com using your Cisco.com ID (CCO ID).

Step 2 Select**Manage Smart Account** under Administration section

Step 3 Select the **Virtual Accounts** tab and then select **New Virtual Account...**.

Step 4 Create two Virtual Accounts and name them as:

- VA–HCS-Ordered
- VA–HCS-Operational

Step 5 Ensure to add the following two users in Cisco HCS Operations Team as Virtual Account User.

alicchan@cisco.com

trgilman@cisco.com

Virtual Account Summary

Virtual Account Summary window displays the list of Virtual accounts. Once a virtual account is selected, you can do the following:

- Admin can change the license mode for any virtual account.
- If no mode was present earlier, then the license mode could be set.
- If no cluster is assigned to the VA, then you can change the mode of the VA.
- If a cluster is assigned to the VA, then you cannot change the mode of the VA (It requires the clusters to be unassigned from the VA before changing the VA license mode). In this scenario, the license mode is noneditable. Hover over the tooltip for the VA to get the information. If the cluster is assigned to the VA, the tooltip states that the mode cannot be changed as clusters are associated with the VA. Once the clusters are unassigned, you can edit the license mode of VA.

  The license mode is not applicable for the virtual account in CSSM. License mode is applicable only on HCM-F. It enables to identify the mode it should set the UC application.

Procedure

Step 1 From the side menu, select **Infrastructure Manager** > **Smart Licensing** > **Virtual Account Summary**.

Step 2 The **Virtual Accounts** page shows the list of virtual accounts, and the following information on virtual accounts:

Fields	Description
Name	Name of virtual account
SA Name	Name of smart account
Access Level	Specifies the access level assigned to the virtual account
Clusters #	Number of clusters assigned to the virtual account
Customer#	Name of customers assigned to the virtual account

Assign and Unassign a Cluster to Virtual Account

If auto registration is enabled then the partner does not need to manually register or unregister unless they need to register clusters to different license repositories, such as, one smart account and one satellite server or two or more satellite servers.

Procedure

Step 1 From the side menu, select **Infrastructure Manager** > **Smart Licensing** > **Virtual Account Summary**.

Step 2 From the **Virtual Accounts** page, click a virtual account name.

Step 3 From the **Edit Virtual Account** page, select the license mode from the **License Mode** dropdown.

Step 4 Click **Assign** in the **Clusters Assigned to *Virtual Account*** section.

Note
- You cannot assign the cluster to the virtual account if the license mode for the virtual account is not set. A warning message is displayed asking to add the license mode for the VA.
- You cannot change the license mode of a virtual account if a cluster is assigned to the virtual account. In this scenario, unassign the cluster from the virtual account.

Step 5 From the **Assign Cluster to *Virtual Account*** page, select the cluster by checking the check box.

Note Only clusters higher than 11.x is displayed here.

Step 6 Click **Assign**.

Note
- To unassign a cluster from the virtual account, select the cluster by checking the check box from the **Clusters Assigned to *Virtual Account*** section, and then click **Unassign**.
- To assign or unassign a cluster from the virtual account, use the filter by customer name to filter the clusters.

View the **Cluster Summary** page to ensure that all the clusters are registered, and if it fails to register then refer to the recommended action.

Configuring Operational Licenses

You can use operational license to generate reports in HCM-F for the amount-of-licenses that are ordered by the partner and the amount-of-licenses that are consumed. If you opt for operational license, then you have to create an operational virtual account in CSSM where Cisco stores all the licenses that the partner consumes. An ordered virtual account is also created where the licenses ordered by the partners from CCW are stored and are not used by the UC applications. Operational license can be opted by both Flex and perpetual license user. If you have opted for operational license, the licenses are stored in the operational virtual account in CSSM.

You can autoregister the clusters if you opt for operational licenses.

Note If the clusters are registered in satellite, then HCM-F syncs with CSSM using proxy and gets the details of the satellite operational licenses.

Before you begin

- You must have a Smart Account, Local Account, and Virtual Account in CSSM and Satellite.
- The operational licenses are stored in operational virtual account (va-hcs-operational).
- Set up operational licenses for the clusters.

  If the clusters are migrated to version 12.5 and later, the Flex Usage Report displays additional values for true forwarding, licenses consumed, and compliance check.

Procedure

Step 1 Fill this smart sheet http://cs.co/HCSPartnerRequestForm to get access to the Operational Licenses.

Step 2 Once you receive a confirmation, create the following virtual accounts in CSSM.

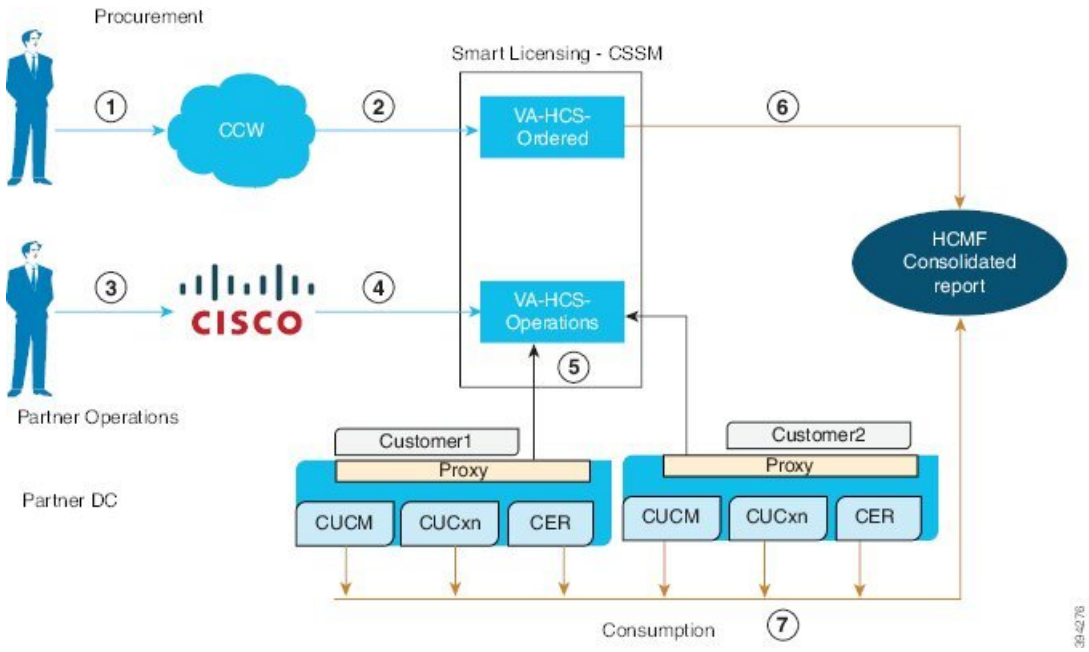
Ordered Virtual Account
Displays the name of the virtual account that stores the licenses that the partners order from CCW. We recommend the Ordered Virtual Account name as va-hcs-ordered.

Operational Virtual Account
Displays the name of the virtual account that stores the Cisco licenses to be consumed. We recommend the Operational Virtual Account name as va-hcs-operational. The clusters are registered to this virtual account in CSSM.

Task Flow of Operational License Without Satellite Account

This is the task flow of the operational license without the Satellite virtual account.

Figure 1: Task Flow of the Operational License Without Satellite Account



Procedure

Step 1 User orders licenses from CCW.

Step 2 For all users ordered licenses, a virtual account is created in CSSM: *va-hcs-ordered*.

Step 3 Fill this smart sheet http://cs.co/HCSPartnerRequestForm to get access to the Operational Licenses.

For more information on the prerequisites, see Configuring Operational Licenses, on page 25.

Step 4 Create an operational virtual account in CSSM, where Cisco deposits all the operational licenses that are to be consumed: *va-hcs-operations*.

Once you have opted for operational license, autoregistration of clusters is possible while you configure a smart account.

Step 5 HCM-F queries ordered virtual account for licenses that are deposited per Subscription ID.

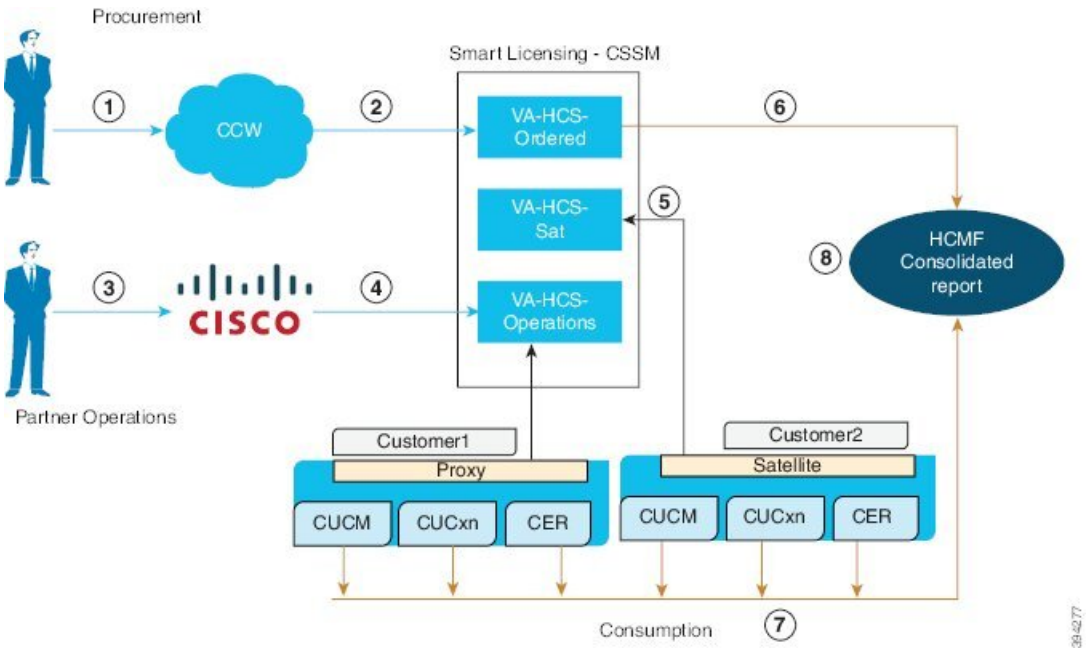
HCM-F is preconfigured to map Customer to Subscription ID.

Step 6 HCM-F queries Cisco Unified Communications applications for the license consumption report. A consolidated report is generated with the ordered license details, consumption details, and compliance status. For more information about the report, see Request or Download Flex Usage Report

Task Flow of Operational License With Satellite Account

This is the task flow of the operational license with the Satellite virtual account.

Figure 2: Task Flow of the Operational License with Satellite Account



Procedure

Step 1 User orders licenses from CCW.

Step 2 For all users ordered licenses, a virtual account is created in CSSM: *va-hcs-ordered*.

Step 3 Fill this smart sheet http://cs.co/HCSPartnerRequestForm to get access to the Operational Licenses.

For more information on the prerequisites, see Configuring Operational Licenses, on page 25.

Step 4 Create an operational virtual account in CSSM, where Cisco deposits all the operational licenses that are to be consumed: *va-hcs-operations*. User has to move the licenses from operations VA in CSSM to satellite VAs.

Autoregistration feature supports only one Satellite account. For using more than one Satellite, user can use the Satellite on board functionality that is provided by HCM-F.

Step 5 HCM-F queries ordered virtual account for licenses that are deposited per Subscription ID.

HCM-F is preconfigured to map Customer to Subscription ID.

Step 6 HCM-F queries Cisco Unified Communications applications for license consumption report.
A consolidated report is generated with the ordered license details, consumption details, and compliance status. For more information about the report, see Request or Download Flex Usage Report

View Cluster Summary

Procedure

Step 1 From the side menu, select **Infrastructure Manager** > **Smart Licensing** > **Cluster Summary**.
The **Cluster Summary** page displays the following:

- List of Unified Communication clusters with the version 12.5 and later.
- List of Expressway E and C clusters with version X12.6 and later that are configured with Smart licensing mode.

Note Registration of Expressway clusters in HCM-F is at the cluster level whereas for the other applications registration in HCM-F is done by node.

Fields	Description
Name	Name of the cluster
Type	Retrieves the type of cluster such as Unified CM, Unity Connection, CER, Expressway-E, Expressway-C from the HCM-F inventory.
Version	Specifies the Cluster version.
Smart Account	Name of the Smart Account that is associated with the virtual account.
Virtual Account	Virtual Account name that the cluster is associated with.

Fields	Description
Status	

Fields	Description
	Displays the status of the clusters, if they are registered, unregistered, partially registered or autoregistered to the virtual account. For example, if the cluster is autoregistered, then the status is displayed as Autoregistered. The information icon provides details about the cluster status, description, and the recommended action. The cluster status is prioritized as follows: • Multiple Virtual Account Registered -Specifies the clusters that are assigned offline using the Expressway user interface, where all the nodes are not registered to the same VA. Partial and mutiple VA applies only to Expressway-E and C clusters. NOTE: For clusters registered as multiple VA registered, you cannot assign/unassign clusters using the HCM-F application. Use the Expressway application to assign the multiple VA registered clusters. • Auto Registration Failed - Auto registration of the cluster fails. • Manual Registration Failed - Manual assignment of cluster fails. • Deregistration Failed - Manual unassignment of the cluster fails. • Deregistered - cluster is unassigned manually. • Partially Registered - cluster is partially assigned when: • All nodes of a cluster are not registered. • If one of the node of the cluster is either registered/unregistered NOTE: Partially Registered status applies only to Expressway E and C clusters. • Auto Registration Inprogress - auto registration of the cluster is in progress. • Auto Deregistration InProgress - Auto deregistration of cluster is in progress. • Auto Registered - cluster is autoregistered to the virtual account. • Manually Registered - cluster is manually

Fields	Description
	assigned to a virtual account. • Deregistered - clusters are not assigned to any virtual account. NOTE: Add all the nodes of the Expressway cluster in HCM-F, to register the cluster. If there is a mismatch in the number of Expressway cluster nodes that is configured in HCM-F, then the registration fails.
Job Status	The information icon provides the provisioning status of the cluster.

Step 2 Hover over the information icon for a cluster in the **Job Status** column to see the job details of the cluster.

Fields	Description
Job Type	Specifies the provisioning status of the cluster.
Entity Type	Specifies the type of the cluster.
Date/Time Initiated	Specifies the data and time when the job was initiated.
Date/Time Completed	Specifies the data and time when the job completed.
Status	Specifies the overall status of the job.
Entity Name	Specifies the entity name of the cluster.
Description	Details of the job.
Status Information	Status of the job
Recommended Action	Describe the action to resolve the issue.

Step 3 To modify a cluster, select a cluster from the list, and modify the details in the **Cluster Summary** page.

For more information about the field details in the **Cluster Summary** page, see *Add Cluster* section in *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide*.

Note If you apply a filter of Type on the Cluster, then the set of keyword values that are allowed for Expressway clusters in Smart licensing mode are: core, edge, expressway,expresswayedge, expressway edge,expresswaycore, and expressway core.

Edit Virtual Account

Use this procedure to change the settings associated with the Virtual Account:

Procedure

Step 1 From the side menu, select **Infrastructure Manager** > **Smart Licensing** > **Virtual Account Summary**

Step 2 Select the virtual account to make changes, the Edit Virtual account window displays.

Field	Description
Name	Name of virtual account
Description	Displays a short description of the account
Smart Account Name	Displays the Smart account name.
Domain Name	Displays the associated domain name of the cluster.
License Mode	Specifies the license mode that is associated with the cluster.
Commercial Access Level	Specifies the access level that is assigned to the virtual account

Step 3 Clusters Assigned- Displays the details of all clusters that are associated with the virtual account. Select unassign, to unassign a cluster for the account. Click Assign, to add a new cluster to the account.

Auto-registration of Clusters Using Direct or Proxy Mode

Note If you enable autoregistration, HCM-F changes the license modes of the UC Applications to HCS mode. Hence, the publisher node of the clusters which are in enterprise mode reboots and the license mode is changed to HCS mode.

You can assign the clusters to the virtual account manually, however, from HCS 12.5 SU1 release you can auto-assign the clusters to the operational virtual account. This procedure enables you to autoregister the clusters to the operational virtual account using the proxy or direct mode.

Note Autoregistration of clusters is possible for only one Smart Account. If **Operational Licenses** are enabled for a smart account, and you try to configure a new smart account or satellite account, the **Operational Licenses** check-box is disabled.

If you have not opted for Operational Licenses, you cannot autoregister the clusters to the operational virtual account.

Note Configure the proxy settings at customer or cluster level before enabling auto-registration for Proxy mode. For more information, see *Add Cluster* in *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide*.

Procedure

Step 1 Navigate to **Infrastructure Manager** > **Smart Licensing** > **Smart Account Summary**. Click **Add New** to configure the smart accounts.

Step 2 Select **Opted Operational Licenses** to register the clusters to the following virtual accounts:

Ordered Virtual Account
Displays the name of the virtual account that stores the licenses that the partners order from CCW. We recommend the Ordered Virtual Account name as va-hcs-ordered.
Operational Virtual Account
Displays the name of the virtual account that stores the Cisco licenses to be consumed. We recommend the Operational Virtual Account name as va-hcs-operational. The clusters are registered to this virtual account in CSSM.

Note
- If the Ordered and Operational VAs are unchanged, a job for auto-registration is not triggered. Only way to trigger the job is to disable and enable the auto-registration again as part of smart account configuration update.
- If the ordererd and operational VAs are different and valid, it first triggers de-registration job for unassigning the clusters from the old operational VA and then trigger auto-registration job for assigning to the new operational VA.
- Any auto-registered cluster can be manually unassigned and re-assigned to different VA. In such case, that cluster is no longer considered as part of the autoregistration process. If at all the cluster has to be part of the auto-registration, then the smart account should be either updated with first disabling and then enabling auto-registration.

Autoregistration of the clusters is possible if any of the following conditions are met:

- When the clusters with version 12.5 is installed, the clusters are automatically autoregistered to the operational virtual account.
- When the clusters are upgraded to 12.5, and you have opted for operational licenses, you can choose to autoregister the clusters to the operational virtual account, otherwise they are manually assigned to the virtual accounts.
- While configuring the smart account, if you opt for operational licenses and enable autoregistration, any existing 12.5 cluster version is autoregistered.

Following are the cluster assignment to virtual account scenarious:

Table 6: Cluster Assignment Scenarios

If...	Then...
You want one of the cluster to be removed from the autoregistered virtual account	You have to unassign the cluster manually from the autoregistered virtual account, and reassign the cluster manually to the specific virtual account.
You want one of the cluster to be reassigned to the autoregistered virtual account	You have to unassign the cluster manually from the specific virtual acount, and reassign the cluster manually to the autoregistered virtual account.

If...	Then...
Any cluster fails to autoregister to the operational virtual account	You can do the following: • An on-demand or auto sync that happens in every 24 hours registers the cluster to the operational virtual account. • You can also disable the autoregistration option and enable it again as part of Smart Account update.

Step 3 Select **Enable Auto Registration of applications (disable if you are using Satellite)** option to autoregister the clusters to the operational virtual account in CSSM, while using the Direct and Proxy as the Transport Mode. De-select the autoregistration option, if you want to autoregister the clusters using the Satellite as the Transport Mode.

Autoregistration is automatically triggered when:

- If any configuration details are wrong during the Smart Account configuration (For example, Proxy hostname, IP address, and so on), update the fileds with the right value, then the autoregistration is automatically triggered.
- In case of proxy mode, if right proxy details are provided at cluster or customer level as part of the update, autoregistration is automatically triggered.
- Any of the operations, such as credential change, network address change to a valid value for a cluster as part of the update also triggers autoregistration.

Autoregistration of Clusters Using Satellite Mode

Autoregistration automatically registers the clusters to the operational virtual account. You can autoregister the clusters by using Satellite mode.

Before you begin

Enabling autoregistration through satellite mode is allowed only if the Operational License is enabled while configuring the smart account as part of either the Proxy or Direct mode.

Procedure

Step 1 Navigate to **Infrastructure Manager** > **Smart Licensing** > **Smart Account Summary**. Click **Add New** to configure the smart accounts.

Step 2 Select **Satellite** as the Transport Mode.

Note Operational License options must be enabled while configuring smart accounts by using the Proxy or Direct mode.

Step 3 Select **Enable Auto Registration** to register the clusters to the operational virtual account.

When you configure a smart account using Satellite as the Transport Mode, the **Enable Auto Registration** option is enabled. You can provide an operational virtual account name, and the clusters are auto-assigned to the virtual account in the satellite server.

HCM-F 12.5 Upgrade Guidelines

Provision the Smart account with client credentials that includes Client ID and Client Secret in HCM-F. This provisioning enables HCM-F to authenticate with the Cisco Authentication Gateway with the client credentials. HCM-F gets the access token from Cisco Authentication Gateway for communicating with CSSM.

Procedure

Step 1 Complete the seps in Initial One Time Setup in CSSM for Smart Licensing, on page 6 topic.

Step 2 Upgrade HCM-F to 12.5(x).

For more information about upgrading HCM-F, see *Upgrade HCM-F* in *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide*.

Set the Transport Mode in HCM-F, navigate to **Smart Licensing** > **Transport Mode**.

Step 3 Provision Smart Account in HCM-F.

Configure the Smart Account or Satellite local account, navigate to **Smart Licensing** > **Configure Smart Accounts**. For details, see *Cisco Hosted Collaboration Solution Smart Licensing Guide*.

Configure the Smart Account, navigate to **Smart Licensing** > **Smart Accounts**. Click **Add New**, to configure smart accounts.

For more information, see Configure Smart Account Access, on page 18.

Note Once the Smart Account is configured, HCM-F synchronizes with CSSM and Satellite and retrieves all the Virtual Account details to HCM-F in **Virtual Account Summary** window (**Smart Licensing** > **Virtual Account Summary**).

Step 4 Upgrade the UC applications.

a. License Conversion and Migration to Smart Licensing

b. Unassign the UC clusters from PLM before you upgrade UC clusters to 12.5(x). Navigate to **License Management** > **License Management Summary**.

c. Upgrade the UC applications.

- To upgrade Unified CM and IM and Presence to 12.5(x), see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide
- To upgrade Cisco Unity Connection to 12.5(x), see Install, Upgrade, and Maintenance Guide for Cisco Unity Connection Guide.
- To upgrade Cisco Emergency Responder (CER) to 12.5(x), see Cisco Emergency Responder Administration Guide

Step 5 Register the UC applications to Virtual Account.

a. Update the Cluster Application Version to 12.5(x). Navigate to **Cluster Management** > **Cluster** to verify the version. For details, see *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide*

Note If you are using Unified CDM, ensure the cluster application version is 12.5(x). If the version is less than 12.5(x), update the cluster application version to 12.5(x).

If you are registering to CSSM by using the proxy mode, then you must set the proxy parameters at the customer and cluster level, otherwise the registration fails. For more information about the proxy parameters at cutomer and cluster level, see *Add Customer*, and *Add Cluster* sections in *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide*.

b. Assign a cluster manually to a Virtual Account, if you have not opted for auto registration.

Assign the License Mode to HCS for a Virtual Account, navigate to **Smart Licensing** > **Virtual Account Summary**.

For details, see Assign and Unassign a Cluster to Virtual Account, on page 24.

Note Ensure the licenses are present in the VA in CSSM.

Step 6 To check that the product instances are populated correctly and licenses are consumed, log in to Cisco Software Central.

Subscription Mapper

HCM-F pulls all the Subscription IDs from CSSM. You can select the customer for each Subscription ID from the **Subscription Mapper** page. When the Flex Usage report is generated, HCM-F uses this mapping to corelate the order and usage information and calculates the Compliance and True Forwarding.

Subscription Mapper page enables you to map the Subscription IDs to a particular customer and select the license model. You can do the following:

- HCM-F identifies the license ordered details per customer and performs the true forwarding calculation and compliance check. For more information about true forwarding calculation, and compliance check, see Request or Download Flex Usage Report.
- You can sort by the End date to identify which all subscriptions are about to expire.
- To update your order, you can click the subscription number and connect to CCW with the Subscription ID.

Before you begin

- Smart Account, virtual account, and satellite account should be configured in HCM-F.
- HCM-F retrieves Subscription IDs from all the virtual account in CSSM and satellite.

Procedure

Step 1 From the side menu, select **Infrastructure Manager** > **Smart Licensing** > **Subscription Mapper**.

Step 2 The **Subscription Mapper** page shows the following information:

Select Subscription ID
Select the Subscription ID from the drop-down list.
Select Customer ID
Select the customer name from the drop-down list to which you want to map the Subscription ID.
You must map a customer to the Subscription ID to retrieve order details for the specific customer.
Select Licensing Model
Select the License model from the drop-down list.

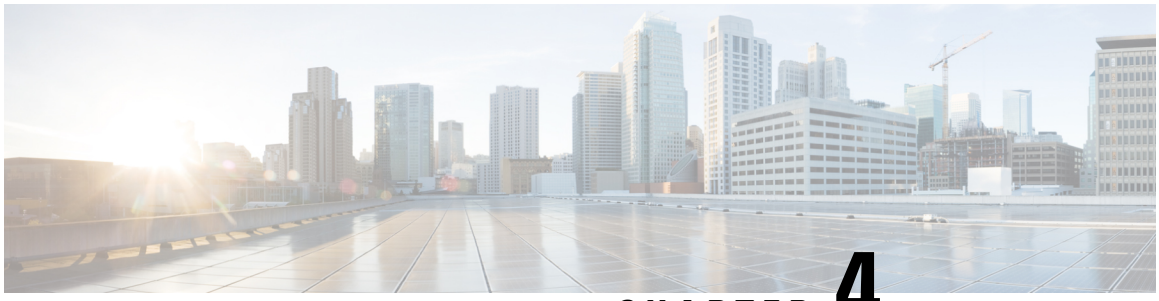
Fields	Description
Subscription ID	Displays the subscription IDs that are retrieved while HCM-F performs a sync with CSSM and satellite.
License Details	Displays the number of licenses that are consumed by each subscription ID. Hover over the **i** icon to see the license details that has the list of license types.
Start Date	Displays the start date of the license type. This is valid only for Flex licenses.
End Date	Displays the end date of the license type. This is valid only for Flex licenses. **Note** For Perpetual licenses Start Date and End date is not valid.
Customer	Displays the name of the customer to which the Subscription ID is mapped.
License Model	Displays the model of the license. The supported options are: Perpetual, Named User, Named User + Perpetual, or Enterprise Agreement.

- If the license model is already mapped, then the same is displayed in the **Subscription Mapper** page.
- If subscription ID is already added, then it is auto-populated.
- Existing configurations are retained.
- Multiple subscription IDs can be mapped to a single customer.
- One subscription ID must be mapped to a single customer.
- All perpetual licenses are automatically mapped to the provider.

Note Perpetual licenses might not have Subscription ID.

What to do next

For the detailed report about the license consumption for the Subscription ID of the customer, see the Flex Usage Report in *Hosted Collaboration Solution Mediation Fulfillment Install and Configure Guide*.



CHAPTER 4

Deployment Scenarios

Scenario: To Migrate On-Premise UC with Dual License Entitlement to HCS

Use this workflow to migrate from Dual Entitelment On-premise Unified Communication applications to HCS 12.5 Smart Licensing:

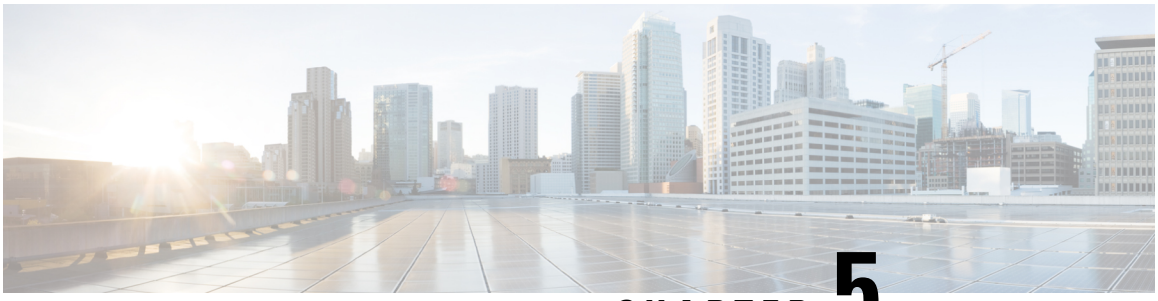
Action	Description
Log in to Cisco Commerce(CCW) and order HCS license.	For more information about operational licenses, seeConfiguring Operational Licenses, on page 25
Create a smart account and virtual account	• Create a Smart Account in CSSM or Satellite. You can also get access to an existing smart account. • Create Virtual Account For more information about the one time setup activities, see Initial One Time Setup in CSSM for Smart Licensing, on page 6 and Initial One Time Setup in CSSM on-prem for Smart Licensing, on page 11
Setup Transport Mode	Setup the transport mode in HCM-F to connect HCM-F and UC applications to CSSM. For more information, see Set Transport Mode, on page 22.

Action	Description
Provision smart account in HCM-F	• Provision the credentials and Smart Account with HCM-F. • HCM-F extracts smart account, local account, and virtual account-related information from CSSM and Satellite. • Creates product registration token to register UC Applications in CSSM and Satellite. • Provide the transport mode in HCM-F to connect HCM-F and UC applications to CSSM and Satellite. For more information, see Provisioning Workflow for Smart Licensing, on page 17 **Note** You can autoregister the clusters to ordered virtual account using HCM-F.
Activate Smart Licensing for Clusters (Cisco Unified Communications Manager, Cisco Unity Connection, Cisco Emergency Responder)	You can assign and unassign clusters to CSSM and Satellite using HCM-F. If autoregistration is enabled, the clusters are automatically assigned to the ordered virtual account. You do not have to manually assign the clusters. For any failed cluster registration, refer to the Cluster Summary page.
Service Inventory and HLM report generated	HCM-F generates the reports to view the licenses from CSSM and Satellite at virtual account-level, or customer-level. For more information on reports, see Smart Licensing Reports, on page 43
Licensing Dashboard	HCM-F provides a view of the licenses at virtual account-level and customer-level.
HCM-F sync with CSSM and Satellite	HCM-F provides on-demand and automatic sync to CSSM and Satellite. You can trigger the sync from HCM-F, then HCM-F pulls the virtual account and smart account details from CSSM or Satellite and refresh the tokens, if needed. You can sync smart accounts and virtual accounts either manually or automatically. HCM-F periodically syncs with CSSM and Satellite every 824 hours. For more information on manual sync, see *Perform Manual Sync* in *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide*.

Scenario: To Migrate Flex Hosted (EA/NU) License

Action	Description
Log in to Cisco Commerce(CCW) and order HCS licenses.	For more information about operational licenses, see Configuring Operational Licenses, on page 25
Create a smart account and virtual account	• Create a Smart Account in CSSM or Satellite. You can also get access to an existing smart account. • Create Virtual Account For more information about the one time setup activities, see Initial One Time Setup in CSSM for Smart Licensing, on page 6 and Initial One Time Setup in CSSM on-prem for Smart Licensing, on page 11
Upgrade HCM-F to 12.5 version	Provision the Smart account with client credentials that includes Client ID and Client Secret in HCM-F. For more information, see HCM-F 12.5 Upgrade Guidelines, on page 35
Setup Transport Mode	Setup the transport mode in HCM-F to connect HCM-F and UC applications to CSSM. For more information, see Set Transport Mode, on page 22.
Provision smart account in HCM-F	• Provision the credentials and Smart Account with HCM-F. • HCM-F extracts smart account, local account, and virtual account-related information from CSSM and Satellite. • Creates product registration token to register UC Applications in CSSM and Satellite. • Provide the transport mode in HCM-F to connect HCM-F and UC applications to CSSM and Satellite. For more information, see Provisioning Workflow for Smart Licensing, on page 17 **Note** You can autoregister the clusters to ordered virtual account using HCM-F.

Action	Description
Activate Smart Licensing for Clusters (Cisco Unified Communications Manager, Cisco Unity Connection, Cisco Emergency Responder)	You can assign and unassign clusters to CSSM and Satellite using HCM-F. If autoregistration is enabled, the clusters are automatically assigned to the ordered virtual account. You do not have to manually assign the clusters.
Cluster Sumary	For any failed cluster registration, refer to the Cluster Summary page.
Service Inventory and HLM report generated	HCM-F generates the reports to view the licenses from CSSM and Satellite at virtual account-level, or customer-level. For more information on reports, see Smart Licensing Reports, on page 43
Licensing Dashboard	HCM-F provides a view of the licenses at virtual account-level and customer-level.
HCM-F sync with CSSM and Satellite	HCM-F provides on-demand and automatic sync to CSSM and Satellite. You can trigger the sync from HCM-F, then HCM-F pulls the virtual account and smart account details from CSSM or Satellite and refresh the tokens, if needed. You can sync smart accounts and virtual accounts either manually or automatically. HCM-F periodically syncs with CSSM and Satellite every 824 hours. For more information on manual sync, see *Perform Manual Sync* in *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide*.



CHAPTER 5

Smart Licensing Reports

Smart Licensing Reports

HCM-F has Service Inventory and HLM (CSV and Excel) reports that have license-related details. Traditionally, these components generate reports after consuming licenses from PLM. These components are enhanced to consume the license data from CSSM or Satellite and generate the reports. If PLMs are also provisioned in the system, then these components query the license details from PLM, Satellite and CSSM, and generate the report in a unified format. Further, you can distinguish whether the licenses are consumed from PLM or Smart Account - Virtual Account name.

The enhanced SI report for smart licensing contains license data from both CSSM , Satellite, and PLM. The report version remains same as no format has been changed. It is possible to have one cluster registered to PLM and another cluster registered to a Virtual Account.

Sample SI Report with Smart Licensing:

- PLM Hostname or IP Address: 200.0.X.XXX
- Smart Account Domain name: smart-account.cisco.com
- Virtual Account name: virtual-account1
- Local Account name: local-account

```
|LICENSESUMMARYSTART|
|SUMMARY|PLMINFO|200.0.X.XXX|HCER|10|HCER_User|10010|0|10010|VALID|

|SUMMARY|PLMINFO|200.0.X.XXX|HUCM|10|HUCM_TelePresenceRoom|45000|0|45000|VALID|
|SUMMARY|PLMINFO|200.0.X.XXX|HUCM|10|HUCM_Essential|56000|0|56000|VALID|
|SUMMARY|PLMINFO|200.0.X.XXX|HUCM|10|HUCM_Basic|56010|0|56010|VALID|
|SUMMARY|PLMINFO|200.0.X.XXX|HUCM|10|HUCM_Foundation|46000|2|45998|VALID|
|SUMMARY|PLMINFO|200.0.X.XXX|HUCM|10|HUCM_Standard|46000|0|46000|VALID|
|SUMMARY|PLMINFO|200.0.X.XXX|HCUC|10|HCUC_SpeechConnectPort|0|0|0|VALID|
|SUMMARY|PLMINFO|200.0.X.XXX|HCUC|10|HCUC_BasicMessaging|13010|0|13010|VALID|
|SUMMARY|PLMINFO|200.0.X.XXX|HCUC|10|HCUC_EnhancedMessaging|13000|0|13000|VALID|
|SUMMARY|PLMINFO|200.0.X.XXX|HCUC|10|HCUC_StandardMessaging|2000|0|2000|VALID|

|SUMMARY|PLMINFO|virtual-account1@smart-account.cisco.com,CSSM,1000,2021-11-26,TERM|HCER|10|HCER_User|10010|0|10010|In
 Compliance|

|SUMMARY|PLMINFO|virtual-account1@smart-account.cisco.com,CSSM,1000,2021-11-26,TERM|HUCM|10|HUCM_TelePresenceRoom|45000|0|45000|In
```

```
 Compliance|
|SUMMARY|PLMINFO|virtual-account1@smart-account.cisco.com,CSSM,1000,2021-11-26,TERM|HUCM|10|HUCM_Essential|56000|0|56000|In
 Compliance|
|SUMMARY|PLMINFO|virtual-account1@local-account,Satellite,1000,2021-11-26,TERM|HUCM|10|HUCM_Basic|56010|0|56010|In
 Compliance|
|SUMMARY|PLMINFO|virtual-account1@smart-account.cisco.com,CSSM,1000,2021-11-26,TERM|HUCM|10|HUCM_Foundation|46000|2|45998|In
 Compliance|
|SUMMARY|PLMINFO|virtual-account1@local-account,Satellite,1000,2021-11-26,TERM|HUCM|10|HUCM_Standard|46000|0|46000|In
 Compliance|
|SUMMARY|PLMINFO|virtual-account1@smart-account.cisco.com,CSSM,1000,2021-11-26,TERM|HCUC|10|HCUC_SpeechConnectPort|0|0|0|In
 Compliance|
|SUMMARY|PLMINFO|virtual-account1@smart-account.cisco.com,CSSM,1000,2021-11-26,TERM|HCUC|10|HCUC_BasicMessaging|13010|0|13010|In
 Compliance|
|SUMMARY|PLMINFO|virtual-account1@local-account.cisco.com,Satellite,1000,2021-11-26,TERM|HCUC|10|HCUC_EnhancedMessaging|13000|0|13000|In
 Compliance|
|SUMMARY|PLMINFO|virtual-account1@smart-account.cisco.com,CSSM,1000,2021-11-26,TERM|HCUC|10|HCUC_StandardMessaging|2000|0|2000|In
 Compliance|

|SUMMARY|CUSTLICENSEINFO|200.0.X.XXX|~|~|C1|HUCM|200.2.1.11|HUCM_TelePresenceRoom|0|
|SUMMARY|CUSTLICENSEINFO|200.0.X.XXX|~|~|C1|HUCM|200.2.1.11|HUCM_Essential|0|
|SUMMARY|CUSTLICENSEINFO|200.0.X.XXX|~|~|C1|HUCM|200.2.1.11|HUCM_Foundation|1|
|SUMMARY|CUSTLICENSEINFO|200.0.X.XXX|~|~|C1|HUCM|200.2.1.11|HUCM_Standard|0|
|SUMMARY|CUSTLICENSEINFO|200.0.X.XXX|~|~|C1|HUCM|200.2.1.11|HUCM_Basic|0|
|SUMMARY|CUSTLICENSEINFO|200.0.X.XXX|~|~|C2|HUCM|200.3.1.11|HUCM_TelePresenceRoom|0|
|SUMMARY|CUSTLICENSEINFO|200.0.X.XXX|~|~|C2|HUCM|200.3.1.11|HUCM_Essential|0|
|SUMMARY|CUSTLICENSEINFO|200.0.X.XXX|~|~|C2|HUCM|200.3.1.11|HUCM_Foundation|1|
|SUMMARY|CUSTLICENSEINFO|200.0.X.XXX|~|~|C2|HUCM|200.3.1.11|HUCM_Standard|0|
|SUMMARY|CUSTLICENSEINFO|200.0.X.XXX|~|~|C2|HUCM|200.3.1.11|HUCM_Basic|0|

|SUMMARY|CUSTLICENSEINFO|virtual-account1@local-account,Satellite|~|~|C3|HUCM|200.2.1.12|HUCM_TelePresenceRoom|0|
|SUMMARY|CUSTLICENSEINFO|virtual-account1@smart-account.cisco.com,CSSM|~|~|C3|HUCM|200.2.1.12|HUCM_Essential|0|
|SUMMARY|CUSTLICENSEINFO|virtual-account1@smart-account.cisco.com,CSSM|~|~|C3|HUCM|200.2.1.12|HUCM_Foundation|1|
|SUMMARY|CUSTLICENSEINFO|virtual-account1@local-account,Satellite|~|~|C3|HUCM|200.2.1.12|HUCM_Standard|0|
|SUMMARY|CUSTLICENSEINFO|virtual-account1@smart-account.cisco.com,CSSM|~|~|C3|HUCM|200.2.1.12|HUCM_Basic|0|

|SUMMARY|SITELICENSEINFO|~|~|C1|~|HCS Foundation|1|
|SUMMARY|SITELICENSEINFO|~|~|C2|~|HCS Foundation|2|
|LICENSESUMMARYEND|
```

The report format is as follows:

|SUMMARY|PLMINFO|*virtual-account1@smart-account.cisco.com,SubsID,Exp.Date,License Model|UC Application|product version|License Model|Installed License Count*
|Required License Count|Available License Count|Status

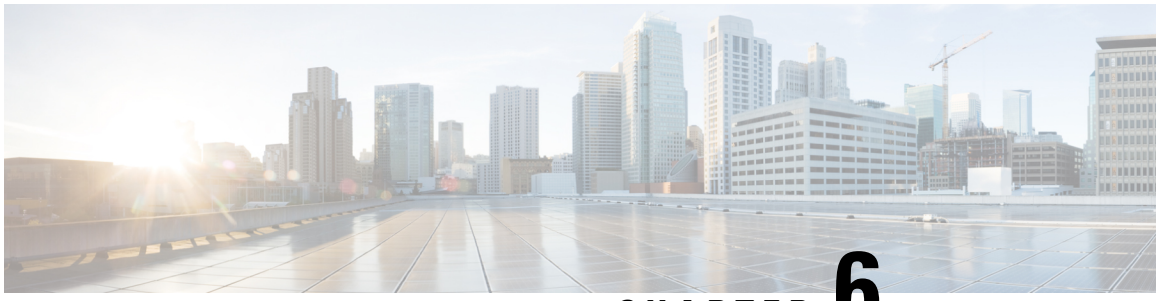
The report format is as follows:

|SUMMARY|PLMINFO|*virtual-account1@smart-account.cisco.com or virtual-account1@local-account,Transport Mode,SubsID,Exp.Date,License Model|UC Application|product version|License Model|Installed License Count*
|Required License Count|Available License Count|Status

Note Similar to Service Inventory report format, the HLM reports maintained with name/hostname/IP address of the PLM are replaced with the Virtual Account and Smart Account names *Virtual Account Name@Smart Account Name*. The LM Name column of the HLM report shows the virtual account along with the PLM.

HCM-F License Dashboard

For more information on License Dashboard and how to view the license summary details, see HCM-F License Dashoard section at *Cisco Hosted Collaboration Solution License Management Guide*.



CHAPTER 6

Troubleshooting Smart Licensing

Troubleshooting Smart Licensing

The HCM-F Smart Licensing operations like Smart Account Sync, Cluster Assignment/Unassignment creates jobs, that can be viewed In HCM-F GUI under **Infrastructure Manager** > **Administration** > **Jobs**.

In case of failure, the **Job Staus Info** column shows the error codes with the corresponding messages and recommendations as listed the following table.

CSSM API Errors

Error Code	Error Message	Recommendation
CSSM1001	CSSM API encountered an Unknown Error	Check HLM Logs (Detailed) for more details
CSSM1002	Unsupported HTTP Method	Check HLM Logs (Detailed) for more details
CSSM1003	CSSM API encountered an Internal Error	Check HLM Logs (Detailed) for more details
CSSM1004	CSSM API is unable to send request	Check HLM Logs (Detailed) for more details
CSSM1005	CSSM Server refused connection	If Proxy is configured, verify network connectivity between HCM-F and Proxy Server
CSSM1006	CSSM API Unknown Host Error	If Proxy is configured, verify Proxy hostname is correct and DNS resolution of CSSM/Proxy/Authentication GW(Transport Mode Setting)

Error Code	Error Message	Recommendation
CSSM1007	CSSM API Socket Timeout Error	If Proxy is configured, verify network connectivity between HCM-F and Proxy Server
CSSM1008	CSSM API No Route To Host Error	If Proxy is configured, verify network connectivity between HCM-F and Proxy Server
CSSM1009	CSSM client creation failed due to invalid Transport Mode	Check HLM Logs (Detailed) for more details
CSSM1010	CSSM client creation failed due to Unknown Error	Check HLM Logs (Detailed) for more details
CSSM1011	CSSM API Authentication Failed Error	Reconfigure client ID and Secret, and perform Smart Account Sync
CSSM1012	CSSM client unable to parse the response	Check HLM Logs (Detailed) for more details
CSSM1013	CSSM client unable to map JSON response	Check HLM Logs (Detailed) for more details
CSSM1014	CSSM client unable to read response due to IO error	Check HLM Logs (Detailed) for more details
CSSM1015	Client credentials may not have access to Smart Account or Domain Name is incorrect	Check if the Client Id and Secret have access to Smart Account and the Domain name is Correct
CSSM1016	CSSM client unable to process response	Check HLM Logs (Detailed) for more details
CSSM1017	CSSM client unable to process JSON response	Check HLM Logs (Detailed) for more details
CSSM1018	CSSM client config validation failed	Check HLM Logs (Detailed) for more details
CSSM1019	Given Smart Account ID does not exist	Check HLM Logs (Detailed) for more details
CSSM1020	CSSM server responded with errors	Check HLM Logs (Detailed) for more details

Cisco Application Adaptor (CAA) Errors

Error Code	Error Message	Recommendation
CAA1001	Service encountered an unknown error	Verify App specific adapter Service is running Scan CAA logs for errors and restart service if necessary.

Error Code	Error Message	Recommendation
CAA1002	Service encountered an SDR error	Verify Cisco CDM Database is running Scan App specific adapter logs for errors.
CAA1003	CAA is unable to find application instance in SDR	Verify Application is configured Scan CAA logs for errors.
CAA1004	No admin credentials configured for application	Verify admin credentials are configured.
CAA1005	CAA does not support this equipment type	Scan CAA logs for errors.
CAA1006	CAA is unable to read the application name from SDR	Verify Cisco CDM Database is running Scan CAA logs for errors.
CAA1007	No service provider address configured for application	Verify service provider address is configured for the application.
CAA1008	No platform credentials configured for the application	Verify if platform credentials are configured.
CAA1009	No Cluster version configured for the application	Verify if cluster version is configured.
CAA1010	No Request Hanlder Mapping found in json	Verify if request handler exist for message type app type and cluster version.
CAA1011	Error occurred in SSH connection	Check if app details platform credentials are correct and session timeout is sufficient.
CAA1012	Invalid Response type provided	Check response type.
CAA1014	Unable to generate CSR for the given certificate type Provide correct certificate type	Check logs for more details.
CAA1015	Certificate import failed due to CSR public key and Certificate public key doesn't match	Verify whether the certificate and CSR has the same algorithm and key.
CAA1016	Certificate import failed due to CSR SAN and Certificate SAN doesn't match	Verify CSR SAN and Certificate SAN.
CAA1017	Error occurred as CSR does not exist in the App	Generate CSR before proceeding with this action.
CAA1018	CA certificate is not available in the trust-store	Upload a CA certificate in trust store.
CAA1019	Error in CA certificate	Upload a CA certificate in trust store.
CAA1020	Error occurred while reading the certificate	Provide a valid CA Certificate.
CAA1021	Certificate is not in PEM format	Provide a valid Certificate.

Error Code	Error Message	Recommendation
CAA1022	Invalid certificate file provided	Provide a valid Certificate.
CAA1023	Error occurred as CSR does not exist in the App	Generate CSR before proceeding with this action.
CAA1024	Error occured as CLI Response Parser is not configured	Configure Parser for CLI command.
CAA1025	Invalid certificate type found	Check if the certificate type is valid.
CAA1026	Certificate Upload failed	Check if the certificate is valid and UC App is provisioned with right version Refer logs for more details.
CAA1027	Certificate operation is not successful Internal error occurred	Check the logs for more details.
CAA1028	Failed to get the REST API client	Verify application is running the supported version.
CAA1029	Error occurred during REST API call to Expressway	Verify credentials are correct and REST service is up on Expressway.
CAA1030	Current version of Expressway is not supported	Use the supported versions of Expressway.
CAA1031	Error occurred as invalid certificate was	Uploaded to Expressway. Verify the CA certificate is available in the trust and uploaded CA signed certificate is valid.
CAA1032	Error occurred as CSR already exist in Expressway	Delete the existing CSR.
CAA1033	Error occurred in CSR generation in Expressway as invalid data was passed fo CSR	Verify the data provided to generate CSR.
CAA1034	No Response Hanlder Mapping found in json	Verify if response handler exist for message type app type and cluster version.
CAA1035	Invalid admin credentials	Verify the user name and password.
CAA1036	CAA encountered an unknown error from the application	Verify the following entities - Cisco AXL Web Service (Cisco Unified CM) is active Publisher Admin/Platform credentials and Network address HCMF) are correct.
CAA1037	CAA encountered error while parsing xml	Make sure the UCApps are returning proper responses.
CAA1038	CAA is unable to determine the application Version	Verify Cisco AXL Web Service Cisco Unified CM) is running on application. Verify application admin credentials and network address.

Error Code	Error Message	Recommendation
CAA1039	API executed by non admin user	Verify the user name and password for admin credentials.
CAA1040	Invalid Proxy details	Verify the Proxy Hostname and Proxy port configured in Transport Mode Setting.
CAA1041	Edit Transport Settings operation is not allowed since product is in Registered state	Sync Smart Account with CSSM and assign cluster to Virtual Account.
CAA1042	Product may already deregistered	Sync Smart Account with with CSSM.
CAA1043	Internal Error occurred while communicating with Unity Connection	Verify the Cisco Smart License Manager and Tomcat service is running in Unity Connection.
CAA1044	Unsupported message received by CAA service	Scan CAA logs for errors.
CAA1045	CAA does not support the application version	Verify if correct cluster version is configured in HCMF.
CAA1046	CAA cannot connect to application	Verify Cisco AXL Web Service is running on Cisco Unified CM application Publisher's admin/platform credentials and network address are correct and network connectivity from HCM-F is established.
CAA1048	Product Registration Token is either invalid or has been expired	Perform Smart Account Sync with CSSM.
CAA1049	Product is in subscriber Node	
CAA1050	Exception occurred while performing product operation	Scan CAA logs for errors.
CAA1051	CAA is unable to add community string on application	Verify application admin credentials and network address are correct. Verify community string does not already exist.
CAA1052	CAA is unable to update community string on application	Verify application admin credentials and network address. Verify community string is present.
CAA1053	CAA is unable to delete community string on application	Verify application admin credentials and network address. Verify community string exists.
CAA1054	CAA is unable to add SNMP V3 user on application	Verify application admin credentials and network address. Verify SNMP V3 user does not already exist.
CAA1055	CAA is unable to update SNMP V3 user on application	Verify application admin credentials and network address. Verify SNMP V3 user exists.
CAA1056	CAA is unable to delete SNMP V3 user on application	Verify application admin credentials and network address. Verify SNMP V3 user is present.

Error Code	Error Message	Recommendation
CAA1057	CAA is unable to restart application SNMP Master Agent	Verify network connection between HCM-F and application. Verify application platform credentials and network address.
CAA1058	CAA is unable to add Remote Syslog configuration on application	Verify application admin credentials and network address.
CAA1059	CAA is unable to update Remote Syslog configuration on application	Verify application admin credentials and network address.
CAA1060	CAA is unable to add Billing Application Server configuration on application	Verify SFTP Credentials and the directory /home/smuser/ exists on billing server. Verify network connection between application and billing server.
CAA1061	CAA is unable to update Billing Application Server configuration on application	Verify SFTP Credentials and the directory /home/smuser/ exists on billing server. Verify network connection between application and billing server.
CAA1062	CAA is unable to remove Billing Application Server configuration on application	Verify application ADMIN credentials and network address. Verify BAS config exists on application.
CAA1063	CAA cannot connect to application platform CLI	Verify platform credentials are configured and network connectivity between HCM-F and application.
CAA1064	CAA is unable to restart application Host Resources Agent	Verify network connection between HCM-F and application. Verify application platform credentials and network address.
CAA1065	Unsupported message received from CAA	Scan CAA logs for errors.
CAA1066	No CUOM is configured for application	Verify CUOM is configured for the application.
CAA1067	No service provider address is configured for CUOM	Verify service provider address is configured for CUOM.
CAA1068	Unable to get process node list from Cisco Unified CM	Verify name in Cisco Unified CM System > Server) matches the hostname or IP configured in HCM-F for Service Provider or Application Space Address.
CAA1069	No HTTP credentials configured for application	Verify if HTTP credentials are configured.
CAA1070	No SFTP credentials configured	Verify if SFTP credentials are configured for billing application server.
CAA1071	No SFTP network address configured	Verify if SFTP network address is configured for billing application server.

Error Code	Error Message	Recommendation
CAA1072	CAA is unable to find the specified phone device on the application	Verify phone device exists on application.
CAA1073	CAA is unable to find the specified user on the application	Verify end user exists in the application.
CAA1074	Failed to get the web-security details from the UC App	Verify if the web-security data is available on the UC App.
CAA1075	Error occured during RIS call	Check if RIS service is up.
CAA1076	Error occured during CCS call	Check if CC service is up.
CAA1077	Error occurred during PAWS call	Check if PAWS service is up.
CAA1078	Error occurred during command execution on CLI	Verify if the command syntax is correct.
CAA1079	Set Transport Mode failed due Invalid format of on-prem Registration url	Please provide the valid on-prem url.
CAA1080	No Clustering Configuration Found in Expressway	Configure proper clustering Expressway.
CAA1081	Registration with Smart Agent failed	Verify the Proxy connection and the Cisco Unified CM connectivity with CSSM. Check CAA/HLM Logs for more details.
CAA1082	DeRegistration with Smart Agent failed	Verify the Proxy connection and the Cisco Unified CM connectivity with CSSM or the product is already unregistered with CSSM. Check CAA/HLM Logs for more details.
CAA1083	Update transport settings failed	Verify the Proxy connection and the Cisco Unified CM connectivity with CSSM or the product is already registered with CSSM. Check CAA/HLM Logs for more details.
CAA1084	Error occurred in SSH connection	Check if platform credentials are correct and session timeout is sufficient.

Smart Licensing Cluster Operation Errors

Error Code	Error Message	Recommendation
SLMCT1001	Virtual Account is not valid	Check if the given Virtual Account is correct
SLMCT1002	Exception occurred while License Mode change	Check if UC application is up and its platform service is running. Check HLM Logs for more details

Error Code	Error Message	Recommendation
SLMCT1003	Cluster License Mode did not change successfully	Check HLM Logs for more details
SLMCT1004	Cluster License Mode Change - JMS timeout occurred	Check if Provisioning Adapter Service is up. Check Logs for more details
SLMCT1005	Cluster License Mode Change - JMS timeout occurred	Check if CAA Service is up. Check Logs for more details
SLMCT1006	Cluster is of unsupported Version	Provide a valid cluster
SLMCT1007	Cluster is already assigned	Perform Smart Account sync with CSSM
SLMCT1008	Cluster doesn't have an application	Assign an application to the Cluster
SLMCT1011	Cluster is already unassigned	Perform Smart Account Sync with CSSM
SLMCT1012	Cluster doesn't have publisher node	Assign a publisher node to cluster
SLMCT1013	Cluster application doesn't have platform credentials	Configure platform credentials for cluster application
SLMCT1014	Cluster application doesn't have admin credentials	Configure admin credentials for cluster application
SLMCT1015	Cluste is of unsupported Type	Supported cluster type are Cisco Unified CM, Cisco Unity Connection and Cisco Emergency Responder
SLMCT1016	Reset Cluster License Mode - did not change successfully	Check HLM Logs for more details
SLMCT1017	Exception occurred while Reset Cluster License Mode	Check if UC Application is up and its platform service is running. Check HLM Logs for more details
SLMCT1018	Cluster License Mode Change - JMS timeout occurred	Check if Provisioning Adapter Service is up. Check Logs for more details
SLMCT1019	Cluster License Mode Change - JMS timeout occurred	Check if CAA Service is Up. Check Logs for more details

Smart Licensing General Errors

Error Code	Error Message	Recommendation
SLM1001	Smart Licensing Product Registration request failed due to exception	Check HLM Logs (Detailed) for more details
SLM1002	Smart Licensing Product Registration failed due to JMS timeout	Check if the CAA CUCM Service is started

Error Code	Error Message	Recommendation
SLM1003	Smart Licensing Get Transport Mode request failed due to exception	Check HLM Logs (Detailed) for more details
SLM1005	Smart Licensing Update Transport Mode request failed due to exception	Check if the UCapp and its services are up. Check logs for exception details
SLM1007	Smart Licensing Cluster Operation - Cluster does't have admin credentials	Check if admin credentials are configured for cluster application
SLM1008	Smart Licensing Cluster Operation - Cluster does't have platform credentials	Check if platform credentials are configured for cluster application
SLM1009	Smart Licensing Cluster Operation - Cluster don't have a publisher node	Check if cluster has publisher node
SLM1010	Smart Licensing Get Product Token - Unable to generate or retrieve product token for the Virtual Account	Check HLM Logs (Detailed) for more details
SLM1011	Smart Licensing Product DeRegistration failed due to JMS timeout	Check if the CAA CUCM Service is started
SLM1012	Smart Licensing Change License Mode - Cluster HostName/IP is not configured	Check if publisher network address is configured
SLM1013	Smart Licensing Change License Mode request failed while get/update transport mode due to exception	Check UCapps platform service is up or Publishers IP/Hostname and platform credentials are valid
SLM1014	Smart Licensing Change License Mode - Virtual Account is not associated with any License Mode	Check if Virtual Account is associated with License Mode
SLM1015	Smart Licensing Sync - an unknown error occured	Check HLM Logs (Detailed) for more details
SLM1016	Smart Licensing Sync - unable to fetch Smart Account details from SDR	Verify Cisco CDM Database is running. Check HLM Logs (Detailed) for more details
SLM1018	Smart Licensing Change Transport Mode failed due to JMS timeout	Check if the CAA CUCM Adapter is started.
SLM1021	Smart Licensing Product DeRegistration failed due to JMS timeout	Check if the CAA CER Service is started
SLM1023	Smart Licensing Change Transport Mode failed due to JMS timeout	Check if the CAA CER Adapter is started
SLM1024	Smart Licensing Change Transport Mode failed due to JMS timeout	Check if the CAA CUCXN Adapter is started

Error Code	Error Message	Recommendation
SLM1025	Smart Licensing Request Failed due to Invalid Cluster Exception	Check HLM Logs (Detailed) for more details

UC Applications API Errors

Error Code	Error Message	Recommendation
UCAPI1001	Updating Cisco Unified CM Billing Server info failed	N/A
UCAPI1002	Updating Cisco Unified CM Remote Syslog info failed	N/A
UCAPI1003	Updating Cisco Unified CM SNMP info failed	N/A
UCAPI1004	Validation of Cisco Unified CM AXL Connection failed	Check AXL services and Platform services are up in Cisco Unified CM
UCAPI1005	Accessing Cisco Unified CM AXL SOAP Port failed	Check AXL services and Platform services are up in Cisco Unified CM
UCAPI1006	Initialization failed	N/A
UCAPI1007	Software Error	N/A
UCAPI1008	Unknown Failure	N/A
UCAPI1009	Connection Timeout	N/A
UCAPI1010	Registration with Smart Agent failed	Verify the Proxy connection and the Cisco Unified CM connectivity with CSSM. Check CAA/HLM Logs for more details.
UCAPI1011	DeRegistration with Smart Agent failed	Verify the Proxy connection and the Cisco Unified CM connectivity with CSSM or the product is already unregistered with CSSM. Check CAA/HLM Logs for more details.
UCAPI1012	Update transport settings failed	Verify the Proxy connection and the Cisco Unified CM connectivity with CSSM or the product is already unregistered with CSSM. Check CAA/HLM Logs for more details.

Smart Licensing Error Code and Message Mapping

REST API	Response	Code	Message	Recommended Action
transportsettings	405	METHOD_NOT_ALLOWED	Edit Transport Settings operation is not allowed since product is in either Registered state or is a Subscriber node	Derigister your product instance and run it from correct node (Publisher only)
transportsettings	500	INTERNAL_SERVER_ERROR	Failed to apply the Transport Settings	Try to run command again with correct information and privilege. If this issue persists, please contact Cisco Technical Support
transportsettings	400	INVALID_PARAMETER	Please enter a valid Transport Mode within the range (0 - 2)	
	400	INVALID_PARAMETER	Please enter a valid Transport Gateway URL	
	400	INVALID_PARAMETER	Please provide valid HTTP/HTTPS Proxy IP Address and/or HTTP/HTTPS Proxy Port	
	400	INVALID_PARAMETER	Please enter a valid HTTP/HTTPS Proxy IP Address	
	400	INVALID_PARAMETER	Please enter a valid HTTP/HTTPS Proxy Port within the range (1 - 65535)	
deregister	405	METHOD_NOT_ALLOWED	Deregistration is not allowed since product is in either unregistered state or is a Subscriber node	Check License status and Node information and take action accordingly

REST API	Response	Code	Message	Recommended Action
deregister	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to an unknown error	Check Register status, if its deregister, remove product instance manually from CSSM. EvtSlmCucDeregistrationFailure SmartLicensingDeregistrationFailure
	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to invalid trust chain pool	
	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to a communication timeout.	
	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to communication send error	
register	400	INVALID_PARAMETER	The Product Instance Registration Token you have entered is either invalid or has been expired. Ensure that you have pasted the entire token and that the token has not expired	EvtSlmCucRegistrationFailure SmartLicensingRegistrationFailure
register	405	METHOD_NOT_ALLOWED	Smart Software Licensing operations are not allowed from Subscriber, licenses for this system are managed by Publisher	
	405	METHOD_NOT_ALLOWED	Product is already registered on CSSM. To Re-register it use 'force' flag	

REST API	Response	Code	Message	Recommended Action
register	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to an unknown error	Check the network connectivity with CSSM. For further troubleshooting, check the CuSlmSvr diagnostic logs. Retry Product Registration. If this issue persists, contact Cisco Technical Support. EvtSlmCucRegistrationFailure SmartLicensingRegistrationFailure
	500	INTERNAL_SERVER_ERROR	The Product Instance was unable to register with Smart Software Licensing	
	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to invalid trust chain pool	
	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to a communication timeout.	
	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to communication send error	
	500	INTERNAL_SERVER_ERROR	Smart License Server is not running. Start Smart License Manager Server from CUCA Serviceability Page	
renewID	405	METHOD_NOT_ALLOWED	Renewal of ID is not allowed since product is in either unregistered state or is a Subscriber node	

REST API	Response	Code	Message	Recommended Action
renewID	500	INTERNAL_SERVER_ERROR	Smart License Server is not running. Start Smart License Manager Server from CUCA Serviceability Page	
	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to a communication timeout	
	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to an unknown error	Check the network connectivity with CSSM. For further troubleshooting, check the CuSlmSvr diagnostic logs. Retry Renew Registration. If this issue persists, contact Cisco Technical Support. EvtSlmCucRenewRegistrationFailure SmartLicensingRenewRegistrationFailure
	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to invalid trust chain pool	
	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to communication send error	
renewAuth	405	METHOD_NOT_ALLOWED	Renewal of Authorization is not allowed since product is in either unregistered state or is a Subscriber node	

REST API	Response	Code	Message	Recommended Action
renewAuth	500	INTERNAL_SERVER_ERROR	Smart License Server is not running. Start Smart License Manager Server from CUCA Serviceability Page	Check the network connectivity with CSSM. For further troubleshooting, check the CuSlmSvr diagnostic logs. Retry Renew Authorization. If this issue persists, contact Cisco Technical Support. EvtSlmCucRenewAuthFailure SmartLicensingRenewAuthFailure
	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to a communication timeout	
	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to an unknown error	
	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to invalid trust chain pool	
	500	INTERNAL_SERVER_ERROR	The requested operation was not successful due to communication send error	
licensedetails	500	INTERNAL_SERVER_ERROR	Unable to fetch license count from database	
All APIs	401	NOT_AUTHORIZED	User is not authorized to perform this operation	Use correct priviledge to run commands AuthenticationFailed