Cisco Smart Software Manager satellite User Guide

First Published: 02/16/2015
Last Modified: 12/21/2017

Contents

Preface

Audience

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

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

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

This document uses the following conventions:

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

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

Obtaining Documentation and Submitting a Service Request

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

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

Cisco Smart Software Manager satellite Overview

About Cisco Smart Software Manager satellite

Cisco Smart Software Manager satellite is a component of Cisco Smart Licensing and works with Cisco Smart Software Manager (Cisco SSM) to intelligently manage customer product licenses, providing near real-time visibility and reporting of Cisco licenses that customers purchase and consume. Test

Customers who, either for policy or network reachability reasons, do not want to manage their Cisco products directly using Cisco Smart Software Manager residing at software.cisco.com, can choose to install Cisco Smart Software Manager satellite on-premises. Devices or software products register and report license consumption to the Cisco Smart Software Manager satellite as though it were a replicate of the Cisco Smart Software Manager hosted within the customer's premises.

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

- CentOS 7.0
- Smart Licensing Receiver
- Smart Software Manager satellite

Features

The next sections describe the Cisco Smart Software Manager satellite features.

Smart Call Home Transport gateway is a secure transport mechanism to transfer Cisco licensing data from the satellite to Cisco Smart Software Manager (the smart licensing back-end).

Default HTTPS User Access

After installation and setup, you access the satellite via a browser. If you select HTTP as the URL, the satellite automatically rolls over to HTTPS.

For example, if you enter **`http://172.125.15.17:8080`**, it defaults to **`https://172.125.15.17:8443`**. Alternatively, you can simply use **`https://172.125.14.17:8443`**. Or if you enter **`http://[2001:420:44ff:1828::106]:8080`**, it defaults to **`https://[2001:420:44ff:1828::106]:8443`**.

Immediate satellite Registration

The satellite registration process is immediate. With previous versions, registration required a 48-hour wait for Cisco to create and sign certificates that were used to ensure secure communications between the satellite and product instances, as well as between the satellite and Cisco Smart Software Manager. With newer versions of Cisco products running Smart Agent 1.5 or later, you are able to manage devices and the satellite immediately after the satellite registration process to Cisco Smart Software Manager completes (without the 48-hour wait). For Cisco products that support Smart Agent 1.5 or earlier, there is still a need for the 48- hour wait after satellite to Cisco SSM registration before product registration can occur.

Automatic HTTPS Registration from Product Instances

With the latest Cisco Smart Software Manager satellite release, newer Cisco products can communicate with Smart Software Manager satellite via HTTPS without the need to manually install a HTTPS certificate (download the certificate from http://www.cisco.com/security/pki/certs/clrca.cer and issue various CLIs) as before. This eliminates the cumbersome task of having to perform this step for every product instance, especially in a large network with thousands of product instances.

High Availability

Cisco Smart Software Manager satellite High Availability (HA) architecture provides redundancy and reliable fail-over in an active-standby configuration that can detect the failure of the active satellite and recovers with no loss of continuous operations and system usability.

Device-Led Migration

Today, classic to Smart license conversion takes place on LRP or CSSM portals based on information available in the SWIFT database. Device-Led Conversion (DLC) allows the device/product instance to initiate a conversion of classic licenses (such as RTU) to Smart licenses that are not on the SWIFT. Upon conversion, these Smart Licenses are deposited into CSSM. Products must be upgraded to a DLC-enabled version, connected to a DLC-enabled CSSM or satellite for this feature to work.

Common Services Platform Collector (CSPC) satellite support

Enable satellite to co-reside with the Common Services Platform Collector (CSPC) virtual machine in a Multi Service Delivery Appliance (MSDA) so that Smart-License enabled products can register with satellite in this environment.

Third Party Software Smart Licensing Integration Support

Support 3rd party software (such as Speech View in Unity Connection and Apple Push Notification (APNs) in Unified Communication Manager) to authorize Smart License enabled Cisco products to use their services.

ISO Packaging

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

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

IPV6 Support

Satellite supports IPv4, dual stack IPv4 and IPv6, and IPv6 addressing schemes.

System Security Enhancements

- CentOS Nessus vulnerability scan issues addressed
- FIPS-140-2 compliance
- All system ciphers updated with SHA-256

System Upgrade

You can upgrade Cisco Smart Software Manager satellite from the user interface either manually or automatically. When you choose to upgrade, the satellite software is modified while the system is running with the current configuration and licensing information. In the event the upgrade fails, the satellite automatically rolls back to the previous version without affecting the satellite operations. The GUI upgrade leverages Cisco Automated Software Delivery (ASD), which allows you to check for an available software upgrade. The feature also provides options to automatically download and install the upgrade. As the name implies, ASD requires the satellite to be connected to cisco.com for the upgrade process.

Note: If you upgrade the satellite to a newer version and the upgrade fails, you can roll back to the previous version of the software. However, if the upgrade completes successfully, you cannot roll back to a previous version. To downgrade to an earlier version, you must have previously performed a backup (using VMware snapshot for example) prior to upgrading. Use the backup image to restore the previous satellite version.

Network Utility

Network setup and troubleshooting tools are provided via a user-friendly GUI, which currently supports IPv4 and IPv6 addresses. The CLI will also be available for configuration to specify IP address, DNS/ NTP addresses, network mask, and default gateway. Network Utility GUI to change network configurations or to run various troubleshooting commands such as `ping`, `traceroute`, and `ns lookup`.

Backup/Restore

Backup and restore enables periodic backups of the satellite databases, configuration, and certificates. You can then rename, download, and restore backups to the same or different host.

Improved Backend Synchronization

Improved synchronization with Cisco SSM enables a more efficient way of exchanging product instances, license usage, and license entitlement and preventing out-of-sync conditions.

Configurable Headers and Footers

Headers and footers on the satellite UI and reports are configurable, enabling them to be customized with meaningful classifications.

Export Control

Export control allows Smart License enabled products that connect to the satellite to generate restricted tokens and activate restricted functionality according to Export Control laws.

Login Failure Message Removal

This feature provides additional security in that it does not display if a user login succeeds or fails. If a failure occurs, you can retry the login after four seconds.

Multiple Network Interfaces

This option enables multiple interfaces for traffic separation between management and product instance registrations.

Restart/Shutdown

Restart or shutdown of the satellite can be initiated from its GUI.

System Setup Overview

Cisco Smart Software Manager satellite graphical interfaces divided into two main sections: a **Navigation** pane on the left and a main **Work** pane.

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

You can use the **Navigation** pane to perform the following tasks:

- View the list of virtual accounts
- Set up synchronization schedules
- Run reports against your virtual accounts
- Administer upgrades and manage users
- Perform system backups and restores
- Generate log files and perform other administration tasks

System Requirements

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

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

- 50GB-200GB hard disk

- 8GB Memory
- 4 CPUs/vCPUs

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

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

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

Supported Web Browsers

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

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

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

Ports Used

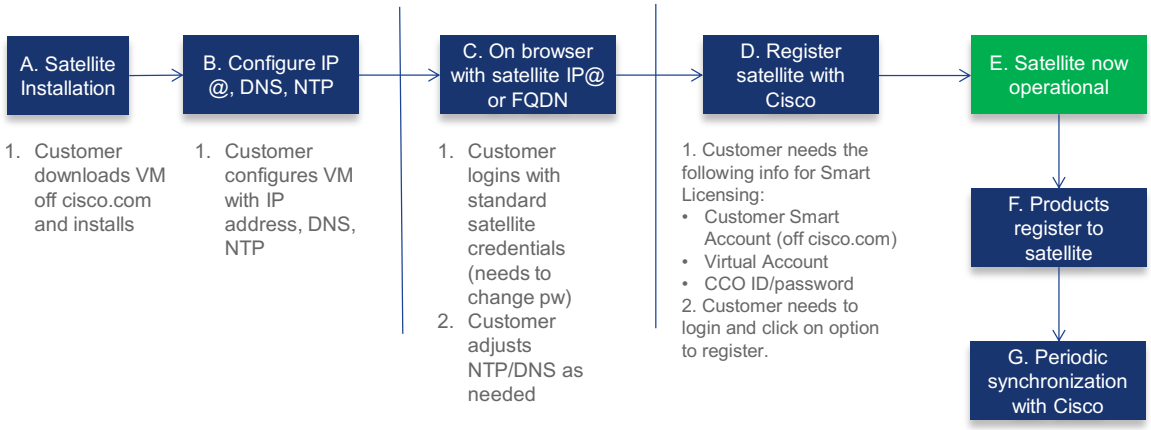
Smart Software Manager satellite uses the following ports for various communication. Please ensure you have the following port numbers configured in your firewall rules:

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

Setting Up Cisco Smart Software Manager satellite

Smart Software Manager satellite can operate either as a standalone server, or in an Active/Standby configurations to offer High Availability (HA). In the High Availability (HA) mode, Cisco SSM satellite High Availability provides for both an Active and a Standby satellite server. The HA configuration ensures all data is replicated between the active and standby satellite automatically. In the event there is a loss of connectivity with the active satellite, an automatic failover occurs and the standby satellite starts responding, enabling a non-disruptive recovery and continuous operations. This switchover from active to standby can take between 30 seconds to 1 minute. When the active satellite resumes normal operation, the standby satellite will seamlessly revert to this standby role.

The following diagram shows the steps to get Smart Software Manager satellite setup and operational:



For deploying satellite, either as a standalone server or the active satellite, use the following configuration steps:

1. Install the satellite.
2. Configure the satellite's IP address, network mask, default gateway.
3. Configure DNS and NTP parameters.
4. To connect to the satellite administration portal, go to **https://<satellite-ip-address>:8443** or **https://FQDN:8443.** The default username/password is **admin/Admin!23**.
5. Configure as a new satellite or from an existing backup file.
6. Synchronize the time with the NTP server.
7. Change any network configuration.
8. Register the satellite to Cisco Smart Software Manager.

To add a standby satellite (HA mode) at any time, use the following configuration steps:

1. Ensure the active satellite is installed and registered (shown above)
2. Install the new standby satellite
3. Configure the standby satellite's IP address, network mask, default gateway

Do **not** register the standby satellite to Cisco Smart Software Manager.

Configuring Cisco Smart Software Manager satellite

After installing the satellite successfully and configuring its IP address, network mask, and default gateway, DNS, and NTP parameters (refer to *Smart Software Manager satellite Installation Guide*), you can enter its IP address on a browser and continue the satellite setup process. Upon logging in using the admin credentials, you are presented with a screen that asks you to select the following options:

- **Configure as new satellite**, or
- **Configure by importing data from a satellite backup file**- this option allows you to browse and restore a backup file on your hard drive.

Click **Next** to continue.

Network Settings

You are presented with the **Network Interfaces, DNS Settings, and NTP Settings, and CSPC Specific Settings** screen with the information configured using CentOS commands above. You can change these parameters by selecting **Edit Network Settings**.

To sync the time with NTP server:

1. Click the **NTP** tab in the **Edit Network Settings** to synchronize the satellite time with the NTP server, or
2. Click on **Sync Time Now** on the **Network Settings** UI to sync the time.
3. Click Next to go to the **Setup Method** tab.

Setup Method Options

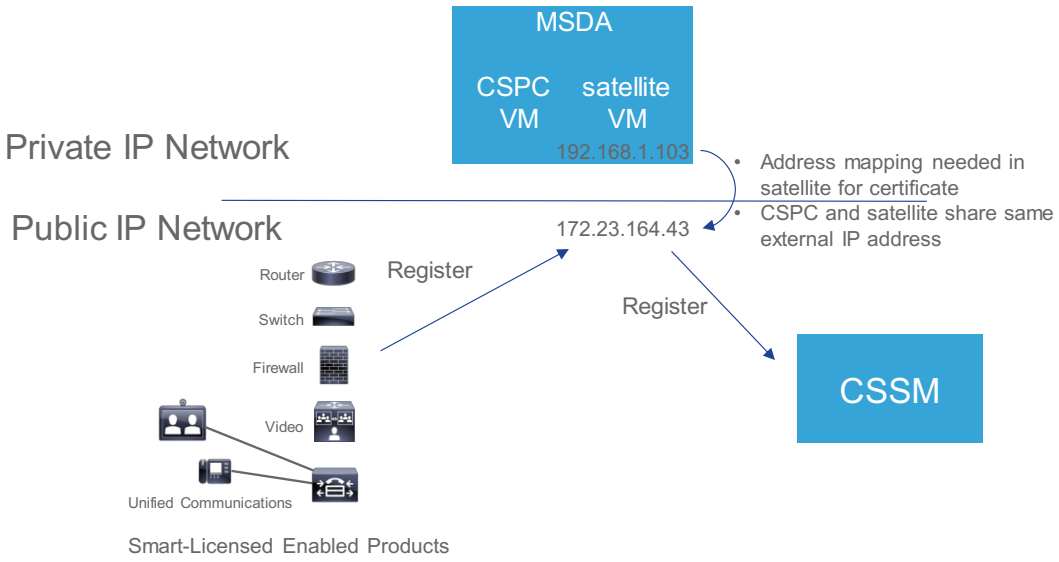
Before registration, set up the satellite with Network or Manual connectivity. In the **Setup Method** screen, you can select either: **Network Setup** (Internet connectivity), or **Manual Setup** (no Internet connectivity).

Click **Next**.

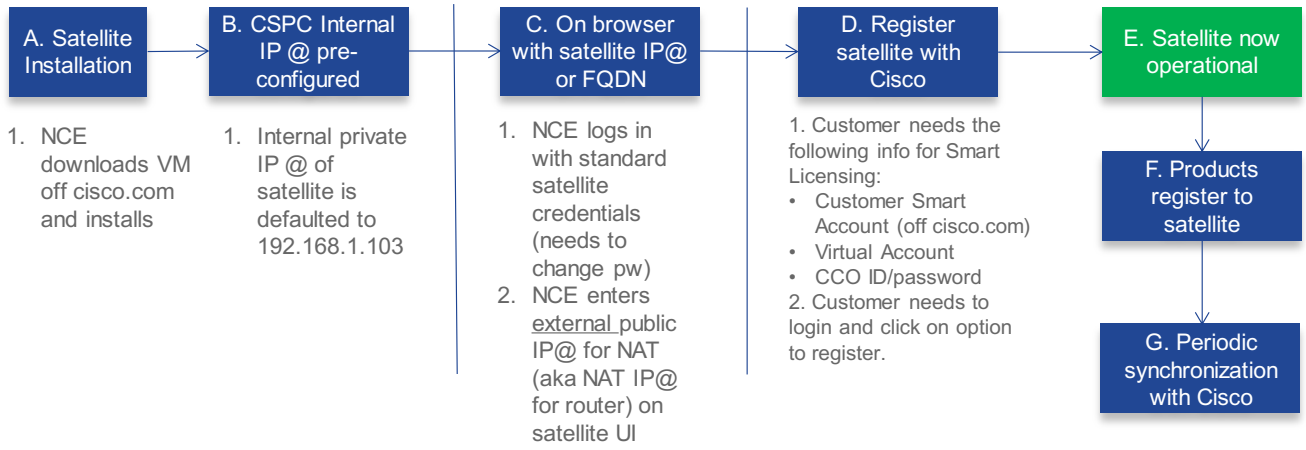
Setting up CSPC

Skip this step if you are not in the CSPC (Common Services Platform Collector) environment. Otherwise, if you have a large MSDA (Multi Service Delivery Appliance) with an already installed CPSC virtual machine and you have Smart-License enabled products that need to register with satellite, you can enable CSPC satellite support. Satellite runs as a separate virtual machine from CSPC within the MSDA appliance; however, there are some inter-dependencies requiring you to configure satellite differently. **CSPC is supported in satellite standalone mode only (no High Availability).**

The following diagram depicts an example of CSPC satellite environment. In this diagram, the MSDA resides in a private network and the Smart-License enabled products reside in the public network. Therefore, a fixed address translation requires satellite users to configure the satellite public IP address so that these products can register to satellite and satellite can register to Cisco Smart Software Manager (CSSM).



The CSPC satellite setup process is slightly different from non-CSPC and is depicted as follows:



CSPC Configuration Procedure

1. To connect to the satellite administration portal, go to **https://<public-satellite-ip-address>:8443** or **https://public-FQDN:8443.** The default username/password is **admin/Admin!23**.
2. Configure as a new satellite or from an existing backup file.
3. Click **Next**
4. You are presented with the **Network Interfaces, DNS Settings, NTP Settings, and CSPC Specific Settings** screen
5. Under **CSPC Specific Settings**, you see the message "If you are a CPSC customer, use Edit Network Settings to configure the public Network IP Address or FQDN. Otherwise, please ignore this field".
6. Click on **Edit Network Settings**
7. Navigate to **CSPC** tab, select the **Enable** radio button and enter the external IP address for satellite.
8. Click OK when you see the confirmation message.

9. Note that the **Network Interface**s tab parameters are greyed out when you enable CSPC. This is because the internal IP address cannot be changed in the CSPC satellite environment or satellite will go down. If you **Disable** the public IP address on the **CSPC** tab, thus no longer using the CPSC specific settings, the **Network Interfaces** tab is not greyed-out, allowing you to change the interface addresses.
10. After you click OK, you will be taken back to the **Network Settings** tab where it shows the configured Public Network IP Address under **CSPC Specific Settings** heading.
11. At this point, you can proceed to register the satellite.

Note: If you are in a CSPC environment and have configured NAT in PfSense, use the destination port number in the PfSense configuration for product registration to satellite. Please refer to *Appendix* for more detail.

Registering the satellite

After **Setup Method**, you are in the **Register Satellite** screen. At this point, you must register your satellite with Cisco SSM to establish identity required for secure on-going communication. Registration can be accomplished using the online or offline method through the GUI. The online (network) option requires a network connection; you would use the offline (manual) when you are disconnected from the Cisco Smart Software Manager portal. After you complete the satellite registration process, you receive an immediate response, confirming the satellite registration, from Cisco Smart Software Manager.

Registering via a Network

Procedure

1. Select the **Network Setup** radio button for online registration, and then click **Next**. You are presented with CCO Single Sign-On screen.
2. Click **Log In** and use the CCO credentials.
3. After the Single Sign-On screen, click **Allow**.
4. Enter the satellite name.
5. Select **Smart Account** from the list you have access to.
6. Add a new Virtual Account or use an existing account. You can have multiple virtual accounts.
7. Click **Register Satellite.** A warning alerts you that this process might take some time.
8. Click **Continue** to confirm. The system automatically restarts during this process. After restart, the satellite returns to the same step the user was in before the restart. The system returns to the **Synchronization Settings** page with **Network Setup** options selected.
9. Click **Next.** Note that a periodic synchronization must happen between the satellite and the Cisco Smart Software Manager to update the license entitlement and usage (30 days is recommenced; 90 days is required). For networked environment, this can be scheduled at various intervals.
10. In the next screen with the **Summary** dialog box, you are provided with a summary of the satellite settings. Click **Configure Satellite.** The registration process completes and returns you to the main screen on the **General** tab.

    Note: You can modify this setting and schedule synchronization timing later in the **Synchronization** page of the Cisco Smart Software Manager satellite portal. For more details, see Scheduling Synchronization on page 25.

What to do next

This completes the satellite configuration process. Product Instance can register to the satellite. In addition, you can now navigate to the Cisco Smart Software Manager and view the details of the satellite you just registered under the refreshed **Satellites** pane.

Refer to the other sections of the *User Guide* to view or perform various tasks of Smart Licensing.

Registering Manually

If the satellite is completely disconnected, follow this procedure to register it manually.

Procedure

1. Select the **Manual Setup** radio button for offline registration and click **Next**.
2. Click the **Generate Registration File** and save the file to your computer. The system generates a registration request file.

3. Go to the Cisco Smart Software Manager portal and click **Satellites**.
4. In the **Satellites** tab, click **New Satellite**.
5. In the **New Satellite** dialog box, enter the name of the satellite that requires registration.
6. Click the **Browse** button located next to the **Registration File** field and select the registration file was generated on the satellite in the previous step.
7. In the **Virtual Accounts** field, select an existing Virtual Account that you want the new satellite to manage. You can also create a new Virtual Account if you have the appropriate access (in other words, Smart Account Administrator). You can have multiple virtual accounts.
8. Click the **Create Authorization File**.
9. When promoted, click **Download Authorization File** and save it to your computer. Previously you had to wait 48 hours, but now you can download the registration file immediately. You can also see the new satellite is created in the refreshed **Satellite** tab.
10. In the Cisco Smart Software Manager satellite, at the **Register Satellite** setup, click **Browse** and navigate to the location where the authorization file was downloaded.
11. Click **Upload** to upload the authorization file.
12. Click **Register Satellite.** The system automatically restarts during this process. After restarts, the satellite returns to the same step the user was in before the restart.
13. On the **Synchronization Settings** page, select **Manual Synchronization,** click **Next**. You will get a warning that a periodic synchronization must happen between the satellite and the Cisco Smart Software Manager to update the license entitlement and usage (30 days is recommended; 90 days is mandatory). Any instance of Smart Software Manager satellite that has not synchronized with Smart Software Manager for more than 31 days receives an overdue alert (on day 32 or after). After 90 days of non-synchronization, all product instances associated with it are automatically unregistered, and the satellite is removed from Smart Software Manager.
15. In the satellite **Summary** dialog box, review the summary details, and click **Configure Satellite** if the configuration is correct. The registration process completes and returns you to the main screen on the **General** tab.

Setting Up satellite High Availability

Skip these steps if you are not configuring the satellite for High Availability.

Note that hostnames are pre-set to the following values and cannot be changed:
satellite-node-1
satellite-node-2

Initial Configuration Procedure:

1. From the **Administration** pane, click on the **High Availability** tab.
2. Select **Enable/Disable** to enable High Availability
3. Enter the **Standby IP Address**
4. Enter the **Virtual IP Address**
5. Click **Save.**

NOTE: Once enabled, the active satellite automatically begins the process of replicating data to the standby satellite. **Until the initial Cisco SSM satellite data has finished replication across the nodes, the standby satellite may not be fully available.**

To verify if the HA is functioning, you can connect to the satellite UI using https://VIP-Address:8443. It is recommended that you do not access https://Active-VM:8443 or https://STNDBY-VM:8443 directly.

Fail Over Procedure:

If the active satellite fails, the system will automatically switch to the standby. Once you recover the primary node, it will become active again. When both nodes are up, this recovery process can take up to 10 minutes.

What to do next

This completes the satellite HA configuration process.

Refer to the other sections of the *User Guide* to view or perform various tasks of Smart Licensing.

Using Cisco Smart Software Manager satellite

Licenses, Product Instances, and Registration Tokens

Licenses

- Term licenses—Licenses that automatically expire after a set amount of time: one year, three years, or whatever term was purchased.
- Perpetual licenses—Licenses that do not expire.
- Demo Licenses—Licenses that expire after 60 days. Demo licenses are not intended for production use.

Product Instances

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

Product instances must periodically connect to the Cisco Smart Software Manager satellite servers during a specific renewal period. If a product instance fails to connect, it continues to use the license and retains its latest status from the satellite until its ID certificate expires after one year from the last contact. If you remove the product instance, its licenses are released and made available within the Virtual Account.

Product Instance Registration Tokens

A product requires a registration token to register to the satellite before it can report license consumption. Registration tokens are stored in the Product Instance Registration Token Table that is associated with your Smart Account. After the product is registered, the registration token is no longer necessary and can be revoked and removed from the table. Registration tokens can be valid from 1 to 365 days.

Note: For details on creating a token, see Creating a Product Instance Registration Token on page 20

Logging into the satellite

To provide more security, when you log into the Cisco Smart Software Manger satellite, you are not presented with corresponding messages such as, success, failure, number of attempts, date/time of last login, and date/time of last failure. If the login is successful, the satellite allows you to log in. If it is a failure, the login button on the login dialog box is disabled for four seconds before you can log in again.

All failed attempts are logged using the format of *Date / Time / IP Address / [user] Success/Unsuccessful /Reason* in the log file. The information is available by going to the **Administration** tab and downloading the log zip file. After the log is downloaded, you can un-zip the file and see each attempt (success or failure) with associated details.

Virtual Accounts

Virtual accounts are collections of licenses and product instances. The licenses can be organized for your company into separate logical entities. You can use virtual accounts to organize licenses by business unit, product type, IT group, or what makes sense for your organization. For example, if you segregate your company into different geographic regions, you can allot the virtual account for each region to hold the licenses and product instances for that region.

You can view only those virtual accounts that were assigned for a particular satellite in a Smart Account. Note that a satellite can have multiple virtual accounts, but a virtual account can only belong to one satellite.

When you are working with virtual accounts:

- You can view virtual accounts in Cisco Smart Software Manager satellite, but you cannot create or remove them. Virtual Accounts must be created and managed in the Smart Account Management on software.cisco.com.
- All new licenses and product instances are placed in a virtual account. You choose the virtual account when you register a product instance.
- You can view and obtain the most recent virtual account data after the satellite synchronizes with the Cisco Smart Software Manager.

Virtual Account Panes

Virtual account panes include the following:

- Alert Bar
- General Tab
- License Tab
- Product Instances Tab
- Event Log Tab

Alert Bar

Any license or product instance that is not in compliance with the licensing agreement creates an alert. The **Alert Bar** provides a summary of the alerts in the virtual account. Alerts are listed in the tables on the **Licenses** and **Product Instances** tabs and are summarized in the **Alert Bar**.

If you choose the **Major** or **Minor** button to view alerts, the **Alert Bar**, which appears below the alert buttons, shows one row per alert. If there are no alerts, the alert buttons are hidden.

The main portion of an alert contains the alert description. On the right of an alert are links to appropriate actions.

On the right of the alert is the **Action Due** field, which shows how much time remains for you to take action on the alert.

- The **Major** button enables you to view all major alerts, such as Out-of-Compliance conditions, and take action on a specific alert. In addition to any other action links, all major alerts contain a link to a **Troubleshooting** dialog box that provides information about how to resolve the alert.

- The **Minor** button allows you to view all minor alerts, such as expiring licenses, and take action on a specific alert. Minor alerts are promoted to major alerts if not acted upon within their time limit.

  With minor alerts, you have the following options:

  - **Remind Later**—Notifications are dismissed until half of the time that is displayed in the **Action Due** field has passed.
  - **Dismiss**—No notifications are displayed until the next time that the error is generated.
  - The **Hide Alerts** button allows you to collapse the alerts.

General Tab

The **General** tab displays information about the specific virtual account and the registration tokens that are associated with the virtual account. From the **General** tab, you can do the following:

- View information about the virtual account.
- Edit the virtual account.
- View a list of existing product instance registration tokens.
- Create new product instance registration tokens.
- Copy, download, or revoke registration tokens. Revoked registration tokens can be left in the list or removed.

Licenses Tab

The **Licenses** tab displays information about all of the licenses in your virtual account. From the **Licenses** tab, you can do the following:

- View a list of all licenses in the virtual account.
- Filter the licenses by the license identifier.
- View information about a specific license and which product is using it.
- View information about the alerts for specific licenses and fix the issue.
- Export the list of licenses to a `.csv` file.

Note: You cannot transfer licenses in Cisco Smart Software Manager satellite. You can transfer licenses using Cisco Smart Software Manager.

Product Instances Tab

The **Product Instances** tab displays information about all of the product instances in your virtual account. From the **Product Instances** tab, you can do the following:

- View a list of all product instances.
- Transfer product instances between virtual accounts.
- Filter the product instances by the product identifier.
- View information about a specific product instances and what licenses it consumes.
- View information about the alerts for a specific product instance.
- Remove a specific product instance from the virtual account which in turn removes from the smart account.
- Export a list of product instances to a `.csv` file.

Event Log Tab

The **Event Log** tab displays information about all of the events in a virtual account. Events are actions that you have taken using Cisco Smart Software Manager satellite such as adding and removing licenses and products, adding and renaming virtual accounts, and so on. From the **Event Log** tab, you can do the following:

- View a detailed list of all events in the selected virtual account.
- Filter the events by license or by product.

- Export the list to a `.csv` file.

Note: You can view or obtain the most recently updated data after you have synchronized the satellite with the Cisco Smart Software Manager.

Viewing Virtual Account Information

Procedure

1. In the **Navigation** pane, click a Virtual Account.
2. Click the **General** tab.

Creating a Product Instance Registration Token

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

Cisco Smart Software Manager satellite allows Smart License enabled products that connect to satellite to generate restricted tokens and enable restricted functionality according to Export Control laws. Products that are not successfully registered with a restricted token cannot turn on restricted functionality. This option is available to only those accounts that are permitted to use this functionality.

During a synchronization with Cisco Smart Software Manager, the satellite checks the Smart Account category (A, B, or C) received from Cisco SSM through the previous sync and allows or disallows the restricted token generation accordingly.

The customer categories are:

- Category A: European Union License Free (EULF) - Restricted features are allowed. Customers are located inside the EULF/Eastern Neighboring Countries (ENC) set of countries, roughly US, Canada, EU (European Union), Japan, Australia and New Zealand.
- Category B: Non-EULF, civilian - Restricted Features are allowed. Non - public sector customers located outside of the EULF/ENC require screening to ensure they are non-public sector.
- Category C: Non-EULF, Government / Military - Restricted features are NOT allowed. Public sector (including government, military, and government owed enterprises) located outside of the EULF/ENC to which US export restrictions apply. Category C customers are not allowed to generate restricted tokens in Cisco Smart Satellite Manager or satellite. See Note below.
- C-Pending: Review Pending - Restricted features are NOT allowed.

Note: If a customer classification changes from Category B to Category C, they are no longer eligible to generate restricted tokens, their previous tokens are revoked and the expiration date will change to "Revoked."

Procedure

1. In the **Navigation** pane, click an existing virtual account.
2. On the **General** tab, click **New Token**.
3. In the **Create Registration Token** dialog box, complete the following fields:

Name	Description
Virtual Account field	Already filled out with the virtual account under which the registration token will be created.
Description field	The description of the registration token. **Note:** Specify a description that will help you identify the token.
Expire After field	The time limit for the token to be active up to 365 days. The default is 30 days.

4. If you are a Category A or B customer, you can click on "Allow export controlled functionality on the product registered with this token" box to generate a restricted token. If you are a Category C customer, this option is not available and you can only generate un-restricted tokens.

5. Click **Create Token**.

Viewing Product Instance Registration Tokens

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

Procedure

1. In the **Navigation** pane, click a virtual account.
2. Click the **General** tab.
   This page has two sections: **Virtual Account** and **Product Instance Registration Tokens**.
3. In the **Product Instance Registration Tokens** section, the following details are displayed in a table:

Name	Description
Tokens field	The token ID that was generated. You can click the link to view or copy the entire length of the token string.
Expiration Date field	The time limit for the token to be active.
Description field	The description of the registration token.
Created By field	The user who created the token.
Actions links	Choose one of the following actions: • **Copy**—Copy the token to your clipboard. • **Download**—Download the token to your local machine in a text file format. • **Revoke**—Revoke the token. Revoked tokens can no longer be used. • **Remove**—Remove a revoked token from the Product Instance Registration Token table, only available on Revoked or Expired tokens.

Managing Product Instance Registration Tokens

Procedure

1. In the **Navigation** pane, click an existing virtual account.
2. On the **General** tab, locate the token in the **Product Instance Registration Token** table that you want to manage.
3. In the **Product Instance Registration Token** table, perform one of the following actions:
   - **Copy**—Copy the token to your clipboard.
   - **Download**—Download the token to your local machine in a text file format.
   - **Revoke**—Revoke the token. Revoked tokens can no longer be used.
   - **Remove**—Remove a revoked token from the **Product Instance Registration Token** table.

Viewing Licenses in a Virtual Account

Note: You cannot transfer licenses to or from a different Virtual Account in Cisco Smart Software Manager satellite. You can transfer licenses using Cisco Smart Software Manager.

Procedure

1. In the **Navigation** pane, click a virtual account.

2. Click the **Licenses** tab.
3. You can export the license list to a `.csv` file from this pane.
4. Click the license ID to see detailed information about a license.

   The system displays the **License Detailed Information** dialog box. This dialog box has the tabs **Overview**, **Product Instances**, and **Event Log**.

Viewing Product Instances in a Virtual Account

Procedure

1. In the **Navigation** pane, click a virtual account.
2. Click the **Product Instances** tab.
3. You can export the list of product instances to a `.csv` file.
4. Click the product instance name to see detailed information about a product instance.

   Note: A cluster setup icon by the right side of the product instance indicates a high availability of routers for that specific product instance.

   The system displays the **Product Instance Details** dialog box. This dialog box has the tabs **Overview** and **Event Log**.

What to do next

You can transfer a product instance to a different virtual account or delete product instances.

Transferring a Product Instance

Caution: Transferring a product instance from one virtual account to another virtual account does not result in the corresponding licenses being transferred. You must transfer the licenses separately through Cisco Smart Software Manager.

Procedure

1. In the **Navigation** pane, click an existing virtual account.
2. Click the **Product Instances** tab.
3. In the **Product Instances** table, locate the product instance that you want to transfer.

   Note: Enter a value in the **Filter** combo box and click **Filter** to limit the number of entries that are displayed.

4. In the **Actions** column, click the **Transfer** link for the product instance that you want to transfer.
5. In the **Transfer Product Instance** dialog box, complete the following fields:

Name	Description
Name field	The name of the product instance and the product name.
Transfer To drop-down list	Choose the virtual account that you want to transfer the product instance to.

6. Click **OK** to transfer the product instance.

Removing a Product Instance

When you remove a product instance from the satellite, you are removing it only from the table. The licenses that the product instance used are still available and can be used by other products. You must re-register the product instance with the Cisco Smart Software Manager or satellite, so that Cisco Smart Software Manager or satellite can communicate with the product again.

Procedure

1. In the **Navigation** pane, click an existing virtual account.
2. Click the **Product Instances** tab.
3. In the **Product Instances** table, locate the product instance that you want to remove.

Note: Enter a value in the **Filter** combo box and click **Filter** to limit the number of entries that are displayed.

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

Viewing Event Logs

The event log shows the event message, the time of the event, and the user (if any) associated with the event.

Procedure

1. In the **Navigation** pane, click a virtual account.
2. Click the **Event Log** tab.
3. You can export the event list to a `.csv` file from this pane.

Exporting to CSV Files

Procedure

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

Note: The system uses a platform-dependent dialog box to save the file. The dialog box varies slightly depending on the browser and operating system that you are using.

Understanding Synchronization Alerts and Actions

The synchronization process enables you to setup a connection between the satellite and the Cisco SSM by communicating through cisco.com at different time intervals to transfer data.

The synchronization process between satellite and Cisco SSM has been improved to handle the following situations:

a) Reducing frequent out-of-sync conditions in product instance, license entitlement and consumption that could exist.

b) Changing to a "lean" data model to alleviate entitlement changes in Cisco Smart Software Manager that are not correctly reflected in the satellite in a synchronization.

c) Improving synchronization network response time.

d) Addressing VM snapshots or backup and restore or out-of-order synchronization scenarios that could cause mismatched data between satellite and Cisco SSM.

e) Better handling of error conditions when Cisco SSM is unable to update product instance send from satellite (that is they come from a different virtual account on Cisco SSM).

Cisco SSM has always been the source of truth for all entitlements, virtual accounts, and metadata information. On the other hand, satellite has always been the source of truth for product instance and license consumption information. this means that each system must take whatever is sent by the other system as an undeniable source.

In the past, satellite and Cisco SSM operated on a delta synchronization model, which means that only incremental changes would be sent and received. However, in the case where the satellite database is restored from a previous VM snapshot or backup, this incremental synchronization process can produce mismatched license entitlement and consumption and product instance counts. A full synchronization (versus delta or standard synchronization) is introduced when Cisco SSM detects that it needs the satellite to compile and send a complete list of its data, regardless of when it was created. In return, Cisco SSM also compiles a complete list of its current source of truth elements and passes that along to the satellite.

The synchronization links, buttons, and alerts that you find on the work pane of the Cisco Smart Software Manager satellite are:

- **Last Synchronization (this is a hyperlink)**
- **Synchronize Now / Manual Synchronization buttons**

- **Synchronization Alerts**

Last Synchronization

This hyperlink is available in the upper right corner of the work pane. It enables you to view the synchronization settings and logging of various synchronization activities. Click this link. The dialog has two sections: **Status** and **Settings**.

In the **Status** section, you can view the **Last Successful Synchronization** and the **Next Synchronization Due By** information. Beside the **Status** field, you will find a link to **View Log**. Click this link to view the synchronization activity table that lists the time, type and the status of synchronization. All times on the satellite are log as UTC.

In the **Settings** section, you will find the details pertaining to the mode of synchronization chosen and the results of the synchronization attempts displayed. Click the **Edit** button beside the **Settings** field to modify the synchronization settings. For more details on these settings, see Scheduling Synchronization on page 25

Click **View Synchronization Data File** link in the bottom right of this dialog to download the synchronization data file.

Synchronize Now / Manual Synchronization

This **Synchronization Now** toggle button displayed in the upper right corner, next to the **Last Synchronization** link. This button changes according to the synchronization modes chosen. Each of these scenarios is explained in the following points:

- In the **Synchronization Settings** section of the **Synchronization** page, if you choose **Network Synchronization** mode, the **Synchronize Now** button is displayed. Click this button to synchronize and update satellite data instantly. This method of synchronization works for network deployed environments only.

  Note: Port 443 must be enabled for communications between the satellite and the Cisco Smart Software Manager.

- In the **Synchronization Settings** section, of the **Synchronization** page, if you choose **Manual Synchronization** mode, the **Manual Synchronization** button is displayed. Click this button to use the file-based synchronization option.

Note: For more details, see Scheduling Synchronization on page 25

Synchronization Alerts

The Synchronization alerts indicate an impending problem. The satellite displays alerts on the alert bar in the work pane. Two types of alerts can be generated due to the following conditions:

- **Synchronization Overdue**—Any instance of Cisco Smart Software Manager satellite that has not synchronized with Cisco for over 31 days will receive this overdue alert. All product instances associated with it will automatically be unregistered and the satellite will be removed from the Cisco Smart Software Manager if no synchronization occurs within 90 days.
- **Synchronization Attempt Failed**—This type of alert is displays when you attempt to synchronize data from Cisco Smart Software Manager to Cisco and the network connection fails.

Note: If there are no alerts, the alert buttons are hidden.

The main portion of an alert contains the alert description. On the right of an alert, there are links to appropriate actions. For example, the alert `Synchronization Attempt Failed` has links to the **Dismiss** button that you can use to clear this alert message until the next time that the error is generated.

Synchronization Pane

The **Synchronization** pane includes the following sections:

- **Synchronization Mode**
- **Synchronization Data Security Settings**
- **Synchronization Schedule** available if you choose the **Network Synchronization mode**.

Note: For more information, see Scheduling Synchronization on page 25.

Synchronization Mode

This section allows you to set up the connection between the satellite and the Cisco SSM to synchronize manually or at different time intervals using the following mode options:

- **Network Synchronization**—Data is synchronized and updated on demand or at scheduled time periods in this mode. Port 443 is used for communication between the satellite and the Smart Manager. You can choose this mode if you are able to connect to cisco.com periodically. This type of synchronization is suitable for network enabled environments.
- **Manual Synchronization**—Data is transferred through a file download and upload process in this synchronization mode. You can choose this mode if you do not have network connectivity or cannot establish a connection to communicate with Cisco Smart Software Manager. This mode provides two options: Standard or Full synchronization.

Synchronization Data Security Settings

This section provides you with check boxes to exclude the following secured data while transferring the product instance data file to Cisco cloud portal. It may be one or more of the following:

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

Synchronization Schedule

The **Synchronization Schedule** option is only visible when you choose to perform network synchronization. It allows you to set up a schedule and synchronize data between the satellite and Cisco SSM. You can choose the frequency and the time for scheduling the synchronization.

Scheduling Synchronization

You can schedule a chosen date and time for synchronizing the satellite with the Cisco SSM.

Procedure

1. In the Navigation pane, click **Synchronization**.
   On the Synchronization page, you have two or three sections: **Synchronization Mode**, **Synchronization Data Security Settings** and **Synchronization Schedule** if the Network Synchronization radio button is selected.
2. In the **Synchronization Mode** section, click the **Network Synchronization** radio button.
3. In the **Synchronization Schedule** section, you can set up the synchronization schedule using the following options.

Name	Description
Frequency field	Choose the schedule to synchronize and update data from the drop-down list. It can be one of the following: • **Daily**—This method allows you to synchronize on a daily basis at a specified time. • **Weekly**—This method allows you to synchronize only once a week at a specified time and day of the week. • **Monthly**—This method allows you to synchronize only once a month at a specified time and date.
Time field	The time in an hour and minute format.

Name	Description
Date field	The day of the week chosen for weekly synchronization or a particular date for the monthly synchronization as applicable in the **Frequency** field.

Manual Synchronization

The instructions in this step are applicable when you select **Manual Synchronization** mode. Clicking the **Manual Synchronization** radio button, displays a **Manual Synchronization** menu button in the upper right corner of this page. This button has two pull-down options: Standard Synchronization and Full Synchronization. If you select **Standard Synchronization** and upon processing, Cisco SSM needs a **Full Synchronization**, it notifies you that a full synchronization is needed when you try to download the synchronization response file. At this time, return to satellite and click the **Full Synchronization** option and re-perform it.

In the **Standard** or **Full Synchronization** dialog box, you can the same steps below:

Procedure

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

    After this step completes, the license entitlement and usage on both Cisco SSM and satellite are identical for the virtual accounts that are associated with the satellite.

Reports Pane

The **Reports** pane enables you to run different reports against your virtual accounts. The reports table displays the following information for each supported report. You can run a **Licenses** or **Product Instances** report:

Name	Description
Name area	The name of the Cisco Smart Software Manager satellite report. Click the link to view the specific report page.
Description area	The description of the report.

Running Reports

Procedure

1. In the **Navigation** pane, click **Reports**.
2. On the **Reports** page, choose the report that you want to run.
3. In the **Report Settings** pane, complete the following fields:

Name	Description
Name field	The name that you want to assign to the report.
Description field	The optional description that you want to use for the report.
Virtual Account drop-down list	Choose one or more virtual accounts that you want to run the report against. Choose **All Virtual Accounts** to run the report against all virtual accounts. **Note:** You can run reports for only those virtual accounts to which you have access.
Product Type field (product instance reports only)	The product type that you want to run the report against. You can choose one or more product families.

4. In the **Actions** pane, choose an action. This can be one of the following:
   - **Run Report**
   - **Export to Excel**
   - **Export to CSV**

   Clicking **Run Report** opens the report in a new browser window. Clicking **Export to Excel** or **Export to CSV** opens a **File Save** dialog box.

Administration Pane

As a Cisco Smart Software Manager satellite license administrator, you can use the Administration pane to:

- Create a new user, remove an existing user, and view user profile data on the **Users** tab
- Schedule backups, perform backups and restores of the satellite on the **Backup/Restore** tab
- Upgrade the satellite to a new version on the **Upgrade** tab
- Change network interfaces, DNS, and NTP configurations or run diagnostics like `ping`, `traceroute` and `ns lookup` on the **Network** tab.
- Restart or shut down the satellite, customize headers and footers, or configure SSLv3 by using the **System Settings**
- Generate diagnostic logs of your user experience, which will allow the Cisco Support team to optimize the benefits of Smart Licensing, on the **Diagnostic Logs** tab

The **Users** tab provides a table with the following information and options:

Name	Description
User Name	The name of the user. Click the link to view the complete information of the user.
Full Name	The full name of the user.

Name	Description
Actions	Click **Delete** if you choose to delete a user permanently from the application. Confirm the deletion at the prompt.

The **Administration** pane also provides buttons to create a new administrator sequence and for exporting data to CSV files.

Creating a New Administrator

Use the following procedure to create a new satellite Administrator (the only role on the satellite). This is local to the satellite only and does not affect the Smart Account on Cisco Smart Software Manager.

Procedure

1. In the **Navigation** pane, click **Administration**.
2. On the **Administration** page, click **New Administrator**.
3. In the **New Administrator** dialog box, complete the following fields:

Name	Description
Username field	The name or ID provided for the user. The username should contain a minimum of 4 alphanumeric characters.
Full Name field	The first and last name of the user.
Password field	Enter the user's password. The password should contain a minimum of 6 characters and include 1 number, 1 upper case, and 1 special character.
Re-enter Password field	Re-enter the password.
User must change password at first login check box	Check the check box to force the user to change the password after the first login.

4. Click **OK**.

Backups and Restores

Backup and Restore feature allows you to backup Cisco Smart Software Manager satellite and later restore the satellite to a prior operational state or migrate data from one system to a new one. Note that restore only works on a backup generated using the same major version (e.g. 3.0.x to 3.1.0).

You find the backup and restore functions in the **Administration** pane. To access them, click the **Backup/Restore** tab.

There are several actions you may take from this page:

- **Run Backup Now**
- Create a **Backup Schedule**
- **Restore**

Running On-demand and Scheduled Backups

On-demand Backups

Cisco Smart Software Manager satellite supports on-demand and scheduled backup operations. In addition, you can manage the backup files by renaming, downloading, and restoring backups.

You can initiate on-demand backups at any time by clicking the **Run Backup Now** icon. When this option is selected, the process of collecting needed information to create a backup file begins. Upon successful completion, a message displays indicating that the backup succeeded.

In the event of a failure, satellite displays a major alert indicating the nature of the failure and possible corrective action. Go to the **Diagnostic Logs** tab and click **Generate Zip File**. Send the .zip file to Cisco with your ticket to resolve the failure.

If a backup is attempted while the satellite is actively in the process of performing a backup, a message displays to notify the Administrator that a backup is in progress, and that it must complete before another backup can be started.

Scheduled Backups

Cisco Smart Software Manager satellite allows you to have fully automated backups by creating a backup schedule. You can schedule backups on a daily or weekly basis depending on the desired frequency. If a backup time is not provided, it defaults to 23:00 (one hour before mid-night).

After the user configures a schedule, the satellite automatically performs backups at the chosen interval(s). The backup files are created, stored locally on the satellite, and are accessible from the **Backup Files** section of the **Backup/Restore** tab, in descending order.

To create the backup schedule:

Procedure

1. Check the **Schedule regular backups** box.
2. Choose the **Frequency** from the pull down menu.
3. Choose the **Time** from the hour and minute menu.
4. Click the **Days to be run** boxes.
5. Click **Save**.

Managing Backup Files

You can restore, download, show MD5 Checksum, rename, and delete the backup files by choosing the appropriate action from the Actions drop-down menu in the **Backup Files** section in the **Administration** pane's **Backup/Restore** tab. The actions are as follows:.

- **Backup/Restore** action allows you to revert the satellite to a previous state of operation.
- **Download** action allows backup files to be copied from the satellite for off line storage using your browser. When selected, the browser (optionally) prompts for a destination and the contents of the satellite are downloaded to your device.
- **Show MD5 Checksum** action is provided so that you can verify that files have not been corrupted during a download. The MD5 Checksum is computed when the backup is performed.
- **Rename** allows you to change the name given to the satellite backup file from its default, or prior name. The new backup file name is limited to a maximum of 60 characters, and the valid characters for file names are A-Z\a-z|0-10|-|_|.
- **Delete** allows you to remove a backup file created from the list provided by the satellite. This action is permanent and the backup file cannot be recovered.

Automatic Purging of Backups

The satellite allows a maximum of 20 backup files or up to 80% of the available disk space to be used for backup files. After reaching the threshold of 20 backup files, the satellite automatically deletes the oldest backup file.

Additionally, any backup file 90 days (or older) is automatically deleted. This is because attempting to use a backup file which was created more than 90 days in the past would result in the satellite being unable to register products or synchronize with Cisco SSM due to expired certificates. As these backup files cannot be used, they are automatically deleted without requiring you to perform maintenance.

Procedure

1. In the **Administration** pane click **Backup/Restore**.
2. In the **Backup Files** panel. Choose the file name you want to use under **Backup Files** by clicking on **Actions** drop-down menu.
3. Choose the action you want to perform from the list.

4. To replace all data on the satellite with data contained in the backup file, click **Restore**. A dialog box asks you to confirm the restore from backup operation.
5. Click **Restore from Backup** to start restore.
6. Click **Cancel** to stop restore.
7. A **Restore In Progress** message informing you that the restore is processing and that a system reload is automatically performed afterwards.
8. To download, click **Download** to start the process. A dialog box appears confirming the download has begun.
9. To show MD5 Checksum for that particular file, click **Sow MD5 Checksum**. A dialog box appears showing the name of the backup file name and Checksum.
10. Click **OK** to continue.
11. To **Rename** the backup file, click **Rename**.
12. Enter the new **Backup Name** in the dialog box that is displayed. Note that the new file name must conform to the backup file naming convention.
13. Click **Save** to keep, or **Cancel**.
14. Click **Delete** to remove the backup file you choose.
15. Click **Delete Backup** in displayed dialog box to confirm delete.
16. Click **Cancel** to exit delete.

Restoring a Backup File

The **Restore** action allows you to return a satellite to a previous operational state, or migrate data from one system to a new one. The **Restore** operation requires you to either choose from an existing local backup file from the satellite, or selecting a previously downloaded backup file. After the restore, the current satellite is replaced with the selected backup file. The system restarts with a reminder to synchronize now or later.

In the event the restore fails, the user will receive one of the following messages indicating the reason for the failure.

- **Backup File Not Valid** - *The file you specified is not a valid satellite backup file. The file might be corrupted or is not a .zip file.* This means the file has become corrupted or modified after it was downloaded. Try downloading the file from the satellite again and retry the restore.
- **Backup Version Not Valid** - *The backup file you specified is from an older version of the satellite, version<version-num>, and your satellite is currently running version <version-num>. You can only restore your satellite from a backup taken from the same version.* This means your backup file was created from a different version that is not compatible with the new satellite version (For example, the backup file was created with satellite release 3.0.x and restored on 3.1.0 satellite). Install either the original or compatible satellite version and retry the restore.
- **Restore from Backup Failed** - *An error occurred while attempting to restore this Smart Software Manager satellite from a backup. The satellite has been reverted to its previous status prior to the restore.* This means the restore was not successful, and satellite reverts to its previous state before the restore operation was initiated.

To restore from a local backup file:

Procedure

1. In the **Administration** pane, select the **Backup/Restore** tab.
2. Choose the desired backup .zip file from the list displayed.
3. Select the backup file you want to restore, and choose the **Restore** action from the **Actions** pull-down menu..

Restoring a New Cisco Smart Software Manager satellite

In the event there is need to re-deploy the satellite, you can restore and configure a new satellite from a backup file that was previously created and downloaded. The downloaded backup file can either be restored on the same host (to the same IP address from the backup file) or a different host (to a different IP address from the backup file).

To restore a satellite from a backup:

Procedure

1. Install the satellite using the instructions from the *Cisco Smart Software Manager satellite Installation Guide*
2. During the install process you are presented with a screen which will all you to choose either: **Configure a new satellite** or **Configure by importing data from a satellite backup file**. The latter option restores configuration settings, including registered product instances
3. Select the previously downloaded backup file via the **Choose File** option.
4. Click **Restore**.
5. (Optional) Cancel the file by clicking **Cancel**.

During the restore process, the satellite is not available for other operations. After a successful restore operation, the satellite restarts and the following message displays indicating that the restore is in progress.

Restore in Progress - *The Smart Software satellite is currently being restored from a backup. This process can take some time depending on the number of registered product instances. This page will reload when the process has completed.*

Following the restore, you are prompted to perform synchronization or defer it to a later time using one of the three following options:

- **Network Synchronization**
- **Manual Synchronization**
- **Synchronize Later**

Note that the satellite synchronization to Cisco SSM might be deferred for various operational reasons, and therefore, the satellite does not impose an automatic synchronization. Instead, it provides the following messages to remind you that synchronization might be required to return the satellite to a fully operational state.

If the satellite is restored to the same virtual machine, the following message displays:

The Smart Software Manager satellite was successfully restored from backup. To complete the restore, it is recommended that you synchronize with Cisco Licensing Servers.

If satellite is successfully restored to a different virtual machine message is shown:

The Smart Software Manager satellite was successfully restored from backup. To complete the restore, it is required that the satellite synchronize with Cisco Licensing Servers.

IMPORTANT: Because you have restored to a virtual machine other than the one used to create the original backup, the satellite will be unable to register new product instance until it has synchronized.

Common considerations to defer the synchronization include:

- Recommended: When restoring from the same satellite the backup was generated from, a synchronization is only needed to ensure the license information is properly synchronized with Cisco SSM. Product registration to satellite would still function prior to this synchronization.

Required: If you restore to a satellite which is different from the satellite used to create the backup file, then a synchronization is required to ensure proper operation. Until the synchronization is complete, product registration operations may fail. If the **Synchronize Later** is selected, an alert message appears on the main screen reminding you to synchronize to ensure the satellite has the latest licensing information, and is ready to resume normal operations

Network Configuration

The **Network** tab in **Administration** pane provides setup and troubleshooting tools through the GUI.

Satellite supports multiple interfaces, allowing traffic to be separated for satellite management and product registration.

- The **Administration Network Interface** is always used for the client to connect to the satellite.
- The **Product Registration Interface** can be used to register and synchronize the satellite to Cisco SSM.
- You can set up the IP address, subnet mask and gateway independently on each Network Interface Card (NIC).

The **Network** tab shows the current setup of the satellite interfaces: **Administration Network Interface - eth0** and **Product Registration Interface - eth1**.

DNS Settings shows the current DNS server IP addresses and the associated search domains.

NTP Settings shows the current time on the satellite, the time server name, and an option to **Sync Time Now**.

Edit Network Settings opens a dialog box to change network interfaces, DNS, and NTP configurations.

Launch Network Diagnostics opens a dialog box to run ping, ping6, traceroute, and ns lookup.

Editing Network Settings

If you change the IP Address the following series of actions might be required:

- You might need to update the Smart Call Home transport URL on each of your registered Product Instances so they can continue communicating with the satellite.
- The URL to reach this administrative interface will change.
- You will need to synchronize the satellite to complete the change.
- You will be asked to **Confirm Network Address Change** and given the choice to **Continue** or **Cancel**. If you click **Continue** the change will be made and a page will be displayed with the message **Administration Interface URL Changed**. You will be given the new URL at this point. Be sure to update any bookmarks with the new URL.
- When you go to the new URL and log into the satellite, a **Synchronize Needed to Complete IP Address Change** alert message will be displayed and remains visible until you complete the sync.
- After the sync is completes, an alert informs you to: **Verify Transport Settings on Registered Product Instances** - The network address of this Smart Software Manager satellite has been changed. If necessary, update the Smart Call Home transport URL configured on your registered Product Instances to ensure that they can communicate with the satellite.

Procedure

1. In the **Administration** pane, click the **Network** tab and scroll to the bottom.
2. Click **Edit Network Settings**.
3. On the **Network Interfaces** tab, the **Administration Network Interface Status** drop-down menu is disabled and shows only as **Enabled**. The **Hardware Address** shows below the drop-down menu.
   The **Hardware Address** will show below the drop-down menu.
4. Under **IPv4/IPv6**, the **Configuration** drop-down menu for **Administration Network Interface - eth0** is disabled and will only show as **Manual**. The **IPv4/IPv6 Configuration** drop-down menu is available for **Product Registration Interface - eth1**, with: **DCHP, Manual** or **Not Configured**.
5. Enter the IP Address, Subnet Mask, and Gateway information.
6. (Optional) To change the domain name server configuration, click the **DNS** tab and enter the DNS servers and Search Domains.
7. (Optional) To change the NTP server configuration, click the **NTP** tab and enter the NTP server address.
8. Use the **Sync Time Now** link to immediately sync your satellite server time with the selected NTP server.
9. Click **OK**.

Launching Network Diagnostics

Procedure

1. I n the **Administration** pane, click the **Network** tab and scroll to the bottom.
2. Click **Launch Network Diagnostics**.
3. Enter **Hostname** or **IP Address**.
4. Click **Ping/Traceroute** or **Ping6/Traceroute6** and results will display in the box.
5. Click **Namespace Lookup** and results will display in the box.
6. Click **Clear Output** to clear the output box. Otherwise, multiple **Ping/Ping6**, **Traceroute/Traceroute6** and **Namespace Lookup** will append the results in the output box.
7. Use **Cancel** if you want to cancel the current search.

Systems Settings

The **System Settings** tab in **Administration** allows you to perform Restart/Shutdown of the satellite, set up Headers and Footers, and edit SSLv3 Compatibility parameters.

Satellite Restart/Shutdown

In the **Administration** pane, under the **System Setting** tab, the **Satellite Restart/Shutdown** buttons allow you to gracefully restart or shut down from the GUI.

Procedure

1. To restart, click the **Restart** button.
   If you continue, the satellite is restarted. During the restart, which can take several minutes, the satellite is unreachable to Product Instances and the administrative interface is unavailable.
   a) A dialog box requests that you **Confirm Restart** displays.
   b) If you enter the optional reason for the restart, it is included in the logs.
   c) Click **Restart** to continue the process or **Cancel** to opt out.
2. To shut down the satellite, click **Shutdown**.
   If you continue, the satellite shuts down. After it completes, the satellite is unreachable to Product Instances and the administrative interface is unavailable.
   a) A dialog box requests that you to **Confirm Shutdown** displays.
   b) If you enter a reason for the shut-down, it is included in the logs.
   c) Click **Shutdown** to continue or **Cancel** to opt out.

Configuring Headers and Footers

Custom Headers and Footers are user configurable enabling them to align with federal security classifications. The text you enter displays on the top and bottom of satellite login page, all application pages and reports generated by the satellite. These headers and footers allow you to provide classification markings and other meaningful designations.

Procedure

1. In the **Administration** pane, click **System Settings**.
2. In the Custom Headers/Footers panel, click the **Display custom headers and footers** checkbox.
3. In the Text field, enter the text for your header and footer. A preview of your text is shown in the **Preview** area.
4. In the **Text Size** drop-down menu, select the font size that you want to use.
5. In the **Color** drop-down menu, select the header and footer color that you want.
6. Click **Save**.
7. To disable custom headers and footers:
   a) Under **Custom Headers/Footers**, clear the **Display custom headers and footers** checkbox.
   b) Click **Save**.
   c) Refresh your browser.

Configuring Message of the Day

You can configure a custom Message of The Day that appears when a user logs in to the CentOS system console. Enter the text in the box and click on **Display custom message of the day** icon. This message will override the default console Message of The Day used by CentOS at the log on prompt.

Configuring SSLv3

This tab allows you to enable SSL (Secure Socket Layer) v3 and backward compatibility with certain products. The satellite defaults to TLS (Transport Layer Security), so if a device with an old smart agent image tries to make a handshake with SSLv3, it will fail. Therefore, we provide this option for older products that are still using SSL v3 and enable SSLv3 communication with the satellite.

Procedure

1. In the **Administration** pane, click **System Settings**.
2. In the SSLv3 Compatibility section, set the **Enable SSLv3** check box as desired.
3. Click **Save**.

Diagnostic Logs

You can generate a zip file containing diagnostic log files to send to Cisco support by using the **Diagnostic Logs** tab in **Administration**.

Generating Diagnostic Log Files

Use the following procedure to generate diagnostic logs for your Cisco Support.

Procedure

1. In the **Navigation** pane, click **Administration**.
2. In the **Administration** pane, click **Diagnostic Logs**.
3. Specify the date range for the log file:
   - Select a pre-set the date range from the drop down menu.
   - Select **Date Range** to display a window in which you can enter beginning and ending dates for the data sample.
4. Click **Generate Zip File** to download diagnostic logs to your computer desktop.

   This file should then be sent as an email attachment to Cisco Support.

Upgrading satellite with Automated Software Delivery

Please refer to the Installation Notes for specific satellite release as each patch/upgrade procedure is different.

The satellite includes an upgrade feature called Automated Software Delivery (ASD). With ASD, you can check whether a software upgrade is available. ASD also provides options for you to automatically download and install the upgrade patch. To use ASD, the satellite must be connected to cisco.com to complete the upgrade process.

Using ASD also lets you bypass the End User License Agreement (EULA) acceptance step that is required when you download the upgrade from cisco.com. It only provides the message to inform you that you are bound by the EULA.

Note: ASD will not upgrade satellite between major versions.

To proceed with the network upgrade, see Using the Network Upgrade on page 4.

Using the Network Upgrade

Note: This feature has been deprecated effective Jun, 2017.

When a patch is available, use the following procedure:

Procedure

1. Log in to the Cisco Smart Software Manager satellite and click the **Administration** button.
2. Click the **Upgrade** tab.
3. Under Network Upgrade, click **Check for Upgrade Now**.

- If your satellite has the current version, Cisco Smart Software Manager satellite displays a message that no new version is available.
- If a newer version is available, that version number is shown and you can click **View Release Notes** to review information about this update.

4. Click **Upgrade Now**.
   The system downloads the patch and initiates the upgrade.
   - The download can take up to ten minutes depending on the size of the patch file and the speed of the Internet connection.
   - The system displays the download progress and when that is complete, informs you of the upgrade status.
   - The satellite is automatically restarted at the end of the upgrade process. If the upgrade fails, you can click **View Error Logs** for more information.

   Note: If you need to cancel the upgrade, you can click **Cancel**, but only during the download process. After the upgrade begins, you cannot abort the process.

5. When the upgrade process completes, follow Steps 1 through 3 to verify that the latest version is installed.

Scheduling Network Upgrades

***Note:* This feature has been deprecated effective Jun, 2017**

When a patch is available and you use the network upgrade schedule feature, you choose:

- How often you want Cisco Smart Software Manager satellite to check for updates
- What actions you want Cisco Smart Software Manager satellite to take when a new version is available.

Follow these steps to schedule and configure your network updates:

Procedure

1. Log in to the Cisco Smart Software Manager satellite and click the **Administration** button.
2. Click the **Upgrade** tab.
3. Click the option, **Automatically check for available upgrades**.
4. Use the drop-down menus for Frequency, Time, and Day of Week to configure when and how often you want Cisco Smart Software Manager satellite to check for updates.
5. Click the **If Upgrade Available** drop-down menu to choose an installation method option:
   - **Display Alert Message.** This option displays an alert message that allows you to dismiss it or perform a network upgrade. For information on using the manual upgrade process, see Using the Network Upgrade on page 34
   - **Display Alert and Download Upgrade.** This option automatically downloads a patch file and alerts you after the download completes. However, you can dismiss the alert and perform the upgrade when you want. When you are ready to upgrade, follow the instructions in Using the Network Upgrade on page 34. To begin the upgrade, you click **Upgrade Now**.
   - **Display Alert, Download, and Upgrade.** This option automatically downloads and installs a new upgrade. A message alerts you of a successful upgrade. If the upgrade fails, you can click **View Error Log** to check for the cause.

   Note: All of the installation method options offer a link to the Release Notes within the alert message.

6. Click **Save** to save your changes.

   Note: If you choose the monthly schedule option and the 29th does not exist for that month, the scheduled action rolls over to the next month.

Using the Manual Upgrade

The manual upgrade option is not part of the ASD feature, but is included in the user interface, alongside the ASD options. The manual upgrade allows you to view available satellite patch downloads from cisco.com, but requires that you manually initiate the upgrade, yourself.

Procedure

1. Under the **Manual Upgrade** heading, click **View Available Downloads**, which directs you to the cisco.com satellite download page for the latest release.
2. Download the patch file directly from cisco.com.
3. Select **Choose File** and the patch file you downloaded to your PC from the previous step.
4. Click **Upload** to put it to the satellite.
5. Click **Upgrade Now** to complete the upgrade process.

   After the upgrade completes, you are directed to the satellite login page.

Satellite upgrade procedures varies from release to release. Please refer to the specific install notes for the version or release you are interested in.

Device-Led Conversion Support

A product that utilizes classic licensing mechanism through SWIFT today is undergoing a technology change when moving to Smart Licensing, and the way images and features are enabled is handled differently. In Smart Licensing, PAKs, RTU, and license files have been replaced with entitlements or licenses for simpler operations. Rather than looking for a file or key on the device to enable an image or feature, the device or product instance will simply report license usage to Cisco Smart Software Manager (CSSM) or Smart Software Manager satellite for an entitlement or license that corresponds to the entitlement tag the image or feature is trying to enable.

When a customer upgrades from one version of a product using classic licensing to the next version of the product using Smart Licensing, the device or product instance will now need to have entitlements available in CSSM rather than the license keys or files it had before. There are various ways to make entitlements available in CSSM:

1. Customers order smart enabled SKUs which in turn deliver entitlements (licenses) to CSSM.
2. Customers migrate existing classic licenses from SWIFT to CSSM using License Registration Portal (LRP) or CSSM.

Yet, the above method of making entitlements available in CSSM still does not address all conversions of classic licenses to smart in that many classic licenses use RTU, which are not in the SWIFT database for the conversion to take place on LRP or CSSM portals. The only record of purchases/entitlements is in the device itself.

As a result, we must have some mechanism that converts existing classic licenses and entitlements into the Smart Licensing entitlements, which can only be initiated from the device/product instance. Device-Led Conversion (DLC) allows the device/product instance to initiate the conversion of classic licenses to Smart Licenses so that the entitlement can be reflected in CSSM. Products must be upgraded to a DLC-enabled version, connected to a DLC-enabled CSSM or satellite for this feature to work.

DLC can only occur once if successful. That is, once a license has been converted and deposited in the Virtual Account (where the device registers) as a Smart-enabled license, CSSM will invalidate the corresponding classic license from the backend database and does not allow the device to initiate the conversion again. Upon trying, the device receives “License Already Converted” status. The device itself remembers the status of the conversion across reboots and registrations and will only do one automatic conversion.

DLC is initiated by devices connected to CSSM or satellite. Prior to a conversion request from the device, a Smart Account administrator needs to configure which Virtual Accounts are allowed or disallowed for license conversion. On CSSM, use the following procedure:

1. Navigate to **License Conversion**, **Conversion Settings** tab
2. Select the radio button to Enable DLC on all Virtual Accounts, some Virtual Accounts, or disable it on all Virtual Accounts.
3. Press **Save**.
4. If it’s disable, user will get an error message
5. The default is “Enable”

Conversion Workflow

For device registered to satellite, following is a high level workflow:

1. Device either automatically or manually initiates a migration after a successful registration

   a. Migration can be initiated automatically as part of registration via the command `license smart conversion automatic`, or
   b. A manual "`license smart conversion start`" command needs to be entered on the device to start the conversion.
2. Satellite receives one or multiple migration requests from one or multiple devices. It validates that the request comes from a registered device.
3. Satellite display an alert that the user should initiate a sync due to DLC request(s)
4. Satellite responds to the device and tells it to poll back in 1 hour (3600 seconds).
5. Satellite saves the conversion data so it can send to CSSM on the next synchronization.
6. Satellite passes the encoded conversion data to CSSM in the next sync (network, scheduled, or manual).
7. Satellite waits for a response from CSSM via the next sync (success or failure with a reason)
8. When device polls satellite for status, it will respond with the appropriate response (poll-me-later, agent-not-registered, migrate-success, migrate-failed, invalid message type)
9. Satellite keeps track of device conversion results and provides a report on its UI so users can know the status of the DLC requests/results.

Conversion Reporting

To see a report of the conversion, use the following procedures:
Step 1: Go To **Administration** tab
Step 2: Select **Conversion History**
Step 3: You can see the report showing Product Instance Name, Product Family, Conversion Status, and the Time of Conversion.

As the status changes (e.g., pending to success or failure), the report is updated.

Backup/Restore and Conversion Results

1. When a conversion request is initiated by the device and the license conversion data from the device has been sent to satellite. However, the user performs a satellite database restore to a time before the satellite receiving this information. When the device tries to poll again for status, satellite will return an error since it has no knowledge of the license conversion due to the restore operation. The device automatically retries the conversion.
2. If the device initiates a conversion and it is no longer registered (either as a direct result of a de-registration or a satellite database restore operation before the result comes back. Depending on when the satellite was restored to:
   a. If satellite is restored to before the DLC request, then it wouldn't have knowledge of this request and the device needs to retry the DLC request.
   b. If the satellite is restored to before the device registration, it has no knowledge of the device, so the device needs to re-register and retry the DLC request.
3. The device initiates a conversion, satellite sends the conversion data to CSSM, receives the conversion successful results, and notifies the device. If the satellite is restored to a point before the sync was started but after satellite receives the conversion data from the device, which means it thinks the request is pending. Satellite will send the DLC request and license data in the next sync with CSSM and when it receives a "ALREADY CONVERTED, it will update the UI report accordingly. The device doesn't have to do anything because it has already received its successful status.

Backward Compatibility

Before the satellite can accept registrations from product instances, it has to register with CSSM. Previously, satellite to CSSM registration requires a 48-hour wait because someone has to manually sign the Certificate Signing Request (CSR) from satellite to CSSM. This means that if products want to connect to satellite, it has to wait 48 hours for satellite to be fully registered and functional.

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

In the new implementation, smart agents, satellite and CSSM must exchange a new message type to know if it supports a 3-tier or 4-tier certificate. Products that have not implemented the latest smart agent code (1.4+) needing to register with satellite will need to wait 48-hour as satellite needs to get the 3-tier certificate from CSSM before it can register the product. Product teams can decide to

implement Smart Agent code 1.4+ at their own schedules, so we don't always know what version of Smart Agent they embed. At the time of this writing, these 3-tier products are ASAv, FMC, vCUSP, CBR8, and 5921. To know what version of the Smart Agent, simply issue the command "`license smart status`".

We have the following cases:

Devices with new Smart Agent registering to the latest satellite release

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

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

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

Devices with old Smart Agent registering to the latest satellite release

When you install the latest satellite release, its registration with Cisco Smart Software Manager is instantaneous. During this process, the satellite also requests a previous three-tier certificate. When devices with older Smart Agent registers with the satellite, you get a registration failure message that informs you to wait 2 business days (48 hours) and perform a network or manual synchronization to get the backward compatible (three-tier) certificate and re-register. Afterwards, these devices can successfully register to the satellite.

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

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

  ```
  Compatibility Error: The satellite is not currently compatible with the Smart
  Licensing Agent version on this product. If it has been 48 hours since the satellite
  was registered, synchronize the satellite with Cisco's licensing servers to enable
  compatibility with older agent versions and then try the registration again.
  ```

- User waits for 2 business days
- User runs an on-demand network or manual sync between satellite and Cisco SSM.
- User re-registers the product instance to satellite.

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

```
Version Compatibility Note — Temporarily, this satellite will only be able to register
Product Instances that are using the Smart Licensing Agent version 1.5 or later (use the
"show license" commands on the Product Instance to see the agent version). To enable
registration of Product Instances using older versions of the agent, wait two business
days after the satellite's initial registration and then synchronize the satellite.
```

This means that after 2 business days, the three-tier certificate will be obtained by satellite from Cisco SSM during the sync to support three-tier smart agents.

Troubleshooting

Client Registration Issues

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

- Ensure that the satellite configuration is correct.

  Please refer to the **Network** tab under **Administration** pane in the Smart Software Manager satellite User Guide http://www.cisco.com/web/ordering/smart-software-manager/index.html.

- Verify that the Call-Home configuration on the client points to the satellite.

  Please refer to the section *"Sample of SCH Profile to Use Smart Software Manager satellite on the Cloud Service Router*" in the *Smart Software Manager satellite Installation Guide*

- Verify the token has been generated from the satellite.

  Please refer to Creating a Product Instance Registration Token on page 20.

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

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

Manual Synchronization Issues

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

- Verify the time on the satellite is correct.

  Please refer to the section *"Verifying Time Sync with the NTP"* in the *Smart Software Manager satellite Installation Guide*, available at http://www.cisco.com/web/ordering/smart-software-manager/index.html.

- Ensure port 443 (HTTPS) is allowed through your firewall.
- Verify the licenses in the associated virtual account.
- Make sure that you are uploading and downloading the YAML (request and response) files to the correct satellite. You can do this by verifying that the file names include the name of the satellite that you are synchronizing.

- You may be requested to re-perform a full manual synchronization after a standard manual synchronization as explained previously.

Network Synchronization Issues

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

- Ensure port 443 (HTTPS) is allowed through your firewall.
  - tools.cisco.com ports 443
  - api.cisco.com ports 443
- Verify that the satellite can reach the configured DNS server.
- Verify that the satellite can reach cisco.com.
- Verify that the time on the satellite is correct.

  Please refer the section *"Verifying Time Sync with the NTP"* in the *Smart Software Manager satellite Installation Guide*, available at http://www.cisco.com/web/ordering/smart-software-manager/index.html.
- Verify the associated Virtual Account has the expected licenses

Replacing a Failed Node in The HA Cluster

In the event one the nodes of the HA cluster goes down and it is an irrecoverable failure, it is possible to replace the failed with a new node using a prior snapshot or clone of a satellite HA node. It is recommended you create a snapshot or clone of both the Active (Node-1) and Standby (Node-2) OVAs

Recovery of Node-1 using a Clone of the Node-1 OVA

1. Select the correct snapshot or cloned OVA your created earlier that corresponds to the node you wish to replace.
2. Ensure the OVA is NOT connected to the network
3. Ensure the replacement OVA has the same IP, DNS, NTP, and hostname settings as the failed Node-1.
4. The node needs to be disconnected from network.
5. Login to the shell of Node-1 and check the pacemaker stratus using the "`pcs status`" command
6. Wait until the output of "pcs status" becomes like below:
   ```
   - virtual_ip          Stopped
   - tomcat              Stopped
   - zabbix_server       Stopped
   - httpd_service       Stopped
   ```
7. Stop the following system services using the following commands:
   ```
   [satellite-node-01 ~]# pcs cluster stop [ip addresd of Node-1]
   ```
8. Confirm the following services are stopped
   ```
   [satellite-node-01 ~]# systemctl status mysql
   [satellite-node-01 ~]# systemctl status tomcat
   [satellite-node-01 ~]# systemctl status drbd
   ```
9. On Node-1, start the DRBD synchronization service
   ```
   [satellite-node-01 ~]# systemctl start drbd
   [satellite-node-01 ~]# drbdadm secondary drbd1
   ```
10. Connect Node-1 to the network.
11. Verify Node-1 has become the standby satellite using the command "`drbd-overview`"

```
[satellite-node-01 ~]# drbd-overview
1:drbd1/0  Connected Secondary/Primary UpToDate/UpToDate
```

12. If you observe errors with the DRBD disk replication Node-1 you will need to perform the additional steps,

```
[satellite-node-01 ~]# drbdadm detach drbd1
[satellite-node-01 ~]# drbdadm create-md drbd1
[satellite-node-01 ~]# drbdadm attach drbd1
[satellite-node-01 ~]# drbdadm -- --discard-my-data connect drbd1
[satellite-node-01 ~]# drbdadm connect drbd1
```

    Check to ensure DRBD sync completes before proceeding

13. On Node-2 issue the following command

```
[satellite-node-02 ~]# pcs cluster stop –all
```

14. On to Node-1 issue the following commands

```
[satellite-node-01 ~]#  drbdadm primary drbd1
[satellite-node-01 ~]#  pcs cluster start –all
```

15. On Node-1, verify the status of pcs shows the resources are associated with “satellite-node-01” using the command

```
[satellite-node-01 ~]#  pcs status
```

16. The procedure is now complete

Recovery of Node-2 using a Clone of the Node-2 OVA

1. Select the correct snapshot or cloned OVA your created earlier that corresponds to the node you wish to replace.
2. Ensure the replacement OVA has the same IP, DNS, NTP, and hostname settings as the failed Node-1.
3. On Node-1, check DRBD synchronization using the command "`drbd-overview`" command

```
[satellite-node-01 ~]# drbd-overview
 1:drbd1/0  SyncSource Primary/Secondary UpToDate/Inconsistent
/shared/drbd/mysql xfs 122G 641M 121G 1%
[================>...] sync'ed: 85.0% (26248/163512)K
[satellite-node-01 ~]# drbd-overview
 1:drbd1/0  Connected Primary/Secondary UpToDate/UpToDate /shared/drbd/mysql
xfs 122G 641M 121G 1%
```

4. Once DRBD synchronization completes, restart the HA cluster on Node-1 using thhe using he following commands:

```
[satellite-node-01 ~]#  pcs cluster stop --all
[satellite-node-01 ~]#  pcs cluster start –all
```

5. The procedure is now complete

Note: You maybe experience a short outage as the cluster is performing the restart, this is normal.

Recovery of a Node when no backup is available

1. Obtain an OVA from CCO that matches the version of the failed node
2. Deploy the replacement OVA
3. Configure the replacement OVA has the same IP, DNS, NTP, and hostname settings as the failed node
4. Copy the files from the surviving node (node not being replaced) using the commands:

```
scp –r <ip address of surviving node>:/etc/drbd.d/drbd1.res  /etc/drbd.d/drbd1.res
scp -r <ip address of surviving node>:/etc/corosync/corosync.conf
/etc/corosync/corosync.conf
```

5. On the surviving node, issue the command

```
pcs cluster auth <IP address of the new node> -u hacluster -p 37HRv[wkYp?T
```

6. On the new node execute the following commands

```
systemctl start drbd
```

7. On the new node verify it has become the secondary using the "`drbd-overview`" command:

```
# drbd-overview
1:drbd1/0  Connected Secondary/Primary UpToDate/UpToDate
```

8. If you observe errors with the DRBD disk replication `Node-1` you will need to perform the additional steps

```
# drbdadm detach drbd1
# drbdadm create-md drbd1
# drbdadm attach drbd1
# drbdadm -- --discard-my-data connect drbd1
# drbdadm connect drbd1
```

   Check to ensure DRBD sync completes before proceeding
9. On the surviving node, execute the following commands

```
pcs cluster stop –all
```

10. If the new node is replacing satlite-node-01, then issue the following commands

```
#  drbdadm primary drbd1
```

11. On to new node and issue the following commands

```
#  pcs cluster start –all
```

12. On the surviving node, retart the cluster with the new node using the command

```
#  pcs cluster start --all
```

13. The procedure is now complete

Note: The satellite HA cluster is still accessible while DRBD is replicating the data to new OVA from surviving node. This process can take a significant amount of time. Failover to the newly added node can be done only when synchronization is complete. Synchronization can be check using the procedure outlined in section "Verifying the satellite HA synchronization".

Managing the satellite HA cluster

Restarting the Pacemaker Service

Sometimes Pacemaker is not starting all the resource properly when the active node comes back online. If any functional issues are seen, run below commands

- `pcs cluster stop --all`
- `pcs cluster start -all`

Verifying the Pacemaker Service

The Pacemaker services can be verify using the "`pcs status`" command as follows

```
[satellite-node-01 ~]# pcs status
Cluster name: ha_cluster
WARNING: corosync and pacemaker node names do not match (IPs used in setup?)
Stack: corosync
Current DC: satellite-node-02 (version 1.1.15-11.el7_3.2-e174ec8) - partition with
quorum
Last updated: Tue Jan 17 10:48:01 2017          Last change: Tue Jan 17 10:16:58 2017
by hacluster via crmd on satellite-node-01

2 nodes and 8 resources configured

Online: [ satellite-node-01 satellite-node-02 ]

Full list of resources:

virtual_ip     (ocf::heartbeat:IPaddr2):       Started satellite-node-01
tomcat (ocf::heartbeat:tomcat):        Started satellite-node-01
mysql_service  (ocf::heartbeat:mysql): Started satellite-node-01
zabbix_server  (systemd:zabbix-server):        Started satellite-node-01
httpd_service  (ocf::heartbeat:apache):        Started satellite-node-01
Master/Slave Set: mysql_clone_data [mysql_data]
     Masters: [ satellite-node-01 ]
     Slaves: [ satellite-node-02 ]
mysql_fs       (ocf::heartbeat:Filesystem):    Started satellite-node-01
Daemon Status:
  corosync: active/enabled
pacemaker: active/enabled
  pcsd: active/enabled
```

Verifying the satellite HA synchronization

The synchronization status of the satellite HA cluster can be verified the "`drbd-overview`" command.

Example of the cluster synchronized:

```
[satellite-node-01 ~]# drbd-overview
1:drbd1/0  Connected Secondary/Primary UpToDate/UpToDate
```

Example of the cluster not synchronized

```
[satellite-node-01 ~]# drbd-overview
1:drbd1/0  SyncTarget Secondary/Primary Inconsistent/UpToDate
        [>....................] sync'ed:  0.1% (124472/124548)M
```

Appendix

Registering Product Instances to satellite

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

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

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

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

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

Procedure

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

   Note: CiscoTAC-1 is the default profile.

6. Choose **destination transport http** or **destination transport https**.
   Sets the transport to HTTP or HTTPS. Additionally, depending on your choice, use either example a (for HTTP) or example b (for HTTPS) below.
   a) For **destination address http** use *http from TG*.
   Accesses the SCH Transport Gateway URL.

   Note: The destination URL is http://<*ip-address*>:80/Transportgateway/services/DeviceRequestHandler.

   b) For **destination address https** use *https from TG*.

   Accesses the SCH Transport Gateway URL.

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

If you are in a CSPC environment and have configured NAT in PfSense, use the destination port number in the PfSense configuration for product registration to satellite. For example, if you configure port 7443 for satellite product instance registration, then the transport configuration is as below:

The destination URL is https://<*ip-address*>:7443/Transportgateway/services/DeviceRequestHandler

7. **active**
   Activates the profile specified in step 5.
8. **exit**
   Saves and exits the current configuration mode and returns to privileged EXEC mode.
9. **end**
   Returns to privileged EXEC mode.
10. **wr**

    Saves the configuration.
    The following configuration is only a sample for CSR for HTTP. Please see platform specific configurations for the call-home profile config.

    Example:

```
Router#configure terminal
Router(config)#call-home
Router(cfg-call-home)#contact-email-addr aaa@cisco.com
Router(cfg-call-home)#profile  CiscoTAC-1
Router(cfg-call-home-profile)#active
Router(cfg-call-home-profile)#destination transport-method  http
Router(cfg-call-home-profile)#no destination transport-method  email
Router(cfg-call-home-profile)#destination address http
Router (cfg-call-home-
profile)#http://172.19.76.177:80/Transportgateway/services/DeviceRequestHandler
```

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

    Example:

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

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

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

    Add the URL for satellite and the following command:

```
revocation-check none
```