# Upgrade HCM-F



# Before You Upgrade

Consider these pointers before you upgrade the Hosted Collaboration Media Fulfillment to the latest version:

- Ensure that you have a valid DRF backup of your HCM-F Cluster.

  **Note** Cisco does not support and cannot guarantee that a VMware snapshot can be used to successfully restore Cisco Hosted Collaboration Media Fulfillment application. If you cannot restore the application from a snapshot, your only recourse is to reinstall older version of the Hosted Collaboration Media Fulfillment application and restore using the DRF backup.

- Check the network connectivity.
- Ensure to stop all the sync services.
- Ensure that there are no expired certificates including the trust certificates for the services.

  To list all certificates, run the **show cert list own** and run the **show cert list trust** commands.

  To verify if the own certificates are valid, run the **show cert own <cert name>** command through the CLI on the Cisco HCM-F platform. Check the validity field for the certificate validity information. For example: **show cert own tomcat/tomcat.pem**.

  To check if the trust certificates are valid, run the **show cert trust <filename>** command.

  Based on the certificate issuer, you can regenerate the certificates. To regenerate the self-signed certificate, use the **set cert regen <name>** command. For CA signed certificate, generate CSR using the **set csr gen**

**<name>** command, get it signed by a CA and upload the certificates using the **set cert import <name>** command.

The following are examples of the system security certificates that you can regenerate.

Own Certificates

- tomcat
- ipsec
- tomcat-ECDSA
- ITLRecovery
- authz

# Upgrade Overview

The following Cisco HCM-F upgrade paths are supported:

- 11.5(x) to 12.5(1) and later Service Update releases
- 10.6(x) to 12.5(1) and later Service Update releases

Before you begin to upgrade from 11.5(1) release to 11.5(4)SU1 or 12.5(1), it is mandatory to install the `hcs.CSCvb86072-1-1151patch.cop` file on HCMF.

Upgrade the Cisco HCM-F Application Node before upgrading any Cisco HCM-F Web Services Nodes.

Before you begin the upgrade process, obtain the appropriate upgrade file using one of the following methods:

- Use the Product Upgrade Tool (PUT). To use the PUT, navigate to https://tools.cisco.com/gct/Upgrade/jsp/index.jsp. Enter your Cisco contract number (Smartnet, SASU or ESW) and request the DVD set.
- Purchase the upgrade from Cisco Sales if you don't have a contract for Cisco HCS.

In general, perform the following tasks to upgrade Cisco HCM-F:

- Upgrade Cisco HCM-F
- Validate the Cisco HCM-F Upgrade
- Update the HCM-F Version in Cisco Unified CDM
- Update the Guest operating System

# Upgrade Cisco HCM-F

Before upgrading an HCM-F cluster containing an Application Node, perform the following tasks:

1. Ensure that you have a valid DRF backup of your HCM-F Cluster.
2. On the Application Node CLI, run **show hcs cluster nodes**.

3. On the Application Node CLI, run **show hcs cluster verify detailed**.
4. Cisco HCM-F 12.5(1) SU2 and later releases do not support the WS node. Therefore, if the configuration includes both Application Node and WS node, run **delete hcs cluster node** *WS node host name* to remove the WS node, and then proceed with the upgrade of the application node.
5. If you use Prime Collaboration Assurance, review and perform the task (Enabling HCM-F and Prime Collaboration Assurance to Communicate) in the *Cisco Hosted Collaboration Solution Install Guide* if necessary. The *Cisco Hosted Collaboration Solution Install Guide* is available at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html.

**Note**

- If Cisco HCM-F 10.6(3) SU1 was previously installed, skip to Upgrade a Multinode Environment.
- If you are running RTMT and monitoring performance counters during a Cisco HCM-F upgrade, the performance counters are not updated during and after the upgrade. To continue accurate monitoring of performance counters after the upgrade is finished, either reload the RTMT configuration profile or restart RTMT.

Use this procedure to upgrade a Cisco HCM-F Application Node.

### Procedure

**Step 1** Obtain the upgrade media to upgrade the Cisco HCM-F platform.

If you downloaded the software executable from Cisco.com, do one of the following:

- Prepare to upgrade from a local folder:
  a. Copy the Cisco HCM-F upgrade file to a temporary folder on your local hard drive.
  b. Open an SFTP client and connect to the Cisco HCM-F server using the adminsftp user ID and password that you set up during installation.
  c. Navigate to the upgrade folder by entering **cd upgrade**.
  d. Type **put** <*upgrade filename*> to transfer the file.
- Prepare to load an ISO file:
  a. Copy the Cisco HCM-F upgrade ISO to a data store accessible by the virtual machine.
  b. Attach the ISO image to the virtual machine's DVD drive.
- Put the upgrade file on an FTP or SFTP server that the server that you are upgrading can access. Copy the contents of the upgrade disk or downloaded upgrade files to the remote server. Make sure that the Cisco HCM-F upgrade file filename begins with HCS.

**Step 2** On the virtual machine that you are upgrading, log in to the Cisco HCM-F CLI and enter **utils system upgrade initiate**.

**Step 3** Choose the source from which you want to upgrade:

- 1—Remote Filesystem using SFTP
- 2—Remote Filesystem using FTP
- 3—Local DVD
- 4—Local Upload Directory

**Step 4** Follow the system prompts for the upgrade option that you chose.

**Step 5** The system prompts you when the upgrade process is complete. If you did not choose to automatically switch versions, enter **utils system switch-version**. Then enter **yes** to confirm that you want to reboot the server and switch to the new software version.

**Step 6** After the upgrade completes, log in to the Cisco HCM-F CLI.

- Enter **show version active** to verify that the current version is the upgraded version.
- Post HCM-F upgrade, change the users password for the GUI access.

**Step 7** After the upgrade, when you perform SDR synchronization to populate the servers, perform the VCenterSync operation. See Sync Servers from SDR. Ensure that the cluster applications are associated with the correct virtual machines.

**Step 8** Perform this step if you used the **utils system switch-version** command in Step 5, on page 4.

**Step 9** From the HCM-F CLI, run the **utils service list** command to view the services. Run the **utils service start** *service_name* command to restart any services that were stopped before the upgrade.

# Changes After Upgrade

This section describes the changes after you upgrade Cisco HCM-F 12.5(1) SU2.

## Feature Enhancements

This section describes the changes after you upgrade to Cisco HCM-F 12.5(1) SU2.

### Certificate Management

You can download the certificate status across all the customers and clusters at the provider level using the **Download Certificate Status** option. From the **Infrastructure Manager** tab, select **Service Provider Toolkit > Certificate Management > UC Applications**, and then click **Download Certificate Status**. See Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide for details.

### Onboarding Expressway for Smart Licensing

Cisco HCM-F 12.5(1) SU2 enables Smart Licensing support for Expressway X 12.6 version and later. The HCM-F user interface supports onboarding of the Expressway E and C clusters that are configured with Smart Licensing mode.

See Cluster Summary section in the Cisco Hosted Collaboration Solution Smart Licensing Guide and Add Cluster section in the Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide for detailed information.

### Prime Collaboration Assurance

The Cisco Collaboration Systems Release (CSR) 12.5 SU1release onwards only supports SHA protocol for SNMP V3 in UC applications. To align with CSR and enhance security in HCM-F 12.5.1(SU2) and later release, the default authentication protocol that is supported for UC applications and Expressway clusters is SHA for SNMP V3 configuration.

See the Role of Fulfillment Service in Domain Manager Configuration section Cisco Hosted Collaboration Mediation Fulfillment Maintain and Operate Guide for details.

### Flex Usage Report

#### Support for Shared Architecture

The Flex report is enhanced to segregate the shared customers license usage for Flex & Perpetual license usage.

The Flex Usage report displays the consumption of all subscribers with their associated devices for the shared customer in a separate row when you follow the following configuration guidelines:

1. Specify the customer's domain as **`Customer Extended Name`** in the HCM-F user interface.
2. Save the subscriber's **userID** or **mailID** to include the customer's domain name in Cisco Unified Communications Manager or Cisco Unity Connection.
3. Associate the **Devices** with the **DevicePoolName**. Ensure the name contains the domain name of the customer that is used in Cisco Unified Communications Manager or Cisco Unity Connection.

**Note** When customers share the same cluster but either **Subscribers** or **Devices** are not configured as per the guidelines, the report displays the consumption of all subscribers and the associated devices for each of the shared customers in a single row.

#### For Shared Architecture and Dedicated Instance

The Flex Usage Report is enhanced to include these two fields

- **UC app version**- Displays the version of the UC application cluster that is associated to the customer.
- **Operational License count**- Displays the count of licenses that are installed on the Virtual Account.

See the Flex Usage Report section in the Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide for details.

#### SI Report Enhancements

Service Inventory reports are now supported for Shared Architecture deployments.

You can download the Service Inventory report in both CSV and excel formats. See the Cisco Hosted Collaboration Mediation Fulfillment Maintain and Operate Guide for details.

### Cisco HCM-F Services

The CHPA and UCPA functionality to communicate with UC Applications and Expressway is replaced with CAA services. The following table describes the services that are replaced in this release:

| Cisco HCM-F 12.5(1) and earlier releases | Cisco HCM-F 12.5(1) SU2 and later releases |
|---|---|
| Cisco HCS Provisioning Adapter Service | Cisco HCS CAA CUCM Service<br>Cisco HCS CAA IMP Service |
| UCPA Service | Cisco HCS CAA UCXN Service<br>Cisco HCS CAA CER Service<br>Cisco HCS CAA EXPRESSWAY Service |

### Error Codes

There are a few error codes that are modified based on the changes in the Cisco HCM-F services. Refer to Cisco Hosted Collaboration Mediation Fulfillment Troubleshooting Guide for details.

## Deprecated Features

The following are the deprecated features in Cisco HCM-F:

- Infrastructure Provisioning Adapter (IPA)
- HCS Intelligent Loader (HIL)
- Web Services (WS) Node
- API Gateway

**Note** The API gateway is deprecated as it runs on the WS node.

### Cisco HCM-F User Interface

- **Node Manager**- The Node Manager tab is removed from the Cisco HCM-F interface.
- **Default Credentials**- The following equipment is removed from **Equipment Type** drop-down list (**Infrastructure Manager > Administration > Default Credentials)**:
  - CUOM
  - CCDM
  - CUCDM 8.1.x
  - CUSM
  - vCenter
- **Platform Manager**- The following options are removed from the Platform Manager interface:
  - From the **Tasks** menu
    - Create an Install/Upgrade Task
    - Create a Switch-Version Task

- Create a Restart System Task
- Task List

- **File Servers** from the **Inventory** menu

**Note**

- It is recommended to use Prime Collaboration Deployment for platform management functions, such as installation, upgrade, and restart.
- There is no change with the backup and restore functionality.

### Command Line Interface

The following commands are not supported from this release:

- **set hcs ipa require-vcenter-certificate**
- **set hcs hil target apiversion**
- **set hcs hil target config**
- **set hcs hil target timeout**
- **set hcs cluster node**
- **show hcs hil target apiversion**
- **show hcs hil target config**
- **show hcs hil target timeout**
- **show hcs cluster nodes**
- **show hcs cluster verify**
- **show hcs ipa require-vcenter-certificate**
- **show hcs api gateway proxy***
- **set hcs api gateway proxy***
- **delete hcs cluster node**
- **utils diagnose hcs agp**
- **utils hcs api gateway proxy***

# Update the HCM-F Version in Cisco Unified CDM

After you upgrade Cisco HCM-F, update the version of HCM-F in Cisco Unified Communications Domain Manager (Unified CDM). Updating the version involves the Unified CDM user interface and the Unified CDM command-line interface.

**Note** Cisco HCM-F will deprecate the support of Cisco Unified Communications Domain Manager in the upcoming releases with limited support for existing integration, Cisco HCS partners and customers are advised to take necessary steps to align their requirements.

1. Take the following steps in the Unified CDM interface.
   a. Log in to Unified CDM as hcsadmin.
   b. Navigate to **Device Management** > **HCM-F**.
   c. Select the HCM-F device.
   d. In the **HCM-F Version** field, select the release version.
   e. Click **Save**.
2. In the Unified CDM command-line interface, run the following command: **app start voss-deviceapi**.

**Important** The command enables the **Server Type** field on the Base tab. The field is required when you add a UC application, such as Cisco Unified Communications Manager, or when you upgrade a UC application. The command also displays the **Version** field on the Publisher tab. If you do not run the command after you upgrade HCM-F, you cannot then add or update UC applications.

# Update the Guest Operating System

After completing the upgrade and verifying that the cluster has upgraded, update the Guest Operating System on the VMs. Perform the following procedure for each node in the cluster.

### Procedure

**Step 1** From the CLI, run the **utils system shutdown** command.
**Step 2** Access the vSphere client and verify that the VM is powered off.
**Step 3** Select the VM and click **Edit virtual machine settings**.
**Step 4** In the Virtual Machine Properties window, click the **Options** tab.
**Step 5** For Guest Operating System Version, select **Red Hat Enterprise Linux 6 (64-bit)**.
**Step 6** Click **OK**.
**Step 7** Power on the VM.

# Migrating from Cisco Unified Operations Manager to Cisco Prime Collaboration Assurance

You can migrate the monitoring application from Cisco Unified Operations Manager to Cisco Prime Collaboration Assurance. Use the Migration Utility Tool from the CLI, or use the Infrastructure Manager user interface within Cisco HCM-F.

## Migrate Using the Migration Utility Tool

Use this procedure to migrate one instance of Cisco Unified Operations Manager to one instance of Cisco Prime Collaboration Assurance.

**Procedure**

**Step 1** Enable the Cisco HCS DMA-SA Service. From the CLI, run the **utils service activate Cisco HCS DMA-SA Service** command.

**Step 2** Define the Cisco Prime Collaboration Assurance application in Cisco HCM-F.

a) From the Infrastructure Manager interface, select **Application Management** > **Management Application**.
b) Click **Add New**.
c) In the Application Type field, select **Prime Collaboration**.
d) Enter a name in the Name field.
e) (Optional). Provide a description and select the virtual machine.
f) Click **Save**.
g) Open **Credentials** and click **Add New**. Specify credentials for **ADMIN** and **SFTP** Credential Types.
h) Open **Network Addresses** and click **Add New**. Select **Service Provider Space** as the Network Space and specify the IP address, hostname, and domain of the HCM-F server.
i) Click **Save**.

**Step 3** From the CLI, run the **utils migrate cuom_to_primecollab** command.

**Step 4** Provide the names of the Cisco Unified Operations Manager and Cisco Prime Collaboration Assurance when prompted.

## Migrate Using the Infrastructure Manager User Interface

Use the Infrastructure Manager user interface to change the monitoring application from Cisco Unified Operations Manager to Cisco Prime Collaboration Assurance.

**Note** The Cisco Prime Collaboration Assurance specified for a Customer monitors the Customer's clusters and equipment, unless overridden by a different Cisco Prime Collaboration Assurance specified at the cluster or equipment level. Cisco recommends that you have one instance of Cisco Prime Collaboration Assurance manage all devices and clusters belonging to a Customer. Therefore, steps 3 and 4 of the following procedure are not typically required.

### Procedure

**Step 1** Enable the Cisco HCS DMA-SA Service. From the CLI, run the **utils service activate Cisco HCS DMA-SA Service** command.

**Step 2** Define the Cisco Prime Collaboration Assurance application in Cisco HCM-F.

a) From the Infrastructure Manager interface, select **Application Management** > **Management Application**.
b) Click **Add New**.
c) In the Application Type field, select **Prime Collaboration**.
d) Enter a name in the Name field.
e) Optionally provide a description and select the virtual machine.
f) Click **Save**.
g) Open **Credentials** and click **Add New**. Specify credentials for ADMIN and SFTP credential types.
h) Open **Network Addresses** and click **Add New**. Select **Service Provider Space** as the Network Space and specify the IP address, hostname, and domain of the HCM-F server.
i) Click **Save**.

**Step 3** To update the Monitoring Application for a Customer:

**Note** To migrate all customers automatically, run the **set hcs link auto-primecollab-linkage enable** command from the CLI before performing steps a through e.

a) From the Infrastructure Manager interface, select **Customer Management** > **Customer**.
b) Click the customer you want to update.
c) In the Application Monitoring this Customer field, select your Cisco Prime Collaboration Assurance application.
d) Click **Save**.
e) To monitor data migration job status, select **Administration** > **Jobs**.

**Step 4** To update the Monitoring Application for Customer Equipment:

a) From the Infrastructure Manager interface, select **Customer Management** > **Customer** > **Customer Location** > **Customer Equipment**.
b) Click the customer equipment you want to update.
c) In the Application Monitoring this Customer Equipment field, select your Cisco Prime Collaboration Assurance application.
d) Click **Save**.

**Step 5** To update the Monitoring Application for a Cluster:

a) From the Infrastructure Manager interface, select **Cluster Management** > **Cluster**.
b) Click the cluster you want to update.
c) In the Application Monitoring this Cluster field, select your Cisco Prime Collaboration Assurance application.

d) Click **Save**.