Device Management

Create the HCM-F Device

When you create the HCM-F device, a data sync begins if there is a network connection and the NBI REST service is running on the HCM-F server.

Before You Begin

- Install and configure HCM-F. For more information, see *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide, Release 10.6(1)*.
- Verify that the NBI REST SDR Web Service is running:

1. Log in to HCM-F CLI as user admin.
2. Run the **utils service list** command. Verify that the Cisco HCS NBI REST SDR Web Service is running.
3. If not running, start it with the **utils service start Cisco HCS NBI REST SDR Web Service** command.

Procedure

Step 1 Log in to Cisco Unified Communications Domain Manager 10.x as hcsadmin@sys.hcs.

Step 2 Create a new HCM-F instance:

a) Select **Device Management** > **HCM-F** and click **Add**.
b) Enter the HCM-F Host Name.
c) Enter the HCM-F Admin Username.
d) Enter the HCM-F Admin Password.
e) Select the HCM-F Version from the drop-down list.

Note Once HCM-F Version is set to a new version, it cannot be changed to an older one.

f) Click **Save**.

Step 3 If the previous step fails:

- Verify HCM-F Hostname is correct
- Verify HCM-F Admin Username and Admin Password are correct
- Verify HCM-F Version is correct
- Verify the domain is set correctly via the Cisco Unified Communications Domain Manager 10.6(1) CLI:

1. `ssh platform@<cucdm hostname>`
2. **network domain**

Step 4 After a couple of minutes, verify that the initial sync between Cisco Unified Communications Domain Manager and HCM-F is successful:

a) Select **Provider Management** > **Advanced** > **SDR Service Provider**.
b) The sync is successful if the default entry, "Service Provider Name", appears.

What to Do Next

If the initial sync is still not working after following the above steps, verify the HCM-F REST API is working by browsing to the following URL: `http://<hcmf_app_node_host>/sdr/rest/<hcmf_version>/entity/ServiceProvider`. This should return the JSON representation of the pre-defined ServiceProvider instance in the HCM-F Shared Data Repository (SDR). If you get an error, log in as admin on the HCM-F app node CLI and verify the REST service is running:

To display the services, run the command: **utils service list**.

In the output, you should see `Cisco HCS NBI REST SDR Web Service[STARTED].`

If this service is not started, start it with the command: **utils service start Cisco HCS NBI REST SDR Web Service**

For data sync failures, try importing the new HCM-F:

1. Select **Device Management** > **HCM-F** and click on the HMC-F device.
2. Update the Hostname and click **Save**.

3 Import the new HCM-F:

   a Select **Device Management** > **Advanced** > **Perform Actions**.

   b In the Action field, select Import.

   c In the Device field select the HCM-F server.

   d Click **Save** and wait a few minutes.

4 Check the provider under **Provider Management** > **Advanced** > **SDR Service Provider**.

Cisco Unified Communications Manager Configuration in Cisco Unified CDM

Overview

Cisco Unified Communications Manager devices provide the core call processing capabilities for HCS, and are a critical part of the Cisco Unified Communications Domain Manager provisioning workflows. Cisco Unified Communications Manager devices must be configured before dial plan, user, subscriber, line, and phone configuration can be completed.

Cisco Unified Communications Manager devices can be dedicated to a specific customer, or they can be shared between multiple customers. Cisco Unified Communications Manager devices must then be assigned to one or more Network Device Lists (NDLs), and the NDL is then assigned to one or more sites. The NDL is used to select which Cisco Unified Communications Manager is used for configuration based on the site selected in the hierarchy context.

Shared versus Dedicated

To share the Cisco Unified Communications Manager across multiple customers, add the Cisco Unified Communications Manager at the Provider or Reseller level. To dedicate the Cisco Unified Communications Manager to a single customer, add the Cisco Unified Communications Manager at the Customer level.

When setting up Cisco Unified Communications Manager as a dedicated instance, you can opt to set up Cisco Unified Communications Manager after you create the customer.

Servers within a Cisco Unified Communications Manager Cluster

Within a Cisco Unified Communications Manager cluster, you can configure the following nodes:

- Cisco Unified Communications Manager Publisher
- Cisco Unified Communications Manager Subscriber
- IM and Presence Service Publisher
- IM and Presence Service Subscriber

You must configure a Cisco Unified Communications Manager Publisher node before configuring any other type node.

You must configure an IM and Presence Service Publisher node before configuring an IM and Presence Service Subscriber node.

Synchronization with Cisco Unified Communications Domain Manager 10.6(1)

Configuring a Cisco Unified Communications Manager device on Cisco Unified Communications Domain Manager 10.6(1) creates a scheduled data sync to import model data from the device into Cisco Unified Communications Domain Manager 10.6(1). The scheduled data sync ensures that the Cisco Unified Communications Domain Manager 10.6(1) cache maintains the most current view of the configured device. Any changes to the configuration occurring on the device, including additions, deletions, or modifications, will be reflected in Cisco Unified Communications Domain Manager 10.6(1) after the next data sync.

The data sync occurs once immediately upon creation. The recurring sync is scheduled to occur every 14 days, but is disabled by default. You can enable the sync and modify the schedule from **Device Management** > **CUCM** > **Schedules**. When determining the appropriate schedule setting, the frequency of the sync must be weighed against the additional processing and network activity associated with the data sync. You can also manually run the data sync at any time from **Device Management** > **Advanced** > **Perform Publisher Actions**, or from **Administration Tools** > **Data Sync**.

When you set up an IM and Presence Service server, Cisco Unified Communications Domain Manager 10.6(1) does not communicate directly with the IM and Presence Service server, but the information provided is pushed to HCM-F and Service Assurance for monitoring purposes.

The performance of a data sync can be improved by controlling the types of data that are synced. See Controlling a Data Sync with a Model Type List, on page 19 for more information.

Set up Cisco Unified Communications Manager Servers

Use this procedure to configure Unified CM servers within a Cisco Unified Communications Manager cluster.

Procedure

Step 1 Log in as the appropriate hierarchy administrator.
Only a provider or reseller administrator can create a shared instance. A customer, provider, or reseller administrator can create a dedicated instance.

Step 2 Set the hierarchy path to the correct level. Create a shared instance at the provider or reseller level. Create a dedicated instance at the customer level.

Step 3 Click **Device Management** > **CUCM** > **Servers**.

Step 4 Click **Add**.

Step 5 Enter the Cisco Unified Communications Manager server name in the CUCM Server Name field.

Note A Cisco Unified Communications Manager server that has been configured in HCM-F and synced into Cisco Unified Communications Domain Manager may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the **Migrate from HCM-F to CUCDM** checkbox is displayed. Click **Save** to migrate this server to the current hierarchy level. The fields will be populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.

Step 6 Select **Voice/Video** in the Server Type field.

Step 7 To configure a publisher node, check **Publisher**.
On the **Publisher** tab, you can specify the following information:

Field	Description
Prime Collab	Select the Prime Collaboration management application monitoring this cluster.
Call Processing ID	The Call Processing ID of this cluster

Field	Description
Cluster ID	The Cluster ID of this cluster.
Multi-Tenant	Read-only field. If creating at provider level, this field is set to Shared. If creating at customer level, this field is set to Dedicated.
Version	Select the version of the Cisco Unified Communications Manager Servers in this cluster. The available versions depend on the version of the HCM-F device that has been configured.
Port	The port on the Cisco Unified Communications Manager server to connect to. Default is 8443.
User Move Mode	Set to Automatic to apply Move Filters when users are synced from Cisco Unified Communications Manager. Set to Manual if you want an Administrator to manually move synced in users to a Site.
User Entitlement Profile	Select the Entitlement Profile that specifies which devices and services users synced from this Cisco Unified Communications Manager are entitled to. **Note** A violation of the Entitlement Profile does not prevent a user from being synced to Cisco Unified Communications Domain Manager 10.6(1) from Cisco Unified Communications Manager. However, subsequent updates to the user will fail until the user's configuration satisfies the restrictions set in the Entitlement Profile.

Step 8 For a Unified CM Publisher node, fill in the **Cluster Name** field with the name you want for this cluster. A new cluster is created with this name. This field is required.
For Unified CM Subscribers, select the Cisco Unified Communications Manager cluster from the **Cluster Name** drop down menu.

Step 9 Expand **Network Addresses**.

a) Select the SERVICE_PROVIDER_SPACE address space.
b) The Hostname field is automatically populated with the Cisco Unified Communications Manager Server Name. Edit it if necessary.
c) Enter the IP address of the Cisco Unified Communications Manager Server in the IPV4 Address field.
   Note Either the hostname or the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. Cisco Unified Communications Domain Manager cannot validate an entry that contains a blank space at the end of the hostname or IP address.
d) Fill in the domain of the Cisco Unified Communications Manager application.
e) Provide an optional description for the network address.

If NAT is used, also configure an APPLICATION_SPACE network address.

Step 10 Expand **Credentials**.

a) Add credentials for PLATFORM, ADMIN, HTTP, and SNMP_Vx credential types. Click + to add more credentials.
b) Fill in the user ID and password that you configured when you installed the Cisco Unified Communications Manager.
c) Select RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.
d) Provide an optional description for the credential.

ADMIN, HTTP, PLATFORM, and SNMP are required for PCA to manage Cisco Unified Communications Manager. PLATFORM and ADMIN are also required for Service Inventory to generate reports for UC applications.

Step 11 Click **Save**.
A Cisco Unified Communications Manager network device is created in Cisco Unified Communications Domain Manager 10.6(1). A cluster and Cisco Unified Communications Manager are created in the SDR.

Step 12 Test the connection between Cisco Unified Communications Manager and Cisco Unified Communications Domain Manager 10.6(1)

a) Select **Device Management** > **Advanced** > **CUCM Network Device**.
b) Click the Cisco Unified Communications Manager you just added.
c) Select **Action** > **Test Connection**.

If the test fails, and you used a hostname, make sure Cisco Unified Communications Domain Manager 10.6(1) has the correct DNS and Domain set.

1. Log in to the platform CLI.
2. Query the current DNS setting: `network dns`
3. Set the DNS if needed: `network dns <dns_server_ip_address>`
4. Query the current domain setting: `network domain`
5. Set the domain if needed: `network domain <domain>`

Note Use the CUCM Network Device page only for testing the connection. Do not edit Cisco Unified Communications Manager from this page. To change any configuration of the Cisco Unified Communications Manager, edit it from the **Device Management** > **CUCM** > **Servers** page in Cisco Unified Communications Domain Manager 10.6(1).

Set up IM and Presence Service Servers

Use this procedure to configure IM and Presence Service servers within a Cisco Unified Communications Manager cluster.

Procedure

Step 1 Log in as the appropriate hierarchy administrator.
Only a provider or reseller administrator can create a shared instance. A customer, provider, or reseller administrator can create a dedicated instance.

Step 2 Set the hierarchy path to the correct level. Create a shared instance at the provider or reseller level. Create a dedicated instance at the customer level.

Step 3 Click **Device Management** > **CUCM** > **Servers**.

Step 4 Click **Add**.

Step 5 Enter the IM and Presence Service server name in the CUCM Server Name field.

Note An IM and Presence Service server that has been configured in HCM-F and synced into Cisco Unified Communications Domain Manager may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the **Migrate from HCM-F to CUCDM** checkbox is displayed. Click **Save** to migrate this server to the current hierarchy level. The fields will be populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.

Step 6 Select **IM_P** in the Server Type field.

Step 7 To configure a publisher node, check **Publisher**.

Note The **Publisher** tab is not populated for an IM and Presence Service publisher node.

Step 8 Select the Cisco Unified Communications Manager cluster from the **Cluster Name** drop down menu.

Step 9 Expand **Network Addresses**.

a) Select the SERVICE_PROVIDER_SPACE address space.
b) The Hostname field is automatically populated with the IM and Presence Service Server Name. Edit it if necessary.
c) Enter the IP address of the IM and Presence Service server in the IPV4 Address field.

Note Either the hostname or the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. Cisco Unified Communications Domain Manager 10.6(1) cannot validate an entry that contains a blank space at the end of the hostname or IP address.

d) Fill in the domain of the IM and Presence Service application.
e) Provide an optional description for the network address.

If NAT is used, also configure an APPLICATION_SPACE network address.

Step 10 Expand **Credentials**.

a) Add credentials for PLATFORM, ADMIN, HTTP, and SNMP_Vx credential types. Click + to add more credentials.
b) Fill in the user ID and password that you configured when you installed the IM and Presence Service.
c) Select RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.
d) Provide an optional description for the credential.

ADMIN, HTTP, PLATFORM, and SNMP are required for PCA to manage IM & Presence Service. PLATFORM and ADMIN are also required for Service Inventory to generate reports for UC applications.

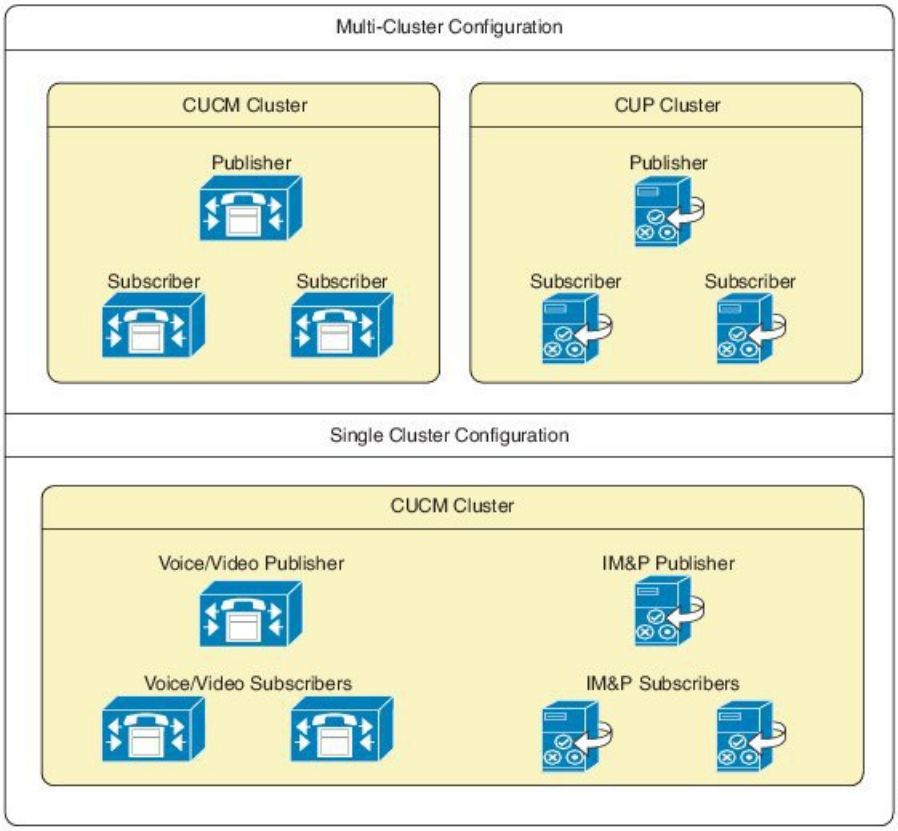
Step 11 Click **Save**.

CUP Cluster Migration

In versions before Cisco Unified Communications Domain Manager 10.6(1), IM and Presence Service (previously known as CUP) was set up in a cluster separate from the Cisco Unified Communications Manager cluster. This configuration is called a multi-cluster configuration. Beginning with Unified CDM 10.6(1), however, the IM and Presence Service servers are set up as part of the Cisco Unified Communications Manager cluster itself, in what is called a single-cluster configuration. The single-cluster configuration correctly represents the Cisco Unified Communications Manager cluster with its IM and Presence Service servers in the management layer. This configuration eliminates the confusion that multi-cluster configurations can cause

for administrators when Cisco Prime Collaboration Assurance and other tools show these servers in different clusters.

Figure 1: Multi-Cluster vs. Single Cluster Configuration



Although the use of multi-cluster configurations is deprecated and highly discouraged, Unified CDM 10.6(1) continues to support multi-cluster configurations for backward compatibility and upgrades. Partners are strongly encouraged to use the single-cluster configuration for new clusters. Convert existing multi-cluster configurations to single-cluster using the migration tool under Device Management.

Migrate CUP to a Cisco Unified Communications Manager Cluster

Use this tool to migrate your CUP (also known as IM and Presence Service) nodes to a Cisco Unified Communications Manager cluster, which is the recommended configuration. Migrating CUP nodes to a Cisco Unified Communications Manager cluster is hierarchy specific; i.e., a Customer CUP node can only be migrated to a Customer Cisco Unified Communications Manager cluster and not to a Provider or Reseller cluster. A Publisher IM_P node is added first, then Subscriber nodes.

When migrating your CUP to a Cisco Unified Communications Manager cluster, the following conditions apply:

- Cluster versions should be same for both the clusters.
- The IPV4 address or hostname and domain configuration should not be duplicated within the cluster.

- Two devices cannot have the same server name.
- No more than one CUP publisher can be migrated to the same Cisco Unified Communications Manager cluster.
- Multiple subscribers can be migrated to the same Cisco Unified Communications Manager cluster.

Procedure

Step 1 Login as a provider, reseller, or customer admin, depending on the hierarchy level where the CUP cluster was configured.

Step 2 Set the hierarchy path to the hierarchy node where the CUP cluster was configured. For a shared configuration, this would be a provider or reseller node. For a dedicated configuration, this would be a customer node.

Step 3 Click **Device Management** > **CUP (deprecated)** > **Migrate CUP to CUCM Cluster**.

Step 4 In the **From CUP Cluster** pull-down menu, click and select the CUP cluster you want to migrate.

Step 5 In the **To CUCM Cluster** pull-down menu, click and select the Cisco Unified Communications Manager cluster to which you want to migrate the CUP cluster.

Step 6 Click **Save**.

The migrated CUP server is removed from the list under **Device Management** > **CUP** > **Servers** and now appears under **Device Management** > **CUCM** > **Servers** as server type IM_P. The cluster name for these migrated servers is now the same as the Cisco Unified Communications Manager cluster name.

Cisco Unified Communications Manager Server Deletion

Be aware that deleting a Cisco Unified Communications Manager Server in Cisco Unified Communications Domain Manager 10.6(1) will also delete local data that has been synced to it from the Cisco Unified Communications Manager Server, including:

- Users
- Dial Plan information
- Configuration parameters

Configure Regions

Regions can only be added at the customer or site hierarchy level but can be modified at any hierarchy level. Regions added directly on Cisco Unified Communications Manager are synced in at the hierarchy level the Cisco Unified Communications Manager is configured at in Cisco Unified Communications Domain Manager 10.6(1).

Procedure

Step 1 Log in as the Provider/Reseller or Customer administrator.

Step 2 Select **Device Management > CUCM > Regions** from the left menu.

Step 3 Perform one of the following:

- To add a new Region, click **Add**.
- To edit an existing Region, click on the name of the Region to be updated.

Step 4 From the **CUCM** pulldown menu, select or modify the Cisco Unified Communications Manager that corresponds to the Region.

Step 5 Enter a unique name for the new Region in the **Name** field, or modify the existing **Name** if desired.

Step 6 In the **Related Regions** field, configure the following options:

Option	Description
Region Name	Drop down menu with list of available regions. This field is mandatory.
Codec Preference	This is a drop-down containing available Audio Codec Preference Lists. The default codec is G.711.
Audio Bandwidth	Maximum Audio Bit Rate (kbps). This field is mandatory.
Video Bandwidth	Maximum Session Bit Rate for Video Calls (kbps). This field is mandatory.
Immersive Video Bandwidth	Maximum Session Bit Rate for Immersive Video Calls (kbps). This field is mandatory.

Step 7 To save a new or updated group, click **Save**.

Delete Region

Regions can be deleted at any hierarchy level. Related regions cannot be removed from a region. They exist until either region is deleted.

Procedure

Step 1 Log in as the Provider/Reseller or Customer administrator.

Step 2 Select **Device Management > CUCM > Regions** from the left menu.

Step 3 From the list of Regions, click on the name of the Region to be deleted.

Step 4 Click **Delete**.

Step 5 From the popup window, click **Yes** to confirm the deletion.

Set up Cisco Unity Connection

Overview

Cisco Unity Connection devices provide voicemail services for HCS deployments, and can be dedicated to a customer or shared across multiple customers. To dedicate a Cisco Unity Connection to a single customer, configure the Cisco Unity Connection at the customer hierarchy node. To share a Cisco Unity Connection across multiple customers, configure the Cisco Unity Connection at a hierarchy node above the customer (reseller, provider, or intermediate node). The Cisco Unity Connection device must be included in one or more Network Device Lists (NDLs), and the NDL must be assigned to one or more sites.

Synchronization with Cisco Unified Communications Domain Manager 10.6(1)

Configuring a Cisco Unity Connection device on Cisco Unified Communications Domain Manager 10.6(1), creates a scheduled data sync to import model data from the device into Cisco Unified Communications Domain Manager 10.6(1). The scheduled data sync ensures that the Cisco Unified Communications Domain Manager 10.6(1) cache maintains the most current view of the configured device. Any changes to the configuration occurring on the device, including additions, deletions, or modifications, will be reflected in Cisco Unified Communications Domain Manager 10.6(1) after the next data sync.

The data sync occurs once immediately upon creation. The recurring sync is scheduled to occur every 14 days, but is disabled by default. You can enable the sync and modify the schedule from **Device Management** > **CUC** > **Schedules**. When determining the appropriate schedule setting, the frequency of the sync must be weighed against the additional processing and network activity associated with the data sync. You can also manually run the data sync at any time from **Device Management** > **Advanced** > **Perform Publisher Actions**, or from **Administration Tools** > **Data Sync**.

The performance of a data sync can be improved by controlling the types of data that are synced. See Controlling a Data Sync with a Model Type List, on page 19 for more information.

Procedure

Step 1 Log in as the appropriate hierarchy administrator.
Only a provider or reseller administrator can create a shared instance. A customer, provider, or reseller administrator can create a dedicated instance.

Step 2 Set the hierarchy path to the correct level. Create a shared instance at the provider or reseller level. Create a dedicated instance at the customer level.

Step 3 Click **Device Management** > **CUC** > **Servers**.

Step 4 Click **Add**.

Step 5 Enter a Cisco Unity Connection server name in the CUC Server Name field.

Note A Cisco Unity Connection server that has been configured in HCM-F and synced into Cisco Unified Communications Domain Manager 10.6(1) may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the **Migrate from HCM-F to CUCDM** checkbox is displayed. Click **Save** to migrate this server to the current hierarchy level. The fields will be populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.

Step 6 Check **Publisher** if you are configuring a publisher node.

Note The **Publisher** tab is populated only when the **Publisher** check box is checked.

On the Publisher tab, you can specify the following information:

Field	Description
Prime Collab	Select the Prime Collaboration management application monitoring this cluster.
Call Processing ID	The Call Processing ID of this cluster
Cluster ID	The Cluster ID of this cluster.
Multi-Tenant	If creating at provider level, this field is read only and set to Shared. If creating at customer level, you can choose between Dedicated and Partitioned.
Version	Select the version of Cisco Unity Connection Servers in this cluster. The available versions depend on the version of HCM-F that has been configured.
Port	The port on the Cisco Unity Connection server to connect to. Default is 8443.

Step 7 Fill in the Cluster Name field with the name you want for this cluster. A new cluster is created with this name. This field is mandatory.

Note If Publisher is not checked, the Cluster field appears as a drop-down list where you select an existing cluster.

Step 8 Expand **Network Addresses**.

a) Select the SERVICE_PROVIDER_SPACE address space.
b) The Hostname field is automatically populated with the Cisco Unity Connection Server Name. Edit it if necessary.
c) Enter the IP address of the Cisco Unity Connection Server in the IPV4 Address field.

Note Either the hostname or the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. Cisco Unified Communications Domain Manager 10.6(1) cannot validate an entry that contains a blank space at the end of the hostname or IP address.

d) Fill in the domain of the Cisco Unity Connection application.
e) Provide an optional description for the network address.

If NAT is used, also configure an APPLICATION_SPACE network address.

Step 9 Expand **Credentials**.

a) Add credentials for PLATFORM, ADMIN, HTTP, and SNMP_Vx credential types. Click + to add more credentials.
b) Fill in the user ID and password that you configured when you installed the Cisco Unity Connection.
c) Select RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.
d) Provide an optional description for the credential.

ADMIN, HTTP, and SNMP are required for PCA to manage Cisco Unity Connection. PLATFORM and ADMIN are required for Service Inventory to generate reports for UC applications.

Step 10 Click **Save**.

Cisco Unity Connection Server Deletion

Be aware that deleting a Cisco Unity Connection Server in Cisco Unified Communications Domain Manager 10.6(1) also deletes local data that has been synced to it from the Cisco Unity Connection Server, including:

- Users
- Dial Plan information
- Configuration parameters

Set up Cisco Emergency Responder

Complete this procedure at any time to configure Cisco Emergency Responder (CER) on Cisco Unified Communications Domain Manager 10.6(1). For more information on CER installation and setup, refer to http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cer/10_5_1/english/administration/guide/CER0_BK_C0C71A60_00_cisco-emergency-responder-administration-guide.html.

Procedure

Step 1 Log in as the appropriate hierarchy administrator.

Step 2 Set the hierarchy path to the correct level. Shared instances are created at the Provider, Reseller, or Customer level. Dedicated instances are created at the customer level.

Step 3 Click **Device Management** > **CER** > **Servers**.

Step 4 Perform one of the following:

- To add a new Cisco Emergency Responder (CER) in Cisco Unified Communications Domain Manager 10.6(1), click **Add**.
- To modify an existing CER, click its name in the list of Cisco Emergency Responders.

Step 5 Enter a name for the Cisco Emergency Responder in the CER_Virtual Server Name Field.

Note A Cisco Emergency Responder server that has been configured in HCM-F and synced into Cisco Unified Communications Domain Manager may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the **Migrate from HCM-F to CUCDM** checkbox is displayed. Click **Save** to migrate this server to the current hierarchy level. The fields will be populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.

Step 6 Check **Publisher** if you are configuring a publisher node.

Note The **Publisher** tab is populated only when the Published check box is checked.

Step 7 Expand **Network Addresses**.

a) Select the SERVICE_PROVIDER_SPACE address space.

b) Enter the IP address of the CER Server in the IPV4 Address field.

Note Either the hostname or the IP address is required. Ensure that the hostname or IP address does not contain a trailing blank space. Cisco Unified Communications Domain Manager 10.6(1) cannot validate an entry that contains a blank space at the end of the hostname or IP address.

c) The Hostname field is automatically populated with the CER Name. Edit it if necessary.

d) Fill in the domain of the CER application.
e) Provide an optional description for the network address.

Step 8 Expand **Credentials**.

a) Add credentials for PLATFORM and ADMIN credential types. Click + to add more credentials.
b) Fill in the user ID and password that you configured when you installed the CER.
c) Select RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.
d) Provide an optional description for the credential.

PLATFORM and ADMIN are required for license management.

Step 9 On the **Publisher** tab, you can specify the following information:

Field	Description
Version	Select the version of the Cisco Emergency Responder Servers in this cluster. The available versions depend on the version of the HCM-F device that has been configured.
Multi-Tenant	Read-only field. If creating at provider level, this field is set to Shared. If creating at customer level, this field is set to Dedicated.

Step 10 Click **Save**.

What to Do Next

Associate CER with Customers, on page 14

Associate CER with Customers

Before You Begin

A customer must be configured before performing this procedure. Perform this procedure at any hierarchy level at or above where the CER is configured, when you configure the VM in Cisco Unified Communications Domain Manager 10.6(1), or perform it at any time after the VM has been created.

Procedure

Step 1 Log in as a Provider or Reseller administrator.

Step 2 Select **Device Management** > **CER** > **Servers**.

Step 3 Click the name of the CER cluster to associate with a customer.

Step 4 Click the **CustomerAssociation** tab.

Note The list of customers that appear on this tab are those at, and below your current hierarchy. For example, if you are at the Provider level, and the CER is at Reseller1, you can see all customers at the Provider level and below. An error will occur if you try to associate a customer out of the CER's scope.

Step 5 Check the box to the left of each customer to be associated with the CER cluster.

Note To remove one or more customer associations from the CER cluster, uncheck the box for each customer to be disassociated from the cluster.

Step 6 Click **Save**.

View Associated Clusters on CER Servers

Before You Begin

Customers must be associated with the Cisco Emergency Responder (CER) cluster in order to be viewed in this procedure, unless the CER is created at customer level. If the CER is created at the customer level, customer information is automatically filled in for the customer where the CER exists.

Procedure

Step 1 Log in as a Provider, Reseller, or Customer administrator.

Step 2 Make sure that the hierarchy is set to the customer you wish to view.

Step 3 Select **Device Management** > **CER** > **Servers**.

Step 4 Click the name of the CER cluster to be viewed.
Information appears about the CER cluster. You can view a list of customers associated with the CER server by selecting the **Customer Association** tab.

Set up Cisco WebEx

For additional information about conferencing, see *Cisco Hosted Collaboration Solution, Release 10.6(1) End-User Provisioning Guide*.

Procedure

Step 1 Log in as a provider or reseller administrator.

Step 2 Select **Device Management** > **WebEx** > **Servers**.

Step 3 Click **Add**.

Step 4 Complete the fields:

Field	Description
Type	WebEx server type. Read-only field set to Cloud-Based.
Protocol	Protocol used to communicate with WebEx server. This field is mandatory and defaults to https.
Address	The IP address or hostname of the WebEx server. This field is mandatory. Example: site-name.webex.com

Field	Description
Port	The port used to communicate with the WebEx Server. Defaults to 443.
Site Name	The name of the site to be managed. Usually matches the start of the WebEx address.
Site Id	An ID for the site being managed. Typically received from Cisco WebEx Site Provisioning group. Provide this field before testing the connection to the WebEx server.
Partner Id	Partner ID. Typically received from Cisco WebEx Site Provisioning group.
REST URI	The relative URI for the XML service on the WebEx server. This field is mandatory and defaults to WBXService/XMLService.
WebEx Id	WebEx administrator ID. Either the WebEX Id or the Email field is mandatory.
Email	Email address of WebEx administrator. Either the WebEX Id or the Email field is mandatory.
Password	Password for the provided WebEx administrator. This field is mandatory.
Repeat Password	Confirm password for the provided WebEx administrator. This field is mandatory.
Version	Supported WebEx version.

Step 5 Click **Save**.

What to Do Next

To test the connection to the WebEx server, select **Device Management** > **Advanced** > **WebEx Network Device**. Click the WebEx server, then select **Action** > **Test Connection**.

Set up Customer Equipment

Use this procedure to associate customer equipment with the Prime Collaboration application that monitors it.

Procedure

Step 1 Log in as a Customer or Site administrator.

Step 2 Set the hierarchy path to the appropriate site.

Step 3 In the left menu, select **Device Management** > **Customer Equipment**.

Step 4 Click **Add**. The following fields appear:

- Customer Equipment Name
- Description
- Media Device
- Gateway
- SRST
- Router
- Cube Enterprise
- Prime Collaboration
- Network Addresses
- Credentials

Note The only required fields are Customer Equipment Name, at least one network address, and one credential if associating Prime Collaboration. Ensure that the network address does not contain a trailing blank space. Cisco Unified Communications Domain Manager 10.6(1) cannot validate an entry that contains a blank space at the end of the hostname or IP address.

Step 5 Click **Save**.

Prime Collaboration Assurance Integration with Cisco Unified Communications Domain Manager 10.6(1)

To enable integration between Cisco Unified Communications Domain Manager 10.6(1) and Prime Collaboration Assurance use the following workflow:

1. Synchronize your customer information with Cisco Unified Communications Domain Manager 10.6(1).
2. Add the local IP address of your Cisco Unity Connection and Cisco IM and Presence Service to Cisco Unified Communications Domain Manager 10.6(1). This ensures that your Prime Collaboration Assurance server has the Private IP Address.
3. Add IM and Presence Service sub node information to Cisco Unified Communications Domain Manager 10.6(1) if the customer has multiple instances of IM and Presence deployed.
4. Ensure that your Unified Communication applications have all needed credentials. At the minimum, you need to have credentials for Administration, platform, SNMP, and HTTP.

Note Depending on what you need to monitor, additional credentials may be needed. For more information about required protocols/support and credentials needed to set up devices for Prime Collaboration Assurance monitoring see Setting up devices for Prime Collaboration Assurance.

5. Ensure that your CUBE_SP and CPE have required credentials (SNMP and CLI).
6. Add Prime Collaboration Assurance to Cisco Unified Communications Domain Manager 10.6(1) under **Device Management** > **Prime Collab** > **Servers**. (Administration and SFTP credentials are needed.)

7 On-board the customer to Prime Collaboration Assurance using the Cisco Unified Communications Domain Manager 10.6(1) Admin GUI. CHPA will push SNMP/Syslog/Billing server configuration information to your Cisco Unified Communications Manager automatically. Syslog/SNMP configurations for Cisco Unity Connection and IM and Presence Service have to be added manually prior to on-boarding.

Note CHPA only supports Cisco Unified Communications Manager in HCS 10.6(1). To ensure successful CHPA configuration, the following credentials need to be configured in the Cisco Unified Communications Manager nodes:

- Administration credentials for Cisco Unified Communications Manager
- Platform credentials for Cisco Unified Communications Manager
- SNMP and HTTP credentials for Unified Communications Manager
- SFTP for Prime Collaboration Assurance

Note The following configuration will be pushed to Cisco Unified Communications Manager:

- The SNMP community string
- CDR (SFTP of Prime Collaboration Assurance server)
- Syslog configuration

JTAPI credentials are optional credentials used for TelePresence session monitoring. They are used to retrieve session status information from TelePresence devices. You must create a JTAPI user in the Unifed Communications Manager with the required permission to receive JTAPI events on endpoints. JTAPI configuration is not supported by CHPA in HCS 10.1(2) and therefore the credentials must be manually configured in the Cisco Unified Communications Manager. Note also that Prime Collaboration Assurance manages multiple call processor clusters and as a result you must ensure that the cluster IDs are unique.

8 Verify the devices are managed in Prime Collaboration Assurance.

Devices supported by Prime Collaboration Assurance can be found at: Supported Devices.

Enable a Scheduled Data Sync

By default, when a Cisco Unified Communications Manager or Cisco Unity Connection device is set up in Cisco Unified Communications Domain Manager 10.6(1), a full data sync instance is created to perform the initial sync of all data from the device. In addition, a Schedule is created to execute that data sync every 14 days, but is disabled by default. It is recommended to run the full data sync manually only when necessary. However, if a regularly scheduled sync is desired, the schedule can be enabled as follows:

Procedure

Step 1 Log in as provider admin.

Step 2 Select **Administration Tools** > **Scheduling**.

Step 3 Select the schedule instance that matches the following naming convention: HcsSync-<ip_address>-<device_name>-SCHED. For example: `HcsSync-192.0.2.24-CUCM01-SCHED`

Step 4 Check the **Active** checkbox.

Step 5 Click the **Multiple Executions** tab, and update the interval, if desired.

Step 6 Click **Save**.

The full data sync will execute immediately, and will execute again according to the schedule.

Manually Run the Default Data Sync

You can always manually run the default data sync when there have been updates to Cisco Unified Communications Manager or Cisco Unity Connection devices that need to be synced into Cisco Unified Communications Domain Manager 10.6(1).

Procedure

Step 1 Log in as a provider or reseller admin.

Step 2 Select **Device Management** > **Advanced** > **Perform Publisher Actions**.

Step 3 For Action, select **Import**.

Step 4 For App Type, select **CUCM Device** or **CUC Device**.

Step 5 Select the device from the Available Clusters list and click **Select**.

Step 6 Click **Save**.

Controlling a Data Sync with a Model Type List

Using a Model Type List (MTL), you can control the types of data that are synced into Cisco Unified Communications Domain Manager 10.6(1) from Cisco Unified Communications Manager or Cisco Unity Connection devices. Controlling the types of data that are synced can greatly improve sync performance. The MTL is a list of device models associated with the device type, for example, Phone and Line device models that are associated with the Cisco Unified Communications Manager device.

These are the possible types of Model Type Lists:

Include Selected Model Types

This list represents the device models to explicitly include in the data sync.

Exclude Selected Model Types

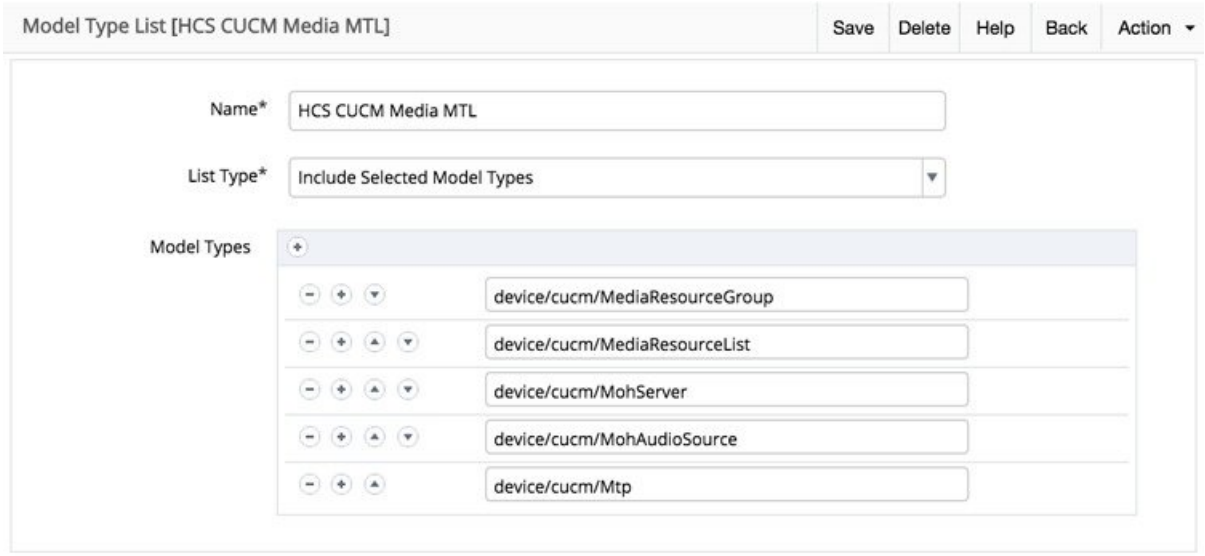
This list represents the device models to explicitly exclude from the data sync.

Ordered List

This list represents the device models to explicitly include in the data sync in the order they must be synced.

A data sync created with an empty Model Type List attribute results in the subsequent import(s) synchronizing all device models for the corresponding device.

Here's an example of an include MTL:



A data sync using this MTL will sync all Media Resource Group, Media Resource Lists, Music on Hold servers and audio sources, and Media Termination Points. No other data will be synced from Cisco Unified Communications Manager.

It is recommended to define MTLs for sets of data that are being modified on the device directly, particularly Cisco Unified Communications Manager because this is where the bulk of the configuration data for each customer resides. By defining MTLs that target specific data sets rather than doing a full sync, the performance of Cisco Unified Communications Domain Manager 10.6(1) can be maintained with better response times and quicker transaction execution. Some Cisco Unified Communications Manager device models to avoid unless needed are Users, Phones, and Lines, as there may be large numbers of these in the Cisco Unified Communications Manager and result in a lengthy data sync operation.

Data sync overhead can be further reduced if you want to sync only new and deleted instances of the device model and not updates to existing instances. This can be done by unchecking the **Refresh Existing Data** checkbox on the Data Sync configuration page. This checkbox controls whether existing device model instances are updated in Cisco Unified Communications Domain Manager 10.6(1) in addition to importing new instances and removing deleted instances. If checked, all device model instances must be synced and examined. If unchecked, only new and deleted instances need to be imported and the data sync will run considerably faster.

Create a Targeted Model Type List

If you manage data on Cisco Unified Communications Manager or Cisco Unity Connection directly on a regular basis, perhaps for configuration that is not orchestrated from Cisco Unified Communications Domain Manager 10.6(1) such as media resources, it is recommended to create a Model Type List and Data Sync specifically targeting the data items you are managing. This ensures each data sync is highly optimized for the data being changed on Cisco Unified Communications Manager directly and minimizing the load on Cisco Unified Communications Domain Manager 10.6(1). To create a targeted Model Type List:

Procedure

Step 1 Log in as hcsadmin.

Step 2 Select **Administration Tools** > **Model Type List**.

Step 3 Click **Add**.

Step 4 Specify the name of the Model Type List.
It is recommended to use a naming convention that makes it easy to identity the MTL in a list view, such as `CUCM Media Resources`.

Step 5 Specify the List Type.
Select **Include Selected Model Types** if the list of device models you want to sync is relatively short.

Select **Exclude Selected Model Types** if the list of device models you want to sync is relatively long. Exclude device models that tend to have lots of instances, like users, phones, and lines.

Select **Ordered List** if the list of device models you want to sync is relatively short and the order in which they are synced matters.

Step 6 Add Model Types to the list of device models that are to be included or excluded according to the List Type selected.
See View List of Device Models, on page 21 for information on how to see a list of available Cisco Unified Communications Manager and Cisco Unity Connection device models.

Step 7 Click **Save**.

View List of Device Models

Use this procedure to see the device models available to use in Model Type Lists for custom data syncs from Cisco Unified Communications Manager or Cisco Unity Connection.

Procedure

Step 1 Log in as hcsadmin.

Step 2 Click the **?** on the menu bar to open Online Help.

Step 3 Select **Model API**.

Step 4 Select **Device/Cuc** or **Device/Cucm**.

All the applicable device models are listed for the selected device.

What to Do Next

When including the device model in a Model Type List, use the format: device/<device_type>/<device_model>. For example, `device/cucm/BillingServer`.

Create a Custom Data Sync

Create a custom data sync to use a targeted Model Type List.

Procedure

Step 1 Log in as hcsadmin.

Step 2 Select **Administration Tools** > **Data Sync**.

Step 3 Click **Add**.

Step 4 Specify the name of the Data Sync.
It is recommend to use a naming convention that makes it easy to identify the data syncs in the list view, such as `C1Pull-CUCM01-DS` where C1 is the customer name, Pull is the data sync type, CUCM01 is the name of the Cisco Unified Communications Manager, and DS stands for Data Sync. You could also include the type of data included in the sync, such as `C1Pull-CUCM01-MediaResources-DS`.

Step 5 For Sync Type, select **Pull from Device**.

Step 6 For Dependency Resolution, select **Default**.

Step 7 Check **Execute Asynchronously** and **Refresh Existing Data**.
Execute Asynchronously means that the sync request will return a reply before its complete when executed from the API. Refresh Existing Data means that all instances of the device models specified in the Model Type List will be updated.

Step 8 Select the targeted Model Type List you defined earlier.

Step 9 Leave Synchronization Order and Model Instance Filter blank.

Step 10 Select the Device Type you are syncing from.

Step 11 Click + on Device Filters to add an entry to the list.

a) For Attribute Name, select **host**.
b) For Condition, select **Equals**.
c) For Value, select the hostname/IP address of the device.

Step 12 Leave Workflows empty.

Step 13 Click **Save**.

What to Do Next

To run the custom data sync, click the data sync from the Data Sync list and click **Execute**.