Manage Phones

Phone Management Overview

This chapter describes how to manage the phones in your network. The topics describe tasks such as adding new phones, moving existing phones to another user, locking phones and resetting phones.

The Cisco IP Phone Administration Guide for your phone model contains configuration information specific to the phone model.

Phone Button Template

Phone button template is created based on the phone models. Some phone models do not use any specific phone button template but some phone models require specific templates, either individual template or device default template.

The **Phone Template Selection for Non-Size Safe Phone** and **Auto Registration Legacy Mode** enterprise parameter on **Enterprise Parameters Configuration** page specifies the type of phone button template used. See the online help for more information about the fields.

Table 1: Phone Button Templates in Different Scenarios

Phone Template Selection for Non-Size Safe Phone	Auto Registration Legacy Mode	Phone
Create an Individual Template	False	Individual phone button template is created when adding a phone through Universal Device Template.
Use Template From Device Defaults	False	Individual phone button template is not created, it takes the phone button template from Device defaults.

Phone Template Selection for Non-Size Safe Phone	Auto Registration Legacy Mode	Phone
Use Template From Device Defaults	True	The values for Device Pool, Phone Template, Calling Search Space, Phone Button Template is taken from Device defaults.
Create an Individual Template	True	The values for Device Pool, Phone Template, Calling Search Space, Phone Button Template is taken from Device defaults. Individual templates are not created. Auto Registration Legacy Mode has the priority.

Phone Management Tasks

Procedure

	Command or Action	Purpose
Step 1	Add New Phone from Template with or Without an End User, on page 3	Add a new phone from universal device template with or without an end user.
Step 2	Add Phone Manually, on page 3	Add a new phone for an end user without device template.
Step 3	Add a New Phone from Template with an End User, on page 4	Add a new phone for an end user and assign a universal device template.
Step 4	Move an Existing Phone, on page 11	Move a configured phone to a different end user.
Step 5	Find an Actively Logged-In Device , on page 11	Search for a specific device or list all devices for which users are actively logged in.
Step 6	Find a Remotely Logged-In Device , on page 12	Search for a specific device or list all devices for which users are logged in remotely.
Step 7	Remotely Lock a Phone, on page 13	Some phones can be locked remotely. When you remotely lock a phone, the phone cannot be used until you unlock it.
Step 8	Reset a Phone to Factory Defaults , on page 14	Reset a phone to its factory settings.

	Command or Action	Purpose
Step 9	Phone Lock/Wipe Report , on page 14	Search for devices that have been remotely locked and/or remotely reset to factory default settings.
Step 10	View LSC Status and Generate a CAPF Report for a Phone, on page 15	Search for LSC expiry status on phones, and also generate a CAPF report.

Add Phone Manually

Perform the following procedure to add a new phone manually with a user.

Procedure

Step 1 From the Cisco Unified CM Administration, choose **Device** > **Phone** > **Find and List Phones**.

Step 2 From **Find and List Phones** page, click **Add New** to manually add a phone.

Add a New Phone page is displayed.

From **Add a New Phone** page, if you click "click here to add a new phone using a Universal Device Template" hyper link, the page is redirected to the **Add a New Phone** page to add a phone from the template with or without adding a user. See Add New Phone from Template with or Without an End User, on page 3 for more information.

Step 3 From the **Phone Type** drop-down list, select the phone model.

Step 4 Click **Next**.
The **Phone Configuration** page is displayed.

Step 5 On **Phone Configuration** page, enter the values in the required fields. See online help for more information on fields.

For additional information about the fields in the Product Specific Configuration area, see the *Cisco IP Phone Administration Guide* for your phone model.

Step 6 Click **Save** to save the phone configuration.

What to do next

Move an Existing Phone to a End User

Add New Phone from Template with or Without an End User

Perform the following procedure to add a new phone from the template with or without adding a user. Cisco Unified Communications Manager uses the universal device template settings to configure the phone.

Before you begin

Ensure that you have configured a universal device template in Cisco Unified Communications Manager.

Procedure

Step 1 From the Cisco Unified CM Administration, choose **Device** > **Phone** > **Find and List Phones**.

Step 2 From **Find and List Phones** page, click **Add New From Template** to add a phone from device template with or without adding an end user.

Add a New Phone page is displayed.

From **Add a New Phone** page, if you click "click here to enter all phone settings manually" hyper link, the page is redirected to the existing **Add a New Phone** page to manually add a phone. See Add Phone Manually, on page 3for more information.

Step 3 From the **Phone Type (and Protocol)** drop-down list, select the phone model.

The protocol drop-down displays only when the phone supports multiple protocols.

Step 4 In the **Name or MAC Address** text box, enter the name or MAC address.

Step 5 From the **Device Template** drop-down list, select a universal device template.

Step 6 From the **Directory Number (Line 1)** drop-down list, select a directory number.

If the directory numbers in the drop-down list exceeds the maximum drop-down limit, the **Find** tab is displayed. Click **Find**, a pop-up dialog box opens with Find Directory Number criteria.

Step 7 (Optional) Click **New**, enter Directory Number, and select a Universal Line template, if you want to create a new directory number and assign it to the device.

You can alternately create a phone using a user associated Directory Number, go to **User Management** > **User/Phone Add** > **Quick/User Phone Add**.

Step 8 (Optional) From the **User** drop-down list, select the end user for whom you want to add a new phone.

Note It is mandatory to select the user for Cisco Dual Mode (mobile) devices.

If the number of end users in the drop-down list exceeds the maximum drop-down limit, the **Find** tab is displayed. Click **Find**, a pop-up dialog box opens with Find end user criteria.

Step 9 Click **Add**.

Note For Non-Size safe phones, the phone templates are created based on the selection of **Phone Template Selection for Non-Size Safe Phone** and **Auto Registration Legacy Mode** parameters on **Enterprise Parameters Configuration** page.

Add Successful message is displayed. Cisco Unified Communications Manager adds the phone and **Phone Configuration** page is displayed. See the online help for more information about the fields on **Phone Configuration** page.

What to do next

Move an Existing Phone to a End User

Add a New Phone from Template with an End User

Perform the following procedure to add a new phone for an end user.

Before you begin

The end user for whom you are adding the phone has a user profile set up that includes a universal device template. Cisco Unified Communications Manager uses the settings from the universal device template to configure the phone.

- End User Management Tasks

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick/User Phone Add**.

Step 2 Click **Find** and select the end user for whom you want to add a new phone.

Step 3 Click the **Manage Devices**.
The Manage Devices window appears.

Step 4 Click **Add New Phone**.
The Add Phone to User popup displays.

Step 5 From the **Product Type** drop-down list, select the phone model.

Step 6 From the **Device Protocol** drop-down list select SIP or SCCP as the protocol.

Step 7 In the **Device Name** text box, enter the device MAC address.

Step 8 From the **Universal Device Template** drop-down list, select a universal device template.

Step 9 If the phone supports expansion modules, enter the number of expansion modules that you want to deploy.

Step 10 If you want to use Extension Mobility to access the phone, check the **In Extension Mobility** check box.

Step 11 Click **Add Phone**.
The Add New Phone popup closes. Cisco Unified Communications Manager adds the phone to the user and uses the universal device template to configure the phone.

Step 12 If you want to make additional edits to the phone configuration, click the corresponding Pencil icon to open the phone in the **Phone Configuration** window.

Collaboration Mobile Convergence Virtual Device Overview

A CMC device is a virtual device which represents the Remote destination associated to it. When an Enterprise phone calls to the CMC device, call gets redirected to the Remote destination.This feature aims at creating a device type **Collaboration Mobile Convergence** that is identical to Spark Remote Device with few customization and provides the following benefits.

- Supports native mobile devices on Cisco Unified Communications Manager with similar functionality to a Spark Remote Devices.
- Takes advantage of as a Spark-RD with capability that includes future development feature parity.
- Allows customization for mobile specific use cases such as call move from Mobile to Deskphone, Deskphone to Mobile. (Add deskpickup timer on Identity page and enable via product support feature setting).
- CMC devices can be included in hunt groups.
- Capable of Shared line with Spark Remote Device.

- License - Count as a separate device for license usage perspective. Any multi-device license bundle should support CMC-RD.

Licensing adjustment for CMC RD device

When a new CMC device is added, it consumes licenses based on the Number/Type of devices associated to the User. The type of license consumed by a CMC device depends on the number of devices the End user associated with it have.

- If you are deploying a CMC device only, use an Enhanced License
- If you are deploying a CMC device and a Spark RD, use an Enhanced License
- If a CMC and a physical device: Enhanced Plus License
- If a CMC, a Spark RD and a physical device: Enhanced Plus License

Add a Collaboration Mobile Convergence Virtual Device

Perform the following procedure to add a Cisco Collaboration Mobile Convergence (CMC) Remote Device for an end user.

Before you begin

The end user for whom you are adding the phone must have a user profile set up that includes a universal device template. Cisco Unified Communications Manager uses the settings from the universal device template to configure the phone.

Procedure

Step 1 In Cisco Unified CM Administration, choose **Device** > **Phone** .

Step 2 Click the **Add New** button.

Step 3 Click the **Click here to enter all phone settings manually** link.
The **Add a New Phone** window appears.

Step 4 From the **Phone Type** drop-down list, select Cisco Collaboration Mobile Convergence and click **Next**.
The **Phone Configuration** window appears.

Step 5 From the **Owner User ID** drop-down, select the End User who will own the device.

Step 6 From the **Device Pool** drop-down, select the Device Pool.

Step 7 Click **Save** .
A warning message pops up to click on the **Apply Config** button to have the changes take effect. Click **Ok**.
Device gets added successfully.

Step 8 To configure **Directory Number**, Click on the CMC device that is added, enter the **Directory Number** and Click **Save**.

Step 9 To add a new **Remote Destination** for the CMC device that is added, click on the link in the Identity box.

Step 10 In the Remote Destination Configuration window, enter the **Name**, **Destination number** and Click **Save**.

Note For one CMC device that is added, only one Remote Destination can be added.

Step 11 To update the existing Remote Destination, enter the **New Name** and Click **Save**.

Step 12 To delete existing Remote Destination, Click the Delete button in the menu.
A message from webpage appears confirming the permanent deletion. Click **Ok**

Step 13 To delete CMC device from the Device Page, Select the **Device** Check box and Click **Delete Selected** from the menu.

CMC RD Feature Interactions

Table 2: CMC RD Feature Interactions

Feature	Interaction
Shared Line handling	• In a set up where you have a shared desk phone with a CMC RD and Spark RD associated , when a user calls from an enterprise phone to a CMC Device DN, all the three - CMC RD, Spark RD and the Shared desk phone rings. • Answering from any of the remote destinations displays the message “Remote in Use” on the shared desk phone. • Answering from any of the shared desk phone disconnects both remote destination phones (CMC RD and Spark RD phones).
CMC Device to work in Call Manager Group (CMG) Setup	• When a CMC device is associated with a Call Manager group, it always runs on primary server and runs on the next active secondary server of the Call Manager Group only if the primary server is down. • If the primary server goes down mid call, then the ongoing call is still preserved and after the call ends, the CMC device registers to secondary server. **Note** When the call is in preserved mode, media between the phones still remains active, but no other actions can be performed except disconnecting the call. • If the Primary server was down initially and call was initiated while the CMC device was registered to Secondary server and then the Primary server comes up during ongoing call, the call will go into preservation mode and after the call ends the CMC device registers to Primary server.

Feature	Interaction
Call Anchoring	All the basic incoming calls from the CMC device and Number to Remote Destination calls are anchored in the enterprise network. When the CMC Remote Device is configured, users can place and receive calls from their mobile device with all calls being anchored to the enterprise: • A user can dial directly to a CMC Remote destination from an Enterprise number.The call is anchored in the enterprise network. In this scenario, the desk phone(shared line of CMC device) does not ring, but remains in **Remote in Use** state. • A user can dial from CMC Remote destination to any Enterprise number. The call is anchored. In this scenario, the desk phone (shared line of CMC device) remains in **Remote in Use** state.
Single Number Reach	• In the Remote Destination configuration page, if the **Enable Single Number Reach** checkbox is unchecked, the call do not get extended to the CMC RD and the call gets rejected. • The incoming calls from Remote Destination and the outbound **Number to Remote Destination** calls do not get affected irrespective of the **Enable Single Number Reach** checkbox selection. • If there is shared desk phone with the CMC device and if the **Enable Single Number Reach** checkbox is unchecked, then the call gets extended to the shared desk phone but not to the CMC RD. **Note** If the **Single Number Reach Voicemail Policy** is set to **user control** the mobility destination number will **NOT** be triggered in the event of a **Blind transfer** to the primary extension. Only the primary extension will be triggered. **User control** setting supports consult transfers. **Timer Control** Voice mail avoidance policy supports both Consult and Blind transfer.

Feature	Interaction
Call Routing based on Time of Day (ToD)	• You can use the Time of Day configurations for the Remote Destination to set up a ring schedule (for example, you can configure specific times such as Monday - Friday between 9 am and 5 pm). Calls will only be redirected to your Remote Destination at those times. Call from the Enterprise phone to CMC number gets routed based on the Ring Schedule fixed in the Remote Destination configuration page. Ring Schedule can be specified as below: • **All the Time** – Call gets routed at any time. There is no restrictions. • **Day(s) of the week** – Calls get routed only on the selected specific day. • **Specific time** - Calls get routed only in the selected office hours. Make sure to select the Time Zone. • When receiving a call during the Ring schedule, call from the Enterprise phone to CMC number gets routed based on the call number or pattern added in the Allowed access list or Blocked access list in the Remote Destination configuration page. • **Allowed access list**- Destination rings only if the caller number or pattern is in the Allowed access list. • **Blocked access list**- Destination do not ring if the caller number or pattern is in the Blocked access list. **Note** At any point of time, only Allowed access list or Blocked access list can be used.
User Locale settings	The CMC Virtual Device uses the locale settings that are configured in the Phone Configuration window to determine locale for the phone display and phone announcements. This policy works for regular calls, and for calls to a Conference Now number. For the announcement part, when calling (any enterprise phone) and called (CMC device) phone with same language selected in User locale settings, the announcement on both calling and Remote Destination is based on the User Locale settings selected in the Phone configuration page. **Note** For example, when calling from a **Remote Destination** which is associated with a CMC device, to a **Conference Now number**, the announcement is based on the User Locale settings selected in the Phone configuration page of the CMC device.

Feature	Interaction
New Access code for HLogin and HLogout	This functionality helps the administrator to set the Hunt Group Login and Logout number for the CMC device using the added service parameters: • Enterprise Feature Access number for Hunt group Login. • Enterprise Feature Access number for Hunt group Logout. When a user enters the Hlogin number from the RD associated to a CMC device, only then the calls will get redirected to the RD on dialing the hunt pilot number associated with the CMC device. When a user enters the Hlogout number from the RD associated to a CMC device, then the calls will not get redirected to the RD on dialing the hunt pilot number associated with the CMC device. By default the CMC device is Hloggedin. In either case, a direct call to the CMC device is not affected.
CMC Remote Destination call extention based on **delay before ringer timer** configured in Database	**If delay before ringing timer in DB is configured as 5000** • When called from an Enterprise phone to CMC number, the shared line rings and the call reaches the Remote Destination after five seconds. • When called from an Enterprise phone to CMC number, if the shared line answers the call before five seconds, the call do not get extended to Remote Destination. • When called from Enterprise phone to CMC number, the shared line rings and if the calling party disconnects the call before five seconds, the call do not get extended to Remote Destination. **If delay before ringing timer in DB is configured as 0** Any call from Enterprise phone to CMC number will alert the Remote Destination and the shared line at the same time.
Bulk Administration Tool (BAT) Support	BAT support is provided for CMC device

CMC RD Feature Restriction

Table 3: CMC RD Feature Restrictions

Feature	Restriction
CMC Remote Destination Association	The following restrictions apply: • You can associate a CMC device to one remote destination only. . • If the end user is deleted, then its associated CMC device and the RD (Remote Destination) is also deleted. **Note** Even if the **Enable Mobility** check box is checked or unchecked, the CMC and the RD is unaffected. The CMC device is not deleted. **Note** Cisco Unified Communications Manager does not support call handle preservation for CMC devices.

Move an Existing Phone

Perform the following procedure to move a configured phone to an end user.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Quick/User Phone Add**.

Step 2 Click **Find** and select the user to whom you want to move an existing phone.

Step 3 Click the **Manage Devices** button.

Step 4 Click the **Find a Phone to Move To This User** button.

Step 5 Select the phone that you want to move to this user.

Step 6 Click **Move Selected**.

Find an Actively Logged-In Device

The Cisco Extension Mobility and Cisco Extension Mobility Cross Cluster features keep a record of the devices to which users are actively logged in. For the Cisco Extension Mobility feature, the actively logged-in device report tracks the local phones that are actively logged in by local users; for the Cisco Extension Mobility

Cross Cluster feature, the actively logged-in device report tracks the local phones that are actively logged in by remote users.

Unified Communications Manager provides a specific search window for searching for devices to which users are logged in. Follow these steps to search for a specific device or to list all devices for which users are actively logged in.

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 Select the **Actively Logged In Device Report** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 3 To find all actively logged-in device records in the database, ensure the dialog box is empty and proceed to step 4.

To filter or search records:

a) From the first drop-down list, select a search parameter.
b) From the second drop-down list, select a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **(+)** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **(–)** button to remove the last added criterion or click the **Clear Filter** button to remove all added search criteria.

Step 4 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list.

Step 5 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Find a Remotely Logged-In Device

The Cisco Extension Mobility Cross Cluster feature keeps a record of the devices to which users are logged in remotely. The Remotely Logged In Device report tracks the phones that other clusters own but that are actively logged in by local users who are using the EMCC feature.

Unified Communications Manager provides a specific search window for searching for devices to which users are logged in remotely. Follow these steps to search for a specific device or to list all devices for which users are logged in remotely.

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 Select **Remotely Logged In Device** from the **Related Links** drop-down list in the upper right corner and click **Go**.

Step 3 To find all remotely logged-in device records in the database, ensure the dialog box is empty and proceed to step 4.

To filter or search records:

a) From the first drop-down list, select a search parameter.
b) From the second drop-down list, select a search pattern.
c) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the **(+)** button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the **(–)** button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 4 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list.

Step 5 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

Remotely Lock a Phone

Some phones can be locked remotely. When you remotely lock a phone, the phone cannot be used until you unlock it.

If a phone supports the Remote Lock feature, a **Lock** button appears in the top right hand corner.

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 From the **Find and List Phones** window, enter search criteria and click **Find** to locate a specific phone.

A list of phones that match the search criteria displays.

Step 3 Choose the phone for which you want to perform a remote lock.

Step 4 On the **Phone Configuration** window, click **Lock**.

If the phone is not registered, a popup window displays to inform you that the phone will be locked the next time it is registered. Click **Lock**.

A **Device Lock/Wipe Status** section appears, with information about the most recent request, whether it is pending, and the most recent acknowledgement.

Reset a Phone to Factory Defaults

Some phones support a remote wipe feature. When you remotely wipe a phone, the operation resets the phone to its factory settings. Everything previously stored on the phone is wiped out.

If a phone supports the remote wipe feature, a **Wipe** button appears in the top right hand corner.

Caution This operation cannot be undone. You should only perform this operation when you are sure you want to reset the phone to its factory settings.

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 In the **Find and List Phones** window, enter search criteria and click **Find** to locate a specific phone.

A list of phones that match the search criteria displays.

Step 3 Choose the phone for which you want to perform a remote wipe.

Step 4 In the **Phone Configuration** window, click **Wipe**.

If the phone is not registered, a popup window displays to inform you that the phone will be wiped the next time it is registered. Click **Wipe**.

A **Device Lock/Wipe Status** section appears, with information about the most recent request, whether it is pending, and the most recent acknowledgment.

Phone Lock/Wipe Report

Unified Communications Manager provides a specific search window for searching for devices which have been remotely locked and/or remotely wiped. Follow these steps to search for a specific device or to list all devices which have been remotely locked and/or remotely wiped.

Procedure

Step 1 Choose **Device** > **Phone**.

The Find and List Phones window displays. Records from an active (prior) query may also display in the window.

Step 2 Select the **Phone Lock/Wipe Report** from the **Related Links** drop-down list in the upper right corner of the window and click **Go**.

Step 3 To find all remotely locked or remotely wiped device records in the database, ensure that the text box is empty; go to Step 4.

To filter or search records for a specific device:

a) From the first drop-down list, select the device operation type(s) to search.
b) From the second drop-down list, select a search parameter.
c) From the third drop-down list, select a search pattern.
d) Specify the appropriate search text, if applicable.

Note To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click the Clear Filter button to remove all added search criteria.

Step 4 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list.

Step 5 From the list of records that display, click the link for the record that you want to view.

Note To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the item that you choose.

View LSC Status and Generate a CAPF Report for a Phone

Use this procedure to monitor Locally Significant Certificate (LSC) expiry information from within the Cisco Unified Communications Manager interface. The following search filters display the LSC information:

- LSC Expires—Displays the LSC expiry date on the phone.
- LSC Issued By—Displays the name of the issuer which can either be CAPF or third party.
- LSC Issuer Expires By—Displays the expiry date of the issuer.

Note The status of **LSC Expires** and **LSC Issuer Expires by** fields are set to "NA" when there is no LSC issued on a new device.

The status of **LSC Expires** and **LSC Issuer Expires by** fields are set to " Unknown" when the LSC is issued to a device before the upgrade to Cisco Unified Communications Manager 11.5(1).

Procedure

Step 1 Choose **Device** > **Phone**.

Step 2 From the first **Find Phone where** drop-down list, choose one of the following criteria:

- LSC Expires
- LSC Issued By
- LSC Issuer Expires By

From the second **Find Phone where** drop-down list, choose one of the following criteria:

- is before
- is exactly
- is after
- begins with
- contains
- ends with
- is exactly
- is empty
- is not empty

Step 3 Click **Find**.
A list of discovered phones displays.

Step 4 From the **Related Links** drop-down list, choose the **CAPF Report in File** and click **Go**.
The report gets downloaded.