



Configure Voice and Video Communication

- [Configure Voice and Video Communication for Cloud-Based Deployments, page 1](#)
- [Configure Voice and Video Communication for On-Premises Deployments, page 2](#)

Configure Voice and Video Communication for Cloud-Based Deployments

Procedure

	Command or Action	Purpose
Step 1	Configure Audio and Video Services, on page 1	
Step 2	Add Teleconferencing Service Name Accounts, on page 2	

Configure Audio and Video Services

Integrate your on-premises Unified Communications environment with the Cisco WebEx Administration Tool. See the following topics for more information:

- *[Getting started with Cisco Unified Communications Manager for Click to Call](#)*
- *[Creating Unified Communications Clusters](#)*

What to Do Next

[Add Teleconferencing Service Name Accounts, on page 2](#)

Add Teleconferencing Service Name Accounts

Users can make teleconference calls with either the default Cisco WebEx audio service or a third-party teleconference provider.

To integrate the third-party teleconference provider audio services with Cisco WebEx, you must add teleconferencing service name accounts. After you add those accounts, users can make teleconference calls with the third-party provider audio services.

For more information about adding teleconferencing service name accounts, see the *Cisco WebEx Site Administration User's Guide*.

Before You Begin

[Configure Audio and Video Services](#), on page 1

Configure Voice and Video Communication for On-Premises Deployments

Procedure

	Command or Action	Purpose
Step 1	Create Software Phone Devices , on page 3	
Step 2	Create Desk Phone Devices , on page 36	
Step 3	Create CTI Remote Devices , on page 42	Complete this task only if you have Cisco Unified Communications Manager 9.x and later.
Step 4	Set Up a CTI Gateway , on page 48	
Step 5	Configure Silent Monitoring and Call Recording , on page 49	Complete this task only if you have Cisco Unified Communications Manager 8.6.
Step 6	Enable URI Dialing , on page 50	Complete this task only if you have Cisco Unified Communications Manager 9.x and later.
Step 7	Call Pickup , on page 53	
Step 8	Hunt Group , on page 58	
Step 9	Configure User Associations , on page 62	
Step 10	Specify Your TFTP Server Address , on page 63	
Step 11	Reset Devices , on page 65	Only if installing Cisco Jabber for Mac
Step 12	Create a CCMCIP Profile , on page 66	

	Command or Action	Purpose
Step 13	Dial Plan Mapping, on page 67	
Step 14	Set Up Mobile Connect, on page 68	
Step 15	Transfer Active VoIP Call to the Mobile Network, on page 73	
Step 16	Set Up Dial via Office, on page 77	
Step 17	Set Up Voicemail Avoidance, on page 83	

Create Software Phone Devices

Procedure

	Command or Action	Purpose
Step 1	Choose one of the following to create a CSF device: <ul style="list-style-type: none"> • If you have Cisco Unified Communications Manager 9.x or later, complete this task:Create CSF Devices, on page 3. • If you have Cisco Unified Communications Manager 8.6(2), complete this task:Create CSF Devices on 8.6(2) and Later, on page 4. 	
Step 2	Install Cisco Options Package File for Devices, on page 7	
Step 3	Create SIP Profiles, on page 8	
Step 4	Setting up System SIP Parameters, on page 9	
Step 5	Create TCT Devices, on page 9	
Step 6	Create TAB Devices, on page 13	
Step 7	Create BOT Devices, on page 14	
Step 8	Add Directory Number to the Device for Mobile Applications, on page 19	
Step 9	Video Desktop Sharing, on page 20	
Step 10	Set Up Secure Phone Capabilities, on page 20	
Step 11	Add Directory Number to the Device for Desktop Applications, on page 18	

Create CSF Devices

Complete the steps in this task to create CSF devices.



Note A CSF should not be associated to multiple users if you intend to use different service profiles for those users.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Device > Phone**.
The **Find and List Phones** window opens.
- Step 3** Select **Add New**.
- Step 4** Select **Cisco Unified Client Services Framework** from the **Phone Type** drop-down list and then select **Next**.
The **Phone Configuration** window opens.
- Step 5** Specify a name for the CSF device in the **Device Name** field.
You should use the *CSFusername* format for CSF device names. For example, you create a CSF device for a user named Tanya Adams, whose username is tadams. In this case, you should specify CSFtadams as the device name.
- Step 6** Set the **Owner User ID** field to the appropriate user.
Important On Cisco Unified Communications Manager version 9.x, the client uses the **Owner User ID** field to get service profiles for users. For this reason, each user must have a device and the **User Owner ID** field must be associated with the user.

If you do not associate users with devices and set the **Owner User ID** field to the appropriate user, the client cannot retrieve the service profile that you apply to the user.
- Step 7** Specify configuration settings on the **Phone Configuration** window as appropriate.
See the *Phone Setup* topic in the Cisco Unified Communications Manager documentation for more information about the configuration settings on the **Phone Configuration** window.

See the *Set Up Secure Phone Capabilities* for instructions on configuring secure CSF devices.
- Step 8** Select **Save**.
A message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.
-

What to Do Next

[Install Cisco Options Package File for Devices](#), on page 7

Create CSF Devices on 8.6(2) and Later

The steps in this section describe how to create CSF devices on Cisco Unified Communications Manager version 8.6(2) and later. CSF devices provide users with software phone capabilities.

As part of the task of creating CSF devices, you can enable video desktop sharing using Binary Floor Control Protocol (BFCP). Cisco Unified Communications Manager handles the BFCP packets that users transmit when using video desktop sharing capabilities. For this reason, you configure Cisco Unified Communications Manager to allow BFCP presentation sharing. On Cisco Unified Communications Manager version 8.6(2)

and later, you must apply a COP file to add an option to allow BFCP presentation sharing on CSF devices. You must then enable BFCP presentation sharing on the CSF devices.

**Note**

- Cisco Unified Communications Manager supports BFCP presentation sharing on version 8.6(1) and later only. You cannot enable BFCP, or provision users with video desktop sharing capabilities, on versions earlier than 8.6(1).
- You can enable video desktop sharing only on software phone devices. You cannot enable video desktop sharing on desk phone devices.
- Users must be on active calls to use video desktop sharing capabilities. You can only initiate video desktop sharing sessions from active calls.
- In hybrid cloud-based deployments, both Cisco WebEx and Cisco Unified Communications Manager provide desktop sharing functionality.
 - If users initiate desktop sharing sessions during an instant messaging session, Cisco WebEx provides desktop sharing capabilities.
 - If users initiate desktop sharing sessions during an audio or video conversation, Cisco Unified Communications Manager provides desktop sharing capabilities.

**Tip**

As of Cisco Unified Communications Manager version 8.6(2), you must enable BFCP on the SIP trunk to allow video desktop sharing capabilities between nodes in a Cisco Unified Communications Manager cluster. To enable BFCP on the SIP trunk, do the following:

- 1 Select **Allow Presentation Sharing using BFCP** in the **Trunk Specific Configuration** section of the SIP profile.
- 2 Select the SIP profile from the **SIP Profile** drop-down list on the CSF device configuration.

What to Do Next

[Install Cisco Options Package File for Devices, on page 7](#)

Apply COP File for BFCP Capabilities

You must apply `cmterm-bfcp-e.8-6-2.cop.sgn` to configure video desktop sharing on Cisco Unified Communication Manager release 8.6.2 and later. This COP file adds an option to enable BFCP on the CSF device.

**Note**

- You must install the COP file each time you upgrade. For example, if you configure video desktop sharing on Cisco Unified Communication Manager Release 8.6.2 .20000-1 and then upgrade to Cisco Unified Communication Manager Release 8.6.2 .20000-2, you must apply the COP file on Cisco Unified Communication Manager Release 8.6.2 .20000-2.
- If you configure video desktop sharing on Cisco Unified Communication Manager Release 8.6.1 and then upgrade to Cisco Unified Communication Manager release 8.6.2, you must apply the COP file on Cisco Unified Communication Manager release 8.6.2 before you can configure video desktop sharing.

Procedure

-
- Step 1** Download the Cisco Jabber administration package from Cisco.com.
- Step 2** Copy `cmterm-bfcp-e.8-6-2.cop.sgn` from the Cisco Jabber administration package to your file system.
- Step 3** Open the **Cisco Unified Communications Manager Administration** interface.
- Step 4** Upload and apply `cmterm-bfcp-e.8-6-2.cop.sgn`.
- Step 5** Restart the server as follows:
- a) Open the **Cisco Unified OS Administration** interface.
 - b) Select **Settings > Version**.
 - c) Select **Restart**.
 - d) Repeat the preceding steps for each node in the cluster, starting with your presentation server.
-

The COP add the **Allow Presentation Sharing using BFCP** field to the **Protocol Specific Information** section on the **Phone Configuration** window for CSF devices.

Create CSF Devices

Complete the steps in this task to create CSF devices.

Procedure

-
- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Device > Phone**.
The **Find and List Phones** window opens.
- Step 3** Select **Add New**.
- Step 4** Select **Cisco Unified Client Services Framework** from the **Phone Type** drop-down list and then select **Next**.
The **Phone Configuration** window opens.
- Step 5** Specify a name for the CSF device in the **Device Name** field.

You should use the *CSFusername* format for CSF device names. For example, you create a CSF device for a user named Tanya Adams, whose username is tadams. In this case, you should specify CSFtadams as the device name.

- Step 6** Specify configuration settings on the **Phone Configuration** window as appropriate. See the *Phone Configuration Settings* topic in the Cisco Unified Communications Manager documentation for more information about the configuration settings on the **Phone Configuration** window. See the *Set Up Secure Phone Capabilities* for instructions on configuring secure CSF devices.
- Step 7** Select **Allow Presentation Sharing using BFCP** in the **Protocol Specific Information** section to enable video desktop sharing. Video desktop sharing using BFCP is not supported if **Trusted Relay Point** or **Media Termination Point** are enabled on the software phone device.
- Step 8** Select **Save**. A message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.
-

What to Do Next

Add a directory number to the device and apply the configuration.

Install Cisco Options Package File for Devices

To make Cisco Jabber available as a device in Cisco Unified Communications Manager, you must install a device-specific Cisco Options Package (COP) file on all your Cisco Unified Communications Manager nodes.

Perform this procedure at a time of low usage; it can interrupt service.

General information about installing COP files is available in the “Software Upgrades” chapter in the *Cisco Unified Communications Operating System Administration Guide* for your release.

Procedure

- Step 1** Download the device COP file.
- Locate the device COP file.
 - Go to the [software downloads site](#).
 - Locate the device COP file for your release.
 - Click **Download Now**.
 - Note the MD5 checksum.
You will need this information later.
 - Click **Proceed with Download** and follow the instructions.
- Step 2** Place the COP file on an FTP or SFTP server that is accessible from your Cisco Unified Communications Manager nodes.
- Step 3** Install this COP file on the Publisher node in your Cisco Unified Communications Manager cluster:
- Open the **Cisco Unified OS Administration** interface.

- b) Select **Software Upgrades > Install/Upgrade**.
- c) Specify the location of the COP file and provide the required information.
For more information, see the online help.
- d) Select **Next**.
- e) Select the device COP file.
- f) Select **Next**.
- g) Follow the instructions on the screen.
- h) Select **Next**.
Wait for the process to complete. This process can take some time.
- i) Reboot Cisco Unified Communications Manager at a time of low usage.
- j) Let the system fully return to service.
Note To avoid interruptions in service, make sure each node returns to active service before you perform this procedure on another server.

Step 4 Install the COP file on each Subscriber node in the cluster.
Use the same process you used for the Publisher, including rebooting the node.

Create SIP Profiles

This procedure is required only when you use Cisco Unified Communication Manager release 9 or earlier and are configuring devices for mobile clients. Use the default SIP profile provided for desktop clients.

If you use Cisco Unified Communication Manager release 9 or earlier, before you create and configure devices for mobile clients, you must create a SIP profile that allows Cisco Jabber to stay connected to Cisco Unified Communication Manager while Cisco Jabber runs in the background.

If you use Cisco Unified Communication Manager Release 10, choose the **Standard SIP Profile for Mobile Device** default profile when you create and configure devices for mobile clients.

Before You Begin

[Install Cisco Options Package File for Devices](#), on page 7

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Device > Device Settings > SIP Profile**.
The **Find and List SIP Profiles** window opens.
- Step 3** Do one of the following to create a new SIP profile:
 - Find the default SIP profile and create a copy that you can edit.
 - Select **Add New** and create a new SIP profile.
- Step 4** In the new SIP profile, set the following values:
 - **Timer Register Delta** to 120

- **Timer Register Expires** to 720
- **Timer Keep Alive Expires** to 720
- **Timer Subscribe Expires** to 21600
- **Timer Subscribe Delta** to 15

Step 5 Select **Save**.

What to Do Next

[Setting up System SIP Parameters](#), on page 9

Setting up System SIP Parameters

If you are connected to a low-bandwidth network and finding it difficult to take an incoming call on your mobile device, you can set the system SIP parameters to improve the condition. Increase the SIP Dual Mode Alert Timer value to ensure that calls to the Cisco Jabber extension are not prematurely routed to the mobile-network phone number.

Before You Begin

This configuration is only for mobile clients.

Cisco Jabber must be running to receive work calls.

[Create SIP Profiles](#), on page 8

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **System > Service Parameters**.
- Step 3** Select the node.
- Step 4** Select the **Cisco CallManager (Active)** service.
- Step 5** Scroll to the **Clusterwide Parameters (System - Mobility)** section.
- Step 6** Increase the **SIP Dual Mode Alert Timer** value to 4500 milliseconds.
- Step 7** Select **Save**.

Note If, after you increase the SIP Dual Mode Alert Timer value, incoming calls that arrive in Cisco Jabber are still terminated and diverted using Mobile Connect, you can increase the SIP Dual Mode Alert Timer value again in increments of 500 milliseconds.

Create TCT Devices

Complete the steps in this task to create TCT devices for Cisco Jabber for iPhone users.



Restriction The maximum number of participants for ad-hoc conferences is limited to six, which is the maximum number of calls for TCT devices.

Before You Begin

Specify the organization top domain name to support registration between Cisco Jabber and the Cisco Unified Communications Manager. In **Unified CM Administration** interface, select **System > Enterprise Parameters**. Under the **Clusterwide Domain Configuration** section, enter the organization top domain name. For example, cisco.com.

[Setting up System SIP Parameters, on page 9](#)

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Device > Phone**.
The **Find and List Phones** window opens.
- Step 3** Select **Add New**.
- Step 4** Select **Cisco Dual Mode for iPhone** from the **Phone Type** drop-down list and then select **Next**.
- Step 5** Specify configuration settings on the **Phone Configuration** window as appropriate. See the *TCT Device Configuration Settings* topic below for information about the specific settings that are required for TCT devices.
- Restriction** Multiple lines are not supported on TCT devices.
- Step 6** Select **Save**.
A message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.
- Step 7** Select **Apply Config**.
-

What to Do Next

[Create TAB Devices, on page 13](#)

TCT Device Configuration Settings

Use the following tables to set up TCT devices on the **Phone Configuration** window.

Restrictions and requirements that are not specific to Cisco Jabber may apply to these values. If you require additional information about any option on the **Phone Configuration** window, see the online help in the **Cisco Unified CM Administration** interface.

Table 1: Device Information Settings

Setting	Description
Device Name	<p>The Device Name:</p> <ul style="list-style-type: none"> • Can represent only one device. If a single user has Cisco Jabber on multiple devices (for example, an iPhone and an iPod Touch), configure separate Cisco Dual Mode for iPhone devices for each in Cisco Unified Communications Manager. • Must start with TCT. • Must be uppercase. • Can contain up to 15 characters total. • Can include only A to Z, 0 to 9, dot (.), dash (-), or underscore (_). <p>Cisco recommends that the device name include the username of the user so it is easy to remember (for example, the recommended device name of user jsmith is TCTJSMITH).</p>
Phone Button Template	Select Standard Dual Mode for iPhone.
Media Resource Group List	<p>Set up the on-hold music to ensure that if a user puts a call on hold, the other party hears on-hold music. This step prevents confusion for the other party.</p> <p>Note You must select an option in the Media Resource Group List to ensure that users can merge the audio for calls.</p> <p>These settings are not specific to this device. For more information about these settings, see the Cisco Unified Communications Manager documentation.</p>
User Hold MOH Audio Source	
Network Hold MOH Audio Source	
Primary Phone	If this user has a desk phone, select the desk phone. Selecting the primary phone sets the device as an adjunct in the Cisco Unified Communications Manager for licensing purposes.

Table 2: Protocol-Specific Information Settings

Setting	Description
Device Security Profile	Select Cisco Dual Mode for iPhone - Standard SIP Non-Secure Profile .

Setting	Description
SIP Profile	<p>Cisco Unified Communications Manager Release 9 and earlier — Select the SIP profile you created in the <i>Create SIP Profiles</i> topic.</p> <p>Cisco Unified Communications Manager Release 10 — Select the default profile for mobile devices: Standard SIP Profile for Mobile Device. If the default profile for mobile devices does not suit your environment, you can create a custom SIP profile.</p>
Other settings in the preceding sections	<p>As appropriate to your deployment.</p> <p>Values that are not described in this document are not specific to Cisco Jabber but you may need to enter them for the device to work properly.</p>

Information in this section is downloaded to the iOS device during initial setup, to automatically set up the client.

Table 3: Product Specific Configuration Layout Settings

Setting	Description
Emergency Numbers	<p>Numbers that, when dialed on an iPhone, connect using the native phone application and the mobile network of the device. If dialed on an iPod, these numbers connect using VoIP calling. For example, 911, 999, 112. These numbers are prepopulated. Update if necessary.</p>
Preset Wi-Fi Networks	<p>The SSIDs for Wi-Fi networks.</p> <p>Cisco Jabber triggers Connect on Demand to Cisco AnyConnect Secure Mobility Client if users are not on a Wi-Fi network listed in this field, or if they are on a mobile data network.</p> <p>Separate multiple SSIDs with forward slash (/).</p> <p>Example: SalesOffice1/CorporateWiFi</p>
On-Demand VPN URL	Enter the URL that you want to use to initiate on-demand VPN.
Default Ringtone	Select Loud or Normal .
Video Capabilities	Default is set to Enabled , which allows users to make and receive video calls.

The following Product Specific Configuration Layout settings are not supported in this release. Leave these settings blank:

- Allow End User Configuration Editing
- iPhone Country Code

- Cisco Usage and Error Tracking
- SIP Digest settings:
 - Enable SIP Digest Authentication
 - SIP Digest Username
- Sign In Feature
- Voicemail settings:
 - Voicemail Username
 - Voicemail Server
 - Voicemail Message Store Username
 - Voicemail Message Store
- Directory settings:
 - Directory Lookup Rules URL
 - Application Dial Rules URL
 - Enable LDAP User Authentication
 - LDAP Username
 - LDAP Password
 - LDAP Server
 - Enable LDAP SSL
 - LDAP Search Base
 - LDAP Field Mappings
 - LDAP Photo Location

Create TAB Devices

Use this procedure to create a softphone device for use with a tablet.

Before You Begin

[Create TCT Devices](#), on page 9

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.

The **Find and List Phones** window opens.

Step 2 Select **Device > Phone**.

Step 3 Select **Add New**.

Step 4 Select **Cisco Jabber for Tablet** from the **Phone Type** dropdown list and select **Next**.
The **Phone Configuration** window opens.

Step 5 Specify a name for the device in the Device Name field. You should use the format **TAB *username*** for tablet device names. For example, you create a device for a user named Tanya Adams, whose username is tadams. In this case, you should specify **TABTADAMS** as the device name.

Note Tablet Phone Device names must be in uppercase.

Step 6 Specify configuration settings on the **Phone Configuration** window as appropriate. See the *Phone Setup* topic in the Cisco Unified Communications Manager documentation for more information about the configuration settings on this window.

Step 7 Select **Save**.

A message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.

What to Do Next

[Create BOT Devices, on page 14](#)

Create BOT Devices

Complete the steps in this task to create BOT devices for Cisco Jabber for Android users.



Restriction The maximum number of participants for ad-hoc conferences is limited to three, which is the maximum number of calls for BOT devices.

Before You Begin

- Verify that the Device Pool that you plan to assign to the Cisco Jabber for Android device is associated with a region that includes support for one of the following codecs: G.711 mu-law, G.711 a-law, G.722.1, or G.729a.
- Specify the organization top domain name to support registration between Cisco Jabber and the Cisco Unified Communications Manager. In **Cisco Unified CM Administration** interface, select **System > Enterprise Parameters**. Under the Clusterwide Domain Configuration section, enter the organization top domain name. For example, cisco.com.
- [Create TAB Devices, on page 13](#)

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device > Phone**.

The **Find and List Phones** window opens.

Step 3 Select **Add New**.

Step 4 Select Cisco Dual Mode for Android from the **Phone Type** drop-down list and then select **Next**.

Step 5 Specify configuration settings on the **Phone Configuration** window as appropriate. See the *BOT Device Configuration Settings* topic below for information about the specific settings that are required for BOT devices.

Restriction Multiple lines are not supported on BOT devices.

Step 6 Select **Save**.

A message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.

Step 7 Select **Apply Config**.

What to Do Next

[Add Directory Number to the Device for Mobile Applications](#), on page 19

BOT Device Configuration Settings

Use the following tables to set up BOT devices on the **Phone Configuration** window.

Restrictions and requirements that are not specific to Cisco Jabber for Android may apply to these values. If you require additional information about any option on the **Phone Configuration** window, see the online help in the **Cisco Unified CM Administration** interface.

Table 4: Device Information Settings

Setting	Description
Device Name	<p>The Device Name:</p> <ul style="list-style-type: none"> • Can represent only one device. If a single user has Cisco Jabber for Android on multiple devices, configure separate Cisco Dual Mode for Android devices for each in Cisco Unified Communications Manager. • Must start with BOT. • Must be uppercase. • Can contain up to 15 characters total. • Can include only the following characters: A to Z, 0 to 9, dot (.), dash (-), or underscore (_). <p>Cisco recommends that the device name include the username of the user so it is easy to remember (for example, the recommended device name of user jsmith is BOTJSMITH).</p>
Phone Button Template	Select Standard Dual Mode for Android.

Setting	Description
Media Resource Group List	Set up the on-hold music to ensure that if a user puts a call on hold, the other party hears on-hold music. This step prevents confusion for the other party.
User Hold MOH Audio Source	
Network Hold MOH Audio Source	
	<p>Note You must select an option in the Media Resource Group List to ensure that users can merge the audio for calls.</p> <p>Note Cisco Jabber for Android does not support Multicast Music on Hold. Ensure that the Media Resource Group List that you apply to the BOT device does not contain multicast-enabled Media Resource Groups.</p> <p>These settings are not specific to this device. For more information about these settings, see the Cisco Unified Communications Manager documentation.</p>
Primary Phone	If this user has a desk phone, select the desk phone. Selecting the primary phone sets the device as an adjunct in Cisco Unified Communications Manager for licensing purposes.
Owner User ID	Select the user. The value must match the Mobility User ID.

Table 5: Protocol-Specific Information Settings

Setting	Description
Device Security Profile	Select Cisco Dual Mode for Android - Standard SIP Non-Secure Profile .
SIP Profile	<p>Cisco Unified Communications Manager Release 9 and earlier — Select the SIP profile you created in <i>Create SIP Profiles</i> topic.</p> <p>Cisco Unified Communications Manager Release 10 — Select the default profile for mobile devices: Standard SIP Profile for Mobile Device. If the default profile for mobile devices does not suit your environment, you can create a custom SIP profile.</p>
Other settings in the preceding sections	<p>As appropriate to your deployment.</p> <p>Values that are not described in this document are not specific to Cisco Jabber but you may need to enter them for the device to work properly.</p>

Information in this section is downloaded to the Android device during initial setup, to automatically set up the client.

Table 6: Product Specific Configuration Layout Settings

Setting	Description
Emergency Numbers	<p>The Emergency Numbers setting is not supported in this release. Leave this setting blank.</p> <p>Important For Release 9.6, emergency calls are placed through Cisco Unified Communications Manager. Ensure that Cisco Unified Communications Manager is set up to properly route emergency calls.</p>
Device Ringtone Volume	<p>Select an option if you want to prevent users from silencing incoming Cisco Jabber for Android calls.</p> <ul style="list-style-type: none"> • Native — (Default) Select this option if you want to allow the user to set any ringtone volume on the Android device, including silent mode or vibrate. • Low, Medium, or High — Select one of these options to specify the <i>minimum</i> ringtone volume on the user's device. Users can specify a louder ringtone volume than the minimum on their device.
Device Ringtone	<p>Select a ringtone option:</p> <ul style="list-style-type: none"> • Native Ringtone — (Default) Cisco Jabber for Android uses the ringtone that the user sets for the native phone application on the Android device. • Cisco Ringtone — Cisco Jabber for Android uses only the Cisco ringtone (even if the user sets a different ringtone for the native phone application on the Android device).
Video Capabilities	<p>Default is set to Enabled, which allows users to make and receive video calls.</p>

The following Product Specific Configuration Layout settings are not supported in this release. Leave these settings blank:

- SIP Digest settings:
 - Enable SIP Digest Authentication
 - SIP Digest Username
- Voicemail settings:
 - Voicemail Username
 - Voicemail Server
 - Voicemail Message Store Username

- Voicemail Message Store
- Directory settings:
 - Directory Lookup Rules URL
 - Application Dial Rules URL
 - Enable LDAP User Authentication
 - LDAP Username
 - LDAP Password
 - LDAP Server
 - Enable LDAP SSL
 - LDAP Search Base
 - LDAP Field Mappings
 - LDAP Photo Location
 - Domain Name
 - Preset Wi-Fi Networks

Add Directory Number to the Device for Desktop Applications

You must add directory numbers to devices in Cisco Unified Communications Manager. This topic provides instructions on adding directory numbers using the **Device > Phone** menu option after you create your device. Under this menu option, only the configuration settings that apply to the phone model or CTI route point display. See the Cisco Unified Communications Manager documentation for more information about different options to configure directory numbers.

Procedure

- Step 1** Locate the Association Information section on the **Phone Configuration** window.
- Step 2** Select **Add a new DN**.
- Step 3** Specify a directory number in the **Directory Number** field.
- Step 4** Specify all other required configuration settings as appropriate.
- Step 5** Associate end users with the directory number as follows:
 - a) Locate the **Users Associated with Line** section.
 - b) Select **Associate End Users**.
 - c) Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
 - d) Select the appropriate users from the list.
 - e) Select **Add Selected**.

The selected users are added to the voicemail profile.

- Step 6** Select **Save**.
- Step 7** Select **Apply Config**.
- Step 8** Follow the prompts on the **Apply Configuration** window to apply the configuration.

Add Directory Number to the Device for Mobile Applications

Before You Begin

[Create BOT Devices](#), on page 14

Procedure

- Step 1** Locate the Association Information section on the **Phone Configuration** window.
- Step 2** Select **Add a new DN**.
- Step 3** Specify a directory number in the Directory Number field.
This can be a new DN. A desk phone with the same DN is not required.
- Step 4** Select one of the following options to set the No Answer Ring Duration (seconds) setting.

Option	Description
Default	Set the value to 12 seconds.
If DVO is enabled	Start with a value of 24 seconds. This value allows time for Cisco Jabber to ring before calls go to voicemail. If you enable DVO and remote destination features, this value is dependent on local mobile voice network connection speeds. Adjust your settings accordingly. Note If you increase the value of this setting, see the related cautions for this setting in the online help in Cisco Unified Communications Manager.
If users have a PIN on the device	Start with the default value. You may need to increase this setting to ensure that users have enough time to enter the PIN and answer the call before the call goes to voicemail. Note If you increase the value of this setting, see the related cautions for this setting in the online help in Cisco Unified Communications Manager.
- Step 5** In the Multiple Call/Call Waiting Settings on Device section, in the **Busy Trigger** field, ensure that the value is set to 3.
- Step 6** Specify all other required configuration settings as appropriate.
- Step 7** Select **Save**.

What to Do Next

[Video Desktop Sharing](#), on page 20

Video Desktop Sharing

Binary Floor Control Protocol (BFCP) provides video desktop sharing capabilities for software phone devices, also known as CSF devices. Cisco Unified Communications Manager handles the BFCP packets that users transmit when using video desktop sharing capabilities. On Cisco Unified Communications Manager version 9.0(1) and later, BFCP presentation sharing is automatically enabled. For this reason, you do not need to perform any steps to enable video desktop sharing on CSF devices.



Note Cisco Jabber for mobile clients can only receive BFCP.



-
- Note**
- You can enable video desktop sharing only on software phone devices. You cannot enable video desktop sharing on desk phone devices.
 - Users must be on active calls to use video desktop sharing capabilities. You can only initiate video desktop sharing sessions from active calls.
 - In hybrid cloud-based deployments, both Cisco WebEx and Cisco Unified Communications Manager provide desktop sharing functionality.
 - If users initiate desktop sharing sessions during an instant messaging session, Cisco WebEx provides desktop sharing capabilities.
 - If users initiate desktop sharing sessions during an audio or video conversation, Cisco Unified Communications Manager provides desktop sharing capabilities.
 - Video desktop sharing using BFCP is not supported if **Trusted Relay Point** or **Media Termination Point** are enabled on the software phone device.
-



-
- Tip** You must enable BFCP on the SIP trunk to allow video desktop sharing capabilities outside of a Cisco Unified Communications Manager cluster. To enable BFCP on the SIP trunk, do the following:
- 1 Select **Allow Presentation Sharing using BFCP** in the Trunk Specific Configuration section of the SIP profile.
 - 2 Select the SIP profile from the SIP Profile drop-down list on the CSF device configuration.
-

Set Up Secure Phone Capabilities

You can optionally set up secure phone capabilities for CSF devices. Secure phone capabilities provide secure SIP signaling, secure media streams, and encrypted device configuration files.

You can optionally set up secure phone capabilities for TCT and TAB devices. Secure phone capabilities provide secure SIP signaling, secure media streams, and encrypted device configuration files.

You can optionally set up secure phone capabilities for BOT devices. Secure phone capabilities provide secure SIP signaling, secure media streams, and encrypted device configuration files.

Before You Begin

[Video Desktop Sharing](#), on page 20

What to Do Next

[Add Directory Number to the Device for Desktop Applications](#), on page 18

Configure the Security Mode

To use secure phone capabilities, you must configure the Cisco Unified Communications Manager security mode using the Cisco CTL Client. You cannot use secure phone capabilities with the nonsecure security mode. At a minimum, you must use mixed mode security.

Mixed mode security:

- Allows authenticated, encrypted, and nonsecure phones to register with Cisco Unified Communications Manager.
- Cisco Unified Communications Manager supports both RTP and SRTP media.
- Authenticated and encrypted devices use secure port 5061 to connect to Cisco Unified Communications Manager.

See the *Cisco Unified Communications Manager Security Guide* for instructions on configuring mixed mode with the Cisco CTL Client.

Create a Phone Security Profile

The first step to setting up secure phone capabilities is to create a phone security profile that you can apply to the device.

Before You Begin

Configure the Cisco Unified Communications Manager security to use mixed mode.

Procedure

-
- Step 1** Select **System > Security > Phone Security Profile**.
 - Step 2** Select **Add New**.
 - Step 3** Select the appropriate phone security profile from the Phone Security Profile type drop-down list and select **Next**.
The **Phone Security Profile Configuration** window opens.
-

Configure the Phone Security Profile

After you add a phone security profile, you must configure it to suit your requirements.

Procedure

Step 1 Specify a name for the phone security profile in the Name field on the **Phone Security Profile Configuration** window.

Restriction You must use fully qualified domain name (FQDN) format for the security profile name if users connect remotely to the corporate network through Expressway for Mobile and Remote Access.

Step 2 Specify values for the phone security profile as follows:

- Device Security Mode — Select one of the following:
 - Authenticated
 - Encrypted
- Transport Type — Leave the default value of **TLS**.
- TFTP Encrypted Config — Select this checkbox to encrypt the CSF device configuration file that resides on the TFTP server.
- Authentication Mode — Select **By Authentication String**.
- Key Size (Bits) — Select the appropriate key size for the certificate.

Note Key size refers to the bit length of the public and private keys that the client generates during the CAPF enrollment process.

The client has been tested using authentication strings with 1024 bit length keys. The client requires more time to generate 2048 bit length keys than 1024 bit length keys. As a result, if you select 2048, you should expect it to take longer to complete the CAPF enrollment process.

Cisco Jabber for Mac has been tested using authentication strings with 1024 bit length keys. The client requires more time to generate 2048 bit length keys than 1024 bit length keys. As a result, if you select 2048, you should expect it to take longer to complete the CAPF enrollment process.

Cisco Jabber for iPgone and iPad has been tested using authentication strings with 1024 bit length keys. The client requires more time to generate 2048 bit length keys than 1024 bit length keys. As a result, if you select 2048, you should expect it to take longer to complete the CAPF enrollment process.

The client has been tested using authentication strings with 1024 bit length keys. The client requires more time to generate 2048 bit length keys than 1024 bit length keys. As a result, if you select 2048, you should expect it to take longer to complete the CAPF enrollment process.

- SIP Phone Port — Leave the default value. The client always uses port 5061 to connect to Cisco Unified Communications Manager when you apply a secure phone profile. The port that you specify in this field only takes effect if you select **Non Secure** as the value for Device Security Mode.

Step 3 Select **Save**.

Configure CSF Devices

Add the phone security profile to the devices and complete other configuration tasks for secure phone capabilities.

Procedure

- Step 1** Open the CSF device configuration window.
- a) Select **Device > Phone**.
The **Find and List Phones** window opens.
 - b) Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of devices.
 - c) Select the CSF device from the list.
The **Phone Configuration** window opens.
- Step 2** Select **Allow Control of Device from CTI** in the Device Information section.
- Step 3** Select **Save**.
- Step 4** Locate the Protocol Specific Information section.
- Step 5** Select the phone security profile from the Device Security Profile drop-down list.
- Step 6** Select **Save**.
-

At this point in the secure phone set up, existing users can no longer use their CSF devices. You must complete the secure phone set up for users to be able to access their CSF devices.

What to Do Next

Specify the certificate settings and generate the authentication string for users.

Configure TCT and TAB Devices

Add the phone security profile to the devices and complete other configuration tasks for secure phone capabilities.

Procedure

- Step 1** Open the TCT or TAB device configuration window.
- a) Select **Device > Phone**.
The **Find and List Phones** window opens.
 - b) Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of devices.
 - c) Select the TCT or TAB device from the list.

The **Phone Configuration** window opens.

- Step 2** Select **Allow Control of Device from CTI** in the Device Information section.
 - Step 3** Select **Save**.
 - Step 4** Locate the Protocol Specific Information section.
 - Step 5** Select the phone security profile from the Device Security Profile drop-down list.
 - Step 6** Select **Save**.
-

At this point in the secure phone set up, existing users can no longer use their TCT or TAB devices. You must complete the secure phone set up for users to be able to access their TCT or TAB devices.

What to Do Next

Specify the certificate settings and generate the authentication string for users.

Configure BOT Devices

Add the phone security profile to the devices and complete other configuration tasks for secure phone capabilities.

Procedure

- Step 1** Open the BOT device configuration window.
 - a) Select **Device > Phone**.
The **Find and List Phones** window opens.
 - b) Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of devices.
 - c) Select the BOT device from the list.
The **Phone Configuration** window opens.
 - Step 2** Locate the Protocol Specific Information section.
 - Step 3** Select the phone security profile from the Device Security Profile drop-down list.
 - Step 4** Select **Save**.
-

At this point in the secure phone set up, existing users can no longer use their BOT devices. You must complete the secure phone set up for users to be able to access their BOT devices.

What to Do Next

Specify the certificate settings and generate the authentication string for users.

Specify Certificate Settings

Specify certificate settings in the CSF device configuration and generate the authentication strings that you provide to users.

Specify certificate settings in the TCT and TAB device configuration and generate the authentication strings that you provide to users.

Specify certificate settings in the BOT device configuration and generate the authentication strings that you provide to users.

Procedure

- Step 1** Locate the Certification Authority Proxy Function (CAPF) Information section on the **Phone Configuration** window.
- Step 2** Specify values as follows:
- Certificate Operation — Select **Install/Upgrade**.
 - Authentication Mode — Select **By Authentication String**.
 - Key Size (Bits) — Select the same key size that you set in the phone security profile.
 - Operation Completes By — Specify an expiration value for the authentication string or leave as default.
- Step 3** Select **Save**.
- Step 4** To create the authentication string you can do one of the following:
- Select **Generate String** in the Certification Authority Proxy Function (CAPF) Information section.
 - Enter a custom string in the Authentication String field.
-

What to Do Next

Provide users with the authentication string.

Provide Users with Authentication Strings

Users must specify the authentication string in the client interface to access their devices and securely register with Cisco Unified Communications Manager.

When users enter the authentication string in the client interface, the CAPF enrollment process begins.



Note

The time it takes for the enrollment process to complete can vary depending on the user's computer or mobile device and the current load for Cisco Unified Communications Manager. It can take up to one minute for the client to complete the CAPF enrollment process.

The client displays an error if:

- Users enter an incorrect authentication string.
Users can attempt to enter authentication strings again to complete the CAPF enrollment. However, if a user continually enters an incorrect authentication string, the client might reject any string the user enters, even if the string is correct. In this case, you must generate a new authentication string on the user's device and then provide it to the user.
- Users do not enter the authentication string before the expiration time you set in the **Operation Completes By** field.

In this case, you must generate a new authentication string on the user's device. The user must then enter that authentication string before the expiration time.



Important

When you configure the end users in Cisco Unified Communications Manager, you must add them to the following user groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**

Users must not belong to the Standard CTI Secure Connection user group.

Secure Phone Details for Cisco Jabber for Windows

Secure Connections

If you enable secure phone capabilities, then:

- SIP connections between CSF devices and Cisco Unified Communications Manager are over TLS.
 - If you select Authenticated as the value for the Device Security Mode field on the phone security profile, the SIP connection is over TLS using NULL-SHA encryption.
 - If you select Encrypted as the value for the Device Security Mode field on the phone security profile, the SIP connection is over TLS using AES 128/SHA encryption.
- Mutual TLS ensures that only CSF devices with the correct certificates can register to Cisco Unified Communications Manager. Likewise, CSF devices can register only to Cisco Unified Communications Manager instances that provide the correct certificate.

If you enable secure phone capabilities for users, their CSF device connections to Cisco Unified Communications Manager are secure. If the other end point also has a secure connection to Cisco Unified Communications Manager, then the call can be secure. However, if the other end point does not have a secure connection to Cisco Unified Communications Manager, then the call is not secure.

Encrypted Media

If you select Encrypted as the value for the Device Security Mode field on the phone security profile, the client uses Secure Realtime Transport Protocol (SRTP) to offer encrypted media streams as follows:

Media Stream	Encryption
Main video stream	Can be encrypted
Main audio stream	Can be encrypted
Presentation video stream Refers to video desktop sharing using BFCP.	Can be encrypted
BFCP application stream Refers to BFCP flow control.	Not encrypted

The ability to encrypt media depends on if the other end points also encrypt media, as in the following examples:

- You enable media encryption for user A and user B. In other words, Device Security Mode is set to Encrypted on the phone security profile for the users' CSF devices.
- You do not enable media encryption for user C. In other words, Device Security Mode is set to Authenticated on the phone security profile for the user's CSF device.
- User A calls user B. The client encrypts the main video stream and audio stream.
- User A calls user C. The client does not encrypt the main video stream and audio stream.
- User A, user B, and user C start a conference call. The client does not encrypt the main video stream or audio stream for any user.

**Note**

The client displays the following lock icon when it can use SRTP for encrypted media streams to other secured clients or conference bridges:



However, not all versions of Cisco Unified Communications Manager provide the ability to display the lock icon. If the version of Cisco Unified Communications Manager you are using does not provide this ability, the client cannot display a lock icon even when it sends encrypted media.

Using Expressway for Mobile and Remote Access

Users cannot complete the enrollment process or use secure phone capabilities from outside the corporate network. This limitation also includes when users connects through Expressway for Mobile and Remote Access; for example,

- 1 You configure a user's CSF device for secure phone capabilities.
- 2 That user connects to the internal corporate network through Expressway for Mobile and Remote Access.
- 3 The client notifies the user that it cannot use secure phone capabilities instead of prompting the user to enter an authentication string.

When users connect to the internal network through Expressway for Mobile and Remote Access and participate in a call:

- Media is encrypted on the call path between the Cisco Expressway-C and devices that are registered to the Cisco Unified Communications Manager using Expressway for Mobile and Remote Access.
- Media is not encrypted on the call path between the Cisco Expressway-C and devices that are registered locally to Cisco Unified Communications Manager.

**Note**

If you change the phone security profile while the client is connected through Expressway for Mobile and Remote Access, you must restart the client for that change to take effect.

Stored Files

The client stores the following files for secure phone capabilities:

- Certificate trust list (.*tlv*)
- Locally significant certificate (.*lsc*)
- Private key for the CSF device (.*key*)

The client downloads and stores certificate trust lists whenever you configure Cisco Unified Communications Manager security as mixed mode. Certificate trust lists enable the client to verify the identity of Cisco Unified Communications Manager nodes.

The client saves the locally significant certificates and private keys after users successfully enter the authentication code and complete the enrollment process. The locally significant certificate and private key enable the client to establish mutual TLS connections with Cisco Unified Communications Manager.

**Note**

The client encrypts the private key before saving it to the file system.

The client stores these files in the following folder:

```
%User_Profile%\AppData\Roaming\Cisco\Unified  
Communications\Jabber\CSF\Security
```

Because the client stores the files in the user's `Roaming` folder, users can sign in to any Microsoft Windows account on the Windows domain to register their CSF devices.

Conference Calls

On conference, or multi-party, calls, the conferencing bridge must support secure phone capabilities. If the conferencing bridge does not support secure phone capabilities, calls to that bridge are not secure. Likewise, all parties must support a common encryption algorithm for the client to encrypt media on conference calls.

CSF device security reverts to the lowest level available on multi-party calls. For example, user A, user B, and user C join a conference call. User A and user B have CSF devices with secure phone capabilities. User C has a CSF device without secure phone capabilities. In this case, the call is not secure for all users.

Sharing Secure CSF Devices between Clients

Clients that do not support secure phone capabilities cannot register to secure CSF devices.

For example, you set up secure phone capabilities on a CSF device to which both Cisco Jabber for Windows version 9.2 and Cisco Jabber for Windows version 9.1 register. However, Cisco Jabber for Windows version 9.1 does not support secure phone capabilities. In this scenario, you must create two different CSF devices, one secure CSF device for Cisco Jabber for Windows version 9.2 and another CSF device that is not secure for Cisco Jabber for Windows version 9.1.

Multiple Users on a Shared Microsoft Windows Account

Multiple users can have unique credentials for the client and share the same Windows account. However, the secure CSF devices are restricted to the Windows account that the users share. Users who share the same Windows account cannot make calls with their secure CSF devices from different Windows accounts.

You should ensure that multiple users who share the same Windows account have CSF devices with unique names. Users cannot register their CSF devices if they share the same Windows account and have CSF devices with identical names, but connect to different Cisco Unified Communications Manager clusters.

For example, user A has a CSF device named CSFcompanyname and connects to cluster 1. User B has a CSF device named CSFcompanyname and connects to cluster 2. In this case, a conflict occurs for both CSF devices. Neither user A or user B can register their CSF devices after both users sign in to the same Windows account.

Multiple Users on a Shared Computer

The client caches the certificates for each user's secure CSF device in a location that is unique to each Windows user. When a user logs in to their Windows account on the shared computer, that user can access only the secure CSF device that you provision to them. That user cannot access the cached certificates for other Windows users.

Secure Phone Details for Cisco Jabber for Mac

Secure Connections

If you enable secure phone capabilities, then:

- SIP connections between CSF devices and Cisco Unified Communications Manager are over TLS.
 - If you select Authenticated as the value for the Device Security Mode field on the phone security profile, the SIP connection is over TLS using NULL-SHA encryption.
 - If you select Encrypted as the value for the Device Security Mode field on the phone security profile, the SIP connection is over TLS using AES 128/SHA encryption.
- Mutual TLS ensures that only CSF devices with the correct certificates can register to Cisco Unified Communications Manager. Likewise, CSF devices can register only to Cisco Unified Communications Manager instances that provide the correct certificate.

If you enable secure phone capabilities for users, their CSF device connections to Cisco Unified Communications Manager are secure. If the other end point also has a secure connection to Cisco Unified Communications Manager, then the call can be secure. However, if the other end point does not have a secure connection to Cisco Unified Communications Manager, then the call is not secure.

Encrypted Media

If you select Encrypted as the value for the Device Security Mode field on the phone security profile, the client uses Secure Realtime Transport Protocol (SRTP) to offer encrypted media streams as follows:

Media Stream	Encryption
Main video stream	Can be encrypted
Main audio stream	Can be encrypted

Media Stream	Encryption
Presentation video stream Refers to video desktop sharing using BFCP.	Not encrypted
BFCP application stream Refers to BFCP flow control.	Not encrypted

The ability to encrypt media depends on if the other end points also encrypt media, as in the following examples:

- You enable media encryption for user A and user B. In other words, Device Security Mode is set to Encrypted on the phone security profile for the users' CSF devices.
- You do not enable media encryption for user C. In other words, Device Security Mode is set to Authenticated on the phone security profile for the user's CSF device.
- User A calls user B. The client encrypts the main video stream and audio stream.
- User A calls user C. The client does not encrypt the main video stream and audio stream.
- User A, user B, and user C start a conference call. The client does not encrypt the main video stream or audio stream for any user.



Note

The client displays the following lock icon when it can use SRTP for encrypted media streams to other secured clients or conference bridges:



However, not all versions of Cisco Unified Communications Manage provide the ability to display the lock icon. If the version of Cisco Unified Communications Manage you are using does not provide this ability, the client cannot display a lock icon even when it sends encrypted media.

Using Expressway for Mobile and Remote Access

Users cannot complete the enrollment process or use secure phone capabilities from outside the corporate network. This limitation also includes when users connects through Expressway for Mobile and Remote Access; for example,

- 1 You configure a user's CSF device for secure phone capabilities.
- 2 That user connects to the internal corporate network through Expressway for Mobile and Remote Access.
- 3 The client notifies the user that it cannot use secure phone capabilities instead of prompting the user to enter an authentication string.

When users connect to the internal network through Expressway for Mobile and Remote Access and participate in a call:

- Media is encrypted on the call path between the Cisco Expressway-C and devices that are registered to the Cisco Unified Communications Manager using Expressway for Mobile and Remote Access.
- Media is not encrypted on the call path between the Cisco Expressway-C and devices that are registered locally to Cisco Unified Communications Manager.

**Note**

If you change the phone security profile while the client is connected through Expressway for Mobile and Remote Access, you must restart the client for that change to take effect.

Stored Files

The client stores the following information for secure phone capabilities:

- Certificate trust list (. `tlv`)
- Locally significant certificate (. `lsc`)
- Private key for the CSF device (. `key`)

The client downloads and stores certificate trust lists whenever you configure Cisco Unified Communications Manager security as mixed mode. Certificate trust lists enable the client to verify the identity of Cisco Unified Communications Manager nodes.

The client saves the locally significant certificates and private keys after users successfully enter the authentication code and complete the enrollment process. The locally significant certificate and private key enable the client to establish mutual TLS connections with Cisco Unified Communications Manager.

**Note**

The client encrypts the private key before saving it to the keychain.

Conference Calls

On conference, or multi-party, calls, the conferencing bridge must support secure phone capabilities. If the conferencing bridge does not support secure phone capabilities, calls to that bridge are not secure. Likewise, all parties must support a common encryption algorithm for the client to encrypt media on conference calls.

CSF device security reverts to the lowest level available on multi-party calls. For example, user A, user B, and user C join a conference call. User A and user B have CSF devices with secure phone capabilities. User C has a CSF device without secure phone capabilities. In this case, the call is not secure for all users.

Sharing Secure CSF Devices between Clients

Clients that do not support secure phone capabilities cannot register to secure CSF devices.

“For example, you set up secure phone capabilities on a CSF device. Two versions of Cisco Jabber register the device. However, one version of Cisco Jabber does not support secure phone capabilities. In this scenario, you must create two different CSF devices, one secure CSF device for Cisco Jabber that supports secure phone capabilities and another CSF device that is not secure for the other Cisco Jabber ”

Multiple Users on a Shared Mac OS Account

Multiple users can have unique credentials for the client and share the same Mac account. However, the secure CSF devices are restricted to the Mac account that the users share. Users who share the same Mac account cannot make calls with their secure CSF devices from different Mac accounts.

You should ensure that multiple users who share the same Mac account have CSF devices with unique names. Users cannot register their CSF devices if they share the same Mac account and have CSF devices with identical names, but connect to different Cisco Unified Communications Manager clusters.

For example, user A has a CSF device named CSFcompanyname and connects to cluster 1. User B has a CSF device named CSFcompanyname and connects to cluster 2. In this case, a conflict occurs for both CSF devices. Neither user A or user B can register their CSF devices after both users sign in to the same Mac account.

Multiple Users on a Shared Computer

The client caches the certificates for each user's secure CSF device in a location that is unique to each Mac user. When a user logs in to their Mac account on the shared computer, that user can access only the secure CSF device that you provision to them. That user cannot access the cached certificates for other Mac users.

Secure Phone Details for Cisco Jabber for iPhone and iPad

Secure Connections

If you enable secure phone capabilities, then:

- SIP connections between TCT or TAB devices and Cisco Unified Communications Manager are over TLS.
 - If you select Authenticated as the value for the Device Security Mode field on the phone security profile, the SIP connection is over TLS using NULL-SHA encryption.
 - If you select Encrypted as the value for the Device Security Mode field on the phone security profile, the SIP connection is over TLS using AES 128 or AES 256 or SHA encryption.
- Mutual TLS ensures that only TCT or TAB devices with the correct certificates can register to Cisco Unified Communications Manager. Likewise, TCT or TAB devices can register only to Cisco Unified Communications Manager instances that provide the correct certificate.

If you enable secure phone capabilities for users, their TCT or TAB device connections to Cisco Unified Communications Manager are secure. If the other end point also has a secure connection to Cisco Unified Communications Manager, then the call can be secure. However, if the other end point does not have a secure connection to Cisco Unified Communications Manager, then the call is not secure.

Encrypted Media

If you select Encrypted as the value for the Device Security Mode field on the phone security profile, the client uses Secure Realtime Transport Protocol (SRTP) to offer encrypted media streams as follows:

Media Stream	Encryption
Main video stream	Can be encrypted
Main audio stream	Can be encrypted

The ability to encrypt media depends on if the other end points also encrypt media, as in the following examples:

- You enable media encryption for user A and user B. In other words, Device Security Mode is set to Encrypted on the phone security profile for the users' TCT or TAB devices.
- You do not enable media encryption for user C. In other words, Device Security Mode is set to Authenticated on the phone security profile for the user's TCT or TAB device.
- User A calls user B. The client encrypts the main video stream and audio stream.
- User A calls user C. The client does not encrypt the main video stream and audio stream.
- User A, user B, and user C start a conference call. The client does not encrypt the main video stream or audio stream for any user.

**Note**

The client displays the following lock icon when it can use SRTP for encrypted media streams to other secured clients or conference bridges:



However, not all versions of Cisco Unified Communications Manager provide the ability to display the lock icon. If the version of Cisco Unified Communications Manager you are using does not provide this ability, the client cannot display a lock icon even when it sends encrypted media.

Using Expressway for Mobile and Remote Access

Users cannot complete the enrollment process from outside the corporate network.

Secure phone capabilities can be used through Expressway for Mobile and Remote Access by installing the Cisco Expressway-C certificate and configuring the Secure Profile Domain as the Phone Security Profile in Cisco Unified Communications Manager.

When users connect through Expressway for Mobile and Remote Access and participate in a call:

- Media is encrypted on the call path between the Cisco Expressway-C and devices that are registered to the Cisco Unified Communications Manager using Expressway for Mobile and Remote Access.
- Media is not encrypted on the call path between the Cisco Expressway-C and devices that are registered locally to Cisco Unified Communications Manager.

**Note**

If you change the phone security profile while the client is connected through Expressway for Mobile and Remote Access, you must restart the client for that change to take effect.

Stored Files

The client stores the following files for secure phone capabilities:

- Certificate trust list (.t1v)
- Locally significant certificate (.lsc)

- Private key for the TCT or TAB device (.key)

The client downloads and stores certificate trust lists whenever you configure Cisco Unified Communications Manager security as mixed mode. Certificate trust lists enable the client to verify the identity of Cisco Unified Communications Manager nodes.

The client saves the locally significant certificates and private keys after users successfully enter the authentication code and complete the enrollment process. The locally significant certificate and private key enable the client to establish mutual TLS connections with Cisco Unified Communications Manager.

**Note**

The client encrypts the private key before saving it to the device trust store.

Conference Calls

On conference, or multi-party, calls, the conferencing bridge must support secure phone capabilities. If the conferencing bridge does not support secure phone capabilities, calls to that bridge are not secure. Likewise, all parties must support a common encryption algorithm for the client to encrypt media on conference calls.

TCT and TAB device security reverts to the lowest level available on multi-party calls. For example, user A, user B, and user C join a conference call. User A and user B have TCT devices with secure phone capabilities. User C has a TCT device without secure phone capabilities. In this case, the call is not secure for all users.

Secure Phone Details for Cisco Jabber for Android**Secure Connections**

If you enable secure phone capabilities, then:

- SIP connections between BOT or TAB devices and Cisco Unified Communications Manager are over TLS.
 - If you select Authenticated as the value for the Device Security Mode field on the phone security profile, the SIP connection is over TLS using NULL-SHA encryption.
 - If you select Encrypted as the value for the Device Security Mode field on the phone security profile, the SIP connection is over TLS using AES 128/SHA encryption.
- Mutual TLS ensures that only BOT devices with the correct certificates can register to Cisco Unified Communications Manager. Likewise, BOT devices can register only to Cisco Unified Communications Manager instances that provide the correct certificate.

If you enable secure phone capabilities for users, their BOT device connections to Cisco Unified Communications Manager are secure. If the other end point also has a secure connection to Cisco Unified Communications Manager, then the call can be secure. However, if the other end point does not have a secure connection to Cisco Unified Communications Manager, then the call is not secure.

Encrypted Media

If you select Encrypted as the value for the Device Security Mode field on the phone security profile, the client uses Secure Realtime Transport Protocol (SRTP) to offer encrypted media streams as follows:

Media Stream	Encryption
Main video stream	Can be encrypted
Main audio stream	Can be encrypted

The ability to encrypt media depends on if the other end points also encrypt media, as in the following examples:

- You enable media encryption for user A and user B. In other words, Device Security Mode is set to Encrypted on the phone security profile for the users' BOT devices.
- You do not enable media encryption for user C. In other words, Device Security Mode is set to Authenticated on the phone security profile for the user's BOT device.
- User A calls user B. The client encrypts the main video stream and audio stream.
- User A calls user C. The client does not encrypt the main video stream and audio stream.
- User A, user B, and user C start a conference call. The client does not encrypt the main video stream or audio stream for any user.

**Note**

The client displays the following lock icon when it can use SRTP for encrypted media streams to other secured clients or conference bridges:



However, not all versions of Cisco Unified Communications Manager provide the ability to display the lock icon. If the version of Cisco Unified Communications Manager you are using does not provide this ability, the client cannot display a lock icon even when it sends encrypted media.

Using Expressway for Mobile and Remote Access

Users cannot complete the enrollment process from outside the corporate network.

Secure phone capabilities can be used through Expressway for Mobile and Remote Access by installing the Cisco Expressway-C certificate and configuring the Secure Profile Domain as the Phone Security Profile in Cisco Unified Communications Manager.

When users connect through Expressway for Mobile and Remote Access and participate in a call:

- Media is encrypted on the call path between the Cisco Expressway-C and devices that are registered to the Cisco Unified Communications Manager using Expressway for Mobile and Remote Access.
- Media is not encrypted on the call path between the Cisco Expressway-C and devices that are registered locally to Cisco Unified Communications Manager.

**Note**

If you change the phone security profile while the client is connected through Expressway for Mobile and Remote Access, you must restart the client for that change to take effect.

Stored Files

The client stores the following files for secure phone capabilities:

- Certificate trust list (.tlv)
- Locally significant certificate (.lsc)
- Private key for the BOT device (.key)

The client downloads and stores certificate trust lists whenever you configure Cisco Unified Communications Manager security as mixed mode. Certificate trust lists enable the client to verify the identity of Cisco Unified Communications Manager nodes.

The client saves the locally significant certificates and private keys after users successfully enter the authentication code and complete the enrollment process. The locally significant certificate and private key enable the client to establish mutual TLS connections with Cisco Unified Communications Manager.



Note

The client encrypts the private key before saving it to the device trust store.

Conference Calls

For audio or video conference calls or multi-party calls, you must set up a secure multimedia conferencing bridge using a Multipoint Control Unit (MCU). When setting up the MCU, you must ensure that you create a secure SIP Trunk Security Profile and set the Device Security Mode to Encrypted. For more information, see the Conference Bridge setup chapter in the *Cisco Unified Communications Manager Administration Guide* for your release.

Create Desk Phone Devices

Users can control desk phones on their computers to place audio calls.

Before You Begin

[Create Software Phone Devices](#), on page 3

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Device > Phone**.
The **Find and List Phones** window opens.
- Step 3** Select **Add New**.
- Step 4** Select the appropriate device from the **Phone Type** drop-down list and then select **Next**.
The **Phone Configuration** window opens.
- Step 5** Complete the following steps in the **Device Information** section:
 - Enter a meaningful description in the **Description** field.
The client displays device descriptions to users. If users have multiple devices of the same model, the descriptions help users tell the difference between multiple devices.

- b) Select **Allow Control of Device from CTI**.

If you do not select **Allow Control of Device from CTI**, users cannot control the desk phone.

Step 6 Set the **Owner User ID** field to the appropriate user.

Important On Cisco Unified Communications Manager version 9.x, the client uses the **Owner User ID** field to get service profiles for users. For this reason, each user must have a device and the **User Owner ID** field must be associated with the user.

If you do not associate users with devices and set the **Owner User ID** field to the appropriate user, the client cannot retrieve the service profile that you apply to the user.

Step 7 Complete the following steps to enable desk phone video capabilities:

- a) Locate the **Product Specific Configuration Layout** section.
b) Select **Enabled** from the **Video Capabilities** drop-down list.

Note If possible, you should enable desk phone video capabilities on the device configuration. However, certain phone models do not include the **Video Capabilities** drop-down list at the device configuration level. In this case, you should open the **Common Phone Profile Configuration** window and then select **Enabled** from the **Video Calling** drop-down list.

See *Desk Phone Video Configuration* for more information about desk phone video.

Step 8 Specify all other configuration settings on the **Phone Configuration** window as appropriate.

See the Cisco Unified Communications Manager documentation for more information about the configuration settings on the **Phone Configuration** window.

Step 9 Select **Save**.

An message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.

What to Do Next

Add a directory number to the device and apply the configuration.

Desk Phone Video Configuration

Desk phone video capabilities let users receive video transmitted to their desk phone devices on their computers through the client.

Set Up Desk Phone Video

To set up desk phone video, you must complete the following steps:

- 1 Physically connect the computer to the computer port on the desk phone device.

You must physically connect the computer to the desk phone device through the computer port so that the client can establish a connection to the device. You cannot use desk phone video capabilities with wireless connections to desk phone devices.

**Tip**

If users have both wireless and wired connections available, they should configure Microsoft Windows so that wireless connections do not take priority over wired connections. See the following Microsoft documentation for more information: *An explanation of the Automatic Metric feature for Internet Protocol routes*.

- 2 Enable the desk phone device for video in Cisco Unified Communications Manager.
- 3 Install Cisco Media Services Interface on the computer.

Cisco Media Services Interface provides the Cisco Discover Protocol (CDP) driver that enables the client to do the following:

- Discover the desk phone device.
- Establish and maintain a connection to the desk phone device using the CAST protocol.

**Note**

Download the **Cisco Media Services Interface** installation program from the download site on cisco.com.

Desk Phone Video Considerations

Review the following considerations and limitations before you provision desk phone video capabilities to users:

- You cannot use desk phone video capabilities on devices if video cameras are attached to the devices, such as a Cisco Unified IP Phone 9971. You can use desk phone video capabilities if you remove video cameras from the devices.
- You cannot use desk phone video capabilities with devices that do not support CTI.
- Video desktop sharing, using the BFCP protocol, is not supported with desk phone video.
- It is not possible for endpoints that use SCCP to receive video only. SCCP endpoints must send and receive video. Instances where SCCP endpoints do not send video result in audio only calls.
- 7900 series phones must use SCCP for desk phone video capabilities. 7900 series phones cannot use SIP for desk phone video capabilities.
- If a user initiates a call from the keypad on a desk phone device, the call starts as an audio call on the desk phone device. The client then escalates the call to video. For this reason, you cannot make video calls to devices that do not support escalation, such as H.323 endpoints. To use desk phone video capabilities with devices that do not support escalation, users should initiate calls from the client.
- A compatibility issue exists with Cisco Unified IP Phones that use firmware version SCCP45.9-2-1S. You must upgrade your firmware to version SCCP45.9-3-1 to use desk phone video capabilities.
- Some antivirus or firewall applications, such as Symantec EndPoint Protection, block inbound CDP packets, which disables desk phone video capabilities. You should configure your antivirus or firewall application to allow inbound CDP packets.

See the following Symantec technical document for additional details about this issue: *Cisco IP Phone version 7970 and Cisco Unified Video Advantage is Blocked by Network Threat Protection*.

- You must not select the **Media Termination Point Required** checkbox on the SIP trunk configuration for Cisco Unified Communications Manager. Desk phone video capabilities are not available if you select this checkbox.

If you encounter an error that indicates desk phone video capabilities are unavailable or the desk phone device is unknown, do the following:

- 1 Ensure you enable the desk phone device for video in Cisco Unified Communications Manager.
- 2 Reset the physical desk phone.
- 3 Exit the client.
- 4 Run services.msc on the computer where you installed the client.
- 5 Restart Cisco Media Services Interface.
- 6 Restart the client.

Add Directory Number to the Device for Desktop Applications

You must add directory numbers to devices in Cisco Unified Communications Manager. This topic provides instructions on adding directory numbers using the **Device > Phone** menu option after you create your device. Under this menu option, only the configuration settings that apply to the phone model or CTI route point display. See the Cisco Unified Communications Manager documentation for more information about different options to configure directory numbers.

Procedure

- Step 1** Locate the Association Information section on the **Phone Configuration** window.
 - Step 2** Select **Add a new DN**.
 - Step 3** Specify a directory number in the **Directory Number** field.
 - Step 4** Specify all other required configuration settings as appropriate.
 - Step 5** Associate end users with the directory number as follows:
 - a) Locate the **Users Associated with Line** section.
 - b) Select **Associate End Users**.
 - c) Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
 - d) Select the appropriate users from the list.
 - e) Select **Add Selected**.
The selected users are added to the voicemail profile.
 - Step 6** Select **Save**.
 - Step 7** Select **Apply Config**.
 - Step 8** Follow the prompts on the **Apply Configuration** window to apply the configuration.
-

Enable Video Rate Adaptation

The client uses video rate adaptation to negotiate optimum video quality. Video rate adaptation dynamically increases or decreases video quality based on network conditions.

To use video rate adaptation, you must enable Real-Time Transport Control Protocol (RTCP) on Cisco Unified Communications Manager .



Note RTCP is enabled on software phone devices by default. However, you must enable RTCP on desk phone devices.

Enable RTCP on Common Phone Profiles

You can enable RTCP on a common phone profile to enable video rate adaptation on all devices that use the profile.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
 - Step 2** Select **Device > Device Settings > Common Phone Profile**.
The **Find and List Common Phone Profiles** window opens.
 - Step 3** Specify the appropriate filters in the **Find Common Phone Profile where** field and then select **Find** to retrieve a list of profiles.
 - Step 4** Select the appropriate profile from the list.
The **Common Phone Profile Configuration** window opens.
 - Step 5** Locate the **Product Specific Configuration Layout** section.
 - Step 6** Select **Enabled** from the **RTCP** drop-down list.
 - Step 7** Select **Save**.
-

Enable RTCP on Device Configurations

You can enable RTCP on specific device configurations instead of a common phone profile. The specific device configuration overrides any settings you specify on the common phone profile.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Device > Phone**.
The **Find and List Phones** window opens.
- Step 3** Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of phones.
- Step 4** Select the appropriate phone from the list.

The **Phone Configuration** window opens.

Step 5 Locate the **Product Specific Configuration Layout** section.

Step 6 Select **Enabled** from the **RTCP** drop-down list.

Step 7 Select **Save**.

Add a CTI Service

The CTI service lets users control devices.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management > User Settings > UC Service**.

The **Find and List UC Services** window opens.

Step 3 Select **Add New**.

The **UC Service Configuration** window opens.

Step 4 In the **Add a UC Service** section, select **CTI** from the **UC Service Type** drop-down list.

Step 5 Select **Next**.

Step 6 Provide details for the instant messaging and presence service as follows:

- a) Specify a name for the service in the **Name** field.
The name you specify displays when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.
- b) Specify the CTI service address in the **Host Name/IP Address** field.
- c) Specify the port number for the CTI service in the **Port** field.

Step 7 Select **Save**.

What to Do Next

Add the CTI service to your service profile.

Apply a CTI Service

After you add a CTI service on Cisco Unified Communications Manager, you must apply it to a service profile so that the client can retrieve the settings.

Before You Begin

- Create a service profile if none already exists or if you require a separate service profile for CTI.
- Add a CTI service.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **User Management > User Settings > Service Profile**.
- Step 3** Find and select your service profile.
- Step 4** In the **CTI Profile** section of the **Service Profile Configuration** window, select up to three services from the following drop-down lists:
- **Primary**
 - **Secondary**
 - **Tertiary**
- Step 5** Select **Save**.
-

Create CTI Remote Devices

CTI remote devices let users control calls on devices other than software phone devices or desk phone devices such as Cisco IP phones.

Extend and Connect Capabilities

Cisco Unified Communications Manager Extend and Connect capabilities let users control calls on devices such as public switched telephone network (PSTN) phones and private branch exchange (PBX) devices.



Note Cisco recommends that you use extend and connect capabilities with Cisco Unified Communications Manager 9.1(1) and later only.

Provisioning CTI Remote Devices

Dedicated Device

You can provision users with dedicated CTI remote devices. For example, each user has a PSTN phone at their workstation. You want to allow the users to make calls with their PSTN phones using the client. You do not plan to provision users with software phone devices or desk phone devices.

To provision CTI remote devices as dedicated devices, you should add remote destinations through the **Cisco Unified CM Administration** interface. This ensures that users can automatically control their phones and place calls when they start the client.

Alternative Device

You can provision CTI remote devices so that users can specify an alternative phone number to their software phone device or desk phone device. For example, each user can work remotely from home. In this case, users can specify their home phone numbers as remote destinations. This allows the users to control home phones with the client.

If you plan to provision CTI remote devices as an alternative device, you should not add remote destinations. Users can add, edit, and delete remote destinations through the client interface.

Enable Users to Modify Remote Destinations

When a user logs in, the client retrieves the user's device list from Cisco Unified Communications Manager.

If that device list contains a software phone device or desk phone device, the client automatically lets users add, edit, and delete remote destinations through the client interface.

If that device list contains only a CTI remote device, the client does not let users add, edit, and delete remote destinations. You must enable users to add, edit, and delete remote destinations in the client configuration.

Using CTI Remote Devices with the Client

If a user is signed in to the client and sets a remote device as active, that device rings when the user receives incoming calls. Additionally, the client routes outgoing calls to the active device when the user is signed in.

If a user is not signed in to the client, and that user receives an incoming call to the directory number, all devices set as remote destinations ring.

Limitations and Known Issues

This section describes limitations and known issues that currently exist for Cisco Unified Communications Manager extend and connect capabilities.

- You can create only one remote destination per user. Do not add two or more remote destinations for a user.
- Two or more users cannot use the same remote destination.
- Users cannot use the same remote destination for multiple devices.
- You cannot provision extend and connect capabilities for devices that you configure as endpoints on the Cisco Unified Communications Manager cluster.
- Incoming calls incorrectly ring on remote devices if the following occurs:
 - 1 A user adds a number for a remote destination.

Cisco Unified Communications Manager routes incoming calls to that remote destination. The user can control the call session with the client.
 - 2 The user changes their phone. For example, the user selects their software phone.

Cisco Unified Communications Manager routes incoming calls to the user's software phone. However, if the user does not answer incoming calls on the software phone within 4 or 5 seconds, the user's remote destination also rings.

To resolve this issue, users must delete numbers for remote destinations when they change their phones.

Enable User Mobility

This task is only for desktop clients.

You must enable user mobility to provision CTI remote devices. If you do not enable mobility for users, you cannot assign those users as owners of CTI remote devices.

Before You Begin

This task is applicable only if:

- You plan to assign Cisco Jabber for Mac or Cisco Jabber for Windows users to CTI remote devices.
- You have Cisco Unified Communication Manager release 9.x and later.

Procedure

- Step 1** Select **User Management > End User**.
The **Find and List Users** window opens.
 - Step 2** Specify the appropriate filters in the **Find User where** field to and then select **Find** to retrieve a list of users.
 - Step 3** Select the user from the list.
The **End User Configuration** window opens.
 - Step 4** Locate the **Mobility Information** section.
 - Step 5** Select **Enable Mobility**.
 - Step 6** Select **Save**.
-

Create CTI Remote Devices

CTI remote devices are virtual devices that monitor and have call control over a user's remote destination.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Device > Phone**.
The **Find and List Phones** window opens.
- Step 3** Select **Add New**.
- Step 4** Select **CTI Remote Device** from the **Phone Type** drop-down list and then select **Next**.
The **Phone Configuration** window opens.
- Step 5** Select the appropriate user ID from the **Owner User ID** drop-down list.
Note Only users for whom you enable mobility are available from the **Owner User ID** drop-down list.
For more information, see *Enable User Mobility*.

Cisco Unified Communications Manager populates the **Device Name** field with the user ID and a **CTIRD** prefix; for example, **CTIRDusername**

- Step 6** Edit the default value in the **Device Name** field, if appropriate.
 - Step 7** Ensure you select an appropriate option from the **Rerouting Calling Search Space** drop-down list in the **Protocol Specific Information** section.
The **Rerouting Calling Search Space** drop-down list defines the calling search space for re-routing and ensures that users can send and receive calls from the CTI remote device.
 - Step 8** Specify all other configuration settings on the **Phone Configuration** window as appropriate.
See the *CTI remote device setup* topic in the Cisco Unified Communications Manager documentation for more information.
 - Step 9** Select **Save**.
The fields to associate directory numbers and add remote destinations become available on the **Phone Configuration** window.
-

Add Directory Number to the Device for Desktop Applications

You must add directory numbers to devices in Cisco Unified Communications Manager. This topic provides instructions on adding directory numbers using the **Device > Phone** menu option after you create your device. Under this menu option, only the configuration settings that apply to the phone model or CTI route point display. See the Cisco Unified Communications Manager documentation for more information about different options to configure directory numbers.

Procedure

- Step 1** Locate the Association Information section on the **Phone Configuration** window.
 - Step 2** Select **Add a new DN**.
 - Step 3** Specify a directory number in the **Directory Number** field.
 - Step 4** Specify all other required configuration settings as appropriate.
 - Step 5** Associate end users with the directory number as follows:
 - a) Locate the **Users Associated with Line** section.
 - b) Select **Associate End Users**.
 - c) Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
 - d) Select the appropriate users from the list.
 - e) Select **Add Selected**.
The selected users are added to the voicemail profile.
 - Step 6** Select **Save**.
 - Step 7** Select **Apply Config**.
 - Step 8** Follow the prompts on the **Apply Configuration** window to apply the configuration.
-

Add a Remote Destination

Remote destinations represent the CTI controllable devices that are available to users.

You should add a remote destination through the **Cisco Unified CM Administration** interface if you plan to provision users with dedicated CTI remote devices. This task ensures that users can automatically control their phones and place calls when they start the client.

If you plan to provision users with CTI remote devices along with software phone devices and desk phone devices, you should not add a remote destination through the **Cisco Unified CM Administration** interface. Users can enter remote destinations through the client interface.



Note

- You should create only one remote destination per user. Do not add two or more remote destinations for a user.
- Cisco Unified Communications Manager does not verify if it can route remote destinations that you add through the **Cisco Unified CM Administration** interface. For this reason, you must ensure that Cisco Unified Communications Manager can route the remote destinations you add.
- Cisco Unified Communications Manager automatically applies application dial rules to all remote destination numbers for CTI remote devices.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **Device > Phone**.
The **Find and List Phones** window opens.

Step 3 Specify the appropriate filters in the **Find Phone where** field to and then select **Find** to retrieve a list of phones.

Step 4 Select the CTI remote device from the list.
The **Phone Configuration** window opens.

Step 5 Locate the **Associated Remote Destinations** section.

Step 6 Select **Add a New Remote Destination**.
The **Remote Destination Information** window opens.

Step 7 Specify JabberRD in the **Name** field.

Restriction You must specify JabberRD in the **Name** field. The client uses only the JabberRD remote destination. If you specify a name other than JabberRD, users cannot access that remote destination.

The client automatically sets the JabberRD name when users add remote destinations through the client interface.

Step 8 Enter the destination number in the **Destination Number** field.

Step 9 Specify all other values as appropriate.

Step 10 Select **Save**.

What to Do Next

Complete the following steps to verify the remote destination and apply the configuration to the CTI remote device:

- 1 Repeat the steps to open the **Phone Configuration** window for the CTI remote device.
- 2 Locate the **Associated Remote Destinations** section.
- 3 Verify the remote destination is available.
- 4 Select **Apply Config**.

**Note**

The **Device Information** section on the **Phone Configuration** window contains a **Active Remote Destination** field.

When users select a remote destination in the client, it displays as the value of **Active Remote Destination**. **none** displays as the value of **Active Remote Destination** if:

- Users do not select a remote destination in the client.
- Users exit or are not signed in to the client.

Add a CTI Service

The CTI service lets users control devices.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **User Management > User Settings > UC Service**.
The **Find and List UC Services** window opens.
- Step 3** Select **Add New**.
The **UC Service Configuration** window opens.
- Step 4** In the **Add a UC Service** section, select **CTI** from the **UC Service Type** drop-down list.
- Step 5** Select **Next**.
- Step 6** Provide details for the instant messaging and presence service as follows:
 - a) Specify a name for the service in the **Name** field.
The name you specify displays when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.
 - b) Specify the CTI service address in the **Host Name/IP Address** field.
 - c) Specify the port number for the CTI service in the **Port** field.
- Step 7** Select **Save**.

What to Do Next

Add the CTI service to your service profile.

Apply a CTI Service

After you add a CTI service on Cisco Unified Communications Manager, you must apply it to a service profile so that the client can retrieve the settings.

Before You Begin

- Create a service profile if none already exists or if you require a separate service profile for CTI.
- Add a CTI service.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **User Management > User Settings > Service Profile**.
- Step 3** Find and select your service profile.
- Step 4** In the **CTI Profile** section of the **Service Profile Configuration** window, select up to three services from the following drop-down lists:
- **Primary**
 - **Secondary**
 - **Tertiary**
- Step 5** Select **Save**.
-

Set Up a CTI Gateway

The client requires a CTI gateway to communicate with Cisco Unified Communications Manager and perform certain functions such as desk phone control.

Add a CTI Gateway Server

This task is applicable only if you have CUCM 8.6 with CUP.

The client requires a CTI gateway to communicate with Cisco Unified Communications Manager and perform certain functions such as desk phone control. The first step to set up a CTI gateway is to add a CTI gateway server on Cisco Unified Presence.

Procedure

- Step 1** Open the **Cisco Unified Presence Administration** interface.
- Step 2** Select **Application > Cisco Jabber > CTI Gateway Server**.
Note In some versions of Cisco Unified Presence, this path is as follows: **Application > Cisco Unified Personal Communicator > CTI Gateway Server**.
The **Find and List CTI Gateway Servers** window opens.
- Step 3** Select **Add New**.
The **CTI Gateway Server Configuration** window opens.
- Step 4** Specify the required details on the **CTI Gateway Server Configuration** window.
- Step 5** Select **Save**.
-

What to Do Next

[Create a CTI Gateway Profile, on page 49](#)

Create a CTI Gateway Profile

After you add a CTI gateway server, you must create a CTI gateway profile and add that server to the profile.

Before You Begin

[Add a CTI Gateway Server, on page 48](#)

Procedure

- Step 1** Open the **Cisco Unified Presence Administration** interface.
- Step 2** Select **Application > Cisco Jabber > CTI Gateway Profile**.
Note In some versions of Cisco Unified Presence, this path is as follows: **Application > Cisco Unified Personal Communicator > CTI Gateway Profile**.
- Step 3** In the **CTI Gateway Profile Configuration** window, specify the required details.
- Step 4** Select **Add Users to Profile** and add the appropriate users to the profile.
- Step 5** Select **Save**.
-

Configure Silent Monitoring and Call Recording

You can set up additional audio path functions for devices such as silent monitoring and call recording.



Note This feature is currently supported on Cisco Jabber for Windows only.

To enable silent monitoring and call recording, you configure Cisco Unified Communications Manager. See the *Monitoring and Recording* section of the *Cisco Unified Communications Manager Features and Services Guide* for step-by-step instructions.

Notes:

- Cisco Jabber does not provide any interface to initiate silent monitoring or call recording. You must use the appropriate software to silently monitor or record calls.
- Cisco Jabber does not currently support monitoring notification tone or recording notification tone.
- You can use silent monitoring and call recording functionality only. Cisco Jabber does not support other functionality such as barging or whisper coaching.
- You might need to download and apply a device package to enable monitoring and recording capabilities on the device, depending on your version of Cisco Unified Communications Manager. Before you start configuring the server, do the following:

- 1 Open the **Phone Configuration** window for the device on which you plan to enable silent monitoring and call recording.
- 2 Locate the **Built In Bridge** field.

If the **Built In Bridge** field is not available on the **Phone Configuration** window, you should download and apply the most recent device packages.

Before You Begin

This feature is supported for on-premises deployment and requires Cisco Unified Communications Manager, Release 8.6.

Enable URI Dialing

URI dialing allows users to make calls and resolve contacts with Uniform Resource Identifiers (URI). For example, a user named Adam McKenzie has the following SIP URI associated with his directory number: `amckenzi@example.com`. URI dialing enables users to call Adam with his SIP URI rather than his directory number.

For detailed information on URI dialing requirements, such as valid URI formats, as well as advanced configuration including ILS setup, see the *URI Dialing* section of the *Cisco Unified Communications Manager System Guide*.

Before You Begin

This feature is supported for on-premises deployment. You can enable URI dialing on Cisco Unified Communications Manager, release 9.1(2) or later.

Associate URIs to Directory Numbers

When users make URI calls, Cisco Unified Communications Manager routes the inbound calls to the directory numbers associated to the URIs. For this reason, you must associate URIs with directory numbers. You can either automatically populate directory numbers with URIs or configure directory numbers with URIs.

Automatically Populate Directory Numbers with URIs

When you add users to Cisco Unified Communications Manager, you populate the **Directory URI** field with a valid SIP URI. Cisco Unified Communications Manager saves that SIP URI in the end user configuration.

When you specify primary extensions for users, Cisco Unified Communications Manager populates the directory URI from the end user configuration to the directory number configuration. In this way, automatically populates the directory URI for the user's directory number. Cisco Unified Communications Manager also places the URI in the default partition, which is **Directory URI**.

The following task outlines, at a high level, the steps to configure Cisco Unified Communications Manager so that directory numbers inherit URIs:

Procedure

- Step 1** Add devices.
 - Step 2** Add directory numbers to the devices.
 - Step 3** Associate users with the devices.
 - Step 4** Specify primary extensions for users.
-

What to Do Next

Verify that the directory URIs are associated with the directory numbers.

Configure Directory Numbers with URIs

You can specify URIs for directory numbers that are not associated with users. You should configure directory numbers with URIs for testing and evaluation purposes only.

To configure directory numbers with URIs, do the following:

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
 - Step 2** Select **Call Routing > Directory Number**.
The **Find and List Directory Numbers** window opens.
 - Step 3** Find and select the appropriate directory number.
The **Directory Number Configuration** window opens.
 - Step 4** Locate the **Directory URIs** section.
 - Step 5** Specify a valid SIP URI in the **URI** column.
 - Step 6** Select the appropriate partition from the **Partition** column.
Note You cannot manually add URIs to the system **Directory URI** partition. You should add the URI to the same route partition as the directory number.
 - Step 7** Add the partition to the appropriate calling search space so that users can place calls to the directory numbers.
 - Step 8** Select **Save**.
-

Associate the Directory URI Partition

You must associate the default partition into which Cisco Unified Communications Manager places URIs with a partition that contains directory numbers.



Important To enable URI dialing, you must associate the default directory URI partition with a partition that contains directory numbers.

If you do not already have a partition for directory numbers within a calling search space, you should create a partition and configure it as appropriate.

Procedure

-
- Step 1** Open the **Cisco Unified CM Administration** interface.
 - Step 2** Select **System > Enterprise Parameters**.
The **Enterprise Parameters Configuration** window opens.
 - Step 3** Locate the **End User Parameters** section.
 - Step 4** In the **Directory URI Alias Partition** row, select the appropriate partition from the drop-down list.
 - Step 5** Click **Save**.
-

The default directory URI partition is associated with the partition that contains directory numbers. As a result, Cisco Unified Communications Manager can route incoming URI calls to the correct directory numbers.

You should ensure the partition is in the appropriate calling search space so that users can place calls to the directory numbers.

Enable FQDN in SIP Requests for Contact Resolution

To enable contact resolution with URIs, you must ensure that Cisco Unified Communications Manager uses the fully qualified domain name (FQDN) in SIP requests.

Procedure

-
- Step 1** Open the **Cisco Unified CM Administration** interface.
 - Step 2** Select **Device > Device Settings > SIP Profile**.
The **Find and List SIP Profiles** window opens.
 - Step 3** Find and select the appropriate SIP profile.
Remember You cannot edit the default SIP profile. If required, you should create a copy of the default SIP profile that you can modify.
 - Step 4** Select **Use Fully Qualified Domain Name in SIP Requests** and then select **Save**.
-

What to Do Next

Associate the SIP profile with all devices that have primary extensions to which you associate URIs.

Call Pickup

Call pickup allows users to pick up incoming calls within their own group. Directory numbers are assigned to call pickup groups and Cisco Unified Communications Manager automatically dials the appropriate call pickup group number. Users select **Pickup** to answer the call.

Group call pickup allows users to pick up incoming calls in another group. Users enter the group pickup number, select **Pickup** and Cisco Unified Communications Manager automatically dials the appropriate call pickup group number.

Other group pickup allows users to pick up incoming calls in a group that is associated with their group. When the user selects **Other Pickup** Cisco Unified Communications Manager automatically searches for the incoming call in the associated groups.

Directed call pickup allows users to pick up an incoming call on a directory number. Users enter the directory number, select **Pickup** and Cisco Unified Communications Manager connects the incoming call.

For more information on configuring call pickup, see the call pickup topics in the relevant Cisco Unified Communications Manager documentation.

Call pickup notifications

For multiple incoming calls, the notification displayed is *Call(s) available for pickup*. When the user selects the call, the call answered is the longest call in the group.

Deskphone mode

In desk phone mode the following limitations apply:

- The Cisco Unified Communications Manager notification settings are not supported for the pickup group. The call pickup notification displayed is *CallerA->CallerB*.
- The Cisco Unified Communications Manager settings for audio and visual settings are not supported. The visual alerts are always displayed.

Shared line behavior

For users that have a deskphone and a CSF softphone with a shared line the following limitations occur:

- Attempt to pickup a call using the softphone when there is no call available, *No call available for Pickup* is displayed on the deskphone.
- Attempt to pickup a call using the deskphone when there is no call available, *No call available for Pickup* is displayed on the softphone.

User not a member of an associated group

For an incoming call to another pickup group where the user is not a member of an associated group:

- Directed call pickup can be used to pickup the incoming call.
- Group pickup does not work

Expected behavior using group call pickup and directed call pickup

The following are expected behaviors when using group call pickup and directed call pickup:

- Enter an invalid number
 - Softphone mode—The conversation window appears and the annunciator is heard immediately
 - Deskphone mode—The conversation window, fast busy tone, or the annunciator followed by the fast busy tone, *Pickup failed* error message.
- Enter a valid number and no current call available to pick up
 - Softphone mode—Tone in headset, no conversation window appears and *No call available for pickup* error message.
 - Deskphone mode—No conversation window and *No call available for pickup* error message.
- Enter directory number of a phone in an associated group and no current call available to pick up
 - Softphone mode—Tone in headset, no conversation window appears and *No call available for pickup* error message.
 - Deskphone mode—No conversation window and *No call available for pickup* error message.
- Enter a directory number of a phone on the same Cisco Unified Communications Manager and not in an associated group
 - Softphone mode—Conversation window appears and fast busy tone.
 - Deskphone mode—Conversation window appears, fast busy tone, and *Pickup failed* error message.
- Enter first digits of a valid group
 - Softphone mode—Tone in headset, conversation window appears, and after 15 seconds annunciator followed by the fast busy tone.
 - Deskphone mode—Conversation window appears, after 15 seconds annunciator, fast busy tone, and *Pickup failed* error message.

Call pickup using a deskphone that is not in a call pickup group

User attempting a call pickup from a deskphone that is not in a call pickup group. The conversation window will appear for a moment. The user should not be configured to use the call pickup feature if they are not members of a call pickup group.

Original recipient information not available

When Cisco Unified Communications Manager *Auto Call Pickup Enabled* setting is true, the recipient information is not available in the client when the call is picked up in softphone mode. If the setting is false, the recipient information is available.

Configure Call Pickup Group

Call pickup groups allow users to pick up incoming calls in their own group.

Procedure

- Step 1** Open the **Cisco Unified Communication Manager** interface.
- Step 2** Select **Call Routing > Call Pickup Group**
The **Find and List Call Pickup Groups** window opens.
- Step 3** Select **Add New**
The **Call Pickup Group Configuration** window opens.
- Step 4** Enter call pickup group information:
- Specify a unique name for the call pickup group.
 - Specify a unique directory number for the call pickup group number.
 - Enter a description.
 - Select a partition.
- Step 5** (Optional) Configure the audio or visual notification in the **Call Pickup Group Notification Settings** section.
- Select the notification policy.
 - Specify the notification timer.
- For further information on call pickup group notification settings see the call pickup topics in the relevant Cisco Unified Communications Manager documentation.
- Step 6** Select **Save**.
-

What to Do Next

Assign a call pickup group to directory numbers.

Assign Directory Number

Assign a call pickup group to a directory number. Only directory numbers that are assigned to a call pickup group can use call pickup, group call pickup, other group pickup, and directed call pickup.

Before You Begin

Before you assign a call pickup group to a directory number, you must create the call pickup group.

Procedure

- Step 1** Open the **Cisco Unified Communications Manager Administration** interface.
- Step 2** Assign a call pickup group to a directory number using one of the following methods:
- Select **Call Routing > Directory Number**, find and select your directory number and in the Call Forward and Call Pickup Settings area select the call pickup group from the call pickup group drop down list.
 - Select **Device > Phone**, find and select your phone and in the **Association Information** list choose the directory number to which the call pickup group will be assigned.

Step 3 To save the changes in the database, select **Save**.

Other Call Pickup

Other Group Pickup allows users to pick up incoming calls in a group that is associated with their own group. The Cisco Unified Communications Manager automatically searches for the incoming call in the associated groups to make the call connection when the user selects **Other Pickup**.

Configure Other Call Pickup

Other Group Pickup allows users to pick up incoming calls in an associated group. Cisco Unified Communications Manager automatically searches for the incoming call in the associated groups to make the call connection when the user selects **Other Pickup**.

Before You Begin

Before you begin, configure call pickup groups.

Procedure

- Step 1** Open the **Cisco Unified Communication Manager Administration** interface.
- Step 2** Select **Call Routing > Call Pickup Group**
The **Find and List Call Pickup Groups** window opens.
- Step 3** Select your call pickup group.
The **Call Pickup Group Configuration** window opens.
- Step 4** In the **Associated Call Pickup Group Information** section, you can do the following:
- Find call pickup groups and add to current associated call pickup groups.
 - Reorder associated call pickup groups or remove call pickup groups.
- Step 5** Select **Save**.
-

Directed Call Pickup

Directed Call Pickup allows a user to pick up a incoming call directly. The user enters the directory number in the client and selects **Pickup**. Cisco Unified Communications Manager uses the associated group mechanism to control if the user can pick up an incoming call using Directed Call Pickup.

To enable directed call pickup, the associated groups of the user must contain the pickup group to which the directory number belongs.

When the user invokes the Directed Call Pickup feature and enters a directory number to pick up an incoming call, the user connects to the call that is incoming to the specified phone whether or not the call is the longest incoming call in the call pickup group to which the directory number belongs.

Configure Directed Call Pickup

Directed call pickup allows you to pick up a incoming call directly. The user enters the directory number in the client and selects **Pickup**. Cisco Unified Communications Manager uses the associated group mechanism to control if the user can pick up an incoming call using Directed Call Pickup.

To enable directed call pickup, the associated groups of the user must contain the pickup group to which the directory number belongs.

When the user invokes the feature and enters a directory number to pick up an incoming call, the user connects to the call that is incoming to the specified phone whether or not the call is the longest incoming call in the call pickup group to which the directory number belongs.

Procedure

-
- Step 1** Configure call pickup groups and add associated groups. The associated groups list can include up to 10 groups.
For more information, see topics related to defining a pickup group for Other Group Pickup.
- Step 2** Enable the Auto Call Pickup Enabled service parameter to automatically answer calls for directed call pickups.
For more information, see topics related to configuring Auto Call Pickup.
-

Auto Call Pickup

You can automate call pickup, group pickup, other group pickup, and directed call pickup by enabling the Auto Call Pickup Enabled service parameter.

When this parameter is enabled, Cisco Unified Communications Manager automatically connects users to the incoming call in their own pickup group, in another pickup group, or a pickup group that is associated with their own group after users select the appropriate pickup on the phone. This action requires only one keystroke.

Auto call pickup connects the user to an incoming call in the group of the user. When the user selects **Pickup** on the client, Cisco Unified Communications Manager locates the incoming call in the group and completes the call connection. If automation is not enabled, the user must select **Pickup** and answer the call, to make the call connection.

Auto group call pickup connects the user to an incoming call in another pickup group. The user enters the group number of another pickup group and selects **Pickup** on the client. Upon receiving the pickup group number, Cisco Unified Communications Manager completes the call connection. If auto group call pickup is not enabled, dial the group number of another pickup group, select **Pickup** on the client, and answer the call to make the connection.

Auto other group pickup connects the user to an incoming call in a group that is associated with the group of the user. The user selects **Other Pickup** on the client. Cisco Unified Communications Manager automatically searches for the incoming call in the associated groups in the sequence that the administrator enters in the **Call Pickup Group Configuration** window and completes the call connection after the call is found. If automation is not enabled, the user must select **Other Pickup**, and answer the call to make the call connection.

Auto directed call pickup connects the user to an incoming call in a group that is associated with the group of the user. The user enters the directory number of the ringing phone and selects **Pickup** on the client. Upon receiving the directory number, Cisco Unified Communications Manager completes the call connection. If

auto directed call pickup is not enabled, the user must dial the directory number of the ringing phone, select **Pickup**, and answer the call that will now ring on the user phone to make the connection.

For more information on **Call Pickup**, see the relevant Cisco Unified Communications Manager documentation.

Configure Auto Call Pickup

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **System > Service Parameters**
- Step 3** Select your server from the Server drop down list and then select the **Cisco Call Manager** service from the Service drop down list.
- Step 4** In the **Clusterwide Parameters (Feature - Call Pickup)** section, select one of the following for **Auto Call Pickup Enabled**:
- true — The auto call pickup feature is enabled.
 - false — The auto call pickup feature is not enabled. This is the default value.
- Step 5** Select **Save**.
-

Hunt Group

A hunt pilot contains a hunt pilot number and an associated hunt list. Hunt pilots provide flexibility in network design. They work in conjunction with route filters and hunt lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

A hunt list contains a set of line groups in a specific order. A single line group can appear in multiple hunt lists. The group call pickup feature and directed call pickup feature do not work with hunt lists.

A line group comprises a group of directory numbers in a specific order. The order controls the progress of the search for available directory numbers for incoming calls.

Cisco Unified Communications Manager determines a call that is to be routed through a defined hunt list, Cisco Unified Communications Manager finds the first available device on the basis of the order of the line groups that a hunt list defines.

Cisco Unified Communications Manager 9.x and later allows configuring of automatic log out of a hunt member when there is no answer.

Logout notification

When a user is auto logged out, manually logged out or logged out by the Cisco Unified Communications Manager administrator a logout notification is displayed.

Line Group

A line group allows you to designate the order in which directory numbers are chosen. Cisco Unified Communications Manager distributes a call to an idle or available member of a line group based on the call distribution algorithm and on the Ring No Answer (RNA) Reversion timeout setting.

Users cannot pick up calls to a DN that belongs to a line group by using the directed call pickup feature.

Configure Line Group

Before You Begin

Configure directory numbers.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Call Routing > Route/Hunt > Line Group**.
The **Find and List Line Groups** window opens.
- Step 3** Select **Add New**.
The **Line Group Configuration** window opens.
- Step 4** Enter settings in the **Line Group Information** section as follows:
- 1 Specify a unique name in the **Line Group Name** field.
 - 2 Specify number of seconds for **RNA Reversion Timeout**.
 - 3 Select a **Distribution Algorithm** to apply to the line group.
- Step 5** Enter settings in the **Hunt Options** section as follows:
- Select a value for **No Answer** from the drop-down list.
 - Select **Automatically Logout Hunt Member on No Answer** to configure auto logout of the hunt list.
 - Select a value for **Busy** from the drop-down list.
 - Select a value for **Not Available** from the drop-down list.
- Step 6** In the **Line Group Member Information** section, you can do the following:
- Find directory numbers or route partitions to add to the line group.
 - Reorder the directory numbers or route partitions in the line group.
 - Remove directory numbers or route partitions from the line group.
- Step 7** Select **Save**.
-

What to Do Next

Configure a hunt list and add the line group to the hunt list.

Hunt List

A hunt list contains a set of line groups in a specific order. A hunt list associates with one or more hunt pilots and determines the order in which those line groups are accessed. The order controls the progress of the search for available directory numbers for incoming calls.

A hunt list comprises a collection of directory numbers as defined by line groups. After Cisco Unified Communications Manager determines a call that is to be routed through a defined hunt list, Cisco Unified Communications Manager finds the first available device on the basis of the order of the line group(s) that a hunt list defines.

The group call pickup feature and directed call pickup feature do not work with hunt lists.

A hunt list can contain only line groups. Each hunt list should have at least one line group. Each line group includes at least one directory number. A single line group can appear in multiple hunt lists.

Configure Hunt List

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Call Routing > Route/Hunt > Hunt List**.
The **Find and Hunt List Groups** window opens.
- Step 3** Select **Add New**.
The **Hunt List Configuration** window opens.
- Step 4** Enter settings in the **Hunt List Information** section as follows:
- 1 Specify a unique name in the **Name** field.
 - 2 Enter a description for the Hunt List.
 - 3 Select a **Cisco Unified Communications Manager Group** from the drop-down list.
 - 4 The system selects **Enable this Hunt List** by default for a new hunt list when the hunt list is saved.
 - 5 If this hunt list is to be used for voice mail, select **For Voice Mail Usage**.
- Step 5** Select **Save** to add the hunt list.
-

What to Do Next

Add line groups to the hunt list.

Add Line Group to Hunt List

Before You Begin

You must configure line groups and configure a hunt list.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
 - Step 2** Select **Call Routing > Route/Hunt > Hunt List**.
The **Find and Hunt List Groups** window opens.
 - Step 3** Locate the hunt list to which you want to add a line group.
 - Step 4** To add a line group, select **Add Line Group**.
The **Hunt List Detail Configuration** window displays.
 - Step 5** Select a line group from the **Line Group** drop-down list.
 - Step 6** To add the line group, select **Save**.
 - Step 7** To add additional line groups, repeat Step 4 to Step 6.
 - Step 8** Select **Save**.
 - Step 9** To reset the hunt list, select **Reset**. When the dialog box appears, select **Reset**.
-

Hunt Pilot

A hunt pilot comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a hunt list. Hunt pilots provide flexibility in network design. They work in conjunction with route filters and hunt lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

For more detailed information on the configuration options for hunt pilots, see the relevant Cisco Unified Communications Manager documentation.

Configure Hunt Pilot

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Call Routing > Route/Hunt > Hunt Pilot**.
The **Find and List Hunt Pilots** window opens.
- Step 3** Select **Add New**.
The **Hunt Pilot Configuration** window opens.

- Step 4** Enter the hunt pilot, including numbers and wildcards.
 - Step 5** Select a hunt list from the **Hunt List** drop-down list.
 - Step 6** Enter any additional configurations in the **Hunt Pilot Configuration** window. For more information on hunt pilot configuration settings, see the relevant Cisco Unified Communications Manager documentation.
 - Step 7** Select **Save**.
-

Configure User Associations

When you associate a user with a device, you provision that device to the user.

Before You Begin

Create and configure Cisco Jabber devices.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **User Management > End User**.
The **Find and List Users** window opens.
- Step 3** Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
- Step 4** Select the appropriate user from the list.
The **End User Configuration** window opens.
- Step 5** Locate the **Service Settings** section.
- Step 6** Select **Home Cluster**.
- Step 7** Select the appropriate service profile for the user from the **UC Service Profile** drop-down list.
- Step 8** Locate the **Device Information** section.
- Step 9** Select **Device Association**.
The **User Device Association** window opens.
- Step 10** Select the devices to which you want to associate the user.
- Step 11** Select **Save Selected/Changes**.
- Step 12** Select **User Management > End User** and return to the **Find and List Users** window.
- Step 13** Find and select the same user from the list.
The **End User Configuration** window opens.
- Step 14** Locate the **Permissions Information** section.
- Step 15** Select **Add to Access Control Group**.
The **Find and List Access Control Groups** dialog box opens.
- Step 16** Select the access control groups to which you want to assign the user.
At a minimum you should assign the user to the following access control groups:
 - **Standard CCM End Users**
 - **Standard CTI Enabled**

Remember If you are provisioning users with secure phone capabilities, do not assign the users to the **Standard CTI Secure Connection** group.

Certain phone models require additional control groups, as follows:

- Cisco Unified IP Phone 9900, 8900, or 8800 series or DX series, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**.
- Cisco Unified IP Phone 6900 series, select **Standard CTI Allow Control of Phones supporting Rollover Mode**.

Step 17 Select **Add Selected**.
The **Find and List Access Control Groups** window closes.

Step 18 Select **Save** on the **End User Configuration** window.

Specify Your TFTP Server Address

The client gets device configuration from the TFTP server. For this reason, you must specify your TFTP server address when you provision users with devices.



Attention

If the client gets the `_cisco-uds` SRV record from a DNS query, it can automatically locate the user's home cluster. As a result, the client can also locate the Cisco Unified Communications Manager TFTP service.

You do not need to specify your TFTP server address if you deploy the `_cisco-uds` SRV record.

Specify Your TFTP Server on Cisco Unified Communications Manager IM and Presence Service

If you are using Cisco Unified Communications Manager release 8.x, complete the steps to specify the address of your TFTP server on Cisco Unified Communications Manager. If you are using Cisco Unified Communications Manager release 9.x, then you do not need to follow the steps below.

Procedure

- Step 1** Open the **Cisco Unified CM IM and Presence Administration** interface.
- Step 2** Select **Application > Legacy Clients > Settings**.
The **Legacy Client Settings** window opens.
- Step 3** Locate the **Legacy Client Security Settings** section.
- Step 4** Specify the IP address of your primary and backup TFTP servers in the following fields:
- **Primary TFTP Server**
 - **Backup TFTP Server**
 - **Backup TFTP Server**

Step 5 Select **Save**.

Specify Your TFTP Server on Cisco Unified Presence

If you are using Cisco Unified Communications Manager release 8.x, complete the steps to specify the address of your TFTP server on Cisco Unified Presence. If you are using Cisco Unified Communications Manager release 9.x, then you do not need to follow the steps below.

Procedure

Step 1 Open the **Cisco Unified Presence Administration** interface.

Step 2 Select **Application > Cisco Jabber > Settings**.

Note In some versions of Cisco Unified Presence, this path is as follows: **Application > Cisco Unified Personal Communicator > Settings**.

The **Cisco Jabber Settings** window opens.

Step 3 Locate the fields to specify TFTP servers in one of the following sections, depending on your version of Cisco Unified Presence:

- **Cisco Jabber Security Settings**
- **CUPC Global Settings**

Step 4 Specify the IP address of your primary and backup TFTP servers in the following fields:

- **Primary TFTP Server**
- **Backup TFTP Server**
- **Backup TFTP Server**

Note Ensure that you enter the fully qualified domain name (FQDN) or IP address for the TFTP servers rather than a host name.

Step 5 Select **Save**.

Specify TFTP Servers in Phone Mode

If you deploy the client in phone mode you can provide the address of the TFTP server as follows:

- Users manually enter the TFTP server address when they start the client.
- You specify the TFTP server address during installation with the TFTP argument.
- You specify the TFTP server address in the Microsoft Windows registry.

Specify TFTP Servers with the Cisco WebEx Administration Tool

If the client connects to the Cisco WebEx Messenger service, you specify your TFTP server address with the Cisco WebEx Administrator Tool.

Procedure

- Step 1** Open the Cisco WebEx Administrator Tool.
 - Step 2** Select the **Configuration** tab.
 - Step 3** Select **Unified Communications** in the **Additional Services** section.
The **Unified Communications** window opens.
 - Step 4** Select the **Clusters** tab.
 - Step 5** Select the appropriate cluster from the list.
The **Edit Cluster** window opens.
 - Step 6** Select **Advanced Server Settings** in the **Cisco Unified Communications Manager Server Settings** section.
 - Step 7** Specify the IP address of your primary TFTP server in the **TFTP Server** field.
 - Step 8** Specify the IP address of your backup TFTP servers in the **Backup Server #1** and **Backup Server #2** fields.
 - Step 9** Select **Save**.
The **Edit Cluster** window closes.
 - Step 10** Select **Save** in the **Unified Communications** window.
-

Reset Devices

After you create and associate users with devices, you should reset those devices.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Device > Phone**.
The **Find and List Phones** window opens.
- Step 3** Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of devices.
- Step 4** Select the appropriate device from the list.
The **Phone Configuration** window opens.
- Step 5** Locate the **Association Information** section.
- Step 6** Select the appropriate directory number configuration.
The **Directory Number Configuration** window opens.
- Step 7** Select **Reset**.

The **Device Reset** dialog box opens.

- Step 8** Select **Reset**.
- Step 9** Select **Close** to close the **Device Reset** dialog box.
-

What to Do Next

[Create a CCMCIP Profile, on page 66](#)

Create a CCMCIP Profile

The client gets device lists for users from the CCMCIP server.



Note If the client gets the `_cisco-uds SRV` record from a DNS query, it can automatically locate the user's home cluster and discover services. One of the services the client discovers is UDS, which replaces CCMCIP.

Before You Begin

[Reset Devices, on page 65](#)

Procedure

- Step 1** Open the **Cisco Unified CM IM and Presence Administration** interface.
- Step 2** Select **Application > Legacy Clients > CCMCIP Profile**.
- Step 3** In the **Find and List CCMCIP Profiles** window, select **Add New**.
- Step 4** In the **CCMCIP Profile Configuration** window, specify service details in the CCMCIP profile as follows:
- Specify a name for the profile in the **Name** field.
 - Specify the fully qualified domain name or IP address of your primary CCMCIP service in the **Primary CCMCIP Host** field.
 - Specify the fully qualified domain name or IP address of your backup CCMCIP service in the **Backup CCMCIP Host** field.
 - Leave the default value for **Server Certificate Verification**.
- Step 5** Add users to the CCMCIP profile as follows:
- Select **Add Users to Profile**.
 - In the **Find and List Users** dialog, specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
 - Select the appropriate users from the list.
 - Select **Add Selected**.
The selected users are added to the CCMCIP profile.
- Step 6** Select **Save**.
-

What to Do Next

[Dial Plan Mapping](#), on page 67

Dial Plan Mapping

You configure dial plan mapping to ensure that dialing rules on Cisco Unified Communications Manager match dialing rules on your directory.

Application Dial Rules

Application dial rules automatically add or remove digits in phone numbers that users dial. Application dialing rules manipulate numbers that users dial from the client.

For example, you can configure a dial rule that automatically adds the digit 9 to the start of a 7 digit phone number to provide access to outside lines.

Directory Lookup Dial Rules

Directory lookup dial rules transform caller ID numbers into numbers that the client can lookup in the directory. Each directory lookup rule you define specifies which numbers to transform based on the initial digits and the length of the number.

For example, you can create a directory lookup rule that automatically removes the area code and two-digit prefix digits from 10-digit phone numbers. An example of this type of rule is to transform 4089023139 into 23139.

Publish Dial Rules

Cisco Unified Communications Manager release 8.6.1 or earlier does not automatically publish dial rules to the client. For this reason, you must deploy a COP file to publish your dial rules. This COP file copies your dial rules from the Cisco Unified Communications Manager database to an XML file on your TFTP server. The client can then download that XML file and access your dial rules.



Remember

You must deploy the COP file every time you update or modify dial rules on Cisco Unified Communications Manager release 8.6.1 or earlier.

Before You Begin

- 1 Create your dial rules in Cisco Unified Communications Manager.
- 2 Download the Cisco Jabber administration package from cisco.com.
- 3 Copy `cmterm-cupc-dialrule-wizard-0.1.cop.sgn` from the Cisco Jabber administration package to your file system.

Procedure

-
- Step 1** Open the **Cisco Unified OS Administration** interface.
- Step 2** Select **Software Upgrades > Install/Upgrade**.
- Step 3** Specify the location of `cmterm-cupc-dialrule-wizard-0.1.cop.sgn` in the **Software Installation/Upgrade** window.
- Step 4** Select **Next**.
- Step 5** Select `cmterm-cupc-dialrule-wizard-0.1.cop.sgn` from the **Available Software** list.
- Step 6** Select **Next** and then select **Install**.
- Step 7** Restart the TFTP service.
- Step 8** Open the dial rules XML files in a browser to verify that they are available on your TFTP server.
- Navigate to `http://tftp_server_address:6970/CUPC/AppDialRules.xml`.
 - Navigate to `http://tftp_server_address:6970/CUPC/DirLookupDialRules.xml`.
- If you can access `AppDialRules.xml` and `DirLookupDialRules.xml` with your browser, the client can download your dial rules.
- Step 9** Repeat the preceding steps for each Cisco Unified Communications Manager instance that runs a TFTP service.
-

What to Do Next

After you repeat the preceding steps on each Cisco Unified Communications Manager instance, restart the client.

Set Up Mobile Connect

Mobile connect, formerly known as Single Number Reach (SNR), allows the native mobile phone number to ring when someone calls the work number if:

- Cisco Jabber is not available.
After Cisco Jabber becomes available again and connects to the corporate network, the Cisco Unified Communications Manager returns to placing VoIP calls rather than using mobile connect.
- The user selects the **Mobile Voice Network** calling option.
- The user selects the **Autoselect** calling option and the user is outside of the Wi-Fi network.

To set up mobile connect, perform the following procedures:

- 1 Enable mobile connect. See the *Enable Mobile Connect* topic.
- 2 Specify one or more remote phone numbers to which mobile connect connects using one or both of the following procedures:
 - (Preferred) To specify the mobile phone number of the mobile device, see the *Add Mobility Identity* topic.
 - (Optional) To specify alternate phone numbers, see the *Add Remote Destination (Optional)* topic.

Alternate numbers can be any type of phone number, such as home phone numbers, conference room numbers, desk phone numbers, or a mobile phone number for a second mobile device.

- 3 Test your settings:
 - Exit Cisco Jabber on the mobile device. For instructions, see the User Guide for your release.
 - Call the Cisco Jabber extension from another phone.
 - Verify that the native mobile network phone number rings and that the call connects when you answer it.

Enable Mobile Connect

Use the following procedure to enable mobile connect for an end user.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Search for and delete any existing remote destination or mobility Identity that is already set up with the mobile phone number as follows:
 - a) Select **Device > Remote Destination**.
 - b) Search for the destination number.
 - c) Delete the destination number.
- Step 3** Configure the end user for mobile connect as follows:
 - a) Select **User Management > End User**.
 - b) Search for the end user.
 - c) Select the user id to open the **End User Configuration** window.
 - d) In the Mobility Information section, check the **Enable Mobility** check box.
 - e) On Cisco Unified Communications Manager Release 9.0 and earlier, specify the Primary User Device.
 - f) Select **Save**.
- Step 4** Configure the device settings for mobile connect as follows:
 - a) Navigate to **Device > Phone**.
 - b) Search for the device that you want to configure.
 - c) Select the device name to open the **Phone Configuration** window.
 - d) Enter the following information:

Setting	Information
Softkey Template	Choose a softkey template that includes the Mobility button. For information about setting up softkey templates, see the related information in the <i>Cisco Unified Communications Manager Administration Guide</i> for your release. This documentation can be found in the maintenance guides list.
Mobility User ID	Select the user.
Owner User ID	Select the user. The value must match the mobility user ID.

Setting	Information
Rerouting Calling Search Space	<p>Choose a Rerouting Calling Search Space that includes both of the following:</p> <ul style="list-style-type: none"> • The partition of the desk phone extension of the user. This requirement is used by the system to provide the Dial via Office feature, not for routing calls. • A route to the mobile phone number. The route to the mobile phone number (that is, the Gateway/Trunk partition) must have a higher preference than the partitions of the enterprise extension that is associated with the device. <p>Note Cisco Jabber allows users to specify a callback number for Dial via Office-Reverse calls that is different from the mobile phone number of the device, and the Rerouting Calling Search Space controls which callback numbers are reachable.</p> <p>If the user sets up the DvO Callback Number with an alternate number, ensure that you set up the trunk Calling Search Space (CSS) to route to destination of the alternate phone number.</p>

e) Select **Save**.

Add Mobility Identity

Use this procedure to add a mobility identity to specify the mobile phone number of the mobile device as the destination number. This destination number is used by features such as Dial via Office or mobile connect.

You can specify only one number when you add a mobility identity. If you want to specify an alternate number such as a second mobile phone number for a mobile device, you can set up a remote destination. The mobility identity configuration characteristics are identical to those of the remote destination configuration.

Procedure

-
- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Navigate to the device that you want to configure as follows:
- Select **Device > Phone**.
 - Search for the device that you want to configure.
 - Select the device name to open the **Phone Configuration** window.
- Step 3** In the **Associated Mobility Identity** section, select **Add a New Mobility Identity**.
- Step 4** Enter the mobile phone number as the destination number.
You must be able to rout this number to an outbound gateway. Generally, the number is the full E.164 number.

Note If you enable the Dial via Office — Reverse feature for a user, you must enter a destination number for the user's mobility identity.

If you enable Dial via Office — Reverse and leave the destination number empty in the mobility identity:

- The phone service cannot connect if the user selects the **Autoselect** calling option while using a mobile data network and VPN.
- The phone service cannot connect if the user selects the **Mobile Voice Network** calling option on any type of network.
- The logs do not indicate why the phone service cannot connect.

Step 5 Enter the initial values for call timers.

These values ensure that calls are not routed to the mobile service provider voicemail before they ring in the client on the mobile device. You can adjust these values to work with the end user's mobile network. For more information, see the online help in Cisco Unified Communications Manager.

The following is an example of mobility Identity timers' information in Cisco Unified Communications Manager 9.x.

Setting	Suggested Initial Value
Answer Too Soon Timer	3000
Answer Too Late Timer	20000
Delay Before Ringing Timer	0 Note This setting does not apply to DvO-R calls.

The following is an example of mobility Identity timers' information in Cisco Unified Communications Manager 10.x.

Setting	Suggested Initial Value
Wait * before ringing this phone when my business line is dialed.*	0.0 seconds
Prevent this call from going straight to this phone's voicemail by using a time delay of * to detect when calls go straight to voicemail.*	3.0 seconds
Stop ringing this phone after * to avoid connecting to this phone's voicemail.*	20.0 seconds

Step 6 Do one of the following:

- Cisco Unified Communications Manager release 9 or earlier — Check the **Enable Mobile Connect** check box.

- Cisco Unified Communications Manager release 10 — Check the **Enable Single Number Reach** check box.

Step 7 If you are setting up the Dial via Office feature, in the Mobility Profile drop-down list, select one of the following options.

Option	Description
Leave blank	Choose this option if you want users to use the Enterprise Feature Access Number (EFAN).
Mobility Profile	Choose the mobility profile that you just created if you want users to use a mobility profile instead of an EFAN.

Step 8 Set up the schedule for routing calls to the mobile number.

Step 9 Select **Save**.

Add Remote Destination (Optional)

Use this procedure to add a remote destination to specify any alternate number as the destination number. The Mobility Identity configuration characteristics are identical to those of the remote destination configuration.

Alternate numbers can be any type of phone number, such as home phone numbers, conference room numbers, desk phone numbers, or multiple mobile phone numbers for additional mobile devices. You can add more than one remote destination.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Navigate to the device that you want to configure as follows:

- Select **Device > Phone**.
- Search for the device that you want to configure.
- Select the device name to open the **Phone Configuration** window.

Step 3 In the **Associated Remote Destinations** section, select **Add a New Remote Destination**.

Step 4 Enter the desired phone number as the Destination Number.

You must be able to rout the number to an outbound gateway. Generally, the number is the full E.164 number.

Step 5 Enter the initial values for the following call timers:

- Answer Too Soon Timer**—Enter 3000
- Answer Too Late Timer**— Enter 20000
- Delay Before Ringing Timer**—0
This setting does not apply to DvO-R calls.

These values ensure that calls are not routed to the mobile service provider voicemail before they ring in the client on the mobile device. For more information, see the online help in Cisco Unified Communications Manager.

Step 6 Do one of the following:

- If you have Cisco Unified Communications Manager Version 9 or earlier, check the **Enable Mobile Connect** check box.
- If you have Cisco Unified Communications Manager Version 10, check the **Enable Single Number Reach** check box.

Step 7 Set up the schedule for routing calls to the mobile number.

Step 8 Select **Save**.

Transfer Active VoIP Call to the Mobile Network

Users can transfer an active VoIP call from Cisco Jabber to their mobile phone number on the mobile network. This feature is useful when a user on a call leaves the Wi-Fi network (for example, leaving the building to walk out to the car), or if there are voice quality issues over the Wi-Fi network. This Cisco Jabber feature is called Move to Mobile.

There are two ways to enable this feature. You can also disable it.

Implementation Method	Description	Instructions
Handoff DN	<p>The mobile device calls Cisco Unified Communications Manager using the mobile network.</p> <p>This method requires a Direct Inward Dial (DID) number.</p> <p>The service provider must deliver the DID digits exactly as configured. Alternately, for Cisco IOS gateways with H.323 or SIP communication to Cisco Unified Communications Manager, you can use Cisco IOS to manipulate the inbound called-party number at the gateway, presenting the digits to Cisco Unified Communications Manager exactly as configured on the handoff DN.</p> <p>This method does not work for iPod Touch devices.</p>	See the <i>Enable Handoff from VoIP to Mobile Network</i> topic.
Mobility Softkey	Cisco Unified Communications Manager calls the phone number of the PSTN mobile service provider for the mobile device.	See the <i>Enable Transfer from VoIP to Mobile Network</i> topic.

Implementation Method	Description	Instructions
None of the above	Disable this feature if you do not want to make it available to users.	Select Disabled for the Transfer to Mobile Network option in the Product Specific Configuration Layout section of the TCT device page. Select Disabled for the Transfer to Mobile Network option in the Product Specific Configuration Layout section of the BOT device page.

Enable Handoff from VoIP to Mobile Network

Set up a directory number that Cisco Unified Communications Manager can use to hand off active calls from VoIP to the mobile network. Match the user's caller ID with the Mobility Identity to ensure that Cisco Unified Communications Manager can recognize the user. Set up the TCT device and mobile device to support handoff from VoIP to the mobile network.

Set up a directory number that Cisco Unified Communications Manager can use to hand off active calls from VoIP to the mobile network. Match the user's caller ID with the Mobility Identity to ensure that Cisco Unified Communications Manager can recognize the user. Set up the BOT device and mobile device to support handoff from VoIP to the mobile network.

Set Up Handoff DN

Before You Begin

Determine the required values. The values that you choose depend on the phone number that the gateway passes (for example, seven digits or ten digits).

Procedure

-
- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Call Routing > Mobility > Handoff Configuration**.
- Step 3** Enter the Handoff Number for the Direct Inward Dial (DID) number that the device uses to hand off a VoIP call to the mobile network.
The service provider must deliver the DID digits exactly as configured. Alternately, for Cisco IOS gateways with H.323 or SIP communication to Cisco Unified Communications Manager, you can use Cisco IOS to manipulate the inbound called-party number at the gateway, presenting the digits to Cisco Unified Communications Manager exactly as configured on the handoff number.
- Note** You cannot use translation patterns or other similar manipulations within Cisco Unified Communications Manager to match the inbound DID digits to the configured Handoff DN.
- Step 4** Select the **Route Partition** for the handoff DID.
This partition should be present in the Remote Destination inbound Calling Search Space (CSS), which points to either the Inbound CSS of the Gateway or Trunk, or the Remote Destination CSS.

This feature does not use the remaining options on this page.

Step 5 Select **Save**.

Match Caller ID with Mobility Identity

To ensure that only authorized phones can initiate outbound calls, calls must originate from a phone that is set up in the system. To do this, the system attempts to match the caller ID of the requesting phone number with an existing Mobility Identity. By default, when a device initiates the Handoff feature, the caller ID that is passed from the gateway to Cisco Unified Communications Manager must exactly match the Mobility Identity number that you entered for that device.

However, your system may be set up such that these numbers do not match exactly. For example, Mobility Identity numbers may include a country code while caller ID does not. If so, you must set up the system to recognize a partial match.

Be sure to account for situations in which the same phone number may exist in different area codes or in different countries. Also, be aware that service providers can identify calls with a variable number of digits, which may affect partial matching. For example, local calls may be identified using seven digits (such as 555 0123) while out-of-area calls may be identified using ten digits (such as 408 555 0199).

Before You Begin

Set up the Mobility Identity. See the *Add Mobility Identity* topic.

To determine whether you need to complete this procedure, perform the following steps. Dial in to the system from the mobile device and compare the caller ID value with the Destination Number in the Mobility Identity. If the numbers do not match, you must perform this procedure. Repeat this procedure for devices that are issued in all expected locales and area codes.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
 - Step 2** Select **System > Service Parameters**.
 - Step 3** Select the active server.
 - Step 4** Select the **Cisco CallManager (Active)** service.
 - Step 5** Scroll down to the **Clusterwide Parameters (System - Mobility)** section.
 - Step 6** Select **Matching Caller ID with Remote Destination** and read essential information about this value.
 - Step 7** Select **Partial Match for Matching Caller ID with Remote Destination**.
 - Step 8** Select **Number of Digits for Caller ID Partial Match** and read the essential requirements for this value.
 - Step 9** Enter the required number of digits to ensure partial matches.
 - Step 10** Select **Save**.
-

Set Up User and Device Settings for Handoff

Before You Begin

- Set up the user device on the Cisco Unified Communications Manager.
- Set up the user with a Mobility Identity.

Procedure

-
- Step 1** In the **Cisco Unified CM Administration** interface, go to the TCT Device page, and select **Use Handoff DN Feature** for the **Transfer to Mobile Network** option.
Do not assign this method for iPod Touch devices. Use the Mobility Softkey method instead.
- Step 2** In the **Cisco Unified CM Administration** interface, go to the BOT Device page, and select **Use Handoff DN Feature** for the **Transfer to Mobile Network** option.
- Step 3** On the iOS device, tap **Settings > Phone > Show My Caller ID** to verify that Caller ID is on.
- Step 4** On some Android device and operating system combinations, you can verify that the Caller ID is on. On the Android device, open the Phone application and tap **Menu > Call Settings > Additional settings > Caller ID > Show Number**.
- Step 5** Test this feature.
-

Enable Transfer from VoIP to Mobile Network

Procedure

-
- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** For system-level settings, check that the Mobility softkey appears when the phone is in the connected and on-hook call states.
- Select **Device > Device Settings > Softkey Template**.
 - Select the same softkey template that you selected when you configured the device for Mobile Connect.
 - In the **Related Links** drop-down list at the upper right, select **Configure Softkey Layout** and select **Go**.
 - In the call state drop-down list, select the On Hook state and verify that the Mobility key is in the list of selected softkeys.
 - In the call state drop-down list, select the Connected state and verify that the Mobility key is in the list of selected softkeys.
- Step 3** Navigate to the device that you want to configure as follows:
- Select **Device > Phone**.
 - Search for the device that you want to configure.
 - Select the device name to open the **Phone Configuration** window.
- Step 4** For the per-user and per-device settings in Cisco Unified Communications Manager, set the specific device to use the Mobility softkey when the device transfers calls to the mobile voice network. Ensure that you have

set up both Mobility Identity and Mobile Connect for the mobile device. After the transfer feature is working, users can enable and disable Mobile Connect at their convenience without affecting the feature. If the device is an iPod Touch, you can configure a Mobility Identity using an alternate phone number such as the mobile phone of the user.

- a) Select the **Owner User ID** on the device page.
- b) Select the **Mobility User ID**. The value usually matches that of the Owner User ID.
- c) In the Product Specific Configuration Layout section, for the Transfer to Mobile Network option, select **Use Mobility Softkey** or **Use HandoffDN Feature**.

Step 5 In the User Locale field, choose **English, United States**.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.

Step 8 Instruct the user to sign out of the client and then to sign back in again to access the feature.

What to Do Next

Test your settings by transferring an active call from VoIP to the mobile network.

Set Up Dial via Office



Important

User-controlled voicemail avoidance, which can be used in conjunction with the DvO feature, is available only on Cisco Unified Communications Manager release 9.0 and later. Timer-controlled voicemail avoidance is available on Cisco Unified Communications Manager release 6.0 and later.

The DvO feature is not supported when users connect to the corporate network using Expressway for Mobile and Remote Access.

The DvO feature allows users to initiate Cisco Jabber outgoing calls with their work number using the mobile voice network for the device.

Cisco Jabber supports DvO-R (DvO-Reverse) calls, which works as follows:




- 1 User initiates a DvO-R call.
- 2 The client notifies Cisco Unified Communications Manager to call the mobile phone number.
- 3 Cisco Unified Communications Manager calls and connects to the mobile phone number.
- 4 Cisco Unified Communications Manager calls and connects to the number that the user dialed.
- 5 Cisco Unified Communications Manager connects the two segments.
- 6 The user and the called party continue as with an ordinary call.

Incoming calls use either Mobile Connect or the Voice over IP, depending on which Calling Options the user sets on the client. Dial via Office does not require Mobile Connect to work. However, we recommend that you enable Mobile Connect to allow the native mobile number to ring when someone calls the work number. From the Cisco Unified Communications Manager user pages, users can enable and disable Mobile Connect, and adjust Mobile Connect behavior using settings (for example, the time of day routing and Delay Before

Ringling Timer settings). For information about setting up Mobile Connect, see the *Set Up Mobile Connect* topic.

The following table describes the calling methods used for incoming and outgoing calls. The calling method (VoIP, Mobile Connect, DvO-R, or native cellular call) varies depending on the selected Calling Options and the network connection.

Table 7: Calling Methods used with Calling Options over Different Network Connections

Connection	Calling Options					
	Voice over IP		Mobile Voice Network		Autoselect	
 Corporate Wi-Fi					Outgoing: VoIP	Incoming: VoIP
 Noncorporate Wi-Fi	Outgoing: VoIP	Incoming: VoIP	Outgoing: DvO-R	Incoming: Mobile Connect		
 Mobile Network (3G, 4G)					Outgoing: DvO-R	Incoming: Mobile Connect
Phone Services are not registered	Outgoing Native Cellular Call					
	Incoming Mobile Connect					

To set up Dial via Office-Reverse (DvO-R), you must do the following:

- 1 Set up the Cisco Unified Communications Manager to support DvO-R. See the *Set Up Cisco Unified Communications Manager to Support DvO* topic for more information.
- 2 Enable DvO on each Cisco Dual Mode for iPhone device. See the *Set Up Dial via Office for Each Device* topic for more information.
- 3 Enable DvO on each Cisco Dual Mode for Android device. See the *Set Up Dial via Office for Each Device* topic for more information.

Set Up Cisco Unified Communications Manager to Support Dial via Office

To set up Cisco Unified Communications Manager to support Dial via Office-Reverse (DvO-R), perform the following procedures:

- 1 Complete one or both of the following procedures.
 - *Set Up Enterprise Feature Access Number*
 - *Set Up Mobility Profile*

- 2 Complete the *Verify Device COP File Version* procedure.
- 3 If necessary, create application dial rules to allow the system to route calls to the Mobile Identity phone number to the outbound gateway. Ensure that the format of the Mobile Identity phone number matches the application dial rules.

Set Up Enterprise Feature Access Number

Use this procedure to set up an Enterprise Feature Access Number for all Cisco Jabber calls that are made using Dial via Office-Reverse.

The Enterprise Feature Access Number is the number that Cisco Unified Communications Manager uses to call the mobile phone and the dialed number unless a different number is set up in Mobility Profile for this purpose.

Before You Begin

- Reserve a Direct Inward Dial (DID) number to use as the Enterprise Feature Access Number (EFAN). This procedure is optional if you already set up a mobility profile.
- Determine the required format for this number. The exact value you choose depends on the phone number that the gateway passes (for example, 7 digits or 10 digits). The Enterprise Feature Access Number must be a routable number.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
 - Step 2** Select **Call Routing > Mobility > Enterprise Feature Access Number Configuration**.
 - Step 3** Select **Add New**.
 - Step 4** In the **Number** field, enter the Enterprise Feature Access number.
Enter a DID number that is unique in the system.

To support dialing internationally, you can prepend this number with \+.
 - Step 5** From the **Route Partition** drop-down list, choose the partition of the DID that is required for enterprise feature access.
This partition is set under **System > Service Parameters**, in the **Clusterwide Parameters (System - Mobility)** section, in the **Inbound Calling Search Space for Remote Destination** setting. This setting points either to the Inbound Calling Search Space of the Gateway or Trunk, or to the Calling Search Space assigned on the **Phone Configuration** window for the device.

If the user sets up the DvO Callback Number with an alternate number, ensure that you set up the trunk Calling Search Space (CSS) to route to destination of the alternate phone number.
 - Step 6** In the **Description** field, enter a description of the Mobility Enterprise Feature Access number.
 - Step 7** (Optional) Check the **Default Enterprise Feature Access Number** check box if you want to make this Enterprise Feature Access number the default for this system.
 - Step 8** Select **Save**.
-

Set Up Mobility Profile

Use this procedure to set up a mobility profile for Cisco Jabber devices. This procedure is optional if you already set up an Enterprise Feature Access Number.

Mobility profiles allow you to set up the Dial via Office-Reverse settings for a mobile client. After you set up a mobility profile, you can assign it to a user or to a group of users, such as the users in a region or location.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
 - Step 2** Select **Call Routing > Mobility > Mobility Profile**.
 - Step 3** In the **Mobility Profile Information** section, in the **Name** field, enter a descriptive name for the mobility profile.
 - Step 4** In the **Dial via Office-Reverse Callback** section, in the **Callback Caller ID** field, enter the caller ID for the callback call that the client receives from Cisco Unified Communications Manager.
 - Step 5** Click **Save**.
-

Verify Device COP File Version

Use the following procedure to verify that you are using the correct device COP file for this release of Cisco Jabber.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
 - Step 2** Select **Device > Phone**.
 - Step 3** Click **Add New**.
 - Step 4** From the **Phone Type** drop-down list, choose **Cisco Dual Mode for iPhone**.
 - Step 5** From the **Phone Type** drop-down list, choose **Cisco Dual Mode for Android**.
 - Step 6** Click **Next**.
 - Step 7** Scroll down to the Product Specific Configuration Layout section, and verify that you can see the **Video Capabilities** drop-down list.
If you can see the **Video Capabilities** drop-down list, the COP file is already installed on your system.
If you cannot see the **Video Capabilities** drop-down list, locate and download the correct COP file.
-

Set Up Dial via Office for Each Device

Use the following procedures to set up Dial via Office - Reverse for each TCT device.

Use the following procedures to set up Dial via Office - Reverse for each BOT device.

- 1 Add a Mobility Identity for each user.
- 2 Enable Dial via Office on each device.
- 3 If you enabled Mobile Connect, verify that Mobile Connect works. Dial the desk phone extension and check that the phone number that is specified in the associated Mobile Identity rings.

Add Mobility Identity

Use this procedure to add a mobility identity to specify the mobile phone number of the mobile device as the destination number. This destination number is used by features such as Dial via Office or mobile connect.

You can specify only one number when you add a mobility identity. If you want to specify an alternate number such as a second mobile phone number for a mobile device, you can set up a remote destination. The mobility identity configuration characteristics are identical to those of the remote destination configuration.

Procedure

-
- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Navigate to the device that you want to configure as follows:
- a) Select **Device > Phone**.
 - b) Search for the device that you want to configure.
 - c) Select the device name to open the **Phone Configuration** window.
- Step 3** In the **Associated Mobility Identity** section, select **Add a New Mobility Identity**.
- Step 4** Enter the mobile phone number as the destination number.
 You must be able to rout this number to an outbound gateway. Generally, the number is the full E.164 number.
- Note** If you enable the Dial via Office — Reverse feature for a user, you must enter a destination number for the user's mobility identity.
- If you enable Dial via Office — Reverse and leave the destination number empty in the mobility identity:
- The phone service cannot connect if the user selects the **Autoselect** calling option while using a mobile data network and VPN.
 - The phone service cannot connect if the user selects the **Mobile Voice Network** calling option on any type of network.
 - The logs do not indicate why the phone service cannot connect.
- Step 5** Enter the initial values for call timers.
 These values ensure that calls are not routed to the mobile service provider voicemail before they ring in the client on the mobile device. You can adjust these values to work with the end user's mobile network. For more information, see the online help in Cisco Unified Communications Manager.

The following is an example of mobility Identity timers' information in Cisco Unified Communications Manager 9.x.

Setting	Suggested Initial Value
Answer Too Soon Timer	3000

Setting	Suggested Initial Value
Answer Too Late Timer	20000
Delay Before Ringing Timer	0 Note This setting does not apply to DvO-R calls.

The following is an example of mobility Identity timers' information in Cisco Unified Communications Manager 10.x.

Setting	Suggested Initial Value
Wait * before ringing this phone when my business line is dialed.*	0.0 seconds
Prevent this call from going straight to this phone's voicemail by using a time delay of * to detect when calls go straight to voicemail.*	3.0 seconds
Stop ringing this phone after * to avoid connecting to this phone's voicemail.*	20.0 seconds

Step 6 Do one of the following:

- Cisco Unified Communications Manager release 9 or earlier — Check the **Enable Mobile Connect** check box.
- Cisco Unified Communications Manager release 10 — Check the **Enable Single Number Reach** check box.

Step 7 If you are setting up the Dial via Office feature, in the Mobility Profile drop-down list, select one of the following options.

Option	Description
Leave blank	Choose this option if you want users to use the Enterprise Feature Access Number (EFAN).
Mobility Profile	Choose the mobility profile that you just created if you want users to use a mobility profile instead of an EFAN.

Step 8 Set up the schedule for routing calls to the mobile number.

Step 9 Select **Save**.

Enable Dial via Office on Each Device

Use this procedure to enable Dial via Office on each device.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
 - Step 2** Navigate to the device that you want to configure as follows:
 - a) Select **Device > Phone**.
 - b) Search for the device that you want to configure.
 - c) Select the device name to open the **Phone Configuration** window.
 - Step 3** In the **Device Information** section, check the **Enable Cisco Unified Mobile Communicator** check box.
 - Step 4** In the **Protocol Specific Information** section, in the **Rerouting Calling Search Space** drop-down list, select a Calling Search Space (CSS) that can route the call to the DvO callback number.
 - Step 5** In the **Product Specific Configuration Layout** section, set the **Dial via Office** drop-down list to **Enabled**.
 - Step 6** Select **Save**.
 - Step 7** Select **Apply Config**.
 - Step 8** Instruct the user to sign out of the client and then to sign back in again to access the feature.
-

What to Do Next

Test this feature.

Set Up Voicemail Avoidance

Voicemail avoidance is a feature that prevents calls from being answered by the mobile service provider voice mail. This feature is useful if a user receives a Mobile Connect call from the enterprise on the mobile device. It is also useful when an incoming DvO-R call is placed to the mobile device.

You can set up Voicemail Avoidance in one of two ways:

- **Timer-controlled** — (Default) With this method, you set timers on the Cisco Unified Communications Manager to determine if the call is answered by the mobile user or mobile service provider voicemail.
- **User-controlled** — With this method, you set the Cisco Unified Communications Manager to require that a user presses any key on the keypad of the device to generate a DTMF tone before the call can proceed.

If you deploy DvO-R, Cisco recommends that you also set user-controlled Voicemail Avoidance. If you set user-controlled Voicemail Avoidance, this feature applies to both DvO-R and Mobile Connect calls.

For more information about voicemail avoidance, see the *Confirmed Answer and DvO VM detection* section in the *Cisco Unified Communications Manager Features and Services Guide* for your release.

Set Up Timer-Controlled Voicemail Avoidance

Set up the timer control method by setting the **Answer Too Soon Timer** and **Answer Too Late Timer** on either the Mobility Identity or the Remote Destination. For more information, see the *Add Mobility Identity* or *Add Remote Destination (Optional)* topics.

Before You Begin

Timer-controlled voicemail avoidance is supported on Cisco Unified Communications Manager, release 6.0 and later.

Set Up User-Controlled Voicemail Avoidance



Important

User-controlled voicemail avoidance is available on Cisco Unified Communications Manager, release 9.0 and later.

Set up User-Controlled Voicemail Avoidance as follows:

- 1 Set up Cisco Unified Communications Manager using the *Set Up Cisco Unified Communications Manager to Support Voicemail Avoidance* topic.
- 2 Set up the device using one of the following topics:
 - *Enable Voicemail Avoidance on Mobility Identity*
 - *Enable Voicemail Avoidance on Remote Destination*



Important

Cisco does not support user-controlled voicemail avoidance when using DvO-R with alternate numbers that the end user sets up in the client. An alternate number is any phone number that the user enters in the DvO Callback Number field on the client that does not match the phone number that you set up on the user's Mobility Identity.

If you set up this feature with alternate numbers, the Cisco Unified Communications Manager connects the DvO-R calls even if the callback connects to a wrong number or a voicemail system.

Set Up Cisco Unified Communications Manager to Support Voicemail Avoidance

Use this procedure to set up the Cisco Unified Communications Manager to support user-controlled Voicemail Avoidance.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **System > Service Parameters**.
- Step 3** In the **Server** drop-down list, select the active Cisco Unified Communications Manager.
- Step 4** In the **Service** drop-down list, select the **Cisco Call Manager (Active)** service.
- Step 5** Configure the settings in the **Clusterwide Parameters (System - Mobility Single Number Reach Voicemail)** section.
- Note** The settings in this section are not specific to Cisco Jabber. For information about how to configure these settings, see the *Confirmed Answer and DvO VM detection* section in the *Cisco Unified Communications Manager Administrator Guide* for your release.
- Step 6** Click **Save**.
-

Enable Voicemail Avoidance on Mobility Identity

Use this procedure to enable user-controlled voicemail avoidance for the end user's mobility identity.

Before You Begin

- Set up the annunciator on the Cisco Unified Communications Manager. For more information, see the *Annunciator setup* section in the *Cisco Unified Communications Manager Administrator Guide* for your release.
- If you set up a Media Resource Group on the Cisco Unified Communications Manager, set up the annunciator on the Media Resource Group. For more information, see the *Media resource group setup* section in the *Cisco Unified Communications Manager Administrator Guide* for your release.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Navigate to the device that you want to configure as follows:
- a) Select **Device > Phone**.
 - b) Search for the device that you want to configure.
 - c) Select the device name to open the **Phone Configuration** window.
- Step 3** In the **Associated Mobility Identity** section, click the link for the Mobility Identity.
- Note** To ensure that the Voicemail Avoidance feature works correctly, the DvO Callback Number that the end user enters in the Cisco Jabber client must match the Destination Number that you enter on the Mobility Identity Configuration screen.
- Step 4** Set the policies as follows:
- Cisco Unified Communications Manager release 9 — In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.
 - Cisco Unified Communications Manager release 10 without Dial via Office — In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.

- Cisco Unified Communications Manager release 10 with Dial via Office
 - In the **Single Number Reach Voicemail Policy** drop-down list, select **Timer Control**.
 - In the **Dial-via-Office Reverse Voicemail Policy** drop-down list, select **User Control**.

Step 5 Click **Save**.

Enable Voicemail Avoidance on Remote Destination

Use this procedure to enable user-controlled voicemail avoidance for the end user's remote destination.

Before You Begin

- Set up the annunciator on the Cisco Unified Communications Manager. For more information, see the *Annunciator setup* section in the Cisco Unified Communications Manager Administrator Guide for your release.
- If you set up a Media Resource Group on the Cisco Unified Communications Manager, set up the annunciator on the Media Resource Group. For more information, see the *Media resource group setup* section in the Cisco Unified Communications Manager Administrator Guide for your release.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Navigate to the device that you want to configure as follows:

- a) Select **Device > Phone**.
- b) Search for the device that you want to configure.
- c) Select the device name to open the **Phone Configuration** window.

Step 3 In the **Associated Remote Destinations** section, click the link for the associated remote destination.

Step 4 Set the policies as follows:

- Cisco Unified Communications Manager release 9 — In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.
- Cisco Unified Communications Manager release 10 without Dial via Office — In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.
- Cisco Unified Communications Manager release 10 with Dial via Office
 - In the **Single Number Reach Voicemail Policy** drop-down list, select **Timer Control**.
 - In the **Dial-via-Office Reverse Voicemail Policy** drop-down list, select **User Control**.

Step 5 If using Cisco Unified Communications Manager Version 10 with the Dial via Office feature,

Step 6 Click **Save**.
