



Cisco Jabber for iPhone 9.5 Server Setup Guide

First Published: October 16, 2013

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

PART I

Configure Directory Integration 1

CHAPTER 1

Configure Directory Integration in On-Premises Deployments 3

Synchronize with the Directory Server 3

Enable Synchronization 3

Specify an LDAP Attribute for the User ID 4

Perform Synchronization 4

Authenticate with the Directory Server 5

CHAPTER 2

Configure Directory Integration in Cloud-Based Deployments 7

Integrate Your Directory 7

Add Directory Groups 7

PART II

Provision Instant Messaging and Presence 9

CHAPTER 3

Provision Instant Messaging and Presence on Cisco Unified Presence 11

Activate and Start Essential Services 11

Pre-Populate Contact Lists in Bulk 12

Enable Messaging Settings 12

Specify Capabilities Assignments 13

Configure Prompts for Presence Subscription Requests 13

CHAPTER 4

Provision Instant Messaging and Presence on Cisco Unified Communications Manager IM and Presence 17

Activate and Start Essential Services 17

Create a Service Profile 18

Pre-Populate Contact Lists in Bulk 19

Enable Messaging Settings 19

Configure Prompts for Presence Subscription Requests	19
Add an Instant Messaging and Presence Service	21
Apply Instant Messaging and Presence Service	21
Configure Users	22
Configure Users Individually	22
Configure Users in Bulk	23

CHAPTER 5**Provision Instant Messaging and Presence in Cloud-Based Deployments 25**

Configure Instant Messaging and Presence	25
Configure Privacy Options	25

PART III**Provision Audio and Video Capabilities 27****CHAPTER 6****Provision Audio and Video Capabilities on Cisco Unified Communications Manager Version**

8.x	29
Create Software Phone Devices	29
Create TCT Software Phone Devices	29
Install Cisco Options Package File for Devices	29
Create SIP Profiles	30
Increase SIP Dual Mode Alert Timer Value	31
Create TCT Devices	32
TCT Device Configuration Settings	32
Add Directory Number to Device	36
Configure User Associations	36
Reset Devices	37
Specify Your TFTP Server Address	38
Specify Your TFTP Server on Cisco Unified Presence	38
Specify TFTP Servers with the Cisco WebEx Administration Tool	38
Create a CCMCIP Profile	39
Set Up Mobile Connect	40
Enable Mobile Connect	41
Add Mobility Identity	42
Add Remote Destination (Optional)	44
Transfer Active VoIP Call to the Mobile Network	45
Enable Handoff from VoIP to Mobile Network	46

Set Up Handoff DN	47
Match Caller ID with Mobility Identity	47
Set Up User and Device Settings for Handoff	48
Enable Transfer from VoIP to Mobile Network	48
Set Up Dial via Office	49
Set Up Cisco Unified Communications Manager to Support DVO	51
Set Up Enterprise Feature Access Number	51
Set Up Mobility Profile	52
Verify Device COP File Version	53
Set Up Dial via Office for Each Device	53
Add Mobility Identity	53
Enable Dial via Office on Each Device	55
Set Up Voicemail Avoidance	55
Set Up Timer-Controlled Voicemail Avoidance	56

CHAPTER 7**Provision Audio and Video Capabilities on Cisco Unified Communications Manager Version 9.x and Higher** 57

Create Software Phone Devices	57
Create TCT Software Phone Devices	57
Install Cisco Options Package File for Devices	58
Create SIP Profiles	59
Increase SIP Dual Mode Alert Timer Value	59
Create TCT Devices	60
TCT Device Configuration Settings	61
Add Directory Number to Device	64
Configure User Associations	64
Specify Your TFTP Server Address	65
Specify Your TFTP Server on Cisco Unified Communications Manager IM and Presence	65
Specify TFTP Servers with the Cisco WebEx Administration Tool	66
Reset Devices	66
Create a CCMCIP Profile	67
Set Up Mobile Connect	68
Enable Mobile Connect	68
Add Mobility Identity	70

- Add Remote Destination (Optional) 72
- Transfer Active VoIP Call to the Mobile Network 73
 - Enable Handoff from VoIP to Mobile Network 74
 - Set Up Handoff DN 75
 - Match Caller ID with Mobility Identity 75
 - Set Up User and Device Settings for Handoff 76
 - Enable Transfer from VoIP to Mobile Network 76
- Set Up Dial via Office 77
 - Set Up Cisco Unified Communications Manager to Support DVO 79
 - Set Up Enterprise Feature Access Number 79
 - Set Up Mobility Profile 80
 - Verify Device COP File Version 81
 - Set Up Dial via Office for Each Device 81
 - Add Mobility Identity 81
 - Enable Dial via Office on Each Device 83
- Set Up Voicemail Avoidance 83
 - Set Up Timer-Controlled Voicemail Avoidance 84
 - Set Up User-Controlled Voicemail Avoidance 84
 - Set Up Cisco Unified Communications Manager to Support Voicemail Avoidance 85
 - Enable Voicemail Avoidance on Mobility Identity 85
 - Enable Voicemail Avoidance on Remote Destination 86

CHAPTER 8

Provision Audio and Video Capabilities in Hybrid Cloud-Based Deployments 89

- Configure Audio and Video Services 89
- Add Teleconferencing Service Name Accounts 89

PART IV

Set Up Voicemail 91

CHAPTER 9

Set Up Voicemail on Cisco Unified Presence 93

- Configure Cisco Unity Connection 93
- Add a Voicemail Server 94
- Create a Voicemail Profile 95
- Configure Retrieval and Redirection 96
- Set a Voicemail Credentials Source 97

CHAPTER 10	Set Up Voicemail on Cisco Unified Communications Manager 99
	Configure Cisco Unity Connection 99
	Add a Voicemail Service 100
	Apply Voicemail Service 101
	Configure Retrieval and Redirection 102
	Set a Voicemail Credentials Source 103

CHAPTER 11	Set Up Voicemail in Hybrid Cloud-Based Deployments 105
	Configure Voicemail 105
	Allow Users to Set Voicemail Server Settings 105

PART V	Set Up Conferencing 107
---------------	--------------------------------

CHAPTER 12	Set Up Conferencing on Cisco Unified Presence 109
	Set Up On-Premises Conferencing 109
	Cisco WebEx Meetings Server Installation and Configuration 109
	Set Up Cisco WebEx Meetings Server on Cisco Unified Presence 109
	Add Cisco WebEx Meetings Server 110
	Add Cisco WebEx Meetings Server to a Profile 111
	Set Up Cloud-Based Conferencing 112
	Integration with Cisco WebEx Meeting Center 112
	Authentication with Cisco WebEx Meeting Center 112
	Set Up Cisco WebEx Meeting Center on Cisco Unified Presence 113
	Add Cisco WebEx Meeting Center 113
	Add Cisco WebEx Meeting Center to a Profile 114

CHAPTER 13	Set Up Conferencing on Cisco Unified Communications Manager 117
	Set Up On-Premises Conferencing 117
	Cisco WebEx Meetings Server Installation and Configuration 117
	Add Cisco WebEx Meetings Server 118
	Add Cisco WebEx Meetings Server to a Profile 119
	Set Up Cloud-Based Conferencing 120
	Integration with Cisco WebEx Meeting Center 120
	Authentication with Cisco WebEx Meeting Center 120

Add Cisco WebEx Meeting Center 121
Add Cisco WebEx Meeting Center to a Profile 122

CHAPTER 14

Set Up Conferencing in Cloud-Based Deployments 125
Configure Cisco WebEx Meeting Center 125
Authentication with Cisco WebEx Meeting Center 125
Specify Conferencing Credentials in the Client 125



PART **I**

Configure Directory Integration

- [Configure Directory Integration in On-Premises Deployments, page 3](#)
- [Configure Directory Integration in Cloud-Based Deployments, page 7](#)



CHAPTER

1

Configure Directory Integration in On-Premises Deployments

Configure directory integration in an on-premises deployment so that user data in Cisco Unified Communications Manager is synchronized with your corporate directory. You can also configure Cisco Unified Communications Manager to proxy authentication to your directory server when users sign in to the client.

- [Synchronize with the Directory Server, page 3](#)
- [Authenticate with the Directory Server, page 5](#)

Synchronize with the Directory Server

Directory server synchronization ensures that contact data in your directory server is replicated to Cisco Unified Communications Manager.

Enable Synchronization

The first step to synchronize with a directory server is to enable synchronization on Cisco Unified Communications Manager.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
 - Step 2** Select **System > LDAP > LDAP System**.
The **LDAP System Configuration** window opens.
 - Step 3** Locate the **LDAP System Information** section.
 - Step 4** Select **Enable Synchronizing from LDAP Server**.
 - Step 5** Select the type of directory server from which you are synchronizing data from the **LDAP Server Type** drop-down list.
-

What to Do Next

Specify an LDAP attribute for the user ID.

Related Topics

[v9.1: LDAP system setup](#)

[v8.6\(1\): LDAP System Configuration](#)

Specify an LDAP Attribute for the User ID

When you synchronize from your directory source to Cisco Unified Communications Manager, you can populate the user ID from an attribute in the directory. The default attribute that holds the user ID is `sAMAccountName`.

Procedure

Step 1 Locate the **LDAP Attribute for User ID** drop-down list on the **LDAP System Configuration** window.

Step 2 Specify an attribute for the user ID as appropriate and then select **Save**.

Important If the attribute for the user ID is other than `sAMAccountName`, you must specify the attribute as the value for the `BDIUserAccountName` parameter in your client configuration file as follows:

```
<BDIUserAccountName>attribute-name</BDIUserAccountName>
```

If you do not specify the attribute in your configuration, and the attribute is other than `sAMAccountName`, the client cannot resolve contacts in your directory. As a result, users do not get presence and cannot send or receive instant messages.

Perform Synchronization

After you add a directory server and specify the required parameters, you can synchronize Cisco Unified Communications Manager with the directory server.

Before You Begin

If your environment includes a presence server, you should ensure the following feature service is activated and started before you synchronize with the directory server:

- Cisco Unified Presence: **Cisco UP Sync Agent**
- Cisco Unified Communications Manager IM and Presence: **Cisco Sync Agent**

This service keeps data synchronized between the presence server and Cisco Unified Communications Manager. When you perform the synchronization with your directory server, Cisco Unified Communications Manager then synchronizes the data with the presence server. However, the **Cisco Sync Agent** service must be activated and started.

Procedure

- Step 1** Select **System > LDAP > LDAP Directory**.
- Step 2** Select **Add New**.
The **LDAP Directory** window opens.
- Step 3** Specify the required details on the **LDAP Directory** window.
See the *Cisco Unified Communications Manager Administration Guide* for more information about the values and formats you can specify.
- Step 4** Select **Save**.
- Step 5** Select **Perform Full Sync Now**.
- Note** The amount of time it takes for the synchronization process to complete depends on the number of users that exist in your directory. If you synchronize a large directory with thousands of users, you should expect the process to take some time.
-

User data from your directory server is synchronized to the Cisco Unified Communications Manager database. Cisco Unified Communications Manager then synchronizes the user data to the presence server database.

Related Topics

- [v9.1: LDAP directory setup](#)
- [v8.6\(1\): LDAP Directory Configuration](#)

Authenticate with the Directory Server

You should configure Cisco Unified Communications Manager to authenticate with the directory server. When users log in to the client, the presence server routes that authentication to Cisco Unified Communications Manager. Cisco Unified Communications Manager then proxies that authentication to the directory server.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **System > LDAP > LDAP Authentication**.
- Step 3** Select **Use LDAP Authentication for End Users**.
- Step 4** Specify LDAP credentials and a user search base as appropriate.
See the *Cisco Unified Communications Manager Administration Guide* for information about the fields on the **LDAP Authentication** window.
- Step 5** Select **Save**.
-

Related Topics

- [v9.1: LDAP authentication setup](#)
- [v8.6\(1\): LDAP Authentication Configuration](#)



CHAPTER 2

Configure Directory Integration in Cloud-Based Deployments

Configure directory integration in a cloud-based deployment to automatically provision and de-provision users and keep user profile information in the Cisco WebEx Administration Tool updated with information in your corporate directory.

- [Integrate Your Directory, page 7](#)

Integrate Your Directory

To set up directory integration, complete the following steps:

- 1 Review the directory integration topics.
See [Directory Integration](#).
- 2 Configure your organization information.
See [Understanding the Configuration Tab](#).
- 3 Create and provision users.
See [Overview of User Management](#).

Related Topics

- [Directory Integration](#)
- [Understanding the Configuration tab](#)
- [Overview of User Management](#)

Add Directory Groups

Directory groups, or enterprise groups, provide contact groups that administrators define for users.


The following are the high-level steps you should complete to add directory groups:

- 1 Set up directory integration.
- 2 Define your directory groups in a comma-separated values (.csv) file.

- 3 Import your directory groups using the Cisco WebEx Administration Tool.

See *Directory Integration* for more information about adding directory groups.

Users cannot create new directory groups or edit existing directory groups in the client. However, users can assign a contact to a directory group that already exists. In the client, users can assign the contact to an existing group as follows:

- 1 On the **Contacts** screen, tap the  button.
- 2 Search for a contact, or enter a username or email address for the contact.
- 3 Tap **Assign to Group**.
- 4 On the **Groups** screen, select a group.
- 5 Tap **Add Contact** to return to the **Add Contact** screen.
- 6 Tap **Done**.

Related Topics

[Directory Integration](#)



PART **II**

Provision Instant Messaging and Presence

- [Provision Instant Messaging and Presence on Cisco Unified Presence, page 11](#)
- [Provision Instant Messaging and Presence on Cisco Unified Communications Manager IM and Presence, page 17](#)
- [Provision Instant Messaging and Presence in Cloud-Based Deployments, page 25](#)



Provision Instant Messaging and Presence on Cisco Unified Presence

Learn how to enable messaging settings and configure instant messaging and presence functionality. Complete the steps to activate and start essential services, enable messaging settings, specify capabilities assignments to users, and configure instant messaging and presence services.

This chapter applies to Cisco Unified Presence version 8.6 and lower.

- [Activate and Start Essential Services, page 11](#)
- [Pre-Populate Contact Lists in Bulk, page 12](#)
- [Enable Messaging Settings, page 12](#)
- [Specify Capabilities Assignments, page 13](#)
- [Configure Prompts for Presence Subscription Requests, page 13](#)

Activate and Start Essential Services

Essential services enable communication between servers and provide capabilities to the client.

Procedure

- Step 1** Open the **Cisco Unified Presence Servicability** interface.
- Step 2** Select **Tools > Control Center - Feature Services**.
- Step 3** Select the appropriate server from the **Server** drop-down list.
- Step 4** Ensure the following services are started and activated:
 - **Cisco UP SIP Proxy**
 - **Cisco UP Sync Agent**
 - **Cisco UP XCP Authentication Service**
 - **Cisco UP XCP Connection Manager**

- Cisco UP XCP Text Conference Manager
- Cisco UP Presence Engine

- Step 5** Select **Tools > Control Center - Network Services**.
- Step 6** Select the appropriate server from the **Server** drop-down list.
- Step 7** Ensure **Cisco UP XCP Router Service** is running.
-

What to Do Next

Depending on your requirements, you might need to activate and start additional services. See the appropriate Cisco Unified Presence documentation to review available services and determine if your deployment requires additional services.

Pre-Populate Contact Lists in Bulk

You can pre-populate user contact lists with the Bulk Administration Tool (BAT). The first step is to create a CSV file that defines the contact list you want to provide to users. You then use the BAT to import that contact list in bulk to a set of users.

In this way you can pre-populate contact lists for users so that they automatically have a set of contacts after the initial launch of the client.

For more information about using BAT and the format of the CSV file, see the *Deployment Guide for Cisco Unified Presence*.

Related Topics

[Deployment Guide for Cisco Unified Presence](#)

Enable Messaging Settings

Complete the steps in this task to enable and configure instant messaging.

Procedure

- Step 1** Open the **Cisco Unified Presence Administration** interface.
- Step 2** Enable messaging settings as follows:
- Select **Messaging > Settings**.
 - Select the following settings:
 - **Enable instant messaging**
 - **Allow clients to log instant message history**
- Step 3** Select **Save**.
-

Related Topics

[How to Configure the Instant Messaging Settings on Cisco Unified Presence](#)

Specify Capabilities Assignments

Complete the steps in this task to provide users with instant messaging and presence capabilities.

Procedure

-
- Step 1** Open the **Cisco Unified Communications Manager Administration** interface.
 - Step 2** Select **System > Licensing > Capabilities Assignment**.
The **Find and List Capabilities Assignments** window opens.
 - Step 3** Specify the appropriate filters in the **Find Capabilities Assignment where** field and then select **Find** to retrieve a list of users.
 - Step 4** Select the appropriate users from the list.
The **Capabilities Assignment Configuration** window opens.
 - Step 5** Select both of the following in the **Capabilities Assignment Configuration** section:
 - **Enable CUP**
 - **Enable CUPC**
 - Step 6** Select **Save**.
-

Configure Prompts for Presence Subscription Requests

You can enable or disable prompts for presence subscription requests from contacts within your organization. The client always prompts users to allow presence subscription requests from contacts outside your organization. Users specify privacy settings in the client as follows:

Inside Your Organization

Users can choose to allow or block contacts from inside your organization.

- If users choose to allow presence subscription requests and
 - you select **Allow users to view the availability of other users without being prompted for approval**, the client automatically accepts all presence subscription requests without prompting users.
 - you do not select **Allow users to view the availability of other users without being prompted for approval**, the client prompts users for all presence subscription requests.
- If users choose to block contacts, only their existing contacts can see their availability status. In other words, only those contacts who have already subscribed to the user's presence can see their availability status.



Note

When searching for contacts in your organization, users can see the temporary availability status of all users in the organization. However, if User A blocks User B, User B cannot see the temporary availability status of User A in the search list.

Outside Your Organization

Users can choose the following options for contacts from outside your organization:

- Have the client prompt them for each presence subscription request.
- Block all contacts so that only their existing contacts can see their availability status. In other words, only those contacts who have already subscribed to the user's presence can see their availability status.

Procedure

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

Step 2 Select **Presence > Settings**.
The **Presence Settings** window opens.

Step 3 Select **Allow users to view the availability of other users without being prompted for approval** to disable prompts and automatically accept all presence subscription requests within your organization. This option has the following values:

Selected

The client does not prompt users for presence subscription requests. The client automatically accepts all presence subscription requests without prompting the users.

Cleared

The client prompts users to allow presence subscription requests. This setting requires users to allow other users in your organization to view their availability status.

Step 4 Select **Save**.



CHAPTER 4

Provision Instant Messaging and Presence on Cisco Unified Communications Manager IM and Presence

Learn how to enable messaging settings and configure instant messaging and presence functionality. Complete the steps to activate and start essential services, add an instant messaging and presence service, apply the service to a service profile, and then configure users.

This chapter applies to Cisco Unified Communications Manager IM and Presence version 9.0(1) and higher.

- [Activate and Start Essential Services, page 17](#)
- [Create a Service Profile, page 18](#)
- [Pre-Populate Contact Lists in Bulk, page 19](#)
- [Enable Messaging Settings, page 19](#)
- [Configure Prompts for Presence Subscription Requests, page 19](#)
- [Add an Instant Messaging and Presence Service, page 21](#)
- [Configure Users, page 22](#)

Activate and Start Essential Services

Essential services enable communication between servers and provide capabilities to the client.

Procedure

- Step 1** Open the **Cisco Unified IM and Presence Servicability** interface.
- Step 2** Select **Tools > Control Center - Feature Services**.
- Step 3** Select the appropriate server from the **Server** drop-down list.
- Step 4** Ensure the following services are started and activated:
 - **Cisco SIP Proxy**

- Cisco Sync Agent
- Cisco XCP Authentication Service
- Cisco XCP Connection Manager
- Cisco XCP Text Conference Manager
- Cisco Presence Engine

- Step 5** Select **Tools > Control Center - Network Services**.
- Step 6** Select the appropriate server from the **Server** drop-down list.
- Step 7** Ensure **Cisco XCP Router Service** is running.
-

What to Do Next

Depending on your requirements, you might need to activate and start additional services. See the appropriate Cisco Unified Communications Manager documentation to review available services and determine if your deployment requires additional services.

Create a Service Profile

You create a service profile that contains the configuration settings for the services you add on Cisco Unified Communications Manager. You add the service profile to the end user configuration for your users. The client can then retrieve settings for available services from the service profile.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **User Management > User Settings > Service Profile**.
The **Find and List Service Profiles** window opens.
- Step 3** Select **Add New**.
The **Service Profile Configuration** window opens.
- Step 4** Enter settings on the **Service Profile Configuration** window as follows:
- a) Specify a unique name for the service profile in the **Name** field.
 - b) Specify an optional description in the **Description** field.
 - c) Select **Make this the default service profile for the system**, if appropriate.
- Step 5** Select **Save**.
-

What to Do Next

Complete the steps to set up instant messaging and presence. You can add your service profile to the end user configuration at the same time that you enable users for instant messaging and presence.

Pre-Populate Contact Lists in Bulk

You can pre-populate user contact lists with the Bulk Administration Tool (BAT). The first step is to create a CSV file that defines the contact list you want to provide to users. You then use the BAT to import that contact list in bulk to a set of users.

In this way you can pre-populate contact lists for users so that they automatically have a set of contacts after the initial launch of the client.

For more information about using BAT and the format of the CSV file, see the *Deployment Guide for IM and Presence Service*.

Related Topics

[Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager](#)

Enable Messaging Settings

Enable and configure instant messaging capabilities.

Procedure

- Step 1** Open the **Cisco Unified CM IM and Presence Administration** interface.
 - Step 2** Select **Messaging > Settings**.
 - Step 3** Select the following options:
 - **Enable instant messaging**
 - **Allow clients to log instant message history**
 - Step 4** Select other messaging settings as appropriate.
 - Step 5** Select **Save**.
-

Related Topics

[Instant messaging settings configuration on IM and Presence](#)

Configure Prompts for Presence Subscription Requests

You can enable or disable prompts for presence subscription requests from contacts within your organization. The client always prompts users to allow presence subscription requests from contacts outside your organization. Users specify privacy settings in the client as follows:

Inside Your Organization

Users can choose to allow or block contacts from inside your organization.

- If users choose to allow presence subscription requests and
 - you select **Allow users to view the availability of other users without being prompted for approval**, the client automatically accepts all presence subscription requests without prompting users.
 - you do not select **Allow users to view the availability of other users without being prompted for approval**, the client prompts users for all presence subscription requests.
- If users choose to block contacts, only their existing contacts can see their availability status. In other words, only those contacts who have already subscribed to the user's presence can see their availability status.



Note

When searching for contacts in your organization, users can see the temporary availability status of all users in the organization. However, if User A blocks User B, User B cannot see the temporary availability status of User A in the search list.

Outside Your Organization

Users can choose the following options for contacts from outside your organization:

- Have the client prompt them for each presence subscription request.
- Block all contacts so that only their existing contacts can see their availability status. In other words, only those contacts who have already subscribed to the user's presence can see their availability status.

Procedure

- Step 1** Open the **Cisco Unified CM IM and Presence Administration** interface.
- Step 2** Select **Presence > Settings**.
The **Presence Settings** window opens.
- Step 3** Select **Allow users to view the availability of other users without being prompted for approval** to disable prompts and automatically accept all presence subscription requests within your organization. This option has the following values:

Selected

The client does not prompt users for presence subscription requests. The client automatically accepts all presence subscription requests without prompting the users.

Cleared

The client prompts users to allow presence subscription requests. This setting requires users to allow other users in your organization to view their availability status.

Step 4 Select **Save**.

Add an Instant Messaging and Presence Service

Provide users with instant messaging and presence capabilities.

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 **IM and Presence** 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) Select **Unified CM (IM and Presence)** from the **Product Type** drop-down list.
 - b) Specify a name for the service in the **Name** field.
The name you specify displays when you add the service to a profile. Ensure the name you specify is unique, meaningful, and easy to identify.
 - c) Specify an optional description in the **Description** field.
 - d) Specify the instant messaging and presence service address in the **Host Name/IP Address** field.
- Step 7** Select **Save**.
-

What to Do Next

Add the instant messaging and presence service to your service profile.

Apply Instant Messaging and Presence Service

After you add an instant messaging and presence 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.

Procedure

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

Configure Users

To configure users, you enable instant messaging and presence and add a service profile to the users.

Configure Users Individually

Enable instant messaging and presence and add your service profile to individual users.

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 username from the list.
The **End User Configuration** window opens.
- Step 5** Locate the **Service Settings** section and do the following:
- a) Select **Enable User for Unified CM IM and Presence**.
 - b) Select your service profile from the **UC Service Profile** drop-down list.
- Important** **Cisco Unified Communications Manager version 9.x only:** If the user has only instant messaging and presence capabilities (IM only), you must select **Use Default**.

For IM only users, Cisco Unified Communications Manager version 9.x always applies the default service profile regardless of what you select from the **UC Service Profile** drop-down list.

Step 6 Select **Save**.

Configure Users in Bulk

Enable instant messaging and presence and add your service profile to multiple users.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Bulk Administration > Users > Update Users > Query**.
The **Find and List Users To Update** 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 **Next**.
The **Update Users Configuration** window opens.
- Step 5** Select both of the **Enable User for Unified CM IM and Presence** check boxes.
Important There are two check boxes for **Enable User for Unified CM IM and Presence**. To disable instant messaging and presence, you select one check box. To enable instant messaging and presence, you select both check boxes.
- Step 6** Select the **UC Service Profile** check box and then select your service profile from the drop-down list.
Important **Cisco Unified Communications Manager version 9.x only:** If the user has only instant messaging and presence capabilities (IM only), you must select **Use Default**.
For IM only users, Cisco Unified Communications Manager version 9.x always applies the default service profile regardless of what you select from the **UC Service Profile** drop-down list.
- Step 7** In the **Job Information** section, specify if you want to run the job immediately or at a later time.
- Step 8** Select **Submit**.
-



CHAPTER 5

Provision Instant Messaging and Presence in Cloud-Based Deployments

Use the Cisco WebEx Administration Tool to provision users with instant messaging and presence capabilities in cloud-based deployments. You can also configure settings for the Cisco WebEx Messenger service such as XMPP federation and instant message logging and archiving.

- [Configure Instant Messaging and Presence, page 25](#)
- [Configure Privacy Options, page 25](#)

Configure Instant Messaging and Presence

When users successfully authenticate to the Cisco WebEx Messenger service, they get instant messaging and presence functionality. You can optionally configure instant messaging and presence federation with the Cisco WebEx Administration Tool.

Related Topics

- [Cisco WebEx federation with other instant messaging providers](#)
- [Specifying IM Federation settings](#)

Configure Privacy Options

You can specify the default settings for presence subscription requests in cloud-based deployments.

Procedure

- Step 1** Open the Cisco WebEx Administration Tool.
- Step 2** Select the **Configuration** tab.
- Step 3** Select **General IM** in the **Connect Client** section.
The **General IM** pane opens.
- Step 4** Select the appropriate options for contact list requests as follows:

Option	Description
Select Allow users to set "Options for contact list requests"	Accept requests automatically from contacts in my organization automatically becomes the default option to configure how the client handles presence subscription requests. Users can change the default option in the Options window.
Do not select Allow users to set "Options for contact list requests"	You configure how the client handles presence subscription requests. Users cannot change this configuration. The settings are not available in the Options window. Select one of the following options: <ul style="list-style-type: none"> • Accept requests automatically from all contacts • Accept requests automatically from contacts in my organization • Prompt me for each request

The options for configuring how the client handles contact list requests are as follows:

Accept requests automatically from all contacts

The client automatically accepts presence subscription requests from any domain.

If you specify this setting, users from any domain can automatically add users to their contact list and view their availability status.

Accept requests automatically from contacts in my organization

The client automatically accepts presence subscription requests only from users in the domains you specify.

To specify a domain, select **Domain(s)** in the **System Settings** section on the **Configuration** tab.

Note When searching for contacts in your organization, users can see the temporary availability status of all users in the organization. However, if User A blocks User B, User B cannot see the temporary availability status of User A in the search list.

Prompt me for each request

The client prompts users to accept each presence subscription request.

Step 5 Select **Save**.



PART

Provision Audio and Video Capabilities

- [Provision Audio and Video Capabilities on Cisco Unified Communications Manager Version 8.x, page 29](#)
- [Provision Audio and Video Capabilities on Cisco Unified Communications Manager Version 9.x and Higher, page 57](#)
- [Provision Audio and Video Capabilities in Hybrid Cloud-Based Deployments, page 89](#)



CHAPTER

6

Provision Audio and Video Capabilities on Cisco Unified Communications Manager Version 8.x

Create software phone devices so that users can send and receive audio and video over their mobile devices. Learn how to enable various features to enhance the audio and video experience for users.

- [Create Software Phone Devices](#), page 29
- [Configure User Associations](#), page 36
- [Reset Devices](#), page 37
- [Specify Your TFTP Server Address](#), page 38
- [Create a CCMCIP Profile](#), page 39
- [Set Up Mobile Connect](#), page 40
- [Transfer Active VoIP Call to the Mobile Network](#), page 45
- [Set Up Dial via Office](#), page 49
- [Set Up Voicemail Avoidance](#), page 55

Create Software Phone Devices

Software phones let users send and receive audio and video through their mobile devices.

Create TCT Software Phone Devices

TCT devices provide capabilities for Cisco Jabber for iPhone to send and receive audio and video through an iOS device.

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 servers. 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.
- a) Locate the device COP file.
 - Go to the [software download site](#).
 - Locate `cmterm-iphone-install-130917.cop.sgn`.
 - b) Click **Download Now**.
 - c) Note the MD5 checksum.
You will need this information later.
 - d) 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 servers.
- Step 3** Install this COP file on the Publisher server in your Cisco Unified Communications Manager cluster:
- a) 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 server returns to active service before you perform this procedure on another server.
- Step 4** Install the COP file on each Subscriber server in the cluster.
Use the same process you used for the Publisher, including rebooting the server.
-

Related Topics

[Cisco Unified Communications Manager Maintain and Operate Guides](#)

Create SIP Profiles

The first step in creating a software phone device is to create a SIP profile that allows Cisco Jabber to stay connected to Cisco Unified Communications Manager while Cisco Jabber runs in the background.

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**.
-

Increase SIP Dual Mode Alert Timer Value

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

Cisco Jabber must be running to receive work calls.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **System > Service Parameters**.
- Step 3** Select the server.
- 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. The 4500 millisecond value is the lowest recommended value.

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 three, 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.

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**.
-

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 Version 9 and lower</p> <p>Select the SIP profile you created in the <i>Create SIP Profiles</i> topic.</p> <p>Cisco Unified Communications Manager Version 10</p> <p>Select the default profile for mobile devices: Standard SIP Profile for Mobile Device.</p> <p>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	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.
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

Related Topics

[Create SIP Profiles, on page 30](#)

Add Directory Number to Device

Procedure

- Step 1** Locate the **Association Information** section on the **Phone Configuration** window.
- Step 2** Select **Add a new DN**.
The **Directory Number Configuration** window opens.
- 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** Set the **No Answer Ring Duration (seconds)** to 24 seconds to allow time for Cisco Jabber to ring before calls go to voicemail.
- Note** If users have a PIN on the device, you may need to increase the No Answer Ring Duration (seconds) setting to ensure that they have enough time to enter the PIN and answer the call before the call goes to voicemail.
If you increase the No Answer Ring Duration (seconds) setting, see 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**.
-

Configure User Associations

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

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 **User Information** section.
- Step 6** Ensure that a Mail ID is associated with this user.
You cannot modify the end user information if synchronization with an LDAP server is enabled. To check whether synchronization with an LDAP server is enabled, select **SystemLDAPLDAP System** and verify if the **Enable Synchronizing from LDAP Server** check box is checked.

- Step 7** Locate the **Device Information** section.
 - Step 8** Select **Device Association**.
The **User Device Association** window opens.
 - Step 9** Select the devices to which you want to associate the user.
 - Step 10** Select **Save Selected/Changes**.
 - Step 11** Select **User Management > End User** and return to the **Find and List Users** window.
 - Step 12** Find and select the same user from the list.
The **End User Configuration** window opens.
 - Step 13** Locate the **Permissions Information** section.
 - Step 14** Select **Add to User Group**.
The **Find and List User Groups** dialog box opens.
 - Step 15** Select the groups to which you want to assign the user.
At a minimum you should assign the user to the following group **Standard CCM End Users**.
 - Step 16** Select the groups to which you want to assign the user.
 - Step 17** Select **Add Selected**.
The **Find and List User Groups** window closes.
 - Step 18** Locate the **Directory Number Associations** section.
 - Step 19** Select the **Primary Extension** for the end user.
 - Step 20** Select **Save** on the **End User Configuration** 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.
-

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.

Specify Your TFTP Server on Cisco Unified Presence

Complete the steps to specify the address of your TFTP server on Cisco Unified Presence.

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**
- Step 5** Select **Save**.
-

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 Administration Tool.

Procedure

- Step 1** Open the Cisco WebEx Administration 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.
-

Create a CCMCIP Profile

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

Procedure

- Step 1** Open the **Cisco Unified Presence Administration** interface.
- Step 2** Select **Application > Cisco Jabber > CCMCIP Profile**.
Note In some versions of Cisco Unified Presence, this path is as follows: **Application > Cisco Unified Personal Communicator > CCMCIP Profile**.
The **Find and List CCMCIP Profiles** window opens.
- Step 3** Select **Add New**.
The **CCMCIP Profile Configuration** window opens.
- Step 4** Specify service details in the CCMCIP profile as follows:
 - a) Specify a name for the profile in the **Name** field.
 - b) Specify the hostname or IP address of your primary CCMCIP service in the **Primary CCMCIP Host** field.
 - c) Specify the hostname or IP address of your backup CCMCIP service in the **Backup CCMCIP Host** field.
 - d) Leave the default value for **Server Certificate Verification**.
- Step 5** Add users to the CCMCIP profile as follows:
 - a) Select **Add Users to Profile**.
The **Find and List Users** dialog box opens.
 - b) Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
 - c) Select the appropriate users from the list.

- d) Select **Add Selected**.
The selected users are added to the CCMCIP profile.

Step 6 Select **Save**.

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.

Related Topics

- [Enable Mobile Connect, on page 41](#)
- [Add Mobility Identity, on page 42](#)
- [Add Remote Destination \(Optional\), on page 44](#)
- [Cisco Jabber for iPhone User Guides](#)

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:
- Select **Device > Remote Destination**.
 - Search for the destination number.
 - Delete the destination number.
- Step 3** Configure the end user for Mobile Connect as follows:
- Select **User Management > End User**.
 - Search for the end user.
 - Select the user id to open the **End User Configuration** window.
 - In the Mobility Information section, check the **Enable Mobility** check box.
 - On Cisco Unified Communications Manager Release 9.0 and earlier, specify the Primary User Device.
 - Select **Save**.
- Step 4** Configure the device settings for Mobile Connect as follows:
- Navigate to **Device > Phone**.
 - Search for the device that you want to configure.
 - Select the device name to open the **Phone Configuration** window.
 - 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 that 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**.

Related Topics

[Cisco Unified Communications Manager Maintain and Operate Guides](#)

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.

This number must be routable 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.

Example:

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.

Step 6 Do one of the following:

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

Option	Description
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**.

Related Topics

[Set Up Enterprise Feature Access Number, on page 51](#)

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:

- 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, select **Add a New Remote Destination**.

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

This number must be routable to an outbound gateway. Generally, the number is the full E.164 number.

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.

For more information, see the online help in Cisco Unified Communications Manager.

Example:

Setting	Suggested Initial Value
Answer Too Soon Timer	3000
Answer Too Late Timer	20000

Setting	Suggested Initial Value
Delay Before Ringing Timer	0 Note This setting does not apply to DVO-R calls.

Step 6 Do one of the following:

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

Related Topics

[Enable Handoff from VoIP to Mobile Network, on page 46](#)

[Enable Transfer from VoIP to Mobile Network, on page 48](#)

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 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** On the iOS device, tap **Settings > Phone > Show My Caller ID** to verify that Caller ID is on.
 - Step 3** 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.

- a) Select **Device > Device Settings > Softkey Template**.
- b) Select the same softkey template that you selected when you configured the device for Mobile Connect.
- c) In the **Related Links** drop-down list at the upper right, select **Configure Softkey Layout** and select **Go**.
- d) 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.
- e) 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:

- 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 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.

Related Topics

[Create TCT Software Phone Devices](#), on page 29

[Set Up Mobile Connect](#), on page 40

Set Up Dial via Office



Important

User-controlled voicemail avoidance, which can be used in conjunction with the Dial via Office 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 Dial via Office feature is not supported with the Extension Mobility feature.

The Dial via Office (DVO) feature allows users to initiate Cisco Jabber *outgoing* calls with their work number using the voice plan for the device.




Cisco Jabber supports Dial via Office-Reverse (DVO-R) calls. DVO-R works as follows:

- 1 User initiates a Dial via Office-Reverse 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 Ringing 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 4: 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	Outgoing: DVO-R	Incoming: Mobile Connect	Outgoing: VoIP	Incoming: VoIP
 Noncorporate Wi-Fi					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.

Related Topics

- [Set Up Mobile Connect, on page 40](#)
- [Set Up Cisco Unified Communications Manager to Support DVO, on page 51](#)
- [Enable Dial via Office on Each Device, on page 55](#)

Set Up Cisco Unified Communications Manager to Support DVO

To set up Cisco Unified Communications Manager to support 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.

Related Topics

- [Set Up Enterprise Feature Access Number, on page 51](#)
- [Set Up Mobility Profile, on page 52](#)
- [Verify Device COP File Version, on page 53](#)

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 screen 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** Click **Next**.
 - Step 6** 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. For more information, see the Cisco Jabber Installation and Configuration Guide for your release.
-

Related Topics

[Cisco Jabber for iPhone Installation and Upgrade Guides](#)

Set Up Dial via Office for Each Device

Use the following procedures to set up Dial via Office - Reverse for each TCT 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.
This number must be routable 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.

Example:

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.

Step 6 Do one of the following:

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

Related Topics

[Set Up Enterprise Feature Access Number, on page 51](#)

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 voicemail. 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.

On Cisco Unified Communications Manager Version 8.x, you can set up Voicemail Avoidance using timers. 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.

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.

Related Topics

[Cisco Unified Communications Manager Features and Services Guide](#)

Set Up Timer-Controlled Voicemail Avoidance

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

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.

Related Topics

[Add Mobility Identity, on page 42](#)

[Add Remote Destination \(Optional\), on page 44](#)



Provision Audio and Video Capabilities on Cisco Unified Communications Manager Version 9.x and Higher

Create software phone devices so that users can send and receive audio and video over their mobile devices. Learn how to enable various features to enhance the audio and video experience for users.

- [Create Software Phone Devices, page 57](#)
- [Configure User Associations, page 64](#)
- [Specify Your TFTP Server Address, page 65](#)
- [Reset Devices, page 66](#)
- [Create a CCMCIP Profile, page 67](#)
- [Set Up Mobile Connect, page 68](#)
- [Transfer Active VoIP Call to the Mobile Network, page 73](#)
- [Set Up Dial via Office, page 77](#)
- [Set Up Voicemail Avoidance, page 83](#)

Create Software Phone Devices

Software phones let users send and receive audio and video through their mobile devices.

Create TCT Software Phone Devices

TCT devices provide capabilities for Cisco Jabber for iPhone to send and receive audio and video through an iOS device.

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 servers.

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.
- a) Locate the device COP file.
 - Go to the [software download site](#).
 - Locate `cmterm-iphone-install-130917.cop.sgn`.
 - b) Click **Download Now**.
 - c) Note the MD5 checksum.
You will need this information later.
 - d) 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 servers.
- Step 3** Install this COP file on the Publisher server in your Cisco Unified Communications Manager cluster:
- a) 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 server returns to active service before you perform this procedure on another server.
- Step 4** Install the COP file on each Subscriber server in the cluster.
Use the same process you used for the Publisher, including rebooting the server.
-

Related Topics

[Cisco Unified Communications Manager Maintain and Operate Guides](#)

Create SIP Profiles

This procedure is required only when you use Cisco Unified Communications Manager Version 9 or lower. If you use Cisco Unified Communications Manager Version 9 or lower, the first step in creating a software phone device is to create a SIP profile that allows Cisco Jabber to stay connected to Cisco Unified Communications Manager while Cisco Jabber runs in the background.

If you use Cisco Unified Communications Manager Version 10, you can use the following default profile for mobile devices instead: **Standard SIP Profile for Mobile Device**. You select this default profile when you configure the device. For more information, see the *TCT Device Configuration Settings* topic.

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**.
-

Related Topics

[TCT Device Configuration Settings, on page 32](#)

Increase SIP Dual Mode Alert Timer Value

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

Cisco Jabber must be running to receive work calls.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **System > Service Parameters**.
- Step 3** Select the server.
- 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. The 4500 millisecond value is the lowest recommended value.

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 three, 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.

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**.

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 5: 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	

Setting	Description
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 6: Protocol-Specific Information Settings

Setting	Description
Device Security Profile	Select Cisco Dual Mode for iPhone - Standard SIP Non-Secure Profile .
SIP Profile	<p>Cisco Unified Communications Manager Version 9 and lower</p> <p>Select the SIP profile you created in the <i>Create SIP Profiles</i> topic.</p> <p>Cisco Unified Communications Manager Version 10</p> <p>Select the default profile for mobile devices: Standard SIP Profile for Mobile Device.</p> <p>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 7: Product Specific Configuration Layout Settings

Setting	Description
Emergency Numbers	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.

Setting	Description
Preset Wi-Fi Networks	The SSIDs for Wi-Fi networks. 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. Separate multiple SSIDs with forward slash (/). Example: SalesOffice1/CorporateWiFi
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

Related Topics

[Create SIP Profiles, on page 30](#)

Add Directory Number to Device

Procedure

-
- Step 1** Locate the **Association Information** section on the **Phone Configuration** window.
- Step 2** Select **Add a new DN**.
The **Directory Number Configuration** window opens.
- 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** Set the **No Answer Ring Duration (seconds)** to 24 seconds to allow time for Cisco Jabber to ring before calls go to voicemail.
- Note** If users have a PIN on the device, you may need to increase the No Answer Ring Duration (seconds) setting to ensure that they have enough time to enter the PIN and answer the call before the call goes to voicemail.
- If you increase the No Answer Ring Duration (seconds) setting, see 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**.
-

Configure User Associations

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

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 **Device Information** section.
- Step 6** Select **Device Association**.
The **User Device Association** window opens.
- Step 7** Select the devices to which you want to associate the user.
- Step 8** Select **Save Selected/Changes**.
- Step 9** Select **User Management > End User** and return to the **Find and List Users** window.
- Step 10** Find and select the same user from the list.
The **End User Configuration** window opens.
- Step 11** Locate the **Permissions Information** section.
- Step 12** Select **Add to Access Control Group**.
The **Find and List Access Control Groups** dialog box opens.
- Step 13** 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**
- Certain phone models require additional control groups, as follows:
- Cisco Unified IP Phone 9900 or 8900 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 14** Select **Add Selected**.
The **Find and List Access Control Groups** window closes.
- Step 15** 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.

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

Complete the steps to specify the address of your TFTP server on Cisco Unified Communications Manager IM and Presence.

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 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 Administration Tool.

Procedure

- Step 1** Open the Cisco WebEx Administration 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.
-

Create a CCMCIP Profile

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

Procedure

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

The selected users are added to the CCMCIP profile.

Step 6 Select **Save**.

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.

Related Topics

- [Enable Mobile Connect, on page 41](#)
- [Add Mobility Identity, on page 42](#)
- [Add Remote Destination \(Optional\), on page 44](#)
- [Cisco Jabber for iPhone User Guides](#)

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:
- Select **Device > Remote Destination**.
 - Search for the destination number.
 - Delete the destination number.
- Step 3** Configure the end user for Mobile Connect as follows:
- Select **User Management > End User**.
 - Search for the end user.
 - Select the user id to open the **End User Configuration** window.
 - In the Mobility Information section, check the **Enable Mobility** check box.
 - On Cisco Unified Communications Manager Release 9.0 and earlier, specify the Primary User Device.
 - Select **Save**.
- Step 4** Configure the device settings for Mobile Connect as follows:
- Navigate to **Device > Phone**.
 - Search for the device that you want to configure.
 - Select the device name to open the **Phone Configuration** window.
 - 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 that 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**.

Related Topics

[Cisco Unified Communications Manager Maintain and Operate Guides](#)

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.

This number must be routable 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.

Example:

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.

Step 6 Do one of the following:

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

Option	Description
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**.

Related Topics

[Set Up Enterprise Feature Access Number, on page 51](#)

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:

- 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, select **Add a New Remote Destination**.

Step 4 Enter the desired phone number as the Destination Number.
This number must be routable to an outbound gateway. Generally, the number is the full E.164 number.

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.

For more information, see the online help in Cisco Unified Communications Manager.

Example:

Setting	Suggested Initial Value
Answer Too Soon Timer	3000
Answer Too Late Timer	20000

Setting	Suggested Initial Value
Delay Before Ringing Timer	0 Note This setting does not apply to DVO-R calls.

Step 6 Do one of the following:

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

Related Topics

[Enable Handoff from VoIP to Mobile Network, on page 46](#)

[Enable Transfer from VoIP to Mobile Network, on page 48](#)

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 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** On the iOS device, tap **Settings > Phone > Show My Caller ID** to verify that Caller ID is on.
 - Step 3** 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.

- a) Select **Device > Device Settings > Softkey Template**.
- b) Select the same softkey template that you selected when you configured the device for Mobile Connect.
- c) In the **Related Links** drop-down list at the upper right, select **Configure Softkey Layout** and select **Go**.
- d) 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.
- e) 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:

- 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 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.

Related Topics

[Create TCT Software Phone Devices](#), on page 29

[Set Up Mobile Connect](#), on page 40

Set Up Dial via Office



Important

User-controlled voicemail avoidance, which can be used in conjunction with the Dial via Office 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 Dial via Office feature is not supported with the Extension Mobility feature.

The Dial via Office (DVO) feature allows users to initiate Cisco Jabber *outgoing* calls with their work number using the voice plan for the device.




Cisco Jabber supports Dial via Office-Reverse (DVO-R) calls. DVO-R works as follows:

- 1 User initiates a Dial via Office-Reverse 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 Ringing 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 8: 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	Outgoing: DVO-R	Incoming: Mobile Connect	Outgoing: VoIP	Incoming: VoIP
 Noncorporate Wi-Fi					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.

Related Topics

- [Set Up Mobile Connect, on page 40](#)
- [Set Up Cisco Unified Communications Manager to Support DVO, on page 51](#)
- [Enable Dial via Office on Each Device, on page 55](#)

Set Up Cisco Unified Communications Manager to Support DVO

To set up Cisco Unified Communications Manager to support 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.

Related Topics

- [Set Up Enterprise Feature Access Number, on page 51](#)
- [Set Up Mobility Profile, on page 52](#)
- [Verify Device COP File Version, on page 53](#)

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 screen 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** Click **Next**.
 - Step 6** 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. For more information, see the Cisco Jabber Installation and Configuration Guide for your release.
-

Related Topics

[Cisco Jabber for iPhone Installation and Upgrade Guides](#)

Set Up Dial via Office for Each Device

Use the following procedures to set up Dial via Office - Reverse for each TCT 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.
This number must be routable 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.

Example:

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.

Step 6 Do one of the following:

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

Related Topics

[Set Up Enterprise Feature Access Number, on page 51](#)

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.

Related Topics

[Cisco Unified Communications Manager Features and Services Guide](#)

Set Up Timer-Controlled Voicemail Avoidance

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

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.

Related Topics

[Add Mobility Identity, on page 42](#)

[Add Remote Destination \(Optional\), on page 44](#)

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.

Related Topics

[Set Up Cisco Unified Communications Manager to Support Voicemail Avoidance](#), on page 85

[Enable Voicemail Avoidance on Mobility Identity](#), on page 85

[Enable Voicemail Avoidance on Remote Destination](#), on page 86

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**.
-

Related Topics

[Cisco Unified Communications Manager Maintain and Operate Guides](#)

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 Version 9

In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.

Cisco Unified Communications Manager Version 10 without Dial via Office

In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.

Cisco Unified Communications Manager Version 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**.
-

Related Topics

[Cisco Unified Communications Manager Maintain and Operate Guides](#)

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 Version 9

In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.

Cisco Unified Communications Manager Version 10 without Dial via Office

In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.

Cisco Unified Communications Manager Version 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**.
-

Related Topics

[Cisco Unified Communications Manager Maintain and Operate Guides](#)



Provision Audio and Video Capabilities in Hybrid Cloud-Based Deployments

In hybrid cloud-based deployments, you can provision users with audio and video capabilities. You should first provision users with audio and video capabilities on Cisco Unified Communications Manager. You then create Unified Communications clusters with the Cisco WebEx Administration Tool to integrate your on-premises environment.

- [Configure Audio and Video Services, page 89](#)
- [Add Teleconferencing Service Name Accounts, page 89](#)

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*

Related Topics

- [Understanding Cisco Unified Communications integration with Cisco WebEx](#)
- [Creating unified communications clusters](#)

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*.

Related Topics

[Cisco WebEx Site User's Administration Guide](#)



PART **IV**

Set Up Voicemail

- [Set Up Voicemail on Cisco Unified Presence, page 93](#)
- [Set Up Voicemail on Cisco Unified Communications Manager, page 99](#)
- [Set Up Voicemail in Hybrid Cloud-Based Deployments, page 105](#)



Set Up Voicemail on Cisco Unified Presence

Setting up voicemail requires you to configure Cisco Unity Connection and then add voicemail profiles on Cisco Unified Presence. You can also configure voicemail retrieval and redirection to enable users to access voice mail messages in the client user interface and send incoming calls to voicemail.

This chapter applies to Cisco Unified Presence version 8.6 and lower.

- [Configure Cisco Unity Connection, page 93](#)
- [Add a Voicemail Server, page 94](#)
- [Create a Voicemail Profile, page 95](#)
- [Configure Retrieval and Redirection, page 96](#)
- [Set a Voicemail Credentials Source, page 97](#)

Configure Cisco Unity Connection

You must complete some specific steps to configure Cisco Unity Connection so that Cisco Jabber can access voicemail services. You should refer to the Cisco Unity Connection documentation for instructions on general tasks such as creating users, passwords, and provisioning users with voicemail access.



Remember Cisco Jabber connects to the voicemail service through a REST interface and supports Cisco Unity Connection version 8.5 or later.

Procedure

Step 1 Ensure the **Connection Jetty** and **Connection REST Service** services are started.

- a) Open the **Cisco Unity Connection Serviceability** interface.
- b) Select **Tools > Service Management**.
- c) Locate the following services in the **Optional Services** section:

- **Connection Jetty**

- **Connection REST Service**

d) Start the services if required.

Step 2 Open the **Cisco Unity Connection Administration** interface.

Step 3 Edit user password settings.

- Select **Users**.
- Select the appropriate user.
- Select **Edit > Password Settings**.
- Select **Web Application** from the **Choose Password** menu.
- Uncheck **User Must Change at Next Sign-In**.
- Select **Save**.

Step 4 Provide users with access to the web inbox.

- Select **Class of Service**.
The **Search Class of Service** window opens.
- Select the appropriate class of service or add a new class of service.
- Select **Allow Users to Use the Web Inbox and RSS Feeds**.
- In the **Features** section, select **Allow Users to Use Unified Client to Access Voice Mail**.
- Select all other options as appropriate.
- Select **Save**.

Step 5 Select API configuration settings.

- Select **System Settings > Advanced > API Settings**.
The **API Configuration** window opens.
 - Select the following options:
 - **Allow Access to Secure Message Recordings through CUMI**
 - **Display Message Header Information of Secure Messages through CUMI**
 - **Allow Message Attachments through CUMI**
 - Select **Save**.
-

Add a Voicemail Server

Complete the steps in this task to add your voicemail server on Cisco Unified Presence.

Procedure

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

Step 2 Select **Application > Cisco Jabber > Voicemail Server**.

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

The **Find and List Voicemail Servers** window opens.

- Step 3** Select **Add New**.
The **Voicemail Server Configuration** window opens.
- Step 4** Select **Unity Connection** from the **Server Type** drop-down list.
- Step 5** Specify details in the **Voicemail Server Configuration** section as follows:

Name

Enter a descriptive name for the server, for example, PrimaryVoicemailServer.

Description

Enter an optional description.

Hostname/IP Address

Enter the address of the voicemail server in one of the following formats:

- Hostname
- IP Address
- FQDN

Port

You do not need to specify a port number. By default, the client always uses port 443 to connect to the voicemail server. For this reason, any value you specify does not take effect.

Protocol Type

You do not need to specify a value. By default, the client always uses HTTPS to connect to the voicemail server. For this reason, any value you specify does not take effect.

- Step 6** Select **Save**.
-

Related Topics

[Configuring Voicemail Server Names and Addresses on Cisco Unified Presence](#)

Create a Voicemail Profile

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

Procedure

- Step 1** Open the **Cisco Unified Presence Administration** interface.
- Step 2** Select **Application > Cisco Jabber > Voicemail Profile**.
- Note** In some versions of Cisco Unified Presence, this path is as follows: **Application > Cisco Unified Personal Communicator > Voicemail Profile**.

The **Find and List Voicemail Profiles** window opens.

Step 3 Select **Add New**.

The **Voicemail Profile Configuration** window opens.

Step 4 Specify the required details on the **Voicemail Profile Configuration** window.

Step 5 Add users to the voicemail profile as follows:

a) Select **Add Users to Profile**.

The **Find and List Users** dialog box opens.

b) Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.

c) Select the appropriate users from the list.

d) Select **Add Selected**.

The selected users are added to the voicemail profile.

Step 6 Select **Save**.

Configure Retrieval and Redirection

Configure retrieval so that users can access voice mail messages in the client interface. Configure redirection so that users can send incoming calls to voicemail. You configure retrieval and redirection on Cisco Unified Communications Manager.

Procedure

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

Step 2 Configure the voicemail pilot.

a) Select **Advanced Features > Voice Mail > Voice Mail Pilot**.

The **Find and List Voice Mail Pilots** window opens.

b) Select **Add New**.

The **Voice Mail Pilot Configuration** window opens.

c) Specify the appropriate details on the **Voice Mail Pilot Configuration** window.

d) Select **Save**.

Step 3 Add the voicemail pilot to the voicemail profile.

a) Select **Advanced Features > Voice Mail > Voice Mail Profile**.

The **Find and List Voice Mail Mail Profiles** window opens.

b) Specify the appropriate filters in the **Find Voice Mail Profile where Voice Mail Profile Name** field and then select **Find** to retrieve a list of profiles.

c) Select the appropriate profile from the list.

The **Voice Mail Pilot Configuration** window opens.

d) Select the voicemail pilot from the **Voice Mail Pilot** drop-down list.

e) Select **Save**.

Step 4 Specify the voicemail profile in the directory number configuration.

- 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 appropriate device from the list.
The **Phone Configuration** window opens.
- d) Locate the **Association Information** section.
- e) Select the appropriate device number.
The **Directory Number Configuration** window opens.
- f) Locate the **Directory Number Settings** section.
- g) Select the voicemail profile from the **Voice Mail Profile** drop-down list.
- h) Select **Save**.

Set a Voicemail Credentials Source

You can specify a voicemail credentials source on Cisco Unified Presence.



Tip

In hybrid cloud-based deployments, you can set a voicemail credentials source as part of your configuration file with the `VoiceMailService_UseCredentialsFrom` parameter. See the *Installation and Configuration Guide* for more information.

Procedure

- Step 1** Open the **Cisco Unified Presence Administration** interface.
- Step 2** Select **Application > Cisco Jabber > Settings**.
In some versions of Cisco Unified Presence this path is as follows: **Application > Cisco Unified Personal Communicator > Settings**
- Step 3** In the **Cisco Jabber Settings** section, select **CUP** from the **Credentials source for voicemail service** drop-down list.

Note Do not select **Web Conferencing** from the **Credentials source for voicemail service** drop-down list. You cannot currently use conferencing credentials as a credentials source for voicemail services.

The user's credentials for Cisco Unified Presence match the user's voicemail credentials. As a result, users do not need to specify their voicemail credentials in the client user interface.

What to Do Next



Important

There is no mechanism to synchronize credentials between servers. If you specify a credentials source, you must ensure that those credentials match the user's voicemail credentials.

For example, you specify that a user's Cisco Unified Presence credentials match the user's Cisco Unity Connection credentials. The user's Cisco Unified Presence credentials then change. You must update the user's Cisco Unity Connection credentials to reflect that change.



CHAPTER 10

Set Up Voicemail on Cisco Unified Communications Manager

Setting up voicemail requires you to configure Cisco Unity Connection and then add voicemail services on Cisco Unified Communications Manager. You can also configure voicemail retrieval and redirection to enable users to access voice mail messages in the client user interface and send incoming calls to voicemail.

This chapter applies to Cisco Unified Communications Manager version 9.0 and higher.

- [Configure Cisco Unity Connection, page 99](#)
- [Add a Voicemail Service, page 100](#)
- [Configure Retrieval and Redirection, page 102](#)
- [Set a Voicemail Credentials Source, page 103](#)

Configure Cisco Unity Connection

You must complete some specific steps to configure Cisco Unity Connection so that Cisco Jabber can access voicemail services. You should refer to the Cisco Unity Connection documentation for instructions on general tasks such as creating users, passwords, and provisioning users with voicemail access.



Remember

Cisco Jabber connects to the voicemail service through a REST interface and supports Cisco Unity Connection version 8.5 or later.

Procedure

Step 1 Ensure the **Connection Jetty** and **Connection REST Service** services are started.

- a) Open the **Cisco Unity Connection Serviceability** interface.
- b) Select **Tools > Service Management**.
- c) Locate the following services in the **Optional Services** section:

- **Connection Jetty**

- **Connection REST Service**

d) Start the services if required.

Step 2 Open the **Cisco Unity Connection Administration** interface.

Step 3 Edit user password settings.

- Select **Users**.
- Select the appropriate user.
- Select **Edit > Password Settings**.
- Select **Web Application** from the **Choose Password** menu.
- Uncheck **User Must Change at Next Sign-In**.
- Select **Save**.

Step 4 Provide users with access to the web inbox.

- Select **Class of Service**.
The **Search Class of Service** window opens.
- Select the appropriate class of service or add a new class of service.
- Select **Allow Users to Use the Web Inbox and RSS Feeds**.
- In the **Features** section, select **Allow Users to Use Unified Client to Access Voice Mail**.
- Select all other options as appropriate.
- Select **Save**.

Step 5 Select API configuration settings.

- Select **System Settings > Advanced > API Settings**.
The **API Configuration** window opens.
 - Select the following options:
 - **Allow Access to Secure Message Recordings through CUMI**
 - **Display Message Header Information of Secure Messages through CUMI**
 - **Allow Message Attachments through CUMI**
 - Select **Save**.
-

Add a Voicemail Service

Allow users to receive voice messages.

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 **Voicemail** from the **UC Service Type** drop-down list.

Step 5 Select **Next**.

Step 6 Specify details for the voicemail service as follows:

Product Type

Select **Unity Connection**.

Name

Enter a descriptive name for the server, for example, PrimaryVoicemailServer.

Description

Enter an optional description.

Hostname/IP Address

Enter the address of the voicemail server in one of the following formats:

- Hostname
- IP Address
- FQDN

Port

You do not need to specify a port number. By default, the client always uses port 443 to connect to the voicemail server. For this reason, any value you specify does not take effect.

Protocol Type

You do not need to specify a value. By default, the client always uses HTTPS to connect to the voicemail server. For this reason, any value you specify does not take effect.

Step 7 Select **Save**.

What to Do Next

Add the voicemail service to your service profile.

Apply Voicemail Service

After you add a voicemail 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 exist or you require a separate service profile for voicemail.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **User Management > User Settings > Service Profile**.
The **Find and List Service Profiles** window opens.
- Step 3** Find and select your service profile.
The **Service Profile Configuration** window opens.
- Step 4** Configure the **Voicemail Profile** section as follows:
- Select up to three services from the following drop-down lists:
 - **Primary**
 - **Secondary**
 - **Tertiary**
 - To synchronize credentials with the voicemail service, select **Unified CM - IM and Presence** from the **Credentials source for voicemail service** drop-down list.
Unified CM - IM and Presence uses the instant messaging and presence credentials to log in to the voicemail service. As a result, users do not need to enter their credentials for voicemail services in the client.
Note Do not select **Web conferencing**. This option uses the conferencing credentials to log in to the voicemail service. You cannot currently synchronize with conferencing credentials.
- Step 5** Select **Save**.
- Step 6** Add users to the service profile.
- Select **User Management > End User**.
The **Find and List Users** dialog box opens.
 - Specify the appropriate filters in the **Find User where** field and then select **Find** to find a user.
 - Click the user in the list.
The **End User Configuration** window appears.
 - Under the **Service Settings** area, check the **Home Cluster** check box.
 - Check the **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)** check box.
 - Select your service profile from the **UC Service Profile** drop-down list.
- Step 7** Select **Save**.
-

Configure Retrieval and Redirection

Configure retrieval so that users can access voice mail messages in the client interface. Configure redirection so that users can send incoming calls to voicemail. You configure retrieval and redirection on Cisco Unified Communications Manager.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Configure the voicemail pilot.
- Select **Advanced Features > Voice Mail > Voice Mail Pilot**.
The **Find and List Voice Mail Pilots** window opens.
 - Select **Add New**.
The **Voice Mail Pilot Configuration** window opens.
 - Specify the appropriate details on the **Voice Mail Pilot Configuration** window.
 - Select **Save**.
- Step 3** Add the voicemail pilot to the voicemail profile.
- Select **Advanced Features > Voice Mail > Voice Mail Profile**.
The **Find and List Voice Mail Mail Profiles** window opens.
 - Specify the appropriate filters in the **Find Voice Mail Profile where Voice Mail Profile Name** field and then select **Find** to retrieve a list of profiles.
 - Select the appropriate profile from the list.
The **Voice Mail Pilot Configuration** window opens.
 - Select the voicemail pilot from the **Voice Mail Pilot** drop-down list.
 - Select **Save**.
- Step 4** Specify the voicemail profile in the directory number configuration.
- Select **Device > Phone**.
The **Find and List Phones** window opens.
 - Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of devices.
 - Select the appropriate device from the list.
The **Phone Configuration** window opens.
 - Locate the **Association Information** section.
 - Select the appropriate device number.
The **Directory Number Configuration** window opens.
 - Locate the **Directory Number Settings** section.
 - Select the voicemail profile from the **Voice Mail Profile** drop-down list.
 - Select **Save**.
-

Set a Voicemail Credentials Source

You can specify a voicemail credentials source for users.

**Tip**

In hybrid cloud-based deployments, you can set a voicemail credentials source as part of your configuration file with the `VoiceMailService_UseCredentialsFrom` parameter. See the *Installation and Configuration Guide* for more information.

Procedure

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

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

Step 3 Select the appropriate service profile to open the **Service Profile Configuration** window.

Step 4 In the **Voicemail Profile** section, select **Unified CM - IM and Presence** from the **Credentials source for voicemail service** drop-down list.

Note Do not select **Web Conferencing** from the **Credentials source for voicemail service** drop-down list. You cannot currently use conferencing credentials as a credentials source for voicemail services.

The user's instant messaging and presence credentials match the user's voicemail credentials. As a result, users do not need to specify their voicemail credentials in the client user interface.

What to Do Next**Important**

There is no mechanism to synchronize credentials between servers. If you specify a credentials source, you must ensure that those credentials match the user's voicemail credentials.

For example, you specify that a user's instant messaging and presence credentials match the user's Cisco Unity Connection credentials. The user's instant messaging and presence credentials then change. You must update the user's Cisco Unity Connection credentials to reflect that change.



CHAPTER 11

Set Up Voicemail in Hybrid Cloud-Based Deployments

In hybrid cloud-based deployments, you can provision users with voicemail capabilities. You must first set up your on-premises deployment of Cisco Unity Connection. You can then configure visual voicemail settings with the Cisco WebEx Administration Tool to integrate your voicemail server.

- [Configure Voicemail, page 105](#)
- [Allow Users to Set Voicemail Server Settings, page 105](#)

Configure Voicemail

To configure your voicemail settings, use the Cisco WebEx Administration Tool.

See also the *Hybrid Cloud-Based Diagram* in the *Deployment Options* chapter of the applicable *Cisco Jabber Installation and Configuration Guide*.

Related Topics

- [Specifying Visual Voicemail settings](#)
- [Cisco Jabber for iPhone Installation and Configuration Guides](#)

Allow Users to Set Voicemail Server Settings

Select an option with the Cisco WebEx Administration Tool so that users can specify voicemail server settings in the client interface.

Procedure

- Step 1** Open the Cisco WebEx Administration Tool.
 - Step 2** Select **Configuration > Unified Communications**.
 - Step 3** Select the **Voicemail** tab.
 - Step 4** Select **Allow user to enter manual settings**
-

The user can access advanced voicemail settings in the client interface by tapping **Settings > Voicemail**.



PART **V**

Set Up Conferencing

- [Set Up Conferencing on Cisco Unified Presence, page 109](#)
- [Set Up Conferencing on Cisco Unified Communications Manager, page 117](#)
- [Set Up Conferencing in Cloud-Based Deployments, page 125](#)



Set Up Conferencing on Cisco Unified Presence

Conferencing capabilities allow users to schedule, attend, and manage Cisco WebEx meetings with Cisco Jabber. You can set up on-premises conferencing with Cisco WebEx Meetings Server or cloud-based conferencing with Cisco WebEx Meeting Center. Review the set up process and what options are available for authenticating with a conferencing server.

This chapter applies to Cisco Unified Presence version 8.6 and lower.

- [Set Up On-Premises Conferencing, page 109](#)
- [Set Up Cloud-Based Conferencing, page 112](#)

Set Up On-Premises Conferencing

Cisco WebEx Meetings Server provides on-premises meeting and conferencing services for the client.

Cisco WebEx Meetings Server Installation and Configuration

The first step in setting up integration between Cisco WebEx Meetings Server and the client is to install and configure Cisco WebEx Meetings Server. You should refer to the Cisco WebEx Meetings Server product documentation for installation and configuration procedures.



Restriction

You cannot currently integrate Cisco Jabber with Cisco WebEx Meetings Server sites that you configure for single sign on (SSO).

Related Topics

[Cisco WebEx Meetings Server Install and Upgrade Guides](#)

Set Up Cisco WebEx Meetings Server on Cisco Unified Presence

The client retrieves Cisco WebEx Meetings Server details from the conferencing profile on Cisco Unified Presence. You must add your details for Cisco WebEx Meetings Server, add Cisco WebEx Meetings Server to a profile, and then add users to the profile.

Add Cisco WebEx Meetings Server

The first step to setting up conferencing on Cisco Unified Presence is to add your details for Cisco WebEx Meetings Server.

Procedure

- Step 1** Open the **Cisco Unified Presence Administration** interface.
- Step 2** Select **Application > Cisco Jabber > Conferencing Server**.
In some versions of Cisco Unified Presence, this path is as follows: **Application > Cisco Unified Personal Communicator > Conferencing Server**.
- Step 3** Select **Add New**.
The **Conferencing Server Configuration** window opens.
- Step 4** Specify details for Cisco WebEx Meetings Server in the following fields:

Name

Enter a name for the configuration.

The name you specify displays when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.

Description

Enter an optional description.

Hostname/IP Address

Enter the site URL for Cisco WebEx Meetings Server.

Port

Leave the default value.

Protocol

Select **HTTPS** from the drop-down list.

Server Type

Select **WebEx** from the drop-down list.

Site ID

Leave the default value.

You do not need to specify a value for this field.

Partner ID

Leave the default value.

You do not need to specify a value for this field.

Step 5 Select **Save**.

Add Cisco WebEx Meetings Server to a Profile

After you add Cisco WebEx Meetings Server on Cisco Unified Presence, you add Cisco WebEx Meetings Server to a conferencing profile. The client can then retrieve the details for Cisco WebEx Meetings Server from the profile and access the conferencing features.

Procedure

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

Step 2 Select **Application > Cisco Jabber > Conferencing Profile**.

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

Step 3 Select **Add New**.

The **Conferencing Profile Configuration** window opens.

Step 4 Specify details for the profile in the following fields:

Name

Enter a name for the configuration.

Description

Enter an optional description.

Primary Conferencing Server

Select the primary instance of Cisco WebEx Meetings Server.

Backup Conferencing Server

Select the backup instance of Cisco WebEx Meetings Server.

Server Certificate Verification

Select one of the following from the drop-down list:

- **Any Certificate**
- **Self Signed or Keystore**
- **Keystore Only**

Step 5 Select the **Make this the default Conferencing Profile for the system** checkbox to set this profile as the system default.

Step 6 Add users to the conferencing profile as follows:

- a) Select **Add Users to Profile** in the **Users in Profile** section.
The **Find and List Users** dialog box opens.

- b) Select **Find** to retrieve a list of users.
- c) Select the appropriate users from the list.
- d) Select **Add Selected**.
The selected users are added to the profile and the **Find and List Users** dialog box closes.

Step 7 Select **Save**.

Set Up Cloud-Based Conferencing

Cisco WebEx Meeting Center provides cloud-based meeting and conferencing services for the client.

Integration with Cisco WebEx Meeting Center

As of this release, there are two types of Cisco WebEx Meeting Center integration for on-premises deployments:

Cloud-Based Integration

An environment in which Cisco WebEx Meeting Center provides the following services to the client:

- Data such as participant chat and roster lists.
- Audio and video capabilities.

Hybrid Cloud-Based Integration

An environment in which:

- Cisco WebEx Meeting Center provides data such as participant chat and roster lists.
- A conferencing bridge provides audio and video capabilities.

Authentication with Cisco WebEx Meeting Center

You can authenticate the client with Cisco WebEx Meeting Center using tightly coupled integration. Tightly coupled integration refers to a configuration that you set up between Cisco WebEx Messenger and Cisco WebEx Meeting Center. When users authenticate with Cisco WebEx Messenger, it passes an authentication token back to the client. The client then passes that authentication token to Cisco WebEx Meeting Center. See the *Overview of Tightly Coupled Integration* topic for more information.

Related Topics

[Overview of Tightly Coupled Integration](#)

[Using SSO with the Cisco WebEx and Cisco WebEx Meeting applications](#)

Set Up Cisco WebEx Meeting Center on Cisco Unified Presence

The client retrieves Cisco WebEx Meeting Center details from the conferencing profile on Cisco Unified Presence. You must add your details for Cisco WebEx Meeting Center, add Cisco WebEx Meeting Center a profile, and then add users to the profile.

Add Cisco WebEx Meeting Center

The first step to setting up conferencing on Cisco Unified Presence is to add your details for Cisco WebEx Meeting Center.

Procedure

-
- Step 1** Open the **Cisco Unified Presence Administration** interface.
 - Step 2** Select **Application > Cisco Jabber > Conferencing Server**.
In some versions of Cisco Unified Presence, this path is as follows: **Application > Cisco Unified Personal Communicator > Conferencing Server**.
 - Step 3** Select **Add New**.
The **Conferencing Server Configuration** window opens.
 - Step 4** Specify details for Cisco WebEx Meeting Center in the following fields:

Name

Enter a name for the configuration.

The name you specify displays when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.

Description

Enter an optional description.

Hostname/IP Address

Specify the hostname of the Cisco WebEx Meeting Center site.

Note You must specify a hostname, not an IP address.

Port

Specify a port number for the Cisco WebEx Meeting Center site.

Protocol

Select **HTTPS** from the drop-down list.

Server Type

Select **WebEx** from the drop-down list.

Site ID

Specify the primary site ID for Cisco WebEx Meeting Center.

Note The **Site ID** field is optional. The client does not require a site ID to integrate with Cisco WebEx Meeting Center.

Partner ID

Specify the appropriate partner ID for Cisco WebEx Meeting Center.

Note The **Partner ID** field is optional. The client does not require a partner ID to integrate with Cisco WebEx Meeting Center.

Step 5 Select **Save**.

Add Cisco WebEx Meeting Center to a Profile

After you add Cisco WebEx Meeting Center on Cisco Unified Presence, you add Cisco WebEx Meeting Center to a conferencing profile. The client can then retrieve the details for Cisco WebEx Meeting Center from the profile and access the conferencing features.

Procedure

-
- Step 1** Open the **Cisco Unified Presence Administration** interface.
- Step 2** Select **Application > Cisco Jabber > Conferencing Profile**.
In some versions of Cisco Unified Presence, this path is as follows: **Application > Cisco Unified Personal Communicator > Conferencing Profile**.
- Step 3** Select **Add New**.
The **Conferencing Profile Configuration** window opens.
- Step 4** Specify details for the profile in the following fields:

Name

Enter a name for the configuration.

Description

Enter an optional description.

Primary Conferencing Server

Select the primary Cisco WebEx Meeting Center site from the drop-down list.

Note The client uses only the site you select from the **Primary Conferencing Server** drop-down list. You do not need to select a site from the **Backup Conferencing Server** drop-down list.

Server Certificate Verification

Select one of the following from the drop-down list:

- Any Certificate
- Self Signed or Keystore
- Keystore Only

Step 5 Select the **Make this the default Conferencing Profile for the system** checkbox to set this profile as the system default.

Step 6 Add users to the conferencing profile as follows:

a) Select **Add Users to Profile** in the **Users in Profile** section.
The **Find and List Users** dialog box opens.

b) Select **Find** to retrieve a list of users.

c) Select the appropriate users from the list.

d) Select **Add Selected**.

The selected users are added to the profile and the **Find and List Users** dialog box closes.

Step 7 Select **Save**.



CHAPTER 13

Set Up Conferencing on Cisco Unified Communications Manager

Conferencing capabilities allow users to schedule, attend, and manage Cisco WebEx meetings with Cisco Jabber. You can set up on-premises conferencing with Cisco WebEx Meetings Server or cloud-based conferencing with Cisco WebEx Meeting Center. Review the set up process and what options are available for authenticating with a conferencing server.

This chapter applies to Cisco Unified Communications Manager version 9.0 and higher.

- [Set Up On-Premises Conferencing, page 117](#)
- [Set Up Cloud-Based Conferencing, page 120](#)

Set Up On-Premises Conferencing

Cisco WebEx Meetings Server provides on-premises meeting and conferencing services for the client.

Cisco WebEx Meetings Server Installation and Configuration

The first step in setting up integration between Cisco WebEx Meetings Server and the client is to install and configure Cisco WebEx Meetings Server. You should refer to the Cisco WebEx Meetings Server product documentation for installation and configuration procedures.



Restriction

You cannot currently integrate Cisco Jabber with Cisco WebEx Meetings Server sites that you configure for single sign on (SSO).

Related Topics

[Cisco WebEx Meetings Server Install and Upgrade Guides](#)

Add Cisco WebEx Meetings Server

The first step to setting up conferencing on Cisco Unified Communications Manager is to add your details for Cisco WebEx Meetings Server.

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 **Conferencing** from the **UC Service Type** drop-down list.
- Step 5** Select **Next**.
- Step 6** Specify details for Cisco WebEx Meetings Server in the following fields:

Product Type

Select **WebEx (Conferencing)**.

Name

Enter a name for the configuration.

The name you specify displays when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.

Description

Enter an optional description.

Hostname/IP Address

Enter the site URL for Cisco WebEx Meetings Server.

Port

Leave the default value.

Protocol

Select **HTTPS** from the drop-down list.

- Step 7** Choose the appropriate value for the **User web conference server as SSO identity provider** check box:

Cleared

Do not use Cisco WebEx as the single sign-on (SSO) identity provider.

Selected

Use Cisco WebEx as the single sign-on (SSO) identity provider.

Note This field is available only if you select **WebEx (Conferencing)** from the **Product Type** drop-down list.

Step 8 Select **Save**.

What to Do Next

Add Cisco WebEx Meetings Server to a service profile.

Add Cisco WebEx Meetings Server to a Profile

After you add Cisco WebEx Meetings Server on Cisco Unified Communications Manager, you add Cisco WebEx Meetings Server to a service profile. The client can then retrieve the details for Cisco WebEx Meetings Server from the profile and access the conferencing features.

Before You Begin

Create a service profile.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **User Management > User Settings > Service Profile**.
The **Find and List Service Profiles** window opens.
- Step 3** Find and select your service profile.
The **Service Profile Configuration** window opens.
- Step 4** Configure the **Conferencing Profile** section as follows:
- a) Select up to three instances of Cisco WebEx Meetings Server from the following drop-down lists:
 - **Primary**
 - **Secondary**
 - **Tertiary**
 - b) Select the appropriate value from the **Server Certificate Verification** drop-down list.
 - c) Select one of the following from the **Credentials source for web conference service** drop-down list:

Not set

The user does not have a credentials source that matches their Cisco WebEx Meetings Server credentials.

Unified CM - IM and Presence

The user's Cisco Unified Communications Manager IM and Presence credentials match their Cisco WebEx Meetings Server credentials.

Voicemail

The user's Cisco Unity Connection credentials match their Cisco WebEx Meetings Server credentials.

Important If you select a credentials source, you must ensure that those credentials match the user's Cisco WebEx Meetings Server credentials.

There is no mechanism to synchronize the credentials you specify in Cisco Unified Communications Manager with credentials you specify in Cisco WebEx Meetings Server. For example, you specify that a user's instant messaging and presence credentials are synchronized with the user's Cisco WebEx Meetings Server credentials. The user's instant messaging and presence credentials then change. You must update the user's Cisco WebEx Meetings Server credentials to match that change.

Step 5 Select **Save**.

Set Up Cloud-Based Conferencing

Cisco WebEx Meeting Center provides cloud-based meeting and conferencing services for the client.

Integration with Cisco WebEx Meeting Center

As of this release, there are two types of Cisco WebEx Meeting Center integration for on-premises deployments:

Cloud-Based Integration

An environment in which Cisco WebEx Meeting Center provides the following services to the client:

- Data such as participant chat and roster lists.
- Audio and video capabilities.

Hybrid Cloud-Based Integration

An environment in which:

- Cisco WebEx Meeting Center provides data such as participant chat and roster lists.
- A conferencing bridge provides audio and video capabilities.

Authentication with Cisco WebEx Meeting Center

You can authenticate the client with Cisco WebEx Meeting Center using tightly coupled integration. Tightly coupled integration refers to a configuration that you set up between Cisco WebEx Messenger and Cisco WebEx Meeting Center. When users authenticate with Cisco WebEx Messenger, it passes an authentication token back to the client. The client then passes that authentication token to Cisco WebEx Meeting Center. See the *Overview of Tightly Coupled Integration* topic for more information.

Related Topics

[Overview of Tightly Coupled Integration](#)

[Using SSO with the Cisco WebEx and Cisco WebEx Meeting applications](#)

Add Cisco WebEx Meeting Center

The first step to setting up conferencing on Cisco Unified Communications Manager is to add your details for Cisco WebEx Meeting Center.

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 **Conferencing** from the **UC Service Type** drop-down list.
- Step 5** Select **Next**.
- Step 6** Specify details for the Cisco WebEx Meeting Center site in the following fields:

Product Type

Select **WebEx (Conferencing)**.

Name

Enter a name for the configuration.

The name you specify displays when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.

Description

Enter an optional description.

Host Name/IP Address

Specify the hostname of the Cisco WebEx Meeting Center site.

Note You must specify a hostname, not an IP address.

Port

Specify a port number for the Cisco WebEx Meeting Center site.

Protocol

Select **HTTPS** from the drop-down list.

- Step 7** Choose the appropriate value for the **User web conference server as SSO identity provider** check box:

Cleared

Do not use Cisco WebEx as the single sign-on (SSO) identity provider.

Selected

Use Cisco WebEx as the single sign-on (SSO) identity provider.

Note This field is available only if you select **WebEx (Conferencing)** from the **Product Type** drop-down list.

Step 8 Select **Save**.

What to Do Next

Add Cisco WebEx Meeting Center to a service profile.

Add Cisco WebEx Meeting Center to a Profile

After you add Cisco WebEx Meeting Center on Cisco Unified Communications Manager, you add Cisco WebEx Meeting Center to a service profile. The client can then retrieve the details for Cisco WebEx Meeting Center from the profile and access the conferencing features.

Before You Begin

Create a service profile.

Procedure

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

Step 2 Select **User Management > User Settings > Service Profile**.
The **Find and List Service Profiles** window opens.

Step 3 Find and select your service profile.
The **Service Profile Configuration** window opens.

Step 4 Configure the **Conferencing Profile** section as follows:

a) Select your service from the **Primary** drop-down list.

Note The client uses only the service you select from the **Primary** drop-down list. You do not need to select services from the **Secondary** or **Tertiary** drop-down lists.

b) Select the appropriate value from the **Server Certificate Verification** drop-down list.

c) Select one of the following from the **Credentials source for web conference service** drop-down list:

Not set

The user does not have a credentials source that matches their Cisco WebEx Meeting Center credentials.

Unified CM - IM and Presence

The user's Cisco Unified Communications Manager IM and Presence credentials match their Cisco WebEx Meeting Center credentials.

Voicemail

The user's Cisco Unity Connection credentials match their Cisco WebEx Meeting Center credentials.

Restriction You cannot specify a credentials source if you use an identity provider for authentication with Cisco WebEx Meeting Center.

Important If you select a credentials source, you must ensure that those credentials match the user's Cisco WebEx Meeting Center credentials.

There is no mechanism to synchronize the credentials you specify in Cisco Unified Communications Manager with credentials you specify in Cisco WebEx Meeting Center. For example, you specify that a user's instant messaging and presence credentials are synchronized with the user's Cisco WebEx Meeting Center credentials. The user's instant messaging and presence credentials then change. You must update the user's Cisco WebEx Meeting Center credentials to match that change.

Step 5 Select **Save**.



CHAPTER 14

Set Up Conferencing in Cloud-Based Deployments

In cloud-based deployments, you can provision users with conferencing capabilities with the Cisco WebEx Administration Tool. Learn how to assign conferencing capabilities to users. Review how to configure authentication with the conferencing server.

- [Configure Cisco WebEx Meeting Center, page 125](#)

Configure Cisco WebEx Meeting Center

You must configure the appropriate settings with the Cisco WebEx Administration Tool and assign the meeting and conferencing capabilities to the appropriate users.

Related Topics

[Understanding Cisco WebEx Connect integration with the Cisco WebEx application](#)

Authentication with Cisco WebEx Meeting Center

You can authenticate the client with Cisco WebEx Meeting Center using tightly coupled integration. Tightly coupled integration refers to a configuration that you set up between Cisco WebEx Messenger and Cisco WebEx Meeting Center. When users authenticate with Cisco WebEx Messenger, it passes an authentication token back to the client. The client then passes that authentication token to Cisco WebEx Meeting Center. See the *Overview of Tightly Coupled Integration* topic for more information.

Related Topics

[Overview of Tightly Coupled Integration](#)

[Using SSO with the Cisco WebEx and Cisco WebEx Meeting applications](#)

Specify Conferencing Credentials in the Client

Users can specify their credentials in the **Settings**.

On the **Settings** screen, under **Accounts**, tap **WebEx Meeting**.

