Cisco Jabber for Mac 9.6 Server Setup Guide

First Published: April 16, 2014

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.

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

Populate User ID and Directory URI 4

Specify an LDAP Attribute for the User ID 5

Specify an LDAP Attribute for the Directory URI 5

Perform Synchronization 5

Authenticate with the Directory Server 6

CHAPTER 2 Configure Directory Integration in Cloud-Based Deployments 9

Integrate Your Directory 9

Add Directory Groups 9

PART II Provision Instant Messaging and Presence 11

CHAPTER 3 Provision Instant Messaging and Presence on Cisco Unified Presence 13

Activate and Start Essential Services 13

Pre-Populate Contact Lists in Bulk 14

Enable Messaging Settings 14

Specify Capabilities Assignments 15

Configure Prompts for Presence Subscription Requests 15

CHAPTER 4 Provision Instant Messaging and Presence on Cisco Unified Communications Manager IM and Presence 19

Activate and Start Essential Services 19

Create a Service Profile 20

Pre-Populate Contact Lists in Bulk 21
Enable Messaging Settings 21
Enable File Transfers and Screen Captures 22
Configure Prompts for Presence Subscription Requests 22
Add an Instant Messaging and Presence Service 24
Apply Instant Messaging and Presence Service 24
Configure Users 25
Configure Users Individually 25
Configure Users in Bulk 26

CHAPTER 5 Provision Instant Messaging and Presence in Cloud-Based Deployments 27
Configure Instant Messaging and Presence 27
Configure Privacy Options 27

PART III Provision Audio and Video Capabilities 29

CHAPTER 6 Provision Audio and Video Capabilities on Cisco Unified Communications Manager Version 8.x 31
Create Software Phone Devices 31
Create CSF Devices on 8.6(1) 31
Create SIP Profiles 32
Create CSF Devices 32
Create CSF Devices on 8.6(2) and Higher 33
Create CSF Devices 33
Set Up Secure Phone Capabilities 33
Configure the Security Mode 34
Create a Phone Security Profile 34
Configure the Phone Security Profile 34
Configure CSF Devices 35
Specify Certificate Settings 36
Provide Users with Authentication Strings 37
Secure Phone Details 38
Add a Directory Number to the Device 40
Create Desk Phone Devices 41
Add a Directory Number to the Device 42

Enable Video Rate Adaptation 43
Enable RTCP on Common Phone Profiles 43
Enable RTCP on Device Configurations 43
Set Up a CTI Gateway 44
Add a CTI Gateway Server 44
Create a CTI Gateway Profile 44
Configure User Associations 45
Reset Devices 46
Specify Your TFTP Server Address 46
Specify Your TFTP Server on Cisco Unified Presence 47
Specify TFTP Servers with the Cisco WebEx Administration Tool 47
Create a CCMCIP Profile 48
Dial Plan Mapping 49
Publish Dial Rules 49

CHAPTER 7 **Provision Audio and Video Capabilities on Cisco Unified Communications Manager Version 9.x and Higher** 51
Create Software Phone Devices 51
Create CSF Devices 51
Set Up Secure Phone Capabilities 52
Configure the Security Mode 52
Create a Phone Security Profile 53
Configure the Phone Security Profile 53
Configure CSF Devices 54
Specify Certificate Settings 55
Provide Users with Authentication Strings 56
Secure Phone Details 56
Add a Directory Number to the Device 59
Create Desk Phone Devices 60
Add a Directory Number to the Device 61
Enable Video Rate Adaptation 61
Enable RTCP on Common Phone Profiles 62
Enable RTCP on Device Configurations 62
Add a CTI Service 63
Apply CTI Service 63

Enable URI Dialing 64
Associate URIs to Directory Numbers 64
Automatically Populate Directory Numbers with URIs 64
Verify Directory URIs 65
Configure Directory Numbers with URIs 65
Associate the Directory URI Partition 66
Enable FQDN in SIP Requests for Contact Resolution 66
Configure User Associations 67
Specify Your TFTP Server Address 68
Specify Your TFTP Server on Cisco Unified Communications Manager IM and Presence Service 68
Specify TFTP Servers with the Cisco WebEx Administration Tool 69
Reset Devices 69
Create a CCMCIP Profile 70
Dial Plan Mapping 71
Publish Dial Rules 71

CHAPTER 8 Provision Audio and Video Capabilities in Hybrid Cloud-Based Deployments 73
Configure Audio and Video Services 73
Add Teleconferencing Service Name Accounts 73

PART IV Set Up Voicemail 75

CHAPTER 9 Set Up Voicemail on Cisco Unified Presence 77
Configure Cisco Unity Connection 77
Add a Voicemail Server 78
Create a Mailstore 79
Create a Voicemail Profile 80
Configure Retrieval and Redirection 81
Set a Voicemail Credentials Source 82

CHAPTER 10 Set Up Voicemail on Cisco Unified Communications Manager 85
Configure Cisco Unity Connection 85
Add a Voicemail Service 86
Apply Voicemail Service 87

Add a Mailstore Service 88
Apply Mailstore Service 89
Configure Retrieval and Redirection 90
Set a Voicemail Credentials Source 91

CHAPTER 11 Set Up Voicemail in Hybrid Cloud-Based Deployments 93
Configure Voicemail 93
Allow Users to Set Voicemail Server Settings 93

PART V Set Up Conferencing 95

CHAPTER 12 Set Up Conferencing on Cisco Unified Presence 97
Set Up On-Premises Conferencing 97
Cisco WebEx Meetings Server Installation and Configuration 97
Authenticate with Cisco WebEx Meetings Server 97
Specify Conferencing Credentials in the Client 98
Specify a Credentials Source on Cisco Unified Presence 98
Set Up Cisco WebEx Meetings Server on Cisco Unified Presence 99
Add Cisco WebEx Meetings Server 99
Add Cisco WebEx Meetings Server to a Profile 100
Set Up Cloud-Based Conferencing 101
Integration with Cisco WebEx Meeting Center 101
Authentication with Cisco WebEx Meeting Center 102
Provide Conferencing Credentials 102
Specify Conferencing Credentials in the Client 102
Specify a Credentials Source on Cisco Unified Presence 102
Set Up Cisco WebEx Meeting Center on Cisco Unified Presence 103
Add Cisco WebEx Meeting Center 104
Add Cisco WebEx Meeting Center to a Profile 105

CHAPTER 13 Set Up Conferencing on Cisco Unified Communications Manager 107
Set Up On-Premises Conferencing 107
Cisco WebEx Meetings Server Installation and Configuration 107
Authenticate with Cisco WebEx Meetings Server 107
Specify Conferencing Credentials in the Client 108

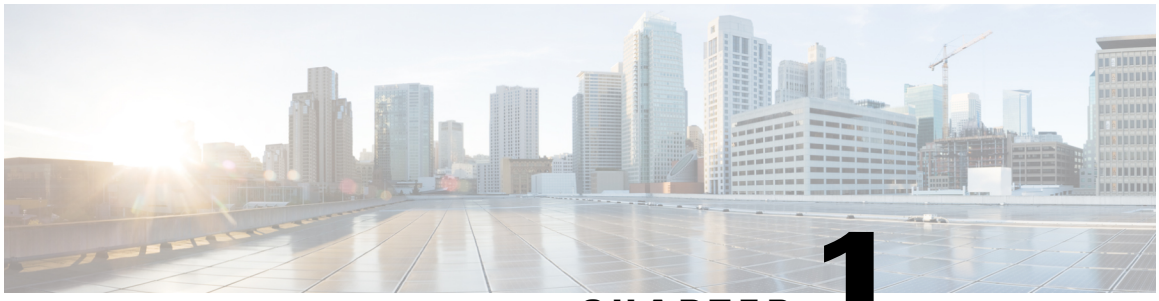
Add Cisco WebEx Meetings Server 108
Add Cisco WebEx Meetings Server to a Profile 109
Set Up Cloud-Based Conferencing 110
Integration with Cisco WebEx Meeting Center 110
Authentication with Cisco WebEx Meeting Center 111
Provide Conferencing Credentials 112
Specify Conferencing Credentials in the Client 112
Add Cisco WebEx Meeting Center 112
Add Cisco WebEx Meeting Center to a Profile 113

CHAPTER 14 Set Up Conferencing in Cloud-Based Deployments 115
Configure Cisco WebEx Meeting Center 115
Authentication with Cisco WebEx Meeting Center 115
Specify Conferencing Credentials in the Client 116

PART I

Configure Directory Integration

- Configure Directory Integration in On-Premises Deployments, page 3
- Configure Directory Integration in Cloud-Based Deployments, page 9



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 6

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

v10.0: LDAP system setup
v9.1: LDAP system setup
v8.6(1): LDAP System Configuration

Populate User ID and Directory URI

When you synchronize your LDAP directory server with Cisco Unified Communications Manager, you can populate the end user configuration tables in both the Cisco Unified Communications Manager and the Cisco Unified Communications Manager IM and Presence Service databases with attributes that contain values for the following:

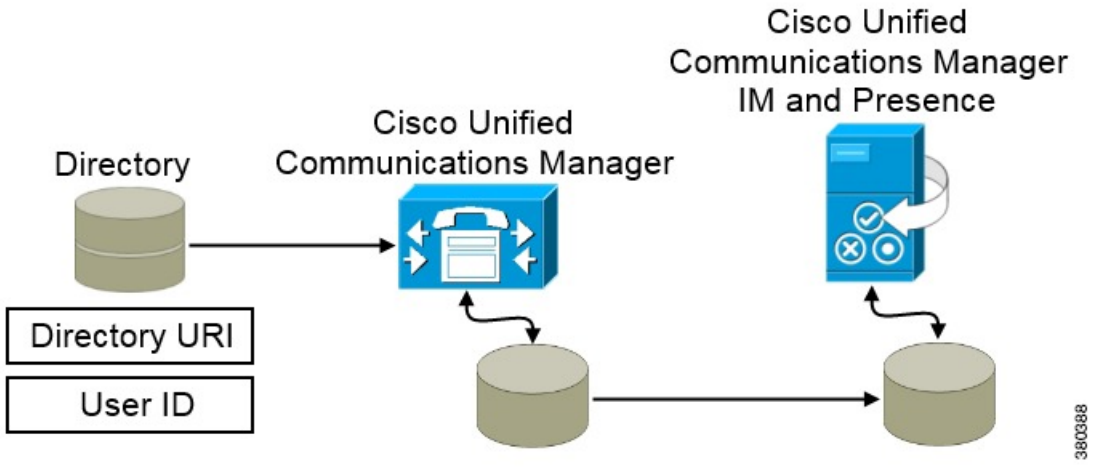
User ID

You must specify a value for the user ID on Cisco Unified Communications Manager. This value is required for the default IM address scheme and for users to log in. The default value is sAMAccountName.

Directory URI

You should specify a value for the directory URI if you plan to:

- Enable URI dialing in Cisco Jabber.
- Use the directory URI address scheme on Cisco Unified Communications Manager IM and Presence Service version 10 and higher.



When Cisco Unified Communications Manager synchronizes with the directory source, it retrieves the values for the directory URI and user ID and populates them in the end user configuration table in the Cisco Unified Communications Manager database.

The Cisco Unified Communications Manager database then synchronizes with the Cisco Unified Communications Manager IM and Presence Service database. As a result, the values for the directory URI and user ID are populated in the end user configuration table in the Cisco Unified Communications Manager IM and Presence Service database.

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.

Specify an LDAP Attribute for the Directory URI

On Cisco Unified Communications Manager version 9.0(1) and higher, you can populate the directory URI from an attribute in the directory. The default attribute is `msRTCSIP-primaryuseraddress`.

Procedure

Step 1 Select **System** > **LDAP** > **LDAP Directory**.

Remember To add or edit an LDAP directory, you must first enable synchronization.

Step 2 Select the appropriate LDAP directory or select **Add New** to add an LDAP directory.

Step 3 Locate the **Standard User Fields To Be Synchronized** section.

Step 4 Select the appropriate LDAP attribute for the **Directory URI** drop-down list.

Step 5 Select **Save**.

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 Service: **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 **Peform 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

v10.0: LDAP directory setup
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**.

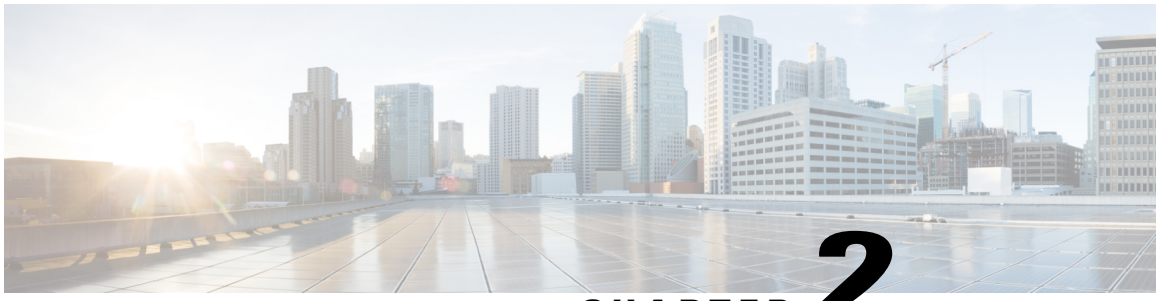
Step 3 Select **Use LDAP Authentication for End Users**.

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

v10.0: LDAP authentication setup
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 9

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.

To add directory groups in the client interface, users select **File** > **New** > **Directory Group** and then search for directory groups.

Note Users cannot edit directory groups to add or remove contacts. However, users can drag and drop contacts from a directory group into their own custom contact groups.

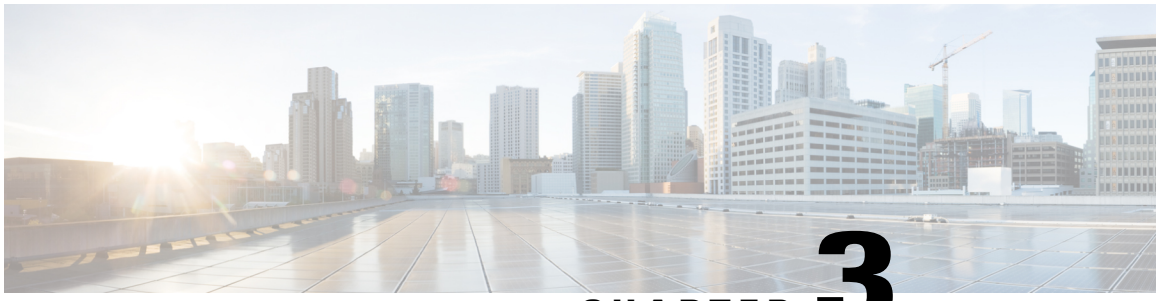
Related Topics

Directory Integration

PART II

Provision Instant Messaging and Presence

- Provision Instant Messaging and Presence on Cisco Unified Presence, page 13
- Provision Instant Messaging and Presence on Cisco Unified Communications Manager IM and Presence, page 19
- Provision Instant Messaging and Presence in Cloud-Based Deployments, page 27



CHAPTER 3

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 13
- Pre-Populate Contact Lists in Bulk, page 14
- Enable Messaging Settings, page 14
- Specify Capabilities Assignments, page 15
- Configure Prompts for Presence Subscription Requests, page 15

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 appropriate for the version of Cisco Unified Presence that you use.

- On Cisco Unified Presence version 8.5 and higher, do the following:
  1. Select **Messaging** > **Settings**.
  2. Select the following settings:
     - **Enable instant messaging**
     - **Allow clients to log instant message history**

- On Cisco Unified Presence version 8.0.3 or 8.0.4, do the following:

1. Select **Presence** > **Settings**.
2. Select **Enable CUPC 7 and IPPM Instant Messaging (cluster-wide)**.

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:

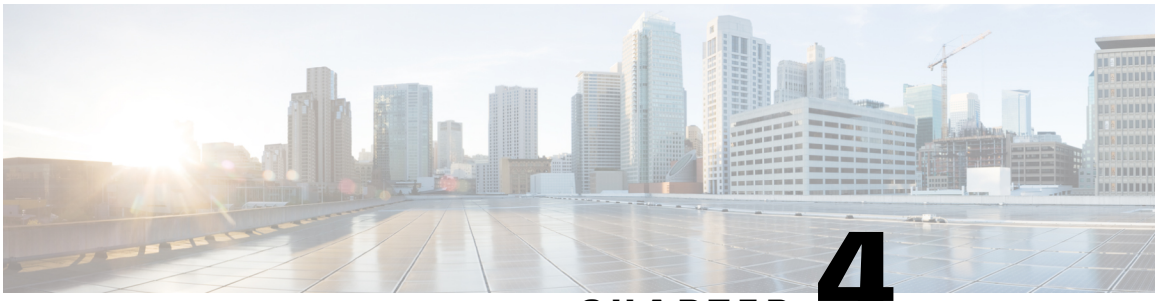
Selected

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 Service version 9.0(1) and higher.

- Activate and Start Essential Services, page 19
- Create a Service Profile, page 20
- Pre-Populate Contact Lists in Bulk, page 21
- Enable Messaging Settings, page 21
- Enable File Transfers and Screen Captures, page 22
- Configure Prompts for Presence Subscription Requests, page 22
- Add an Instant Messaging and Presence Service, page 24
- Configure Users, page 25

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 Serviceability** 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

Enable File Transfers and Screen Captures

You can enable or disable file transfers and screen captures through the Cisco XCP Router service on Cisco Unified Communications Manager IM and Presence Service. File transfers and screen captures setting are enabled by default. However, you should verify the setting when you set up your deployment.

Procedure

Step 1 Open the **Cisco Unified CM IM and Presence Administration** interface.

Step 2 Select **System** > **Service Parameters**.

Step 3 Select the appropriate server from the **Server** drop-down list.

Step 4 Select **Cisco XCP Router** from the **Service** drop-down list.
The **Service Parameter Configuration** window opens.

Step 5 Locate the **Enable file transfer** parameter.

Step 6 Select the appropriate value from the **Parameter Value** drop-down list..

Step 7 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 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.

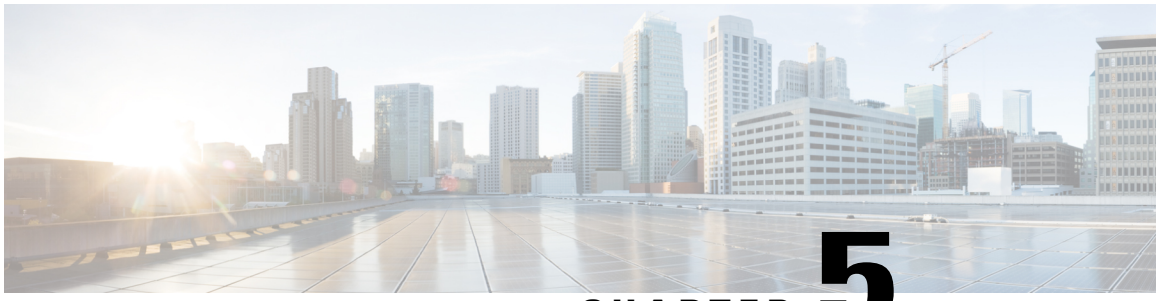
Step 6 Select the **UC Service Profile** check box and then select your service profile from the drop-down list.

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 27
- Configure Privacy Options, page 27

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: • **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

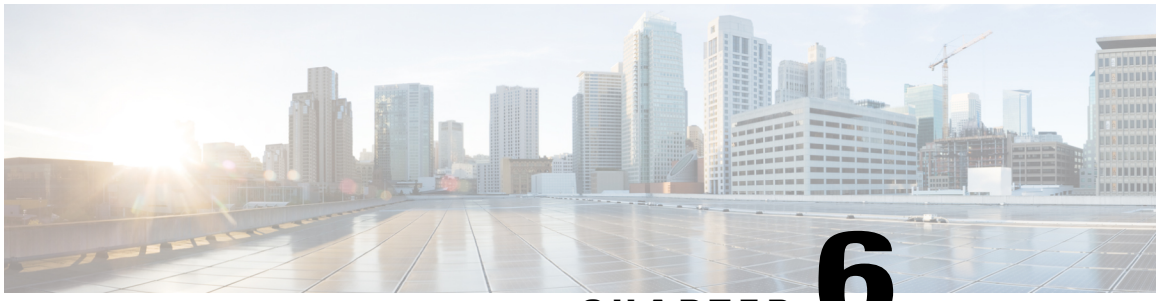
The client prompts users to accept each presence subscription request.

Step 5 Select **Save**.

PART III

Provision Audio and Video Capabilities

- Provision Audio and Video Capabilities on Cisco Unified Communications Manager Version 8.x, page 31
- Provision Audio and Video Capabilities on Cisco Unified Communications Manager Version 9.x and Higher, page 51
- Provision Audio and Video Capabilities in Hybrid Cloud-Based Deployments, page 73



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 on their computers. Create desk phone devices that users can control with Cisco Jabber. Learn how to enable different audio and video features. Understand which server profiles you should create and which user associations you must assign.

Note The client does not support audio and video calling on Cisco Unified Communications Manager Version 8.x when users connect to the corporate network using Expressway for Mobile and Remote Access.

- Create Software Phone Devices, page 31
- Create Desk Phone Devices, page 41
- Configure User Associations, page 45
- Reset Devices, page 46
- Specify Your TFTP Server Address, page 46
- Create a CCMCIP Profile, page 48
- Dial Plan Mapping, page 49

Create Software Phone Devices

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

Create CSF Devices on 8.6(1)

The steps in this section describe how to create CSF devices on Cisco Unified Communications Managerversion 8.6(1). CSF devices provide users with software phone capabilities.

Create SIP Profiles

The first step in creating a software phone device is to create a SIP profile. You cannot edit or configure the default SIP profile. For this reason, you must create a new SIP profile.

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.

Create CSF Devices

Complete the steps in this task to create CSF devices.

Procedure

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

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

Step 3 Select **Add New**.

Step 4 Select **Cisco Unified Client Services Framework** from the **Phone Type** drop-down list and then select **Next**.
The **Phone Configuration** window opens.

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

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

See the *Set Up Secure Phone Capabilities* for instructions on configuring secure CSF devices.

Step 7 Select **Save**.
A message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.

What to Do Next

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

Create CSF Devices on 8.6(2) and Higher

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

Create CSF Devices

Complete the steps in this task to create CSF devices.

Procedure

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

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

Step 3 Select **Add New**.

Step 4 Select **Cisco Unified Client Services Framework** from the **Phone Type** drop-down list and then select **Next**.
The **Phone Configuration** window opens.

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

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

See the *Set Up Secure Phone Capabilities* for instructions on configuring secure CSF devices.

Step 7 Select **Save**.
A message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.

What to Do Next

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

Set Up Secure Phone Capabilities

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

Configure the Security Mode

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

Mixed mode security:

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

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

Related Topics

Cisco Unified Communications Manager Security Guide, Release 8.6(1)
Cisco Unified Communications Manager Security Guide, Release 9.1(1)
Cisco Unified Communications Manager Security Guide, Release 10.0(1)

Create a Phone Security Profile

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

Before You Begin

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

Procedure

Step 1 Select **System** > **Security** > **Phone Security Profile**.

Step 2 Select **Add New**.

Step 3 Select **Cisco Unified Client Services Framework** from the **Phone Security Profile Type** drop-down list and then select **Next**.
The **Phone Security Profile Configuration** window opens.

Configure the Phone Security Profile

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

Procedure

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

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

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

Device Security Mode

Select one of the following:

- **Authenticated**
- **Encrypted**

Transport Type

Leave the default value of **TLS**.

TFTP Encrypted Config

Select this checkbox to encrypt the CSF device configuration file that resides on the TFTP server.

Authentication Mode

Select **By Authentication String**.

Key Size (Bits)

Select the appropriate key size for the certificate.

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

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

SIP Phone Port

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

Step 3 Select **Save**.

Configure CSF Devices

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

Procedure

Step 1 Open the CSF device configuration window.

a) Select **Device** > **Phone**.
The **Find and List Phones** window opens.

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

c) Select the CSF device from the list.
The **Phone Configuration** window opens.

Step 2 Select **Allow Control of Device from CTI** in the **Device Information** section.

Step 3 Select **Save**.

Step 4 Locate the **Protocol Specific Information** section.

Step 5 Select the phone security profile from the **Device Security Profile** drop-down list.

Step 6 Select **Save**.

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

What to Do Next

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

Specify Certificate Settings

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

Procedure

Step 1 Locate the **Certification Authority Proxy Function (CAPF) Information** section on the **Phone Configuration** window.

Step 2 Specify values as follows:

Certificate Operation

Select **Install/Upgrade**.

Authentication Mode

Select **By Authentication String**.

Key Size (Bits)

Select the same key size that you set in the phone security profile.

Operation Completes By

Specify an expiration value for the authentication string or leave as default.

Step 3 Select **Save**.

Step 4 Create the authentication string.
You can do one of the following:

- Select **Generate String** in the **Certification Authority Proxy Function (CAPF) Information** section.
- Enter a custom string in the **Authentication String** field.

What to Do Next

Provide users with the authentication string.

Provide Users with Authentication Strings

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

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

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

The client displays an error if:

- Users enter an incorrect authentication string.

  Users can attempt to enter authentication strings again to complete the CAPF enrollment. However, if a user continually enters an incorrect authentication string, the client might reject any string the user enters, even if the string is correct. In this case, you must generate a new authentication string on the user's CSF device and then provide it to the user.

- Users do not enter the authentication string before the expiration time you set in the **Operation Completes By** field.

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

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

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

Users must not belong to the following user group:

Standard CTI Secure Connection

Secure Phone Details

Secure Connections

If you enable secure phone capabilities, then:

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

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

Encrypted Media

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

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

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

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

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

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

Using Expressway for Mobile and Remote Access

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

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

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

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

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

Stored Files

The client stores the following information for secure phone capabilities:

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

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

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

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

Conference Calls

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

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

Sharing Secure CSF Devices between Clients

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

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

Multiple Users on a Shared Mac OS Account

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

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

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

Multiple Users on a Shared Computer

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

Add a Directory Number to the Device

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

Procedure

Step 1 Locate the **Association Information** section on the **Phone Configuration** window.

Step 2 Select **Add a new DN**.
The **Directory Number Configuration** window opens.

Step 3 Specify a directory number in the **Directory Number** field.

Step 4 Specify all other required configuration settings as appropriate.

Step 5 Associate end users with the directory number as follows:

a) Locate the **Users Associated with Line** section.

b) Select **Associate End Users**.
The **Find and List Users** dialog box opens.

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

d) Select the appropriate users from the list.

e) Select **Add Selected**.
The selected users are added to the voicemail profile.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.
The **Apply Configuration** window opens.

Step 8 Follow the prompts on the **Apply Configuration** window to apply the configuration.

Create Desk Phone Devices

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

Procedure

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

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

Step 3 Select **Add New**.

Step 4 Select the appropriate device from the **Phone Type** drop-down list and then select **Next**.
The **Phone Configuration** window opens.

Step 5 Complete the following steps in the **Device Information** section:

a) Enter a meaningful description in the **Description** field.
The client displays device descriptions to users. If users have multiple devices of the same model, the descriptions help users tell the difference between multiple devices.

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

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

Step 7 Select **Save**.
An message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.

What to Do Next

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

Add a Directory Number to the Device

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

Procedure

Step 1 Locate the **Association Information** section on the **Phone Configuration** window.

Step 2 Select **Add a new DN**.
The **Directory Number Configuration** window opens.

Step 3 Specify a directory number in the **Directory Number** field.

Step 4 Specify all other required configuration settings as appropriate.

Step 5 Associate end users with the directory number as follows:

a) Locate the **Users Associated with Line** section.
b) Select **Associate End Users**.
The **Find and List Users** dialog box opens.
c) Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
d) Select the appropriate users from the list.
e) Select **Add Selected**.
The selected users are added to the voicemail profile.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.
The **Apply Configuration** window opens.

Step 8 Follow the prompts on the **Apply Configuration** window to apply the configuration.

Enable Video Rate Adaptation

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

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

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

Enable RTCP on Common Phone Profiles

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

Procedure

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

Step 2 Select **Device** > **Device Settings** > **Common Phone Profile**.
The **Find and List Common Phone Profiles** window opens.

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

Step 4 Select the appropriate profile from the list.
The **Common Phone Profile Configuration** window opens.

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

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

Step 7 Select **Save**.

Enable RTCP on Device Configurations

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

Procedure

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

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

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

Step 4 Select the appropriate phone from the list.

The **Phone Configuration** window opens.

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

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

Step 7 Select **Save**.

Set Up a CTI Gateway

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

Add a CTI Gateway Server

The first step in setting up a CTI gateway is to add a CTI gateway server on Cisco Unified Presence.

Procedure

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

Step 2 Select **Application** > **Cisco Jabber** > **CTI Gateway Server**.

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

The **Find and List CTI Gateway Servers** window opens.

Step 3 Select **Add New**.

The **CTI Gateway Server Configuration** window opens.

Step 4 Specify the required details on the **CTI Gateway Server Configuration** window.

Step 5 Select **Save**.

Create a CTI Gateway Profile

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

Procedure

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

Step 2 Select **Application** > **Cisco Jabber** > **CTI Gateway Profile**.

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

The **CTI Gateway Profile Configuration** window opens.

Step 3 Specify the required details on the **CTI Gateway Profile Configuration** window.

Step 4 Select **Add Users to Profile** and add the appropriate users to the profile.

Step 5 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 User Group**.
The **Find and List User Groups** dialog box opens.

Step 13 Select the groups to which you want to assign the user.
At a minimum you should assign the user to the following groups:

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

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

Certain phone models require additional 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 the groups to which you want to assign the user.

Step 15 Select **Add Selected**.
The **Find and List User Groups** window closes.

Step 16 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.

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

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

Specify Your TFTP Server on Cisco Unified 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**.

Dial Plan Mapping

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

Application Dial Rules

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

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

Directory Lookup Dial Rules

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

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

Publish Dial Rules

Cisco Unified Communications Manager version 8.5 or lower does not automatically publish dial rules to the client. For this reason, you must deploy a COP file to publish your dial rules. This COP file copies your dial rules from the Cisco Unified Communications Manager database to an XML file on your TFTP server. The client can then download that XML file and access your dial rules.

Remember You must deploy the COP file every time you update or modify dial rules on Cisco Unified Communications Manager version 8.5 or lower.

Before You Begin

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

Procedure

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

Step 2 Select **Software Upgrades** > **Install/Upgrade**.

Step 3 Specify the location of `cmterm-csf-dialrule-wizard-0.1.cop.sgn` in the **Software Installation/Upgrade** window.

Step 4 Select **Next**.

Step 5 Select `cmterm-csf-dialrule-wizard-0.1.cop.sgn` from the **Available Software** list.

Step 6 Select **Next** and then select **Install**.

Step 7 Restart the TFTP service.

Step 8 Open the dial rules XML files in a browser to verify that they are available on your TFTP server.

a) Navigate to `http://`*`tftp_server_address`*`:6970/CUPC/AppDialRules.xml`.

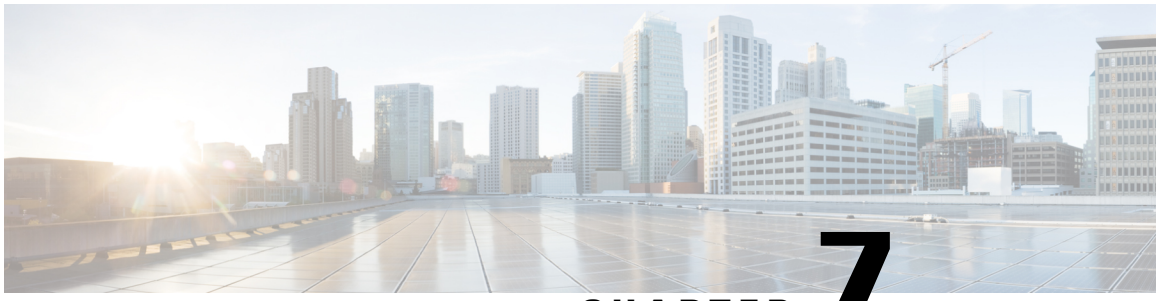
b) Navigate to `http://`*`tftp_server_address`*`:6970/CUPC/DirLookupDialRules.xml`.

If you can access `AppDialRules.xml` and `DirLookupDialRules.xml` with your browser, the client can download your dial rules.

Step 9 Repeat the preceding steps for each Cisco Unified Communications Manager instance that runs a TFTP service.

What to Do Next

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



CHAPTER 7

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 on their computers. Create desk phone devices that users can control with Cisco Jabber. Learn how to enable different audio and video features. Understand which server profiles you should create and which user associations you must assign.

- Create Software Phone Devices, page 51
- Create Desk Phone Devices, page 60
- Enable URI Dialing, page 64
- Configure User Associations, page 67
- Specify Your TFTP Server Address, page 68
- Reset Devices, page 69
- Create a CCMCIP Profile, page 70
- Dial Plan Mapping, page 71

Create Software Phone Devices

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

Create CSF Devices

Complete the steps in this task to create CSF devices.

Procedure

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

Step 2 Select **Device** > **Phone**.

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

Step 3 Select **Add New**.

Step 4 Select **Cisco Unified Client Services Framework** from the **Phone Type** drop-down list and then select **Next**. The **Phone Configuration** window opens.

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

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

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

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

Step 7 Specify configuration settings on the **Phone Configuration** window as appropriate.
See the *Phone Setup* topic in the Cisco Unified Communications Manager documentation for more information about the configuration settings on the **Phone Configuration** window.

See the *Set Up Secure Phone Capabilities* for instructions on configuring secure CSF devices.

Step 8 Select **Save**.
A message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.

What to Do Next

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

Set Up Secure Phone Capabilities

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

Configure the Security Mode

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

Mixed mode security:

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

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

Related Topics

Cisco Unified Communications Manager Security Guide, Release 8.6(1)
Cisco Unified Communications Manager Security Guide, Release 9.1(1)
Cisco Unified Communications Manager Security Guide, Release 10.0(1)

Create a Phone Security Profile

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

Before You Begin

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

Procedure

Step 1 Select **System** > **Security** > **Phone Security Profile**.

Step 2 Select **Add New**.

Step 3 Select **Cisco Unified Client Services Framework** from the **Phone Security Profile Type** drop-down list and then select **Next**.
The **Phone Security Profile Configuration** window opens.

Configure the Phone Security Profile

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

Procedure

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

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

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

Device Security Mode

Select one of the following:

- **Authenticated**
- **Encrypted**

Transport Type

Leave the default value of **TLS**.

TFTP Encrypted Config

Select this checkbox to encrypt the CSF device configuration file that resides on the TFTP server.

Authentication Mode

Select **By Authentication String**.

Key Size (Bits)

Select the appropriate key size for the certificate.

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

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

SIP Phone Port

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

Step 3 Select **Save**.

Configure CSF Devices

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

Procedure

Step 1 Open the CSF device configuration window.

a) Select **Device** > **Phone**.
The **Find and List Phones** window opens.

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

c) Select the CSF device from the list.

The **Phone Configuration** window opens.

Step 2 Select **Allow Control of Device from CTI** in the **Device Information** section.

Step 3 Select **Save**.

Step 4 Locate the **Protocol Specific Information** section.

Step 5 Select the phone security profile from the **Device Security Profile** drop-down list.

Step 6 Select **Save**.

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

What to Do Next

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

Specify Certificate Settings

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

Procedure

Step 1 Locate the **Certification Authority Proxy Function (CAPF) Information** section on the **Phone Configuration** window.

Step 2 Specify values as follows:

Certificate Operation

Select **Install/Upgrade**.

Authentication Mode

Select **By Authentication String**.

Key Size (Bits)

Select the same key size that you set in the phone security profile.

Operation Completes By

Specify an expiration value for the authentication string or leave as default.

Step 3 Select **Save**.

Step 4 Create the authentication string.
You can do one of the following:

- Select **Generate String** in the **Certification Authority Proxy Function (CAPF) Information** section.
- Enter a custom string in the **Authentication String** field.

What to Do Next

Provide users with the authentication string.

Provide Users with Authentication Strings

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

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

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

The client displays an error if:

- Users enter an incorrect authentication string.

  Users can attempt to enter authentication strings again to complete the CAPF enrollment. However, if a user continually enters an incorrect authentication string, the client might reject any string the user enters, even if the string is correct. In this case, you must generate a new authentication string on the user's CSF device and then provide it to the user.

- Users do not enter the authentication string before the expiration time you set in the **Operation Completes By** field.

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

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

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

Users must not belong to the following user group:

Standard CTI Secure Connection

Secure Phone Details

Secure Connections

If you enable secure phone capabilities, then:

- SIP connections between CSF devices and Cisco Unified Communications Manager are over TLS.
  - If you select **Authenticated** as the value for the **Device Security Mode** field on the phone security profile, the SIP connection is over TLS using NULL-SHA encryption.

- If you select **Encrypted** as the value for the **Device Security Mode** field on the phone security profile, the SIP connection is over TLS using AES 128/SHA encryption.

- Mutual TLS ensures that only CSF devices with the correct certificates can register to Cisco Unified Communications Manager. Likewise, CSF devices can register only to Cisco Unified Communications Manager instances that provide the correct certificate.

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

Encrypted Media

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

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

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

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

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

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

Using Expressway for Mobile and Remote Access

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

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

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

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

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

Stored Files

The client stores the following information for secure phone capabilities:

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

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

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

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

Conference Calls

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

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

Sharing Secure CSF Devices between Clients

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

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

Multiple Users on a Shared Mac OS Account

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

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

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

Multiple Users on a Shared Computer

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

Add a Directory Number to the Device

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

Procedure

Step 1 Locate the **Association Information** section on the **Phone Configuration** window.

Step 2 Select **Add a new DN**.
The **Directory Number Configuration** window opens.

Step 3 Specify a directory number in the **Directory Number** field.

Step 4 Specify all other required configuration settings as appropriate.

Step 5 Associate end users with the directory number as follows:

a) Locate the **Users Associated with Line** section.

b) Select **Associate End Users**.

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

c) Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
d) Select the appropriate users from the list.
e) Select **Add Selected**.
The selected users are added to the voicemail profile.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.
The **Apply Configuration** window opens.

Step 8 Follow the prompts on the **Apply Configuration** window to apply the configuration.

Create Desk Phone Devices

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

Procedure

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

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

Step 3 Select **Add New**.

Step 4 Select the appropriate device from the **Phone Type** drop-down list and then select **Next**.
The **Phone Configuration** window opens.

Step 5 Complete the following steps in the **Device Information** section:

a) Enter a meaningful description in the **Description** field.
The client displays device descriptions to users. If users have multiple devices of the same model, the descriptions help users tell the difference between multiple devices.

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

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

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

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

Step 7 Specify all other configuration settings on the **Phone Configuration** window as appropriate.
See the Cisco Unified Communications Manager documentation for more information about the configuration settings on the **Phone Configuration** window.

Step 8 Select **Save**.

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

What to Do Next

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

Add a Directory Number to the Device

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

Procedure

Step 1 Locate the **Association Information** section on the **Phone Configuration** window.

Step 2 Select **Add a new DN**.
The **Directory Number Configuration** window opens.

Step 3 Specify a directory number in the **Directory Number** field.

Step 4 Specify all other required configuration settings as appropriate.

Step 5 Associate end users with the directory number as follows:

a) Locate the **Users Associated with Line** section.
b) Select **Associate End Users**.
The **Find and List Users** dialog box opens.
c) Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
d) Select the appropriate users from the list.
e) Select **Add Selected**.
The selected users are added to the voicemail profile.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.
The **Apply Configuration** window opens.

Step 8 Follow the prompts on the **Apply Configuration** window to apply the configuration.

Enable Video Rate Adaptation

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

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

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

Enable RTCP on Common Phone Profiles

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

Procedure

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

Step 2 Select **Device** > **Device Settings** > **Common Phone Profile**.
The **Find and List Common Phone Profiles** window opens.

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

Step 4 Select the appropriate profile from the list.
The **Common Phone Profile Configuration** window opens.

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

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

Step 7 Select **Save**.

Enable RTCP on Device Configurations

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

Procedure

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

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

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

Step 4 Select the appropriate phone from the list.
The **Phone Configuration** window opens.

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

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

Step 7 Select **Save**.

Add a CTI Service

The CTI service lets users control devices.

Procedure

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

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

Step 3 Select **Add New**.
The **UC Service Configuration** window opens.

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

Step 5 Select **Next**.

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

a) Specify a name for the service in the **Name** field.
The name you specify displays when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.

b) Specify an optional description in the **Description** field.

c) Specify the CTI service address in the **Host Name/IP Address** field.

d) Specify the port number for the CTI service in the **Port** field.

Step 7 Select **Save**.

What to Do Next

Add the CTI service to your service profile.

Apply CTI Service

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

Before You Begin

Create a service profile if none already exist or you require a separate service profile for CTI.

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 **CTI Profile** section, select up to three services from the following drop-down lists:

- **Primary**
- **Secondary**
- **Tertiary**

Step 5 Select **Save**.

Enable URI Dialing

You can enable URI dialing on Cisco Unified Communications Manager version 9.1(2) and higher.

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

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

Related Topics

Cisco Unified Communications Manager Maintain and Operate Guides

Associate URIs to Directory Numbers

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

Automatically Populate Directory Numbers with URIs

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

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

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

Procedure

Step 1 Add devices.

Step 2 Add directory numbers to the devices.

Step 3 Associate users with the devices.

Step 4 Specify primary extensions for users.

What to Do Next

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

Verify Directory URIs

After you specify primary extensions for users, you should complete the following steps to verify that the directory URIs are associated with the directory numbers.

Procedure

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

Step 2 Select **Call Routing** > **Directory Number**.
The **Find and List Directory Numbers** window opens.

Step 3 Find and select the appropriate directory number.
The **Directory Number Configuration** window opens.

Step 4 Locate the **Directory URIs** section.

The primary directory URI for the directory number should correspond to the end user with whom you associated the device.

The partition should be **Directory URI**. This partition is the default into which Cisco Unified Communications Manager places URIs.

Configure Directory Numbers with URIs

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

To configure directory numbers with URIs, do the following:

Procedure

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

Step 2 Select **Call Routing** > **Directory Number**.
The **Find and List Directory Numbers** window opens.

Step 3 Find and select the appropriate directory number.

The **Directory Number Configuration** window opens.

Step 4 Locate the **Directory URIs** section.

Step 5 Specify a valid SIP URI in the **URI** column.

Step 6 Select the appropriate partition from the **Partition** column.

Note You cannot manually add URIs to the system **Directory URI** partition. You should add the URI to the same route partition as the directory number.

Step 7 Add the partition to the appropriate calling search space so that users can place calls to the directory numbers.

Step 8 Select **Save**.

Associate the Directory URI Partition

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

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

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

Procedure

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

Step 2 Select **System** > **Enterprise Parameters**.
The **Enterprise Parameters Configuration** window opens.

Step 3 Locate the **End User Parameters** section.

Step 4 In the **Directory URI Alias Partition** row, select the appropriate partition from the drop-down list.

Step 5 Select **Save**.

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

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

Enable FQDN in SIP Requests for Contact Resolution

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

Procedure

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

Step 2 Select **Device** > **Device Settings** > **SIP Profile**.
The **Find and List SIP Profiles** window opens.

Step 3 Find and select the appropriate SIP profile.
Remember You cannot edit the default SIP profile. If required, you should create a copy of the default SIP profile that you can modify.

Step 4 Select **Use Fully Qualified Domain Name in SIP Requests** and then select **Save**.

What to Do Next

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

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 **Service Settings** section.

Step 6 Select the appropriate service profile for the user from the **UC Service Profile** drop-down list.

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 Access Control Group**.
The **Find and List Access Control Groups** dialog box opens.

Step 15 Select the access control groups to which you want to assign the user.

At a minimum you should assign the user to the following access control groups:

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

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

Certain phone models require additional control groups, as follows:

- Cisco Unified IP Phone 9900 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 16 Select **Add Selected**.
The **Find and List Access Control Groups** window closes.

Step 17 Select **Save** on the **End User Configuration** window.

Specify Your TFTP Server Address

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

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

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

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

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

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.

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

You do not need to create a CCMCIP profile if you deploy the `_cisco-uds` SRV record.

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**.

Dial Plan Mapping

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

Application Dial Rules

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

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

Directory Lookup Dial Rules

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

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

Publish Dial Rules

Cisco Unified Communications Manager version 8.5 or lower does not automatically publish dial rules to the client. For this reason, you must deploy a COP file to publish your dial rules. This COP file copies your dial rules from the Cisco Unified Communications Manager database to an XML file on your TFTP server. The client can then download that XML file and access your dial rules.

Remember You must deploy the COP file every time you update or modify dial rules on Cisco Unified Communications Manager version 8.5 or lower.

Before You Begin

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

Procedure

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

Step 2 Select **Software Upgrades** > **Install/Upgrade**.

Step 3 Specify the location of `cmterm-csf-dialrule-wizard-0.1.cop.sgn` in the **Software Installation/Upgrade** window.

Step 4 Select **Next**.

Step 5 Select `cmterm-csf-dialrule-wizard-0.1.cop.sgn` from the **Available Software** list.

Step 6 Select **Next** and then select **Install**.

Step 7 Restart the TFTP service.

Step 8 Open the dial rules XML files in a browser to verify that they are available on your TFTP server.

a) Navigate to `http://`*`tftp_server_address`*`:6970/CUPC/AppDialRules.xml`.

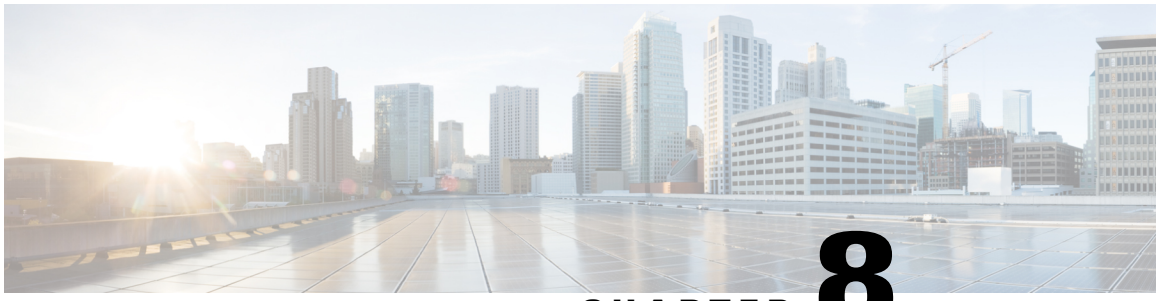
b) Navigate to `http://`*`tftp_server_address`*`:6970/CUPC/DirLookupDialRules.xml`.

If you can access `AppDialRules.xml` and `DirLookupDialRules.xml` with your browser, the client can download your dial rules.

Step 9 Repeat the preceding steps for each Cisco Unified Communications Manager instance that runs a TFTP service.

What to Do Next

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



CHAPTER 8

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 73
- Add Teleconferencing Service Name Accounts, page 73

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*.

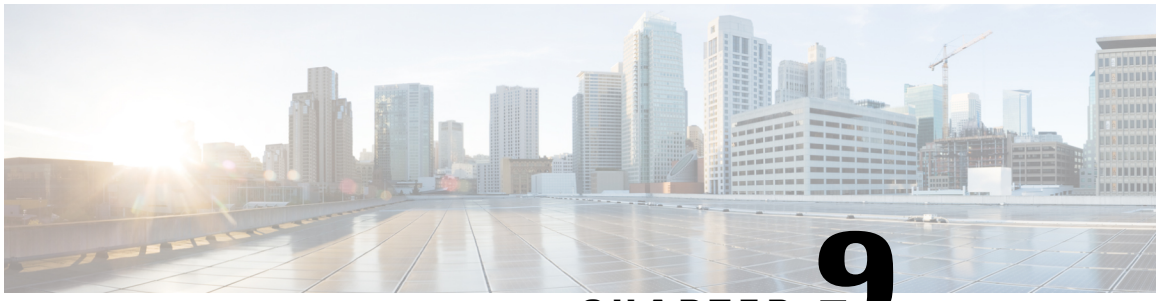
Related Topics

Cisco WebEx Site User's Administration Guide

PART IV

Set Up Voicemail

- Set Up Voicemail on Cisco Unified Presence, page 77
- Set Up Voicemail on Cisco Unified Communications Manager, page 85
- Set Up Voicemail in Hybrid Cloud-Based Deployments, page 93



CHAPTER 9

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 77
- Add a Voicemail Server, page 78
- Create a Mailstore, page 79
- Create a Voicemail Profile, page 80
- Configure Retrieval and Redirection, page 81
- Set a Voicemail Credentials Source, page 82

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.

a) Select **Users**.
b) Select the appropriate user.
c) Select **Edit** > **Password Settings**.
d) Select **Web Application** from the **Choose Password** menu.
e) Uncheck **User Must Change at Next Sign-In**.
f) Select **Save**.

Step 4 Provide users with access to the web inbox.

a) Select **Class of Service**.
The **Search Class of Service** window opens.
b) Select the appropriate class of service or add a new class of service.
c) Select **Allow Users to Use the Web Inbox and RSS Feeds**.
d) Select all other options as appropriate.
e) Select **Save**.

Step 5 Select API configuration settings.

a) Select **System Settings** > **Advanced** > **API Settings**.
The **API Configuration** window opens.
b) 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**

c) 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 Mailstore

Complete the steps in this task to create a mailstore on Cisco Unified Presence.

Procedure

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

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

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

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

Step 3 Select **Add New**.
The **Mailstore Configuration** window opens.

Step 4 Specify details on the **Mailstore Configuration** window as follows:

Name

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

Description

Enter an optional description.

Hostname/IP Address

Enter the address of the mailstore 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 mailstore 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 mailstore server. For this reason, any value you specify does not take effect.

Step 5 Select **Save**.

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.

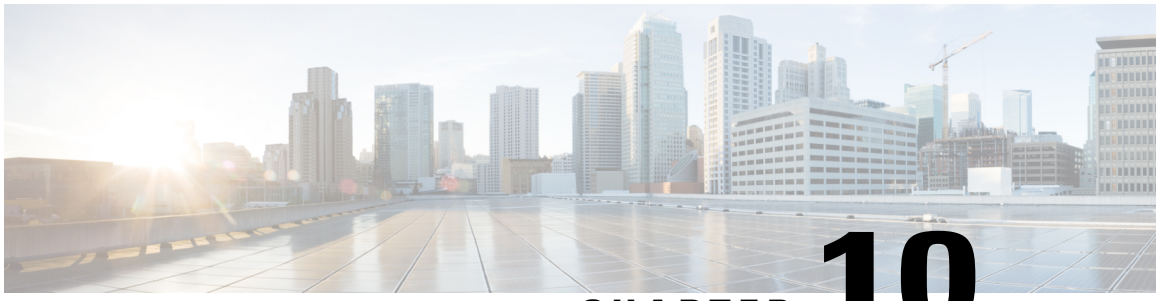
Note Do not select **Web Conferencing** from the **Credentials source for voicemail service** drop-down list. You cannot currently use conferencing credentials as a credentials source for voicemail services.

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 85
- Add a Voicemail Service, page 86
- Add a Mailstore Service, page 88
- Configure Retrieval and Redirection, page 90
- Set a Voicemail Credentials Source, page 91

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.

a) Select **Users**.
b) Select the appropriate user.
c) Select **Edit** > **Password Settings**.
d) Select **Web Application** from the **Choose Password** menu.
e) Uncheck **User Must Change at Next Sign-In**.
f) Select **Save**.

Step 4 Provide users with access to the web inbox.

a) Select **Class of Service**.
The **Search Class of Service** window opens.
b) Select the appropriate class of service or add a new class of service.
c) Select **Allow Users to Use the Web Inbox and RSS Feeds**.
d) Select all other options as appropriate.
e) Select **Save**.

Step 5 Select API configuration settings.

a) Select **System Settings** > **Advanced** > **API Settings**.
The **API Configuration** window opens.
b) 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**

c) 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:

a) Select up to three services from the following drop-down lists:

- **Primary**
- **Secondary**
- **Tertiary**

b) 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**.

Add a Mailstore Service

The mailstore service provides users with visual voicemail 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 **MailStore** from the **UC Service Type** drop-down list.

Step 5 Select **Next**.

Step 6 Provide details for the mailstore service as follows:

Name

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

Description

Enter an optional description.

Hostname/IP Address

Enter the address of the mailstore 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 mailstore 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 mailstore server. For this reason, any value you specify does not take effect.

Step 7 Select **Save**.

What to Do Next

Add the mailstore service to your service profile.

Apply Mailstore Service

After you add a mailstore 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 the mailstore service.

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 **MailStore Profile** section as follows:

a) Select up to three services from the following drop-down lists:

- **Primary**

- **Secondary**
- **Tertiary**

b) Specify appropriate values for the following fields:

- **Inbox Folder**
- **Trash Folder**
- **Polling Interval**

Step 5 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 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

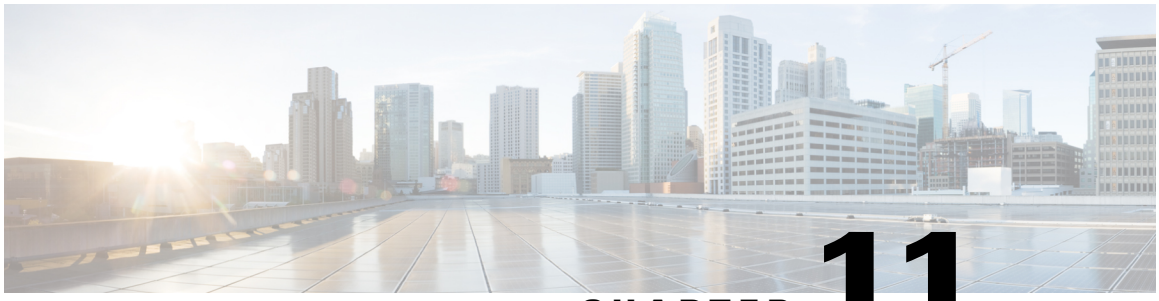
Step 1 Open the **Cisco Unified CM Administration** interface.
Step 2 Select **User Management** > **User Settings** > **Service Profile**.
Step 3 Select the appropriate service profile to open the **Service Profile Configuration** window.
Step 4 In the **Voicemail Profile** section, select **Unified 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 93
- Allow Users to Set Voicemail Server Settings, page 93

Configure Voicemail

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

Related Topics

Specifying Visual Voicemail settings

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.

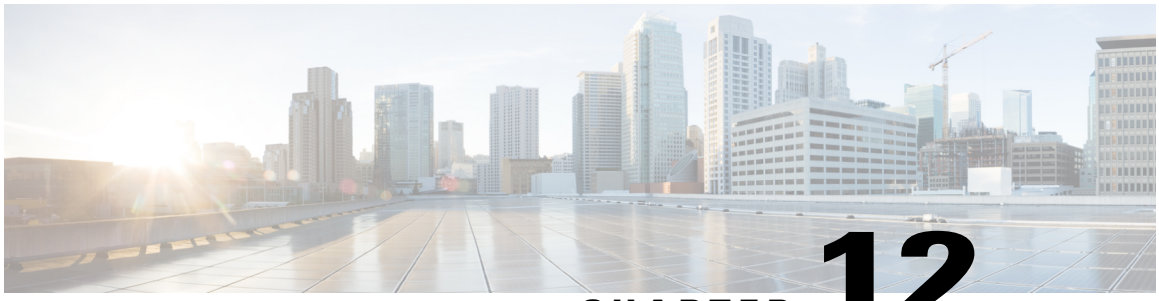
Step 4 Select **Allow user to enter manual settings**

The user can access advanced voicemail settings in the **Phone Accounts** tab on the **Options** window in the client interface.

PART V

Set Up Conferencing

- Set Up Conferencing on Cisco Unified Presence, page 97
- Set Up Conferencing on Cisco Unified Communications Manager, page 107
- Set Up Conferencing in Cloud-Based Deployments, page 115



CHAPTER 12

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 97
- Set Up Cloud-Based Conferencing, page 101

Set Up On-Premises Conferencing

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

Note The client does not support on-premises conferencing when users connect to the corporate network using Expressway for Mobile and Remote Access.

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.

Related Topics

Cisco WebEx Meetings Server Install and Upgrade Guides

Authenticate with Cisco WebEx Meetings Server

Cisco Jabber supports the following methods of authentication with Cisco WebEx Meetings Server:

Users manually enter credentials in the client

Each user can enter their credentials in the **Meetings** tab on the **Preferences** window to authenticate directly with Cisco WebEx Meetings Server.

You set a credentials source on Cisco Unified Presence

If the users' credentials for Cisco WebEx Meetings Server match their credentials for Cisco Unified Presence or Cisco Unity Connection, you can set a credentials source. The client then automatically authenticates to Cisco WebEx Meetings Server with the users' credential source.

You configure single sign-on (SSO) with Cisco WebEx Meetings Server

If you configure SSO with Cisco WebEx Meetings Server, Cisco Jabber can seamlessly integrate with the SSO environment. In this case, you do not need to specify credentials in order for users to authenticate with Cisco WebEx Meetings Server.

Specify Conferencing Credentials in the Client

Users can specify their credentials in the **Meetings** tab on the **Preferences** window.

Specify a Credentials Source on Cisco Unified Presence

Complete the steps in this task to specify a credentials source on Cisco Unified Presence.

Important There is no mechanism to synchronize credentials you specify in Cisco Unified Presence with credentials you specify in Cisco WebEx Meetings Server.

If you specify a credentials source in Cisco Unified Presence, you must ensure that those credentials match the user's Cisco WebEx Meetings Server credentials.

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

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 one of the following from the **Credentials source for web conferencing service** drop-down list:

Not set

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

CUP

The user's Cisco Unified Presence credentials match their Cisco WebEx Meetings Server credentials.

Voicemail

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

Step 4 Select **Save**.

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

Cisco Jabber supports the following types of authentication with Cisco WebEx Meeting Center:

Direct Authentication

The client can pass user credentials directly to Cisco WebEx Meeting Center.

To enable direct authentication, complete the following steps:

1. Create user accounts for Cisco WebEx Meeting Center using the Cisco WebEx Administration Tool.

   Cisco WebEx Meeting Center must validate user credentials in a direct authentication scenario. The user accounts hold the credentials so that Cisco WebEx Meeting Center can validate them when the client attempts to authenticate.

2. Provide Cisco WebEx Meeting Center user credentials to the client.

Authentication with an Identity Provider

The client can redirect authentication from Cisco WebEx Meeting Center to an identity provider.

To enable authentication with an identity provider, complete the following steps:

1. Set up your identity provider as appropriate.

   When users attempt to authenticate with Cisco WebEx Meeting Center, the client redirects that authentication to your identity provider. Your identity provider then validates the credentials and passes an authentication token back to the client. The client then passes that token to Cisco WebEx Meeting Center to complete the authentication process.

2. Provide Cisco WebEx Meeting Center user credentials to the client.

Related Topics

Overview of Loosely Coupled Integration
Using SSO with the Cisco WebEx and Cisco WebEx Meeting applications

Provide Conferencing Credentials

Choose one of the following methods to provide conferencing credentials to the client:

- Users individually specify their credentials in the **Meetings** tab on the **Preferences** window.
- You specify a credentials source for the conferencing service on Cisco Unified Presence.

Specify Conferencing Credentials in the Client

Users can specify their credentials in the **Meetings** tab on the **Preferences** window.

Specify a Credentials Source on Cisco Unified Presence

Complete the steps in this task to specify a credentials source on Cisco Unified Presence.

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

Important There is no mechanism to synchronize credentials you specify in Cisco Unified Presence with credentials you specify in Cisco WebEx Meeting Center.

If you specify a credentials source in Cisco Unified Presence, you must ensure that those credentials match the user's Cisco WebEx Meeting Center credentials.

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

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 one of the following from the **Credentials source for web conferencing service** drop-down list:

Not set

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

CUP

The user's Cisco Unified Presence credentials match their Cisco WebEx Meeting Center credentials.

Voicemail

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

Step 4 Select **Save**.

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 CenterCisco 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 107
- Set Up Cloud-Based Conferencing, page 110

Set Up On-Premises Conferencing

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

Note The client does not support on-premises conferencing when users connect to the corporate network using Expressway for Mobile and Remote Access.

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.

Related Topics

Cisco WebEx Meetings Server Install and Upgrade Guides

Authenticate with Cisco WebEx Meetings Server

Cisco Jabber supports the following methods of authentication with Cisco WebEx Meetings Server:

Users manually enter credentials in the client

Each user can enter their credentials in the **Meetings** tab on the **Preferences** window to authenticate directly with Cisco WebEx Meetings Server.

You set a credentials source on Cisco Unified Communications Manager

If the users' credentials for Cisco WebEx Meetings Server match their credentials for Cisco Unified Communications Manager IM and Presence Service or Cisco Unity Connection, you can set a credentials source. The client then automatically authenticates to Cisco WebEx Meetings Server with the users' credential source.

You configure single sign-on (SSO) with Cisco WebEx Meetings Server

If you configure SSO with Cisco WebEx Meetings Server, Cisco Jabber can seamlessly integrate with the SSO environment. In this case, you do not need to specify credentials in order for users to authenticate with Cisco WebEx Meetings Server.

Specify Conferencing Credentials in the Client

Users can specify their credentials in the **Meetings** tab on the **Preferences** window.

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 Service 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

Cisco Jabber supports the following types of authentication with Cisco WebEx Meeting Center:

Direct Authentication

The client can pass user credentials directly to Cisco WebEx Meeting Center.

To enable direct authentication, complete the following steps:

1. Create user accounts for Cisco WebEx Meeting Center using the Cisco WebEx Administration Tool.

   Cisco WebEx Meeting Center must validate user credentials in a direct authentication scenario. The user accounts hold the credentials so that Cisco WebEx Meeting Center can validate them when the client attempts to authenticate.

2. Provide Cisco WebEx Meeting Center user credentials to the client.

Authentication with an Identity Provider

The client can redirect authentication from Cisco WebEx Meeting Center to an identity provider.

To enable authentication with an identity provider, complete the following steps:

1. Set up your identity provider as appropriate.

   When users attempt to authenticate with Cisco WebEx Meeting Center, the client redirects that authentication to your identity provider. Your identity provider then validates the credentials and passes an authentication token back to the client. The client then passes that token to Cisco WebEx Meeting Center to complete the authentication process.

2. Provide Cisco WebEx Meeting Center user credentials to the client.

Related Topics

Overview of Loosely Coupled Integration
Using SSO with the Cisco WebEx and Cisco WebEx Meeting applications

Provide Conferencing Credentials

Choose one of the following methods to provide conferencing credentials to the client:

- Users individually specify their credentials in the **Meetings** tab on the **Preferences** window.
- You specify a credentials source on Cisco Unified Communications Manager when you apply the conferencing service to the service profile. See the topic in this section that describes how to add the conferencing server to the service profile for instructions.

Specify Conferencing Credentials in the Client

Users can specify their credentials in the **Meetings** tab on the **Preferences** window.

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 Service credentials match their Cisco WebEx Meeting Center credentials.

Voicemail

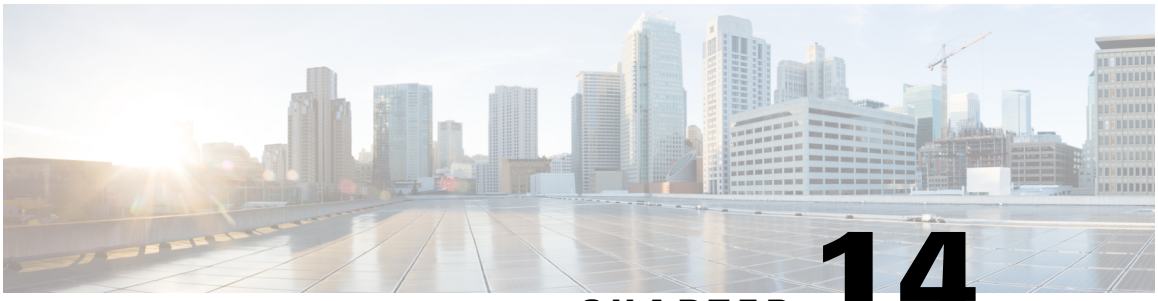
The user's Cisco Unity Connection credentials match their Cisco WebEx Meeting Center credentials.

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 115

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.

Users can add additional Cisco WebEx meeting sites in the Cisco Jabber client. However, users cannot add a meeting site that is configured for SSO, this site must be created in the Cisco WebEx Administration Tool.

Related Topics

Understanding Cisco WebEx Connect integration with the Cisco WebEx application

Authentication with Cisco WebEx Meeting Center

You can use the following types of authentication with Cisco WebEx Meeting Center:

Tightly Coupled Integration with the Cisco WebEx Messenger Service

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.

Direct Authentication

The client can pass user credentials directly to Cisco WebEx Meeting Center.

To enable direct authentication, complete the following steps:

1. Create user accounts for Cisco WebEx Meeting Center using the Cisco WebEx Administration Tool.

   Cisco WebEx Meeting Center must validate user credentials in a direct authentication scenario. The user accounts hold the credentials so that Cisco WebEx Meeting Center can validate them when the client attempts to authenticate.

2. Specify Cisco WebEx Meeting Center credentials in the client interface.

See the *Overview of Loosely Coupled Integration* topic for more information.

Authentication with an Identity Provider

The client can redirect authentication from Cisco WebEx Meeting Center to an identity provider.

To enable authentication with an identity provider, complete the following steps:

1. Set up your identity provider as appropriate.

   When users attempt to authenticate with Cisco WebEx Meeting Center, the client redirects that authentication to your identity provider. Your identity provider then validates the credentials and passes an authentication token back to the client. The client then passes that token to Cisco WebEx Meeting Center to complete the authentication process.

2. Specify Cisco WebEx Meeting Center credentials in the client interface.

See the *Using SSO with the Cisco WebEx and Cisco WebEx Meeting applications* topic for more information about managing user identities with the Cisco WebEx Messenger service.

Related Topics

Overview of Tightly Coupled Integration
Overview of Loosely 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 **Meetings** tab on the **Preferences** window.