Cisco Jabber for Windows 9.7 Server Setup Guide

First Published: March 26, 2014

Last Modified: December 10, 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)

CONTENTS

CHAPTER 1

Introduction

This guide provides instructions to help you set up and configure services for Cisco Jabber.

You should complete the relevant tasks in this guide to provision services before you install the client. In this way, you can ensure that base services are available before you launch the client for the first time.

For example, if you plan on installing Cisco Jabber in the default product mode, where instant messaging and presence capabilities provide base services, you should do the following:

1. Synchronize and authenticate with the directory source.
2. Provision instant messaging and presence services.
3. Install and test Cisco Jabber.
4. Provision additional services as required.

Important This guide consolidates information into task-based workflows for services and features that are specific to Cisco Jabber.

You should use this guide to set up a lab deployment for testing and evaluation purposes. Consult the primary server documentation, as appropriate, to review requirements and additional tasks you must complete before you deploy Cisco Jabber to a production environment.

PART I

Configure Directory Integration

CHAPTER 2

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

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:

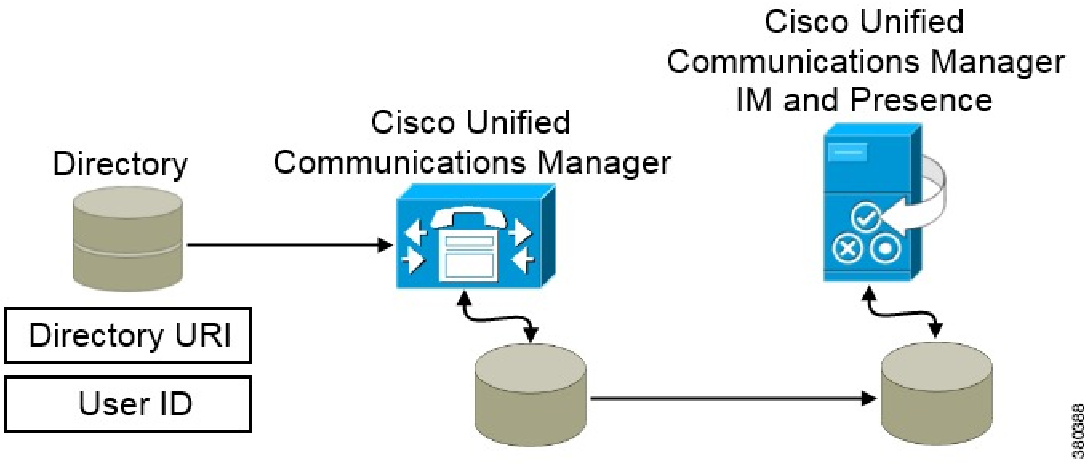
User ID

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 sign 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.


Cisco Unified Communications Manager IM and Presence
Cisco Unified Communications Manager
Directory
Directory URI
User ID
380388

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` and you are using the default IM address scheme in Cisco Unified Communications Manager IM and Presence Service, you must specify the attribute as the value for the parameter in your client configuration file as follows:

The EDI parameter is `UserAccountName`.

```
<UserAccountName>attribute-name</UserAccountName>
```

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 later, 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 **Perform Full Sync Now**.

Note The amount of time it takes for the synchronization process to complete depends on the number of users that exist in your directory. If you synchronize a large directory with thousands of users, you should expect the process to take some time.

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

Related Topics

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 sign 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 3

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

Procedure

Step 1 Review the directory integration topics, see *Directory Integration*.

Step 2 Configure your organization information, see *Understanding the Configuration Tab*.

Step 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.

Procedure

Step 1 Set up directory integration.

Step 2 Define your directory groups in a comma-separated values (`.csv`) file.

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

Related Topics

Directory Integration

PART II

Provision Instant Messaging and Presence

CHAPTER 4

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

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.

Cisco Jabber supports up to 300 contacts in a client contact list.

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**.

Important Cisco Jabber for Windows does not support the following settings on the **Presence Settings** window:

- **Use DND status when user is on the phone**
- **Use DND status when user is in a meeting**

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 when using Cisco Unified Presence.

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**.

Configure Presence for Microsoft SharePoint 2010 and 2013

If your organization defines users' profiles where their IM address is different from their email address, then some additional configuration is required to enable presence integration between the client and Microsoft SharePoint 2010 and 2013.

Before You Begin

All sites are in sync with Microsoft SharePoint Central Administration (CA).

Synchronization between Microsoft SharePoint and Active Directory has been set up.

Procedure

Step 1 Open a file with a text editor and insert the code below into it. Save the file with an .LDF extension.

```
dn: CN=ms-RTC-SIP-PrimaryUserAddress,CN=Schema,CN=Configuration,DC=X
changetype: add
adminDescription: msRTCSIP-PrimaryUserAddress
adminDisplayName: msRTCSIP-PrimaryUserAddress
description: Valid SIP URI.
objectclass: attributeSchema
attributeID: 1.2.840.113556.1.6.24.1.1
#schemaIDGUID:{45FC6F43-C8EB-40d4-91F3-763C46F6F250}
schemaIDGUID:: RfxvQ8jrQNSR83Y8RvbyUA==
oMSyntax: 64
attributeSyntax: 2.5.5.12
rangeLower: 0
rangeUpper: 454
isSingleValued: TRUE
searchFlags: 5
isMemberOfPartialAttributeSet: TRUE
ldapDisplayName: msRTCSIP-PrimaryUserAddress
#Base 64 Encoded GUID of :E2D6986B2C7F4CDA9851D5B5F3FB6706
attributeSecurityGUID:: a5jW4n8s2kyYUdW18/tnBg==

dn:
changetype: modify
```

```
replace: schemaupdatenow
schemaupdatenow: 1
-


##############################################################
# Add our attributes to contact object
##############################################################


dn: CN=User,CN=Schema,CN=Configuration,DC=X
# NT User Data
changetype: modify
add: mayContain
mayContain: msRTCSIP-PrimaryUserAddress
-

dn: CN=Contact,CN=Schema,CN=Configuration,DC=X
# NT Contact Data
changetype: modify
add: mayContain
mayContain: msRTCSIP-PrimaryUserAddress
-

dn:
changetype: modify
replace: schemaupdatenow
schemaupdatenow: 1
-
```

Step 2 Copy the .LDF file onto the Active Directory.

Step 3 Run the following command, ensuring you replace the variables with the appropriate values:

```
ldifde -i -v -k -s <servername> -f <ldf filename> -c DC=X <defaultNamingContext> -b <admin
 account> <login domain> <password>
```

Where the variables are described below:

Table 1: .LDF Command Variables

Variable	Description
<servername>	The name of the Active Directory: AD.
<ldf filename>	The name of the .LDF file that you saved in Step 1.
<defaultNamingContext>	The name of the database on the domain controller.
<admin account>	The username of the administrative account from which you are performing this configuration.
<login domain>	The login domain of the admin account.
<password>	The password for the admin account.

Example:

```
ldifde -i -v -k -s DC1 -f schema.ldf -c DC=X "DC=contoso,DC=com" -b administrator contoso
```

Step 4 Update the SharePoint central administration (CA) profile pages for the users, with the following information:

Table 2: SharePoint 2013 Fields and Values

Field	Value
SharePoint CA **SIP Address** profile field	Leave blank
SharePoint CA **Work email** profile field	For example, john4mail@example.pst

Table 3: SharePoint 2010 Fields and Values

Field	Value
SharePoint CA **SIP Address** profile field	For example, john4mail@example.pst
SharePoint CA **Work email** profile field	Leave blank

Step 5 Specify a value in the AD field **msRTCSIP-PrimaryUserAddress**. For example, sip:john@example.pst.

Disable Temporary Presence in Cisco Unified Presence

Disable temporary presence to increase privacy control. When you configure this parameter, Cisco Jabber displays availability status only to contacts in a user's contact list.

Procedure

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

Step 2 Select **Presence** > **Settings**.

Step 3 Uncheck **Enable ad-hoc presence subscriptions** and then select **Save**.
Cisco Jabber does not display temporary presence. Users can see availability status only for contacts in their contact list.

CHAPTER 5

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

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.

Import Bulk Contact Lists

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.

Cisco Jabber supports up to 300 contacts in a client contact list.

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 Message 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**.

Important Cisco Jabber does not support the following settings on the **Presence Settings** window on Cisco Unified Communications Manager IM and Presence Service version 9.0.x:

- **Use DND status when user is on the phone**
- **Use DND status when user is in a meeting**

Related Topics

Instant messaging settings configuration on IM and Presence

Enable File Transfers and Screen Captures

Note File transfers and screen captures are only supported on the desktop clients.

You can enable or disable file transfers and screen captures on *Cisco Unified Communication Manager IM and Presence Service 9.x and later*, through the Cisco XCP Router service on Cisco Unified Communications Manager IM and Presence Service. File transfers and screen captures parameter is 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**.

Disable Temporary Presence in Cisco Unified Communications Manager IM and Presence

Disable temporary presence to increase privacy control. When you configure this parameter, Cisco Jabber displays availability status only to contacts in a user's contact list.

Procedure

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

Step 2 Select **Presence** > **Settings**.

Step 3 Uncheck **Enable ad-hoc presence subscriptions** and then select **Save**.
Cisco Jabber does not display temporary presence. Users can see availability status only for contacts in their contact list.

Add an IM and Presence Service

Provide users with IM and Presence Service 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 IM 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.

Important The service address must be a fully qualified domain name or IP address.

Step 7 Select **Save**.

What to Do Next

Add the IM and Presence Service to your service profile.

Apply an IM and Presence Service

After you add an IM 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 Click **Save**.

Configure Presence for Microsoft SharePoint 2010 and 2013

If your organization defines users' profiles where their IM address is different from their email address, then some additional configuration is required to enable presence integration between the client and Microsoft SharePoint 2010 and 2013.

Before You Begin

All sites are in sync with Microsoft SharePoint Central Administration (CA).

Synchronization between Microsoft SharePoint and Active Directory has been set up.

Procedure

Step 1 Open a file with a text editor and insert the code below into it. Save the file with an .LDF extension.

```
dn: CN=ms-RTC-SIP-PrimaryUserAddress,CN=Schema,CN=Configuration,DC=X
changetype: add
adminDescription: msRTCSIP-PrimaryUserAddress
adminDisplayName: msRTCSIP-PrimaryUserAddress
description: Valid SIP URI.
objectclass: attributeSchema
attributeID: 1.2.840.113556.1.6.24.1.1
#schemaIDGUID:{45FC6F43-C8EB-40d4-91F3-763C46F6F250}
schemaIDGUID:: RfxvQ8jrQNSR83Y8RvbyUA==
oMSyntax: 64
attributeSyntax: 2.5.5.12
rangeLower: 0
rangeUpper: 454
isSingleValued: TRUE
searchFlags: 5
isMemberOfPartialAttributeSet: TRUE
ldapDisplayName: msRTCSIP-PrimaryUserAddress
#Base 64 Encoded GUID of :E2D6986B2C7F4CDA9851D5B5F3FB6706
attributeSecurityGUID:: a5jW4n8s2kyYUdW18/tnBg==

dn:
changetype: modify
replace: schemaupdatenow
schemaupdatenow: 1
-


##############################################################
# Add our attributes to contact object
##############################################################


dn: CN=User,CN=Schema,CN=Configuration,DC=X
# NT User Data
changetype: modify
add: mayContain
mayContain: msRTCSIP-PrimaryUserAddress
-

dn: CN=Contact,CN=Schema,CN=Configuration,DC=X
# NT Contact Data
changetype: modify
add: mayContain
mayContain: msRTCSIP-PrimaryUserAddress
-

dn:
changetype: modify
replace: schemaupdatenow
```

```
schemaupdatenow: 1
-
```

Step 2 Copy the .LDF file onto the Active Directory.

Step 3 Run the following command, ensuring you replace the variables with the appropriate values:

```
ldifde -i -v -k -s <servername> -f <ldf filename> -c DC=X <defaultNamingContext> -b <admin
 account> <login domain> <password>
```

Where the variables are described below:

Table 4: .LDF Command Variables

Variable	Description
<servername>	The name of the Active Directory: AD.
<ldf filename>	The name of the .LDF file that you saved in Step 1.
<defaultNamingContext>	The name of the database on the domain controller.
<admin account>	The username of the administrative account from which you are performing this configuration.
<login domain>	The login domain of the admin account.
<password>	The password for the admin account.

Example:

```
ldifde -i -v -k -s DC1 -f schema.ldf -c DC=X "DC=contoso,DC=com" -b administrator contoso
```

Step 4 Update the SharePoint central administration (CA) profile pages for the users, with the following information:

Table 5: SharePoint 2013 Fields and Values

Field	Value
SharePoint CA **SIP Address** profile field	Leave blank
SharePoint CA **Work email** profile field	For example, john4mail@example.pst

Table 6: SharePoint 2010 Fields and Values

Field	Value
SharePoint CA **SIP Address** profile field	For example, john4mail@example.pst
SharePoint CA **Work email** profile field	Leave blank

Step 5 Specify a value in the AD field **msRTCSIP-PrimaryUserAddress**. For example, sip:john@example.pst.

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**. 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**.

Configure Persistent Chat

Persistent Chat must be enabled and configured on Cisco Unified Communications Manager IM and Presence Service before it can be used by the client.

Before You Begin

Persistent Chat is only available on Cisco Unified Communications Manager IM and Presence Service 10.0 and later.

Persistent Chat is only available for Cisco Jabber for Windows.

Refer to *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* for your release for information on the database configuration necessary to support the Persistent Chat feature. It is available here: http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_installation_and_configuration_guides_list.html. Database configuration must be performed before continuing with this task.

Local chat message archiving must be enabled for Persistent Chat. Local chat message archiving is enabled on Cisco Unified Communications Manager IM and Presence Service using the **Allow clients to log instant message history** setting. Refer to Enable Message Settings, on page 25 for information on this setting.

Procedure

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

Step 2 Select **Messaging** > **Group Chat and Persistent Chat**.

Step 3 Select **Enable Persistent Chat**.

Step 4 Ensure the settings **How many users can be in a room at one time** and **How many hidden users can be in a room at one time** under the **Occupancy Settings** section contain the same, non-zero value.

Step 5 Configure the remaining settings as appropriate for your Persistent Chat deployment. Cisco recommends the Persistent Chat settings in following table.

Persistent Chat Setting	Recommended Value	Notes
System automatically manages primary group chat server aliases	Disabled	
Enable Persistent Chat	Enabled	
Archive all room joins and exits	Administrator Defined	This value is not currently used by Cisco Jabber for Persistent Chat.
Archive all room messages	Enabled	
Allow only group chat system administrators to create persistent chat rooms	Administrator Defined	Cisco recommends using the value Enabled unless Cisco Unified Personal Communicator is deployed in the enterprise environment.
Maximum number of persistent chat rooms allowed	Administrator Defined	
Number of connections to the database	Default Value	
Database connection heartbeat interval (seconds)	Default Value	
Timeout value for persistent chat rooms (minutes)	Default Value	
Maximum number of rooms allowed	Default Value	
Rooms are for members only by default	Disabled	
Room owners can change whether or not rooms are for members only	Enabled	Cisco Jabber requires this value to be Enabled.
Only moderators can invite people to members-only rooms	Enabled	Cisco Jabber requires this value to be Enabled.
Room owners can change whether or not only moderators can invite people to members-only rooms	Enabled	
Users can add themselves to rooms as members	Disabled	This value is not currently used by Cisco Jabber for Persistent Chat.
Room owners can change whether users can add themselves to rooms as members	Disabled	This value is not currently used by Cisco Jabber for Persistent Chat.
Members and administrators who are not in a room are still visible in the room	Enabled	Cisco Jabber requires this value to be Enabled.
Room owners can change whether members and administrators who are not in a room are still visible in the room	Enabled	
Rooms are backwards-compatible with older clients	Disabled	This value is not currently used by Cisco Jabber for Persistent Chat.

Persistent Chat Setting	Recommended Value	Notes
Room owners can change whether rooms are backwards-compatible with older clients	Disabled	This value is not currently used by Cisco Jabber for Persistent Chat.
Rooms are anonymous by default	Disabled	This value is not currently supported by Cisco Jabber for Persistent Chat. Cisco Jabber cannot join anonymous rooms.
Room owners can change whether or not rooms are anonymous	Disabled	This value is not currently supported by Cisco Jabber for Persistent Chat. Cisco Jabber cannot join anonymous rooms.
Lowest participation level a user can have to invite others to the room	Default Value	This value is not currently used by Cisco Jabber for Persistent Chat.
Room owners can change the lowest participation level a user can have to invite others to the room	Disabled	This value is not currently used by Cisco Jabber for Persistent Chat.
How many users can be in a room at one time	Administrator Defined	Cisco recommends using the default value.
How many hidden users can be in a room at one time	Administrator Defined	This value must be the same as the value used for the **How many users can be in a room at one time** setting.
Default maximum occupancy for a room	Default Value	
Room owners can change default maximum occupancy for a room	Default Value	
Lowest participation level a user can have to send a private message from within the room	Default Value	
Room owners can change the lowest participation level a user can have to send a private message from within the room	Default Value	
Lowest participation level a user can have to change a room's subject	Moderator	
Room owners can change the lowest participation level a user can have to change a room's subject	Disabled	
Remove all XHTML formatting from messages	Disabled	This value is not currently used by Cisco Jabber for Persistent Chat.
Room owners can change XHTML formatting setting	Disabled	This value is not currently used by Cisco Jabber for Persistent Chat.
Rooms are moderated by default	Disabled	This value is not currently used by Cisco Jabber for Persistent Chat.

Persistent Chat Setting	Recommended Value	Notes
Room owners can change whether rooms are moderated by default	Default Value	This value is not currently used by Cisco Jabber for Persistent Chat.
Maximum number of messages that can be retrieved from the archive	Default Value	
Number of messages in chat history displayed by default	Administrator Defined	Cisco recommends a value between 15 and 50. The **Number of messages in chat history displayed by default** setting does not apply retroactively to Persistent Chat rooms. Rooms created before the setting is changed will continue to use their originally configured value.
Room owners can change the number of messages displayed in chat history	Default Value	This value is not currently used by Cisco Jabber for Persistent Chat.

Note Persistent Chat rooms inherit their settings at the time of creation. Values changed after a room is created only apply to rooms created after the change has taken effect.

What to Do Next

Ensure you configure any client-specific parameters for Persistent Chat. For more information, see Client Parameters.

Enable file transfer in Chat rooms. For more information, see Enable File Transfer and Screen Captures for Group Chats and Chat Rooms

CHAPTER 6

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 IM and Presence Service

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

Related Topics

Cisco WebEx federation with other instant messaging providers

Specifying IM Federation settings

Configure Presence for Microsoft SharePoint 2010 and 2013

If your organization defines users' profiles where their IM address is different from their email address, then some additional configuration is required to enable presence integration between the client and Microsoft SharePoint 2010 and 2013.

Before You Begin

All sites are in sync with Microsoft SharePoint Central Administration (CA).

Synchronization between Microsoft SharePoint and Active Directory has been set up.

Procedure

Step 1 Open a file with a text editor and insert the code below into it. Save the file with an .LDF extension.

```
dn: CN=ms-RTC-SIP-PrimaryUserAddress,CN=Schema,CN=Configuration,DC=X
changetype: add
adminDescription: msRTCSIP-PrimaryUserAddress
adminDisplayName: msRTCSIP-PrimaryUserAddress
description: Valid SIP URI.
objectclass: attributeSchema
attributeID: 1.2.840.113556.1.6.24.1.1
#schemaIDGUID:{45FC6F43-C8EB-40d4-91F3-763C46F6F250}
schemaIDGUID:: RfxvQ8jrQNSR83Y8RvbyUA==
oMSyntax: 64
attributeSyntax: 2.5.5.12
rangeLower: 0
rangeUpper: 454
isSingleValued: TRUE
searchFlags: 5
isMemberOfPartialAttributeSet: TRUE
ldapDisplayName: msRTCSIP-PrimaryUserAddress
#Base 64 Encoded GUID of :E2D6986B2C7F4CDA9851D5B5F3FB6706
attributeSecurityGUID:: a5jW4n8s2kyYUdW18/tnBg==

dn:
changetype: modify
replace: schemaupdatenow
schemaupdatenow: 1
-


##############################################################
# Add our attributes to contact object
##############################################################


dn: CN=User,CN=Schema,CN=Configuration,DC=X
# NT User Data
changetype: modify
add: mayContain
mayContain: msRTCSIP-PrimaryUserAddress
-

dn: CN=Contact,CN=Schema,CN=Configuration,DC=X
# NT Contact Data
changetype: modify
add: mayContain
mayContain: msRTCSIP-PrimaryUserAddress
-

dn:
changetype: modify
replace: schemaupdatenow
```

```
schemaupdatenow: 1
-
```

Step 2 Copy the .LDF file onto the Active Directory.

Step 3 Run the following command, ensuring you replace the variables with the appropriate values:

```
ldifde -i -v -k -s <servername> -f <ldf filename> -c DC=X <defaultNamingContext> -b <admin
 account> <login domain> <password>
```

Where the variables are described below:

Table 7: .LDF Command Variables

Variable	Description
<servername>	The name of the Active Directory: AD.
<ldf filename>	The name of the .LDF file that you saved in Step 1.
<defaultNamingContext>	The name of the database on the domain controller.
<admin account>	The username of the administrative account from which you are performing this configuration.
<login domain>	The login domain of the admin account.
<password>	The password for the admin account.

Example:

```
ldifde -i -v -k -s DC1 -f schema.ldf -c DC=X "DC=contoso,DC=com" -b administrator contoso
```

Step 4 Update the SharePoint central administration (CA) profile pages for the users, with the following information:

Table 8: SharePoint 2013 Fields and Values

Field	Value
SharePoint CA **SIP Address** profile field	Leave blank
SharePoint CA **Work email** profile field	For example, john4mail@example.pst

Table 9: SharePoint 2010 Fields and Values

Field	Value
SharePoint CA **SIP Address** profile field	For example, john4mail@example.pst
SharePoint CA **Work email** profile field	Leave blank

Step 5 Specify a value in the AD field **msRTCSIP-PrimaryUserAddress**. For example, sip:john@example.pst.

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

CHAPTER 7

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

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.

As part of the task of creating CSF devices, you can enable video desktop sharing using Binary Floor Control Protocol (BFCP). Cisco Unified Communications Manager handles the BFCP packets that users transmit when using video desktop sharing capabilities. For this reason, you configure Cisco Unified Communications Manager to allow BFCP presentation sharing. On Cisco Unified Communications Manager version 8.6(1), you enable BFCP presentation sharing on a SIP profile. You must then apply that SIP profile to the CSF devices.

Note

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

Create SIP Profiles

The first step in creating a software phone device is to create a SIP profile so that you can enable video desktop sharing. 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.

Enable Video Desktop Sharing on SIP Profiles

You should enable BFCP on the SIP profile before you apply the SIP profile to CSF devices.

Note You cannot migrate a BFCP-enabled SIP profile to Cisco Unified Communications Manager version 8.6(2) or higher. If you configure video desktop sharing on Cisco Unified Communications Manager 8.61 and then upgrade to Cisco Unified Communications Manager 8.62, you must configure video desktop sharing on version 8.6.2.

Video desktop sharing using BFCP is not supported if **Trusted Relay Point** or **Media Termination Point** are enabled on the software phone device.

Procedure

Step 1 Open the **Cisco Unified Communications Manager Administration** interface.

Step 2 Enable video desktop sharing on the SIP profile.

- For individual profiles, do the following:
  1. Select **Device** > **Device Settings** > **SIP Profile**.
  2. Select your SIP profile.
  3. In the **SIP Profile Information** section, select **Allow Presentation Sharing Using BFCP**.
  4. Select **Save**.
- For multiple profiles, do the following:
  1. Select **Bulk Administration** > **Phones** > **Export Phones** > **All Details**.
  2. Select **Bulk Administration** > **Upload/Download Files** and download the exported `CSV` file.
  3. Open the `CSV` file with any editor.
  4. Insert a column named Allow presentation sharing using BFCP into the `CSV` file.
  5. Set the value of the column to `Y` for all required devices.
  6. Save the `CSV` file.
  7. Select **Bulk Administration** > **Phones** > **Insert Phones**.
  8. Select the **Override the existing configuration** option.
  9. Import the `CSV` file.
  10. Select **Run Immediately**.
  11. Select **Submit**.

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 the SIP profile on which you enabled BFCP presentation sharing from the **SIP Profile** drop-down list.

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.

Create CSF Devices on 8.6(2) and Later

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

As part of the task of creating CSF devices, you can enable video desktop sharing using Binary Floor Control Protocol (BFCP). Cisco Unified Communications Manager handles the BFCP packets that users transmit when using video desktop sharing capabilities. For this reason, you configure Cisco Unified Communications Manager to allow BFCP presentation sharing. On Cisco Unified Communications Manager version 8.6(2) and later, you must apply a COP file to add an option to allow BFCP presentation sharing on CSF devices. You must then enable BFCP presentation sharing on the CSF devices.

Note

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

Tip

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

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

Apply COP File for BFCP Capabilities

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

Note

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

Procedure

Step 1 Download the Cisco Jabber administration package from Cisco.com.

Step 2 Copy `cmterm-bfcp-e.8-6-2.cop.sgn` from the Cisco Jabber administration package to your file system.

Step 3 Open the **Cisco Unified Communications Manager Administration** interface.

Step 4 Upload and apply `cmterm-bfcp-e.8-6-2.cop.sgn`.

Step 5 Restart the server as follows:

a) Open the **Cisco Unified OS Administration** interface.
b) Select **Settings** > **Version**.
c) Select **Restart**.
d) Repeat the preceding steps for each node in the cluster, starting with your presentation server.

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

Create CSF Devices

Complete the steps in this task to create CSF devices.

Procedure

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

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

Step 3 Select **Add New**.

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

Step 5 Specify a name for the CSF device in the **Device Name** field.
You should use the 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 **Allow Presentation Sharing using BFCP** in the **Protocol Specific Information** section to enable video desktop sharing.
Video desktop sharing using BFCP is not supported if **Trusted Relay Point** or **Media Termination Point** are enabled on the software phone device.

Step 8 Select **Save**.

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

What to Do Next

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

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 the appropriate phone security profile from the Phone Security Profile type drop-down list and select **Next**.
The **Phone Security Profile Configuration** window opens.

Configure the Phone Security Profile

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

Procedure

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

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

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

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

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

  The client has been tested using authentication strings with 1024 bit length keys. The client requires more time to generate 2048 bit length keys than 1024 bit length keys. As a result, if you select 2048, you should expect it to take longer to complete the CAPF enrollment process.
- 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 To create the authentication string you can do one of the following:

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

What to Do Next

Provide users with the authentication string.

Provide Users with Authentication Strings

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

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

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

The client displays an error if:

- Users enter an incorrect authentication string.

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

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

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

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

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

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

Secure Phone Details for Cisco Jabber for Windows

Secure Connections

If you enable secure phone capabilities, then:

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

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

Encrypted Media

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

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

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

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

- User A, user B, and user C start a conference call. The client does not encrypt the main video stream or audio stream for any user.

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

🔒

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

Using Expressway for Mobile and Remote Access

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

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

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

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

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

Stored Files

The client stores the following files for secure phone capabilities:

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

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

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

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

The client stores these files in the following folder: `%User_Profile%\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\Security`

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

Conference Calls

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

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

Sharing Secure CSF Devices between Clients

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

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

Multiple Users on a Shared Microsoft Windows Account

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

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

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

Multiple Users on a Shared Computer

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

Add Directory Number to the Device for Desktop Applications

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

Procedure

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

Step 2 Select **Add a new DN**.
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** window 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 Complete the following steps to enable desk phone video capabilities:

a) Locate the **Product Specific Configuration Layout** section.

b) Select **Enabled** from the **Video Capabilities** drop-down list.

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

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

Step 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.

Desk Phone Video Configuration

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

Set Up Desk Phone Video

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

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

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

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

2 Enable the desk phone device for video in Cisco Unified Communications Manager.

3 Install Cisco Media Services Interface on the computer.

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

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

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

Desk Phone Video Considerations

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

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

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

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

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

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

Related Topics

Cisco IP Phone version 7970 and Cisco Unified Video Advantage is Blocked by Network Threat Protection

Add Directory Number to the Device for Desktop Applications

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

Procedure

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

Step 2 Select **Add a new DN**.
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** window 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 Silent Monitoring and Call Recording

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

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

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

Notes:

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

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

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

Related Topics

v8.6(1): Monitoring and Recording

v9.1: Monitoring and Recording

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

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

Procedure

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

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

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

The **Cisco Jabber Settings** window opens.

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

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

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

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

Step 5 Select **Save**.

Specify TFTP Servers in Phone Mode

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

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

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 phone numbers. An example of this type of rule is to transform `4089023139` into `23139`.

Publish Dial Rules

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

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

Before You Begin

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

Procedure

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

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

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

Step 4 Select **Next**.

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

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

Step 7 Restart the TFTP service.

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

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 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.

On Cisco Unified Communications Manager version 9.x and higher you can also set up CTI remote devices to provision users with Extend and Connect capabilities.

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.

Video Desktop Sharing

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

Note

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

Tip

You must enable BFCP on the SIP trunk to allow video desktop sharing capabilities outside of a Cisco Unified Communications Manager cluster. To enable BFCP on the SIP trunk, do the following:

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

Set Up Secure Phone Capabilities

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

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 the appropriate phone security profile from the Phone Security Profile type drop-down list and select **Next**.
The **Phone Security Profile Configuration** window opens.

Configure the Phone Security Profile

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

Procedure

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

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

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

- Device Security Mode — Select one of the following:
  - Authenticated
  - Encrypted
- Transport Type — Leave the default value of **TLS**.
- TFTP Encrypted Config — Select this checkbox to encrypt the CSF device configuration file that resides on the TFTP server.
- Authentication Mode — Select By Authentication String.

- Key Size (Bits) — Select the appropriate key size for the certificate.

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

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

- 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 To create the authentication string you can do one of the following:

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

What to Do Next

Provide users with the authentication string.

Provide Users with Authentication Strings

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

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

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

The client displays an error if:

- Users enter an incorrect authentication string.

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

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

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

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

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

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

Secure Phone Details for Cisco Jabber for Windows

Secure Connections

If you enable secure phone capabilities, then:

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

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

Encrypted Media

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

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

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

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

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

🔒

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

Using Expressway for Mobile and Remote Access

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

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

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

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

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

Stored Files

The client stores the following files for secure phone capabilities:

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

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

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

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

The client stores these files in the following folder:
`%User_Profile%\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\Security`

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

Conference Calls

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

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

Sharing Secure CSF Devices between Clients

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

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

Multiple Users on a Shared Microsoft Windows Account

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

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

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

Multiple Users on a Shared Computer

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

Add Directory Number to the Device for Desktop Applications

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

Procedure

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

Step 2 Select **Add a new DN**.
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** window 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 Complete the following steps to enable desk phone video capabilities:

a) Locate the **Product Specific Configuration Layout** section.

b) Select **Enabled** from the **Video Capabilities** drop-down list.

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

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

Step 8 Specify all other configuration settings on the **Phone Configuration** window as appropriate.
See the Cisco Unified Communications Manager documentation for more information about the configuration settings on the **Phone Configuration** window.

Step 9 Select **Save**.
An message displays to inform you if the device is added successfully. The **Association Information** section becomes available on the **Phone Configuration** window.

What to Do Next

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

Desk Phone Video Configuration

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

Set Up Desk Phone Video

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

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

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

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

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

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

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

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

Desk Phone Video Considerations

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

- You cannot use desk phone video capabilities on devices if video cameras are attached to the devices, such as a Cisco Unified IP Phone 9971. You can use desk phone video capabilities if you remove video cameras from the devices.
- You cannot use desk phone video capabilities with devices that do not support CTI.
- Video desktop sharing, using the BFCP protocol, is not supported with desk phone video.
- It is not possible for endpoints that use SCCP to receive video only. SCCP endpoints must send and receive video. Instances where SCCP endpoints do not send video result in audio only calls.
- 7900 series phones must use SCCP for desk phone video capabilities. 7900 series phones cannot use SIP for desk phone video capabilities.

- If a user initiates a call from the keypad on a desk phone device, the call starts as an audio call on the desk phone device. The client then escalates the call to video. For this reason, you cannot make video calls to devices that do not support escalation, such as H.323 endpoints. To use desk phone video capabilities with devices that do not support escalation, users should initiate calls from the client.
- A compatibility issue exists with Cisco Unified IP Phones that use firmware version SCCP45.9-2-1S. You must upgrade your firmware to version SCCP45.9-3-1 to use desk phone video capabilities.
- Some antivirus or firewall applications, such as Symantec EndPoint Protection, block inbound CDP packets, which disables desk phone video capabilities. You should configure your antivirus or firewall application to allow inbound CDP packets.

  See the following Symantec technical document for additional details about this issue: *Cisco IP Phone version 7970 and Cisco Unified Video Advantage is Blocked by Network Threat Protection*.
- You must not select the **Media Termination Point Required** checkbox on the SIP trunk configuration for Cisco Unified Communications Manager. Desk phone video capabilities are not available if you select this checkbox.

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

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

Related Topics

Cisco IP Phone version 7970 and Cisco Unified Video Advantage is Blocked by Network Threat Protection

Add Directory Number to the Device for Desktop Applications

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

Procedure

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

Step 2 Select **Add a new DN**.

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** window 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**.

Create CTI Remote Devices

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

Extend and Connect Capabilities

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

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

Provisioning CTI Remote Devices

Dedicated Device

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

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

Alternative Device

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

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

Enable Users to Modify Remote Destinations

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

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

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

Using CTI Remote Devices with the Client

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

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

Limitations and Known Issues

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

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

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

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

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

Related Topics

Extend and Connect

Enable User Mobility

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

Procedure

Step 1 Select **User Management** > **End User**.
The **Find and List Users** window opens.

Step 2 Specify the appropriate filters in the **Find User where** field to and then select **Find** to retrieve a list of users.

Step 3 Select the user from the list.
The **End User Configuration** window opens.

Step 4 Locate the **Mobility Information** section.

Step 5 Select **Enable Mobility**.

Step 6 Select **Save**.

Create CTI Remote Devices

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

Procedure

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

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

Step 3 Select **Add New**.

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

Step 5 Select the appropriate user ID from the **Owner User ID** drop-down list.

Note Only users for whom you enable mobility are available from the **Owner User ID** drop-down list. For more information, see *Enable User Mobility*.

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

Step 6 Edit the default value in the **Device Name** field, if appropriate.

Step 7 Ensure you select an appropriate option from the **Rerouting Calling Search Space** drop-down list in the **Protocol Specific Information** section.
The **Rerouting Calling Search Space** drop-down list defines the calling search space for re-routing and ensures that users can send and receive calls from the CTI remote device.

Step 8 Specify all other configuration settings on the **Phone Configuration** window as appropriate.
See the *CTI remote device setup* topic in the Cisco Unified Communications Manager documentation for more information.

Step 9 Select **Save**.
The fields to associate directory numbers and add remote destinations become available on the **Phone Configuration** window.

Related Topics

Create CTI Remote Devices

Add Directory Number to the Device for Desktop Applications

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

Procedure

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

Step 2 Select **Add a new DN**.

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** window 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.

Add a Remote Destination

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

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

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

Note

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

Procedure

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

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

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

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

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

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

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

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

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

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

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

Step 9 Specify all other values as appropriate.

Step 10 Select **Save**.

What to Do Next

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

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

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

When users select a remote destination in the client, it displays as the value of **Active Remote Destination**.

none displays as the value of **Active Remote Destination** if:

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

Add a CTI Service

The CTI service lets users control devices.

Procedure

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

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

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

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

Step 5 Select **Next**.

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

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

b) Specify 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**.

Configure Silent Monitoring and Call Recording

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

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

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

Notes:

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

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

Related Topics

v8.6(1): Monitoring and Recording

v9.1: Monitoring and Recording

Enable URI Dialing

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

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 System Guide, Release 9.0(1)
Cisco Unified Communications Manager System Guide, Release 9.1(1)

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

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

Procedure

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

Step 2 Select **Application** > **Legacy Clients** > **Settings**.
The **Legacy Client Settings** window opens.

Step 3 Locate the **Legacy Client Security Settings** section.

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

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

Step 5 Select **Save**.

Specify TFTP Servers in Phone Mode

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

- Users manually enter the TFTP server address when they start the client.

- You specify the TFTP server address during installation with the TFTP argument.

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.

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 fully qualified domain name or IP address of your primary CCMCIP service in the **Primary CCMCIP Host** field.
c) Specify the fully qualified domain name 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 phone numbers. An example of this type of rule is to transform `4089023139` into `23139`.

Publish Dial Rules

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

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

Before You Begin

1 Create your dial rules in Cisco Unified Communications Manager.

2 Download the Cisco Jabber administration package from `Cisco.com`.

3 Copy `cmterm-cupc-dialrule-wizard-0.1.cop.sgn` from the Cisco Jabber administration package to your file system.

Procedure

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

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

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

Step 4 Select **Next**.

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

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

Step 7 Restart the TFTP service.

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

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

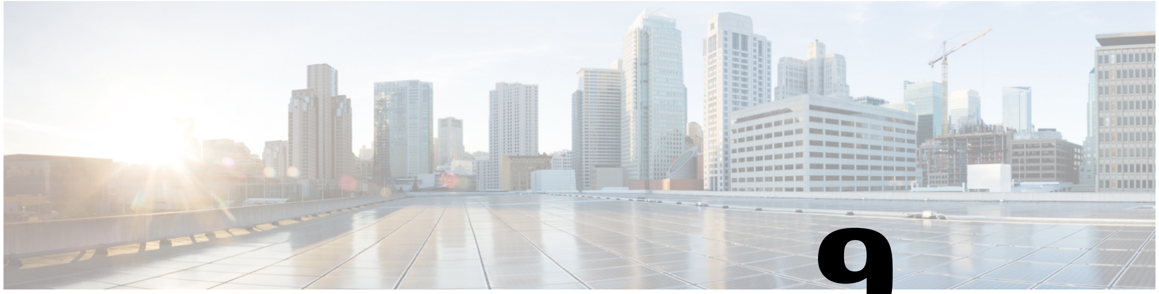
b) Navigate to `http://`*`tftp_server_address`*`:6970/CUPC/DirLookupDialRules.xml`.

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 9

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

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

CHAPTER 10

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 for Use with Cisco Jabber

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.

Before You Begin

Ensure that you have Cisco Unified Communications Manager 8.x.

If you have Cisco Unified Communications Manager 9.x or later, see Add a Voicemail Service, on page 114.

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**.

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 IP address or the fully qualified domain name (FQDN) of the voicemail server.
- **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.

Before You Begin

Ensure that you have Cisco Unified Communications Manager 8.x and Cisco Unified Presence.

If you have Cisco Unified Communications Manager 9.x or later, see Add a Mailstore Service, on page 116.

Procedure

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

Step 2 Depending on your version of Cisco Unified Presence, select one of the following paths:

- **Application** > **Cisco Jabber** > **Mailstore**
- **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 as follows:

- **Name—**Enter a descriptive name for the server, for example, PrimaryMailStoreServer.
- **Description—**Enter an optional description.
- **Hostname/IP Address—**Enter the hostname, IP Address, or Fully Qualified Domain Name (FQDN) of the mailstore server.
-
- **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 Depending on your version of Cisco Unified Presence, select one of the following:

- **Application** > **Cisco Jabber** > **Voicemail Profile**
- **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.

Step 5 Add users to the voicemail profile as follows:

a) Select **Add Users to Profile**.
b) To retrieve a list of users, in the **Find User where** field, specify the appropriate filters and then select **Find**.
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 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.

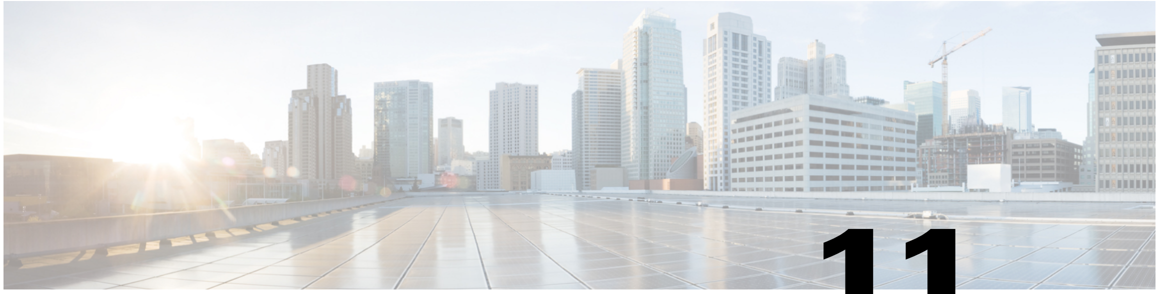
Note Do not select **Web Conferencing** from the **Credentials source for voicemail service** drop-down list. You cannot currently use conferencing credentials as a credentials source for voicemail services.

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 11

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 for Use with Cisco Jabber

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.

Before You Begin

Ensure that you have Cisco Unified Communications Manager 9.x or later.

If you have Cisco Unified Communications Manager 8.x, see Add a Voicemail Server, on page 108.

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 In the **Find and List UC Services** window, select **Add New**.

Step 4 In the **Add a UC Service** section, select **Voicemail** from the **UC Service Type** drop-down list and select **Next**

Step 5 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 IP address or the fully qualified domain name (FQDN) of the voicemail server.
- **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**.

What to Do Next

Apply the voicemail service to your service profile.

Apply a 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 sign 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 sign in to the voicemail service. You cannot currently synchronize with conferencing credentials.

Step 5 Click **Save**.

Add a Mailstore Service

The mailstore service provides users with visual voicemail capabilities.

Before You Begin

Ensure that you have Cisco Unified Communications Manager 9.x or later.

If you have Cisco Unified Communications Manager 8.x, see Create a Mailstore, on page 109.

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**.

Step 4 In the **Add a UC Service** section, from the **UC Service Type** drop-down list, select **MailStore** and then click **Next**.

Step 5 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 IP address or the Fully Qualified Domain Name (FQDN) of the mailstore server.
-
- **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 6 Select **Save**.

What to Do Next

Apply 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 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.

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.

Cloud-Based deployments can use the configuration file parameter `VoicemailService_UseCredentialsFrom`. Set this parameter to the value `phone` to use the Cisco Unified Communications Manager credentials to sign in to Cisco Unity Connection.

CHAPTER 12

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

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

CHAPTER 13

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

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 **Options** 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 **Options** window.

To open the **Options** window, select **File** > **Options**.

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 on Cisco Unified Presence

Procedure

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

Step 2 Depending on your version of Cisco Unified Presence, select one of the following:.

- **Application** > **Cisco Jabber** > **Conferencing Server**
- **Application** > **Cisco Unified Personal Communicator** > **Conferencing Server**

Step 3 Select **Add New**.
The **Conferencing Server Configuration** window opens.

Step 4 Complete the following fields:

- **Name —** Enter a name for the configuration. The name is displayed 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 —** Accept the default value.
- **Protocol —** Select **HTTPS**.
- **Server Type —** Select **WebEx**.
- **Site ID —** You do not need to specify a value for this field.
- **Partner ID —** 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 and add it to a service profile, the client can access conferencing features.

Procedure

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

Step 2 Depending on your version of Cisco Unified Presence, select one of the following:

- **Application** > **Cisco Jabber** > **Conferencing Profile**
- **Application** > **Cisco Unified Personal Communicator** > **Conferencing Profile**

Step 3 Select **Add New**.
The **Conferencing Profile Configuration** window opens.

Step 4 Complete 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.

Step 5 From the **Server Certificate Verification** drop-down list, select one of the following:

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

Step 6 To set this profile as the system default, check **Make this the default Conferencing Profile for the system**.

Step 7 In the **Users in Profile** section, select **Add Users to Profile**.

Step 8 In the **Find and List Users** window, select **Find** to retrieve a list of users.

Step 9 Select the appropriate users from the list and then select **Add Selected**.
The selected users are added to the profile.

Step 10 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

To integrate with Cisco WebEx Meeting Center in an on-premises deployment, select one of the following integration options:

- Cloud-based integration—Cisco WebEx Meeting Center provides data, such as participant chat and roster lists, and audio and video capabilities.
- Hybrid cloud-based integration—Cisco WebEx Meeting Center provides data, such as participant chat and roster lists, and 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 **Options** 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 **Options** window.

To open the **Options** window, select **File** > **Options**.

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 optional primary site ID for Cisco WebEx Meeting Center.
- Partner ID — Specify the optional appropriate partner ID for Cisco WebEx Meeting Center.

Step 5 Select **Save**.

Add Cisco WebEx Meeting Center to a Profile

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

Procedure

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

Step 2 Select **Application** > **Cisco Jabber** > **Conferencing Profile**.
In some versions of Cisco Unified Presence, this path is as follows: **Application** > **Cisco Unified Personal Communicator** > **Conferencing Profile**.

Step 3 Select **Add New**.
The **Conferencing Profile Configuration** window opens.

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

- **Name —** Enter a name for the configuration.
- **Description —** Enter an optional description.
- **Primary Conferencing Server —** Select the primary Cisco WebEx Meeting Center site from the drop-down list.

  Note The client uses only the site you select from the **Primary Conferencing Server** drop-down list. You do not need to select a site from the **Backup Conferencing Server** drop-down list.
- **Server Certificate Verification —** Select one of the following from the drop-down list:
  - **Any Certificate**
  - **Self Signed or Keystore**
  - **Keystore Only**

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

Step 6 Add users to the conferencing profile as follows:

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

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

c) Select the appropriate users from the list.

d) Select **Add Selected**.
The selected users are added to the profile and the **Find and List Users** dialog box closes.

Step 7 Select **Save**.

CHAPTER 14

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

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

For Cisco Jabber for Windows, each user can enter their credentials in the **Options** 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 **Options** window.

To open the **Options** window, select **File** > **Options**.

Add Cisco WebEx Meetings Server on Cisco Unified Communications Manager

To configure conferencing on Cisco Unified Communications Manager, you must add a Cisco WebEx Meetings Server.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface and select **User Management** > **User Settings** > **UC Service**.
The **Find and List UC Services** window opens.

Step 2 Select **Add New**.

Step 3 In the **Add a UC Service** section, from the **UC Service Type** drop-down list, select **Conferencing** and then select **Next**.

Step 4 Complete the following fields:

- **Product Type —** Select **WebEx (Conferencing)**.
- **Name —** Enter a name for the configuration. The name you specify is displayed 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. This URL is case sensitive and must match the case that was configured for the site URL in Cisco WebEx Meetings Server.
- **Port —** Leave the default value.
- **Protocol —** Select **HTTPS**.

Step 5 To use Cisco WebEx as the single sign-on (SSO) identity provider, check**User web conference server as SSO identity provider**.

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

Step 6 Select **Save**.

What to Do Next

Add the Cisco WebEx Meetings Server to a service profile.

Add the Cisco WebEx Meetings Server to a Service Profile

After you add Cisco WebEx Meetings Server and add it to a service profile, the client can access conferencing features.

Before You Begin

Create a service profile.

Add Cisco WebEx Meetings Server on Cisco Unified Communications Manager.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface and select **User Management** > **User Settings** > **Service Profile**

Step 2 Find and select your service profile.

Step 3 In the **Conferencing Profile** section, from the **Primary**, **Secondary**, and **Tertiary** drop-down lists, select up to three instances of Cisco WebEx Meetings Server.

Step 4 From the **Server Certificate Verification** drop-down list, select the appropriate value.

Step 5 From the **Credentials source for web conference service** drop-down list, select one of the following:

- **Not set —** Select this option if the user does not have a credentials source that matches their Cisco WebEx Meetings Server credentials or if you use SSO at the meeting site.
- **Unified CM - IM and Presence —** Select this option if the Cisco Unified Communications Manager IM and Presence Service credentials for the user match their Cisco WebEx Meetings Server credentials.
- **Voicemail —** Select this option if the Cisco Unity Connection credentials for the user match their Cisco WebEx Meetings Server credentials.

Note You cannot synchronize the credentials you specify in Cisco Unified Communications Manager with credentials you specify in Cisco WebEx Meetings Server. For example, if you specify that instant messaging and presence credentials for a user are synchronized with their Cisco WebEx Meetings Server credentials, the instant messaging and presence credentials for that user change. You must update the Cisco WebEx Meetings Server credentials for that user to match that change.

Step 6 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

To integrate with Cisco WebEx Meeting Center in an on-premises deployment, select one of the following integration options:

- Cloud-based integration—Cisco WebEx Meeting Center provides data, such as participant chat and roster lists, and audio and video capabilities.
- Hybrid cloud-based integration—Cisco WebEx Meeting Center provides data, such as participant chat and roster lists, and 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 **Options** 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 **Options** window.

To open the **Options** window, select **File** > **Options**.

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**.

Step 4 In the **Add a UC Service** section, from the **UC Service Type** drop-down list, select **Conferencing** and then select **Next**.

Step 5 Complete the following fields:

- **Product Type —** Select **WebEx (Conferencing)**.
- **Name —** Enter a name for the configuration. The name is displayed 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 —** Enter the Cisco WebEx Meeting Center site hostname. Do not enter an IP address.
- **Port —** Enter the Cisco WebEx Meeting Center site port number.
- **Protocol —** Select **HTTPS**.

Step 6 To use Cisco WebEx as the single sign-on (SSO) identity provider, check**User web conference server as SSO identity provider**.

Note This field is available only if you select **WebEx (Conferencing)** as the **Product Type**.

Step 7 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 15

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

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 **Options** window.

To open the **Options** window, select **File** > **Options**.