On-Premises Deployment for Cisco Jabber 14.0

First Published: 2021-03-25

Last Modified: 2024-04-01

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

CONTENTS

New and Changed Information

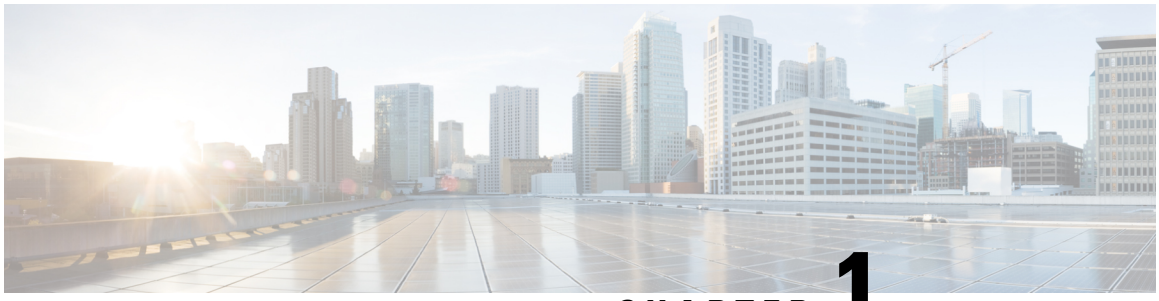
New and Changed Information

Date	Status	Description	Location
March 2021		Initial Publication	

New and Changed Information

PART I

Introduction



CHAPTER 1

Cisco Jabber Overview

Purpose of this Guide

The *Cisco Jabber Deployment and Installation Guide* includes the following task-based information required to deploy and install Cisco Jabber:

- Configuration and installation workflows that outline the processes to configure and install on-premises deployments.
- How to configure the various services that the Cisco Jabber client interacts with, such as IM and Presence Service, Voice and Video Communication, Visual Voicemail, and Conferencing.
- How to configure directory integration, certificate validation, and service discovery.
- How to install the clients.

Before you deploy and install Cisco Jabber, see the *Cisco Jabber Planning Guide* at http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html to determine the deployment options that best suit your business needs.

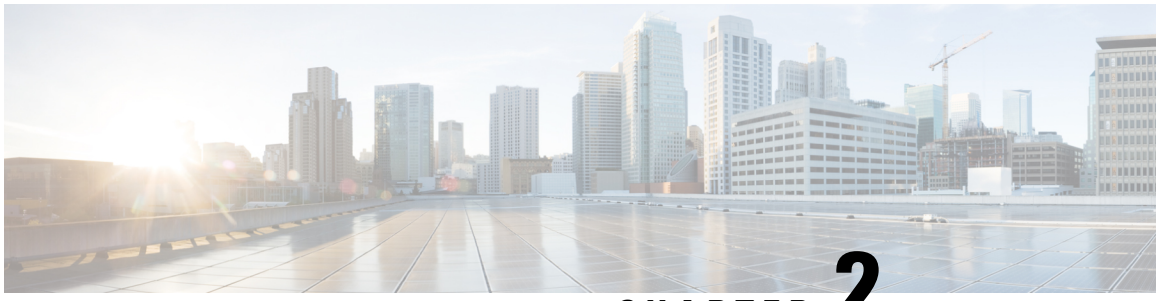
About Cisco Jabber

Cisco Jabber is a suite of Unified Communications applications that allow seamless interaction with your contacts from anywhere. Cisco Jabber offers IM, presence, audio and video calling, voicemail, and conferencing.

The applications in the Cisco Jabber family of products are:

- Cisco Jabber for Windows
- Cisco Jabber for Mac
- Cisco Jabber for iPhone and iPad
- Cisco Jabber for Android
- Cisco Jabber Softphone for VDI

For more information about the Cisco Jabber suite of products, see https://www.cisco.com/go/jabber or https://www.cisco.com/c/en/us/products/unified-communications/jabber-softphone-for-vdi/index.html .



CHAPTER 2

Configuration and Installation Workflows

Purpose of Configuration Workflows

Configuration and installation workflows outline the processes to configure and install on-premises deployment. Before you deploy and install Cisco Jabber, see the Cisco Jabber Planning Guide at Install and Upgrade Guides to determine the deployment options that best suit your business needs.

Prerequisites

- Installation servers must be started and active
- Activate and Start Essential Services, on page 3
- Install Cisco Options Package File for Devices, on page 4

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.

Install Cisco Options Package File for Devices

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

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

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

Procedure

Step 1 Download the device COP file.

a) Locate the device COP file.

- Go to the software downloads site.
- Locate the device COP file for your release.

b) Click **Download Now**.

c) Note the MD5 checksum.

You will need this information later.

d) Click **Proceed with Download** and follow the instructions.

Step 2 Place the COP file on an FTP or SFTP server that is accessible from your Cisco Unified Communications Manager nodes.

Step 3 Install this COP file on the Publisher node in your Cisco Unified Communications Manager cluster:

a) Open the **Cisco Unified OS Administration** interface.

b) Select **Software Upgrades** > **Install/Upgrade**.

c) Specify the location of the COP file and provide the required information.

For more information, see the online help.

d) Select **Next**.

e) Select the device COP file.

f) Select **Next**.

g) Follow the instructions on the screen.

h) Select **Next**.

Wait for the process to complete. This process can take some time.

i) Reboot Cisco Unified Communications Manager at a time of low usage.
j) Let the system fully return to service.

Note To avoid interruptions in service, make sure each node returns to active service before you perform this procedure on another server.

Step 4 Install the COP file on each Subscriber node in the cluster.

Use the same process you used for the Publisher, including rebooting the node.

Deployment and Installation Workflows

Full UC Deployment

Procedure

	Command or Action	Purpose
Step 1	Read the Cisco Jabber Planning Guide located at http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html.	• Choose your deployment scenario. • Review requirements to confirm that you meet them. • Review contact sources to determine which contact source you will use.
Step 2	Create Default Service Profile, on page 11	Create a default service profile to add services.
Step 3	Contact Source, on page 13	Configure a contact source for your users.
Step 4	Configure Instant Messaging and Presence Service, on page 21	Set up the Cisco Unified Communications IM & Presence service.
Step 5	Configure Voicemail, on page 27	Set up voicemail for your users.
Step 6	Configure Webex Conferencing, on page 35	Set up conferencing with Webex Meetings Server.
Step 7	Configure CTI Service, on page 39	Set up a CTI service and provide Jabber with devices that are associated with users.
Step 8	Users, on page 43	Set up users for Jabber.

	Command or Action	Purpose
Step 9	Configure Softphone, on page 57	Set up softphone devices for users.
Step 10	Configure Deskphone Control, on page 67	Create deskphone devices and enable features.
Step 11	Configure Extend and Connect, on page 75	Set up options for users to extend calls to remote devices.
Step 12	Configure Service Discovery, on page 81	Choose a service discovery option for your users.
Step 13	Configure Certificate Validation, on page 93	Set up the required certificates for each server.
Step 14	Configure the Clients, on page 97	Choose what features to include in the client configuration files.
Step 15	Deploy Cisco Jabber Applications and Jabber Softphone for VDI, on page 109	Choose how to install the clients for your users.

Jabber IM Only Deployment

Procedure

	Command or Action	Purpose
Step 1	Read the Cisco Jabber Planning Guide located at http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html.	• Choose your deployment scenario. • Review requirements to confirm that you meet them. • Review contact sources to determine which contact source you will use.
Step 2	Create Default Service Profile, on page 11	Create a default service profile to add services.
Step 3	Contact Source, on page 13	Configure a contact source for your users.
Step 4	Configure Instant Messaging and Presence Service, on page 21	Set up the Cisco Unified Communications IM & Presence service.
Step 5	Configure Webex Conferencing, on page 35	Set up conferencing with Webex Meetings Server.
Step 6	Users, on page 43	Set up users for Jabber.
Step 7	Configure Service Discovery, on page 81	Choose a service discovery option for your users.
Step 8	Configure Certificate Validation, on page 93	Set up the required certificates for each server.
Step 9	Configure the Clients, on page 97	Choose what features to include in the client configuration files.

	Command or Action	Purpose
Step 10	Deploy Cisco Jabber Applications and Jabber Softphone for VDI, on page 109	Choose how to install the clients for your users.

Phone Only Mode Deployment

Procedure

	Command or Action	Purpose
Step 1	Read the Cisco Jabber Planning Guide located at http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html.	• Choose your deployment scenario. • Review requirements to confirm that you meet them. • Review contact sources to determine which contact source you will use.
Step 2	Create Default Service Profile, on page 11	Create a default service profile to add services.
Step 3	Configure Voicemail, on page 27	Set up voicemail for your users.
Step 4	Configure Webex Conferencing, on page 35	Set up conferencing with Webex Meetings Server.
Step 5	Configure CTI Service, on page 39	Set up a CTI service and provide Jabber with devices that are associated with users.
Step 6	Users, on page 43	Set up users for Jabber.
Step 7	Configure Softphone, on page 57	Set up softphone devices for users.
Step 8	Configure Service Discovery, on page 81	Choose a service discovery option for your users.
Step 9	Configure Certificate Validation, on page 93	Certificates are required for each service to which the Jabber clients connect.
Step 10	Configure the Clients, on page 97	Choose what features to include in the client configuration files.
Step 11	Deploy Cisco Jabber Applications and Jabber Softphone for VDI, on page 109	Choose how to install the clients for your users.

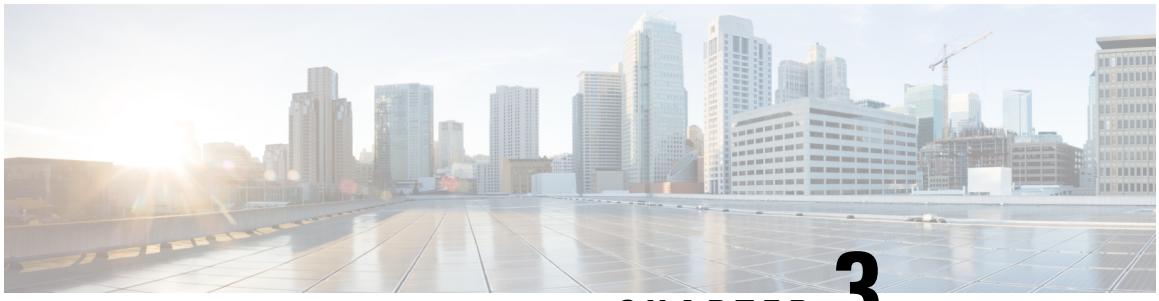
Phone Mode with Contacts Deployment

Procedure

	Command or Action	Purpose
Step 1	Read the Cisco Jabber Planning Guide located at http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html.	• Confirm that you meet the requirements. • Determine which contact sources you will use.
Step 2	Create Default Service Profile, on page 11	Create a default service profile to add services.
Step 3	Contact Source, on page 13	Configure a contact source for your users.
Step 4	Manage Presence Settings, on page 25	Choose if your users have presence in the client.
Step 5	Disable Instant Message Settings, on page 25	Remove instant messaging for this phone mode with contacts deployment.
Step 6	Configure Voicemail, on page 27	Set up voicemail for your users.
Step 7	Configure Webex Conferencing, on page 35	Set up conferencing with Webex Meetings Server.
Step 8	Configure CTI Service, on page 39	Set up a CTI service and provide Jabber with devices that are associated with users.
Step 9	Users, on page 43	Set up users for Jabber.
Step 10	Configure Softphone, on page 57	Set up softphone devices for users.
Step 11	Configure Deskphone Control, on page 67	Create deskphone devices and enable features.
Step 12	Configure Extend and Connect, on page 75	Set up options for users to extend calls to remote devices.
Step 13	Configure Service Discovery, on page 81	Choose a service discovery option for your users.
Step 14	Configure Certificate Validation, on page 93	Set up the required certificates for each server.
Step 15	Configure the Clients, on page 97	Choose what features to include in the client configuration files.
Step 16	Deploy Cisco Jabber Applications and Jabber Softphone for VDI, on page 109	Choose how to install the clients for your users.

PART II

Services

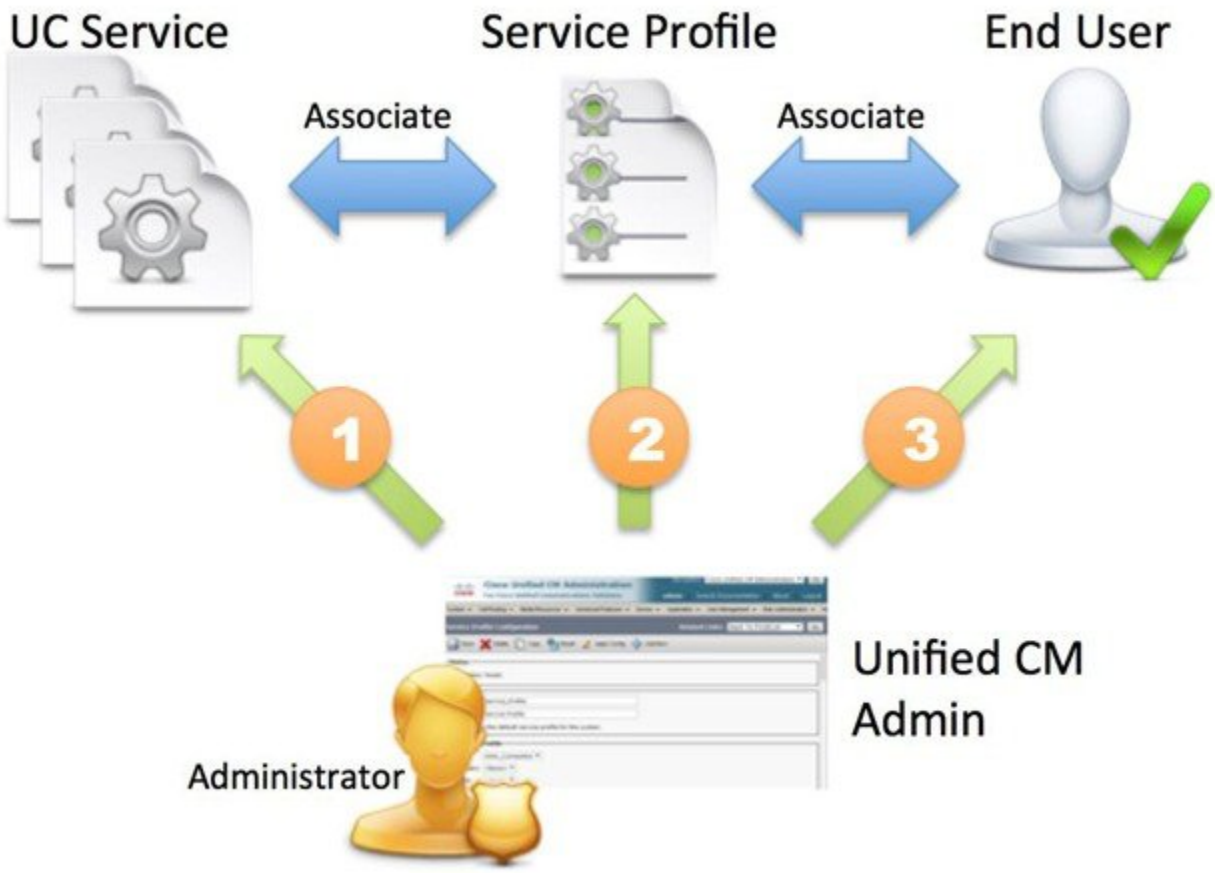


CHAPTER 3

Create Default Service Profile

Overview of service profile

Figure 1: Service profiles workflow



1. Create UC services.

2. Associate the UC Service with the Service Profile.
3. Associate the User with the Service Profile.

Create default service profile

Create a service profile to add the UC services.

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.

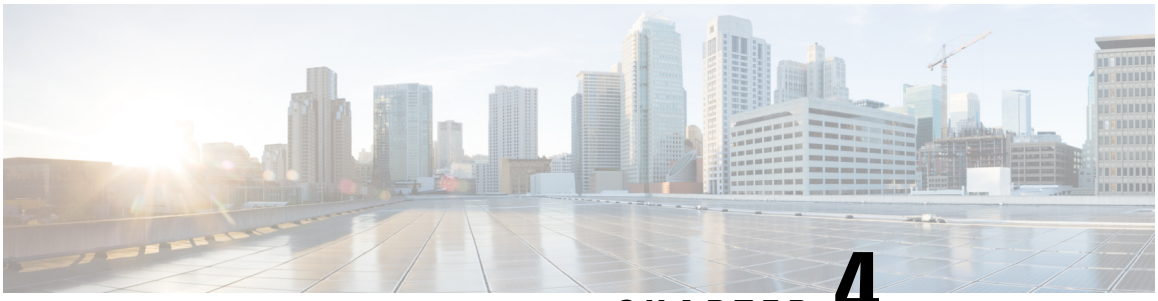
Step 4 Enter a name for the service profile in the **Name** field.

Step 5 Select **Make this the default service profile for the system** if you want the service profile to be the default for the cluster.

Step 6 Select **Save**.

What to do next

Create the UC services for your deployment.



CHAPTER 4

Contact Source

Configure Contact Source Workflow

Procedure

	Command or Action	Purpose
Step 1	Configure directory integration: • Configure Directory Integration in a Service Profile, on page 14 • Advanced Directory Integration in the Configuration File, on page 19	Configure directory integration through service profiles using Cisco Unified Communications Manager or with the configuration file.
Step 2	Optional: Configure Photos, on page 18	Review the options for configuring photos for users.
Step 3	Optional: Configure Intradomain Federation for CDI, on page 19	Let Cisco Jabber users communicate with users who are provisioned on different systems and who are using client applications other than Cisco Jabber.

Client Configuration for Directory Integration

You can configure directory integration through service profiles using Cisco Unified Communications Manager release 9 or later or with the configuration file. Use this section to learn how to configure the client for directory integration.

When both a service profile and a configuration file are present, the following table describes which parameter value takes precedence.

Service Profile	Configuration File	Which Parameter Value Takes Precedence?
Parameter value is set	Parameter value is set	Service profile
Parameter value is set	Parameter value is blank	Service profile
Parameter value is blank	Parameter value is set	Configuration file
Parameter value is blank	Parameter value is blank	Service profile blank (default) value

Configure Directory Integration in a Service Profile

With Cisco Unified Communications Manager release 9 and later, you can provision users with service profiles and deploy the `_cisco-uds` SRV record on your internal domain server. The client can then automatically discover Cisco Unified Communications Manager and retrieve the service profile to get directory integration configuration.

Procedure

	Command or Action	Purpose
Step 1	Add a Directory Service, on page 14	Create a Directory UC Service.
Step 2	Apply Directory Service to a Service Profile, on page 15	Add the Directory UC Service to the Service Profile.

Add a Directory Service

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 Select **Directory** from the **UC Service Type** menu and then select **Next**.

Step 5 Set all appropriate values for the directory service.

To configure Cisco Jabber directory searches on the Global Catalog, add the following values:

- **Port**—3268
- **Protocol**—TCP

Step 6 Select **Save**.

What to do next

Apply Directory Service.

Apply Directory Service to a Service Profile

Procedure

Step 1 Select **User Management** > **User Settings** > **Service Profile**.
The **Find and List Service Profiles** window opens.

Step 2 Select **Add New**.
The **Service Profile Configuration** window opens.

Step 3 Add the directory services to the directory profile. See the *Directory Profile Parameters* topic for information about the specific settings that are needed for the directory profile.

Step 4 Select **Save**.

Directory Profile Parameters

The following table lists the configuration parameters you can set in the directory profile:

Directory Service Configuration	Description
Primary server	Specifies the address of the primary directory server. This parameter is required for manual connections where the client cannot automatically discover the directory server.
Secondary server	Specifies the address of the backup directory server.
Use UDS for Contact Resolution	Specifies if the client uses UDS as a contact source. **True (Default)** Use UDS as a contact source. When this option is selected the following parameters in this table are not used. **False** Use CDI as a contact source. The following parameters are used to connect to the LDAP server. By default, UDS provides contact resolution when users connect to the corporate network through Expressway for Mobile and Remote Access.

Directory Service Configuration	Description
Use Logged On User Credential	Specifies if the client uses the logged on username and password for LDAP contact resolution. If you have configured Active Directory (AD) SSO, this will take priority over this setting. **True (default)** Use logged on user credentials. This is the same as specifying `CUCM` as the value for the LDAP_UseCredentialsFrom parameter. **False** Do not use logged on user credentials. When you have SSO configured, Jabber uses those credentials before using the ConnectionUsername and ConnectionPassword parameters. You must specify the logged on user credentials with the following parameters: • ConnectionUsername • ConnectionPassword
Username	Lets you manually specify a shared username that the client can use to authenticate with the directory server. By default, Cisco Jabber desktop clients use Kerberos or client certificate authentication. You should use this parameter only in deployments where you cannot authenticate with the directory server using either Kerberos or client certificate authentication. Use only a well-known or public set of credentials for an account that has read-only permissions.
Password	Lets you manually specify a shared password that the client can use to authenticate with the directory server. By default, Cisco Jabber desktop clients use Kerberos or client certificate authentication. You should use this parameter only in deployments where you cannot authenticate with the directory server using either Kerberos or client certificate authentication. Use only a well-known or public set of credentials for an account that has read-only permissions.

Directory Service Configuration	Description
Search Base 1 **Search Base 2** **Search Base 3** **Search Base 4** **Search Base 5**	Specifies a location in the directory server from which searches begin. In other words, a search base is the root from which the client executes a search. By default, the client searches from the root of the directory tree. You can specify the value of up to three search bases in your OU to override the default behavior. Active Directory does not typically require a search base. Specify search bases for Active Directory only for specific performance requirements. Specify a search base for directory servers other than Active Directory to create bindings to specific locations in the directory. **Tip** Specify an OU to restrict searches to certain user groups. For example, a subset of your users have instant messaging capabilities only. Include those users in an OU and then specify that as a search base.
Recursive Search on All Search Bases	Select this option to perform a recursive search of the directory starting at the search base. Use recursive searches to allow the Cisco Jabber client contact search queries to search all of the LDAP directory tree from a given search context (search base). This is a common option when searching LDAP. This is a required field. The default value is True.
Search Timeout	Specifies the timeout period for directory queries in seconds. The default value is 5.
Base Filter	Specifies a base filter for Active Directory queries. Specify a directory subkey name only to retrieve objects other than user objects when you query the directory. The default value is `(&(&(objectCategory=person)(objectClass=user)`.

Directory Service Configuration	Description
Predictive Search Filter	Defines filters to apply to predictive search queries. You can define multiple, comma-separated values to filter search queries. The default value is `ANR`. When Cisco Jabber performs a predictive search, it issues a query using Ambiguous Name Resolution (ANR). This query disambiguates the search string and returns results that match the attributes that are set for ANR on your directory server. **Important** Configure your directory server to set attributes for ANR if you want the client to search for those attributes.

Attribute Mappings

It is not possible to change the default attribute mappings in a service profile. If you plan to change any default attribute mappings, you must define the required mappings in a client configuration file.

Configure Photos

Cisco Jabber uses the following methods to configure Photos for users:

- **Active Directory Binary Objects**—No configuration needed, Cisco Jabber retrieves the binary photo from the thumbnailPhoto attribute.
- **PhotoURL attribute**—Use the PhotoSource parameter in the jabber-config.xml file to specify an attribute in your directory. The client will retrieve the attribute and determine if it is a URL or binary data and display the photo from either source.

  CDI parameter: PhotoSource

  Example:

  ```
  <Directory>
   <PhotoSource>url</PhotoSource>
  </Directory>
  ```

- **URI Substitution**—For your directory server type, use the following parameters in the jabber-config.xml file:

  CDI parameters:

  - PhotoUriSubstitutionEnabled
  - PhotoUriWithToken
  - PhotoUriSubstitutionToken

  Example:

```
<PhotoUriSubstitutionEnabled>True</PhotoUriSubstitutionEnabled>
<PhotoUriSubstitutionToken>sAMAccountName</PhotoUriSubstitutionToken>
<PhotoUriWithToken>http://example.com/photo/sAMAccountName.jpg</PhotoUriWithToken>
```

UDS parameters:

- UdsPhotoUriWithToken

Example:

```
<UDSPhotoUriWithToken>http://example.com/photo/sAMAccountName.jpg</UDSPhotoUriWithToken>
```

Advanced Directory Integration in the Configuration File

You can configure directory integration in the Cisco Jabber configuration file. For more information see the *Directory* chapter in the *Parameters Reference Guide for Cisco Jabber*.

Important When a Service Profile and a configuration file are present, settings in the Service Profile always take priority.

Federation

Federation lets Cisco Jabber users communicate with users who are provisioned on different systems and who are using client applications other than Cisco Jabber.

Configure Intradomain Federation for CDI

In addition to configuring intradomain federation on the presence server, you might need to specify some configuration settings in the Cisco Jabber configuration files.

To resolve contacts during contact search or retrieve contact information from your directory, Cisco Jabber requires the contact ID for each user. Cisco Unified Communications Manager IM & Presence server uses a specific format for resolving contact information that does not always match the format on other presence servers such as Microsoft Office Communications Server or Microsoft Live Communications Server.

Procedure

Step 1 Set the value of the UseSIPURIToResolveContacts parameter to true:

Step 2 Specify an attribute that contains the Cisco Jabber contact ID that the client uses to retrieve contact information. The default value is `msRTCSIP-PrimaryUserAddress`, or you can specify another attribute in the SipUri parameter.

Note When you deploy intradomain federation and the client connects with Expressway for Mobile and Remote Access from outside the firewall, contact search is supported only when the contact ID uses one of the following formats:

- sAMAccountName@domain
- UserPrincipleName (UPN)@domain
- EmailAddress@domain
- employeeNumber@domain
- phoneNumber@domain

Step 3 In the UriPrefix parameter, specify any prefix text that precedes each contact ID in the SipUri parameter.

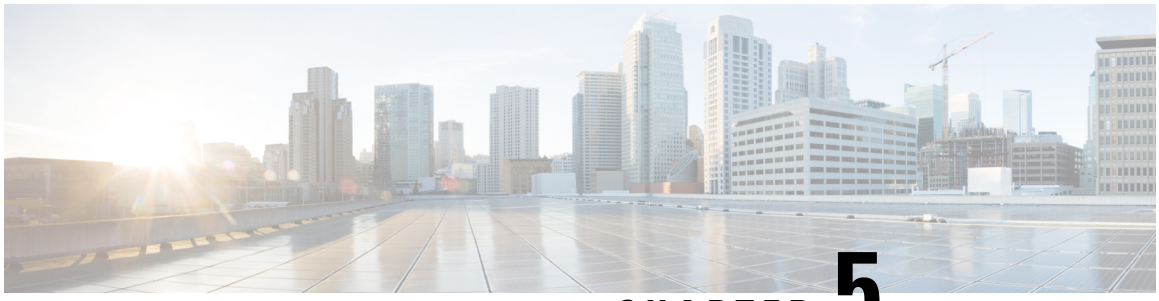
Example:

For example, you specify `msRTCSIP-PrimaryUserAddress` as the value of SipUri. In your directory the value of `msRTCSIP-PrimaryUserAddress` for each user has the following format: `sip:`*`username@domain`*.

Example

The following XML snippet provides an example of the resulting configuration:

```
<Directory>
  <UseSIPURIToResolveContacts>true</UseSIPURIToResolveContacts>
  <SipUri>non-default-attribute</SipUri>
  <UriPrefix>sip:</UriPrefix>
</Directory>
```



CHAPTER 5

Configure Instant Messaging and Presence Service

IM and Presence Service Workflow with Cisco Unified Communications Manager Release 10.5 and Later

Procedure

	Command or Action	Purpose
Step 1	Configure IM Address Scheme, on page 23	Configure an IM address for users.
Step 2	Enable Message Settings, on page 24	In the Cisco Unified Communications IM and Presence service, set the options to enable instant message and logging.

IM and Presence Service Workflow with Cisco Unified Communications Manager Release 9.x and Later

Procedure

	Command or Action	Purpose
Step 1	Enable Message Settings, on page 24	In the Cisco Unified Communications IM and Presence service, set the options to enable instant message and logging.
Step 2	Add an IM and Presence Service, on page 22	Create an IM and Presence UC Service.
Step 3	Apply an IM and Presence Service, on page 23	Add the IM and Presence UC Service to the Service Profile.

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**.

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

Add an IM and Presence Service, on page 22

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 IM Address Scheme

This feature is supported on Cisco Unified Communications Manager IM and Presence Service release 10.x or later. For versions of Cisco Unified Communications Manager IM and Presence Service release 9.x and earlier the default IM address scheme used is UserID@[Default Domain].

Procedure

Step 1 Choose the **IM Address Scheme**.

a) Open **Cisco Unified CM IM and Presence Administration**.
b) Select **Presence** > **Settings** > **Advanced Configuration**
The **Advanced Presence Settings** window opens.
c) Select **IM Address Scheme** and from the list choose one of the following:

- UserID@[Default Domain]

  If you use the UserID, ensure that you configure a default domain. For example, services must be named `cups.com` and not `cups`.

- Directory URI

Step 2 Select the required mapping.

a) Open **Cisco Unified CM Administration**.
b) Select **System** > **LDAP** > **LDAP Directory**.
The **Find and List LDAP Directories** window opens.
c) Find and select the directory from the list.
The **LDAP Directory** window opens.
d) In the **Standard User Fields To Be Synchronized** section choose the mapping:

- User ID mapped to an LDAP field, the default is **sAMAccountName**.
- Directory URI mapped to either **mail** or **msRTCSIP-primaryuseraddress**.

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**
- **Allow cut & paste in instant messages**

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 release 9.0.x:

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

What to do next

- If you have Cisco Unified Communications Manager IM and Presence Service release 9.x and later, Add an IM and Presence Service, on page 22.

Disable Instant Message Settings

In a phone mode with contacts deployment, you can turn off instant messaging for your users as instant messaging doesn't apply to phone mode deployments.

Procedure

Step 1 From **Cisco Unified CM IM and Presence Administration** go to**Messaging** > **Settings**.

Step 2 Uncheck **Enable instant messaging** and click **Save**.

What to do next

Restart the Cisco XCP Router service.

Manage Presence Settings

The presence setting for your users is enabled by default. However, in a phone mode with contacts deployment you can disable the presence setting and your users won't see any presence in the client.

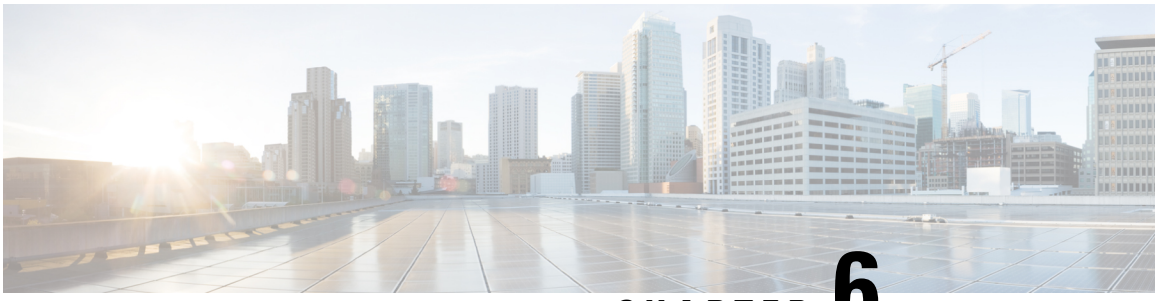
Procedure

Step 1 From **Cisco Unified CM IM and Presence Administration**, go to **Presence** > **Settings** > **Standard Configuration**.

Step 2 Uncheck **Enable availability sharing** and click **Save**.

What to do next

Restart the Cisco XCP Router service.



CHAPTER 6

Configure Voicemail

Configure Voicemail Workflow

Procedure

	Command or Action	Purpose
Step 1	Configure Cisco Unity Connection for Use with Cisco Jabber, on page 27	Configure Cisco Unity Connection so that Cisco Jabber can access voicemail services.
Step 2	Configure Retrieval and Redirection, on page 29	Configure retrieval so that users can access voice mail messages. Configure redirection so that users can send incoming calls to voicemail.
Step 3	Add a Voicemail Service, on page 30	Add a Voicemail UC service. Jabber uses this information to connect to the voicemail server.
Step 4	Apply a Voicemail Service, on page 31	Apply the Voicemail UC service to the service profile.
Step 5	Set a Voicemail Credentials Source, on page 32	Set the credentials for connecting to the Voicemail server.

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 release 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) In the **Features** section, select **Allow Users to Use Unified Client to Access Voice Mail**.
e) Select all other options as appropriate.
f) 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**.

What to do next

If you have Cisco Unified Communications Manager release 9.x and later, Add a Voicemail Service, on page 30.

Configure Retrieval and Redirection

Configure retrieval so that users can access voicemail 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**.

What to do next

Set a Voicemail Credentials Source, on page 32

Add a Voicemail Service

Add a voicemail service, to allow users to receive voice messages.

Before you begin

Configure Cisco Unity Connection for Use with Cisco Jabber, on page 27

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**.
UC Service Configuration window opens.

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.
- **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 a Voicemail Service, on page 31

Apply a Voicemail Service

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

Note Cisco Jabber does not read Voicemail UC Service Profile when it is deployed only in the Phone mode.

For Cisco Jabber to retrieve the voicemail server information, update the `jabber-config.xml` file with the voicemail parameters.

```
<Voicemail>
<VoicemailService_UseCredentialsFrom>phone</VoicemailService_UseCredentialsFrom>
<VoicemailPrimaryServer>X.X.X.X</VoicemailPrimaryServer>
</Voicemail>
```

After updating, upload the `jabber-config.xml` file to all the Cisco Unified Communications Manager TFTP servers and restart the TFTP service on TFTP server nodes. Then reset the Jabber client.

Before you begin

Add a Voicemail Service, on page 30

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) For **Credentials source for voicemail service**, select one of the following:

- **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.
- **Web conferencing** — This option is not supported, it uses the conferencing credentials to sign in to the voicemail service. You cannot currently synchronize with conferencing credentials.
- **Not set** — This option is selected for Phone mode deployments.

Step 5 Click **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_UseCredentialsForm parameter.

Before you begin

Configure Retrieval and Redirection, on page 29

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.

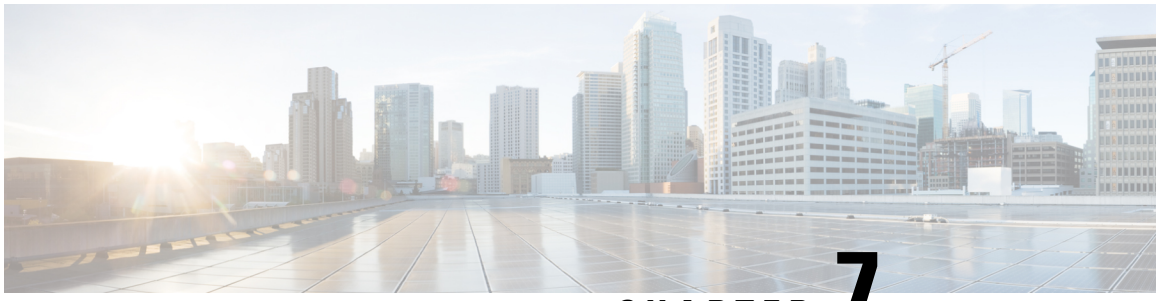
The user's instant messaging and presence credentials match the user's voicemail credentials. As a result, users do not need to specify their voicemail credentials in the client user interface.

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 7

Configure Webex Conferencing

Configure Conferencing for an On-Premises Deployment

When you implement an on-premises deployment for Cisco Jabber, you can configure conferencing on-premises with Webex Meetings Server, or in the cloud in Webex Meetings Center.

Configure On-Premises Conferencing using Webex Meetings Server

Procedure

	Command or Action	Purpose
Step 1	Authenticate Webex Meetings Server, on page 35.	
Step 2	Add Webex Meetings Server on Cisco Unified Communications Manager, on page 36.	

Authenticate Webex Meetings Server

Procedure

To authenticate with Webex Meetings Server, complete one of the following options:

- Configure single sign-on (SSO) with Webex Meetings Server to integrate with the SSO environment. In this case, you do not need to specify credentials for users to authenticate with Webex Meetings Server

- Set a credentials source on Cisco Unified Communications Manager. If the users' credentials for 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 Webex Meetings Server with the users' credential source.
- Instruct users to manually enter credentials in the client.

What to do next

Add Webex Meetings Server on Cisco Unified Communications Manager, on page 36

Add Webex Meetings Server on Cisco Unified Communications Manager

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

Before you begin

Authenticate with 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.
- **Hostname/IP Address** — Enter the site URL for Webex MeetingsServer. This URL is case sensitive and must match the case that was configured for the site URL in Webex Meetings Server.
- **Port** — Leave the default value.
- **Protocol** — Select **HTTPS**.

Step 5 To use 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 Webex Meetings Server to a Service Profile, on page 37

Add the Webex Meetings Server to a Service Profile

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

Before you begin

Create a service profile.

Add Webex Meetings Server on Cisco Unified Communications Manager, on page 36

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 Webex Meetings Server.

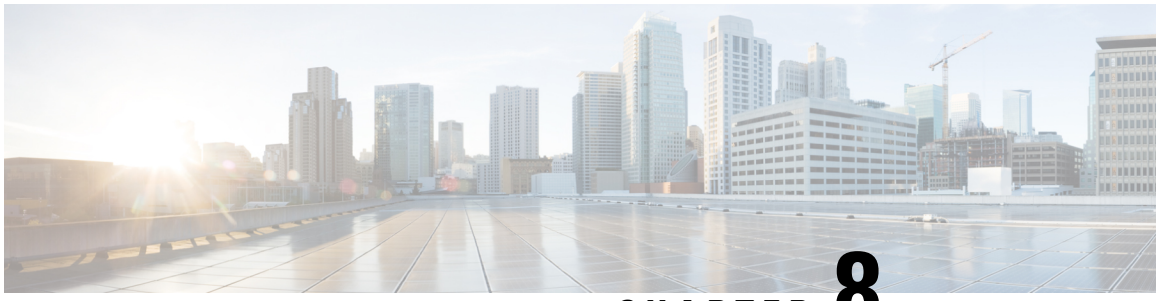
Step 4 From the **Server Certificate Verification** drop-down list, select the appropriate value.

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 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 Webex Meetings Server credentials.
- **Voicemail**—Select this option if the Cisco Unity Connection credentials for the user match their Webex Meetings Server credentials.

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

Step 6 Select **Save**.



CHAPTER 8

Configure CTI Service

Configure CTI Service Workflow

The CTI Service provides Jabber with the location of the UDS device service. The UDS device service provides Jabber with the devices that are associated with the user, for example: a softphone or deskphone devices.

Procedure

	Command or Action	Purpose
Step 1	Add a CTI Service, on page 39	Create a CTI UC service to provide Jabber with the location of the CTI service.
Step 2	Apply a CTI Service, on page 40	Apply the CTI UC service to the service profile.

Add a CTI Service

The CTI service provides Jabber with the address of the UDS device service. The UDS device service provides a list of devices associated with the user.

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 CTI service as follows:

a) Specify a name for the service in the **Name** field.

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

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

Enter the address in the form of a hostname, IP address, or fully qualified domain name (FQDN). This value corresponds to the Unified CM publisher that's running the CTI Manager service. You'll create a second service for the subscriber.

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

Step 7 Select **Save**.

What to do next

Create a second CTI service for the Unified CM subscriber.

Add the CTI service to your service profile.

Apply a CTI Service

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

Before you begin

- Create a service profile if none already exists or if you require a separate service profile for CTI.
- Add CTI services for the Unified CM publisher and subscriber.

Procedure

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

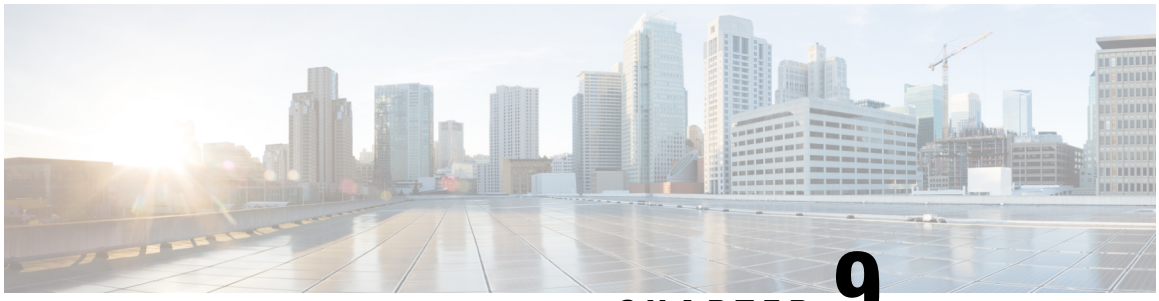
Step 2 Select **User Management** > **User Settings** > **Service Profile**.
Find and List Service Profiles window opens.

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

Step 4 Navigate to **CTI Profile** section, and select up to three services from the following drop-down lists:

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

Step 5 Select **Save**.



CHAPTER 9

Users

LDAP Synchronization Overview

Lightweight Directory Access Protocol (LDAP) synchronization helps you to provision and configure end users for your system. During LDAP synchronization, the system imports a list of users and associated user data from an external LDAP directory into the Cisco Unified Communications Manager database. In addition, you can configure a regular synchronization schedule to pick up any changes in your employee data.

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`.

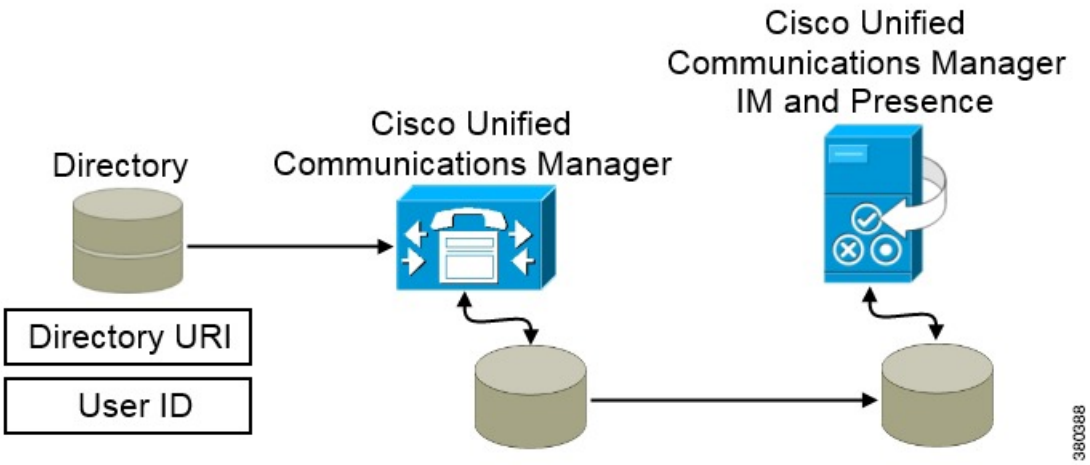
Important If the attribute for the user ID is other than `sAMAccountName` and you are using the default IM address scheme in Cisco Unified Communications Manager IM and Presence Service, you must specify the attribute as the value for the parameter in your client configuration file as follows:

The CDI 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.

- **Directory URI**—You should specify a value for the directory URI if you plan to:
  - Enable URI dialing in Cisco Jabber.
  - Use the directory URI address scheme on Cisco Unified Communications Manager IM and Presence Service version 10 and higher.



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

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

Configure Users Workflow

Procedure

	Command or Action	Purpose
Step 1	Activate Services, on page 45	Turn on the required services to synchronize user settings from your LDAP directory with Cisco Unified Communications Manager and with the IM and Presence Service.
Step 2	Enable LDAP Directory Synchronization, on page 46	Allow Cisco Unified Communications Manager to synchronize user settings from your LDAP directory. Select the attribute from your LDAP directory that you want Cisco Unified Communications Manager to synchronize with for the **User ID**.
Step 3	Configure LDAP Directory Sync, on page 46	Configure Cisco Unified Communications Manager to synchronize with your LDAP directory. Set up an automatic synchronization schedule, map the standard user fields, and assign the imported users to access control groups.
Step 4	Authentication options, on page 48	Select your authentication option: • Enable SAML SSO in the client. • Authenticate with the LDAP server.
Step 5	Perform Synchronization , on page 51	Synchronize Cisco Unified Communications Manager with the directory server.
Step 6	Associate Service Profile to User, on page 51	Associate the service profile to the users.
Step 7	Prepopulate Contact Lists in Bulk, on page 53	Populate the contact list for your users.

Activate Services

You must activate the following services before you can integrate with your corporate LDAP server:

- Cisco DirSync service—you must activate this service if you want to synchronize end user settings from a corporate LDAP directory.
- (Cisco Unified Communications Manager IM and Presence Service) Cisco Sync Agent service—this service keeps data synchronized between the IM and Presence Service node and Cisco Unified Communications Manager. When you perform the synchronization with your directory server, Cisco Unified Communications Manager then synchronizes the data with IM and Presence Service.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.
Step 2 From the **Server** drop-down list box, choose the publisher node.
Step 3 Under **Directory Services**, click the **Cisco DirSync** radio button.
Step 4 Click **Save**.
Step 5 Choose **Tools** > **Control Center - Network Services**.
Step 6 From the **Server** drop-down list box, choose the IM and Presence Service node.
Step 7 Under **IM and Presence Services**, click the **Cisco Sync Agent** radio button.
Step 8 Click **Save**.

Enable LDAP Directory Synchronization

Perform this procedure if you want to configure Cisco Unified Communications Manager to synchronize end user settings from a corporate LDAP directory.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP System**.

The **LDAP System Configuration** window opens.

Step 2 Check the **Enable Synchronizing from LDAP Server** check box to allow Cisco Unified Communications Manager to import users from your LDAP directory.
Step 3 From the **LDAP Server Type** drop-down list box, choose the type of LDAP directory server that your company uses.
Step 4 From the **LDAP Attribute for User ID** drop-down list box, choose the attribute from your corporate LDAP directory that you want Cisco Unified Communications Manager to synchronize with for the **User ID** field in the **End User Configuration** window.

This value is required for the default IM address scheme and for users to sign in. The default value is `sAMAccountName`.

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.

Step 5 Click **Save**.

Configure LDAP Directory Sync

Use this procedure to configure Cisco Unified Communications Manager to synchronize with an LDAP directory. LDAP directory synchronization allows you to import end user data from an external LDAP directory

into the Cisco Unified Communications Manager database such that it displays in **End User Configuration** window. You can set up a sync schedule so that updates made to the LDAP directory propagate to Cisco Unified Communications Manager regularly.

For help with the fields and their descriptions, refer to the online help.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Directory**.

Step 2 Perform one of the following steps:

- Click **Find** and select an existing LDAP directory.
- Click **Add New** to create a new LDAP directory.

Step 3 In the **LDAP Configuration Name** text box, assign a unique name to the LDAP directory.

Step 4 In the **LDAP Manager Distinguished Name** field, enter a user ID with access to the LDAP directory server.

Step 5 Enter and confirm the password details.

Step 6 In the **LDAP Directory Synchronization Schedule** fields, create a schedule that Cisco Unified Communications Manager uses to synchronize data with the external LDAP directory.

Step 7 Complete the **Standard User Fields to be Synchronized** section. For each End User field, choose an LDAP attribute. The synchronization process assigns the value of the LDAP attribute to the end user field in Cisco Unified Communications Manager.

a) Select one of the following LDAP attributes from the **Directory URI** drop-down list:

- **msRTCSIP-primaryuseraddress**—This attribute is populated in the AD when Microsoft Lync or Microsoft OCS are used. This is the default attribute.
- **mail**

Step 8 To assign the imported end users to an access control group that is common to all the imported end users, do the following:

a) Click **Add to Access Control Group**.
b) In the popup window, click the corresponding check box for each access control group that you want to assign to the imported end users.
c) Click **Add Selected**.

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

- **Standard CCM End Users**
- **Standard CTI Enabled**—This option is used for desk phone control.

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

Certain phone models require additional control groups, as follows:

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

Note For Cisco Unified Communications Manager 9.x, you must assign end users to access control groups on the **End User Configuration** window (**User Management** > **End User**).

Step 9 In the **LDAP Server Information** area, enter the hostname or IP address of the LDAP server.

Step 10 If you want to create a secure connection to the LDAP server, check the **Use TLS** check box.

Step 11 Click **Save**.

Authentication options

Authenticate with the LDAP Server

Perform this procedure if you want to enable LDAP authentication so that end user passwords are authenticated against the password that is assigned in the company LDAP directory. LDAP authentication gives system administrators the ability to assign an end user a single password for all company applications. This configuration applies to end user passwords only and does not apply to end user PINs or application user passwords. When users sign in to the client, the presence service routes that authentication to Cisco Unified Communications Manager. Cisco Unified Communications Manager then sends 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**.

Configure the Client to Authenticate with the LDAP Server

If you are configuring authentication to use LDAP credentials, you must also configure the client.

Procedure

Step 1 Update the `jabber-config.xml` file with the LDAP_UseCredentialsFrom parameter.

Example:

<LDAP_UseCredentialsFrom>*CUCM*</LDAP_UseCredentialsFrom>

Step 2 If the LDAP server is deployed in a different domain than the domain where Cisco Unified Communications Manager IM and Presence service and Cisco Unified Communications Manager are deployed, configure the LDAPUserDomain parameter. If you don't configure this parameter, by default it uses the value for the PresenceDomain mandatory parameter.

Example:

<LdapUserDomain>*example.com*</LdapUserDomain>

Authenticate with Anonymous Binding

You can configure anonymous binding as a means of authenticating users to the LDAP server. Using anonymous binding prevents users from entering credentials on the **Accounts** tab of the **Options** menu in Jabber.

Procedure

In the jabber-config.xml file, configure the LdapAnonymousBinding parameter with true or false values.

Example:

<LdapAnonymousBinding>true</LdapAnonymousBinding>

For more information on configuring this parameter, see the *Parameters Reference Guide for Cisco Jabber*.

Manual User Authentication

You can set up service authentication where users manually enter their own credentials in the Jabber client for the required services.

Users are manually prompted to enter their own credentials when no service authentication is configured (for example, in service profiles or on the LDAP server).

Users enter their credentials on the **Accounts** tab of the **Options** menu in Jabber.

Enable SAML SSO in the Client

Before you begin

- Enable SSO on Cisco Unified Communications Applications 10.5.1 Service Update 1—For information about enabling SAML SSO on this service, read the *SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 10.5*.
- Enable SSO on Cisco Unity Connection version 10.5—For more information about enabling SAML SSO on this service, read *Managing SAML SSO in Cisco Unity Connection*.

Procedure

Step 1 Deploy certificates on all servers so that the certificate can be validated by a web browser, otherwise users receive warning messages about invalid certificates. For more information about certificate validation, see *Certificate Validation*.

Step 2 Ensure Service Discovery of SAML SSO in the client. The client uses standard service discovery to enable SAML SSO in the client. Enable service discovery by using the following configuration parameters: ServicesDomain, VoiceServicesDomain, and ServiceDiscoveryExcludedServices. For more information about how to enable service discovery, see *Configure Service Discovery for Remote Access*.

Step 3 Define how long a session lasts.

A session is comprised of cookie and token values. A cookie usually lasts longer than a token. The life of the cookie is defined in the Identity Provider, and the duration of the token is defined in the service.

Step 4 When SSO is enabled, all Cisco Jabber users sign in using SSO by default. Administrators can change this on a user-by-user basis so that certain users do not use SSO and instead sign in with their Cisco Jabber username and password. To disable SSO for a Cisco Jabber user, set the value of the SSO_Enabled parameter to FALSE.

If you have configured Cisco Jabber not to ask users for their email address, their first sign in to Cisco Jabber may be non-SSO. In some deployments, the parameter ServicesDomainSsoEmailPrompt needs to be set to ON. This ensures that Cisco Jabber has the information required to perform a first-time SSO sign in. If users signed in to Cisco Jabber previously, this prompt is not needed because the required information is available.

Certificate-Based SSO Authentication for Mobile Clients

This configuration is only necessary for Cisco Jabber for iPhone and iPad. Cisco Jabber for Android requires no similar configuration.

To enable this feature, configure the same settings for SSO Login Behavior for iOS in both Cisco Unified Communications Manager and Cisco Unity Connection.

With Expressway for Mobile and Remote Access, configure Jabber for iPhone and iPad clients to use the embedded Safari browser in the VCS Expressway admin console. For more information, see the Cisco Expressway installation guides at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.html.

You cannot enable the Common Identity (CI) for Webex Messenger. To enable embedded Safari to connect to voicemail using client certificate-based SSO authentication, you must disable CI.

Configuring Certificate-Based SSO Authentication on Cisco Unified Communications Manager

This configuration is only supported on Cisco Unified Communications Manager 11.5 or later.

Procedure

Step 1 In Cisco Unified CM Administration, go to **System** > **Enterprise Parameters**.

Step 2 In the **SSO configuration** section, scroll down to **SSO Login Behavior for iOS** and choose **Use native browser**.

Step 3 Select **Save**

Configuring Certificate-Based SSO Authentication on Cisco Unity Connection

Procedure

Step 1 In Cisco Unity Connection Administration, go to **System Settings** > **Enterprise Parameters**.

Step 2 In the **SSO Configuration** section, scroll down to **SSO Login Behavior for iOS** and choose **Use native browser**.

Step 3 Select **Save**.

Perform Synchronization

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

Procedure

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

Step 2 Click **Find** and select the LDAP directory that you configured.

The **LDAP Directory** window opens.

Step 3 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 IM and Presence Service database.

Associate Service Profile to User

Associate Service Profile to Individual Users

Associate service profiles with 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.

Step 6 Select **Home Cluster**.

Step 7 For Phone mode deployments, ensure the **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)** option is not selected.

For all other deployments, check the **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)** checkbox.

Step 8 Select your service profile from the **UC Service Profile** drop-down list.

Important Cisco Unified Communications Manager release 9.x only—If the user has only instant messaging and presence capabilities (IM only), select **Use Default**. Cisco Unified Communications Manager release 9.x applies the default service profile regardless of what you select from the **UC Service Profile** drop-down list.

Step 9 Select **Save**.

Associate Service Profile to Users in Bulk

Add the 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 For Phone mode deployments, disable instant messaging and presence, check one check box for **Enable User for Unified CM IM and Presence**.

For all other deployments, select both check boxes for **Enable User for Unified CM IM and Presence**.

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 release 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 release 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**.

Prepopulate Contact Lists in Bulk

You can pre-populate user contact lists with the Bulk Administration Tool (BAT).

In this way you can prepopulate 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.

Procedure

	Command or Action	Purpose
Step 1	Create a CSV file that defines the contact list you want to provide to users.	Create CSV to Import Contact Lists, on page 53
Step 2	Use the BAT to import the contact list in bulk to a set of users.	Upload Contact List Using BAT, on page 54

Create CSV to Import Contact Lists

Structure of the CSV File

The CSV file must have the following format:

<User ID>, <User Domain>, <Contact ID>, <Contact Domain>, <Nickname>, <Group Name>

Sample CSV file entry:

```
userA,example.com,userB,example.com,buddyB,General
```

Table 1: Description of Input File Parameters

Parameter	Description
User ID	Required parameter. The user ID of the IM and Presence Service user. It can have a maximum 132 characters.
User Domain	Required parameter. The Presence domain of the IM and Presence Service user. It can have a maximum of 128 characters.

Parameter	Description
Contact ID	Required parameter. The user ID of the contact list entry. It can have a maximum of 132 characters.
Contact Domain	Required parameter. The Presence domain of the contact list entry. The following restrictions apply to the format of the domain name: • Length must be less than or equal to 128 characters • Contains only numbers, upper- and lowercase letters, and hyphens (-) • Must not start or end with hyphen (-) • Length of label must be less than or equal to 63 characters • Top-level domain must be characters only and have at least two characters
Nickname	The nickname of the contact list entry. It can have a maximum of 255 characters.
Group Name	Required parameter. The name of the group to which the contact list entry is to be added. It can have a maximum of 255 characters.

Upload Contact List Using BAT

Before you begin

Create a CSV file with contacts.

Procedure

Step 1 Open the **Cisco Unified CM IM and Presence Administration** interface.
Step 2 Select **Bulk Administration** > **Upload/Download Files**.
Step 3 Select **Add New**.
Step 4 Select **Choose File** to locate and choose the CSV file.
Step 5 Choose **Contact Lists** as the target.
Step 6 Choose **Import Users' Contacts - Custom File** as the Transaction Type.
Step 7 Select **Save** to upload the file.

Configure Authentication for UDS Contact Search

Cisco Jabber supports authenticated directory queries when searching for contacts. The authentication is configured on Cisco Unified Communications Manager release 11.5 or later.

Procedure

Step 1 コマンドライン インターフェイスにログインします。

Step 2 **utils contactsearchauthentication status** コマンドを実行し、このノードの連絡先検索の認証の設定を確認します。

Step 3 連絡先検索の認証の設定が必要な場合、

- 認証を有効にするには、**utils contactsearchauthentication enable** コマンドを実行します。
- 認証を無効にするには、**utils contactsearchauthentication disable** コマンドを実行します。

Step 4 すべての のクラスタノードに対してこの手順を繰り返します。

Note 変更を有効にするには、電話をリセットする必要があります。

Enable Extended UDS Contact Source

Before you begin

Extended UDS contact search is only available on Cisco Unified Communications Manager release 11.5(1) or later.

Procedure

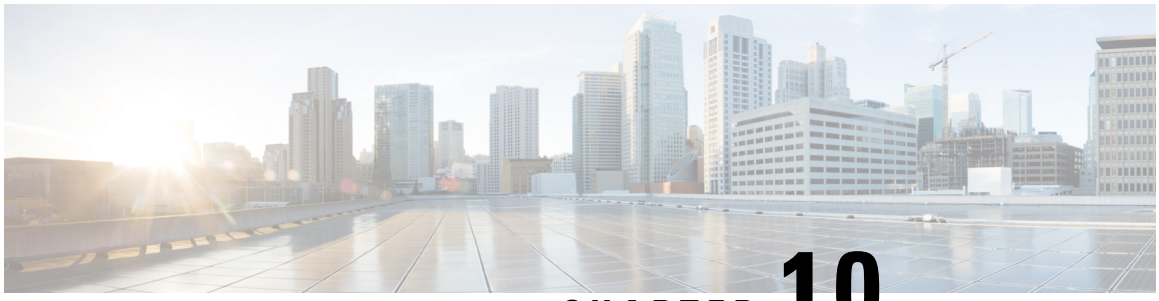
Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **System** > **LDAP** > **LDAP Search**

Step 3 To enable user searches to be performed using an enterprise LDAP directory server, check the **Enable user search to Enterprise Directory Server** check box.

Step 4 Configure the fields in the **LDAP Search Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 Select **Save**.



CHAPTER 10

Configure Softphone

Create Softphones Workflow

Procedure

	Command or Action	Purpose
Step 1	Create and Configure Cisco Jabber Devices, on page 57	Create at least one device for every user who accesses Cisco Jabber. Generate an authentication string to provide to users.
Step 2	Add a directory number to the device, on page 61	For each device you create, add a directory number.
Step 3	Associate Users with Devices, on page 61	Associate users with devices.
Step 4	Create Mobile SIP Profiles, on page 62.	Complete this task if you have Cisco Unified Communications Manager release 9 and plan to configure devices for mobile clients.
Step 5	Configure the Phone Security Profile, on page 64	Complete this task to set up secure phone capabilities for all devices.

Create and Configure Cisco Jabber Devices

Create at least one device for every user that accesses Cisco Jabber. A user can have multiple devices.

Note Users can only remove participants from a conference call when using the softphone (CSF) device for calls.

Before you begin

- Install COP files.
- Create SIP profiles if you have Cisco Unified Communications Manager release 9 or earlier and plan to configure devices for mobile clients.
- Create the Phone Security Profile if you plan to set up secure phone capabilities for all devices.
- If you are using CAPF enrollment, for Cisco Unified Communications Manager release 10 or later, ensure that the Cisco Certificate Authority Proxy Function (CAPF) service parameters value for **Certificate Issuer to Endpoint** is **Cisco Certificate Authority Proxy Function**. This is the only option supported by Cisco Jabber. For information on configuring the CAPF service parameter see the *Update CAPF Service Parameters* topic in the Cisco Unified Communications Manager Security Guides.
- Before you create TCT devices, BOT devices, or TAB devices for Cisco Jabber for mobile users, specify the organization top domain name to support registration between Cisco Jabber and the Cisco Unified Communications Manager. In Unified CM Administration interface, select **System** > **Enterprise Parameters**. Under the Clusterwide Domain Configuration section, enter the organization top domain name. For example, cisco.com. This top domain name is used by Jabber as the DNS domain of the Cisco Unified Communications Manager servers for phone registration. For example, CUCMServer1@cisco.com.

Procedure

Step 1 Log in to the **Cisco Unified CM Administration** interface.

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

Step 3 Select **Add New**.

Step 4 From the **Phone Type** drop-down list, select the option that is applicable to the device type you are configuring and then select **Next**.

For Jabber users, you can only create one type of device per user although you can create multiple devices for each user. For example, you can create one tablet device and one CSF device but not two CSF devices.

- **Cisco Unified Client Services Framework**—Select this option to create a CSF device for Cisco Jabber for Mac or Cisco Jabber for Windows.
- **Cisco Dual Mode for iPhone**—Select this option to create a TCT device for an iPhone.
- **Cisco Jabber for Tablet**—Select this option to create a TAB device for an iPad or an Android tablet or for Chromebooks.
- **Cisco Dual Mode for Android**—Select this option to create a BOT device for an Android device.

Step 5 From the **Owner User ID** drop-down list, select the user for whom you want to create the device.

For the **Cisco Unified Client Services Framework** option in a Phone mode deployment, ensure that **User** is selected.

Step 6 In the **Device Name** field, use the applicable format to specify a name for the device:

If You Select	Required Format
Cisco Unified Client Services Framework	• Valid characters: a–z, A–Z, 0–9. • 15-character limit.
Cisco Dual Mode for iPhone	• The device name must begin with *TCT*. For example, if you create a TCT device for user, Tanya Adams, whose username is tadams, enter **TCTTADAMS**. • Must be uppercase. • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-). • 15-character limit.
Cisco Jabber for Tablet	• The device name must begin with *TAB*. For example, if you create a TAB device for user, Tanya Adams, whose username is tadams, enter **TABTADAMS**. • Must be uppercase. • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-). • 15-character limit.
Cisco Dual Mode for Android	• The device name must begin with *BOT*. For example, if you create a BOT device for user, Tanya Adams, whose username is tadams, enter **BOTTADAMS**. • Must be uppercase. • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-). • 15-character limit.

Step 7 If you are using CAPF enrollment, complete the following steps to generate an authentication string:

a. Users can use the authentication string that you can provide to access their devices and securely register to Cisco Unified Communications Manager, navigate to the **Certification Authority Proxy Function (CAPF) Information** section.

b. From the **Certificate Operation** drop-down list, select **Install/Upgrade**.

c. From the **Authentication Mode** drop-down list, select **By Authentication String** or **By Null String**. Using the CAPF Authentication mode **By Null String** with JVDI and Jabber for Windows CSF devices is not supported. It causes Jabber registration with Cisco Unified Communications Manager to fail.

d. Click **Generate String**. The Authentication String autopopulates with a string value. This is the string that you will provide to end users.

e. From the **Key Size (Bits)** drop-down list, select the same key size that you set in the phone security profile.

f. In the **Operation Completes By** fields, specify an expiration value for the authentication string or leave as default.

g. If you are using a group configuration file, specify it in the **Cisco Support Field** of the **Desktop Client Settings.** Cisco Jabber does not use any other settings that are available on the **Desktop Client Settings**.

Step 8 Select **Save**.

Step 9 Click **Apply Config**.

What to do next

Add a Directory Number to the device.

Provide Users with Authentication Strings

If you are using CAPF enrollment to configure secure phones, then you must 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.

Add a directory number to the device

After you create and configure each device, you must add a directory number to the device. This topic provides instructions on adding directory numbers using the **Device** > **Phone** menu option.

Before you begin

Create a device.

Procedure

Step 1 Locate the **Association Information** section on the **Phone Configuration** window.
Step 2 Click **Add a new DN**.
Step 3 In the **Directory Number** field, specify a directory number.
Step 4 In the **Users Associated with Line** section, click **Associate End Users**.
Step 5 In the **Find User where** field, specify the appropriate filters and then click **Find**.
Step 6 From the list that appears, select the applicable users and click **Add Selected**.
Step 7 Specify all other required configuration settings as appropriate.
Step 8 Select **Apply Config**.
Step 9 Select **Save**.

Associate Users with Devices

On Cisco Unified Communications Manager version 9.x only, when the client attempts to retrieve the service profile for the user, it first gets the device configuration file from Cisco Unified Communications Manager. The client can then use the device configuration to get the service profile that you applied to the user.

For example, you provision Adam McKenzie with a CSF device named `CSFAKenzi`. The client retrieves `CSFAKenzi.cnf.xml` from Cisco Unified Communications Manager when Adam signs in. The client then looks for the following in `CSFAKenzi.cnf.xml`:

```
<userId  serviceProfileFile="identifier.cnf.xml">amckenzi</userId>
```

For this reason, if you are using Cisco Unified Communications Manager version 9.x, you should do the following to ensure that the client can successfully retrieve the service profiles that you apply to users:

- Associate users with devices.
- Set the **User Owner ID** field in the device configuration to the appropriate user. The client will retrieve the Default Service Profile if this value is not set.

Before you begin

Note Do not associate a CSF to multiple users if you intend to use different service profiles for these users.

Procedure

Step 1 Associate users with devices.

a) Open the **Unified CM Administration** interface.
b) Select **User Management** > **End User**.
c) Find and select the appropriate user.
The **End User Configuration** window opens.
d) Select **Device Association** in the **Device Information** section.
e) Associate the user with devices as appropriate.
f) Return to the **End User Configuration** window and then select **Save**.

Step 2 Set the **User Owner ID** field in the device configuration.

a) Select **Device** > **Phone**.
b) Find and select the appropriate device.
The **Phone Configuration** window opens.
c) Locate the **Device Information** section.
d) Select **User** as the value for the **Owner** field.
e) Select the appropriate user ID from the **Owner User ID** field.
f) Select **Save**.

Create Mobile SIP Profiles

This procedure is required only when you use Cisco Unified Communication Manager release 9 and are configuring devices for mobile clients. Use the default SIP profile provided for desktop clients. Before you create and configure devices for mobile clients, you must create a SIP profile that allows Cisco Jabber to stay connected to Cisco Unified Communication Manager while Cisco Jabber runs in the background.

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

Procedure

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

Step 2 Select **Device** > **Device Settings** > **SIP Profile**.

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

Step 3 Do one of the following to create a new SIP profile:

- Find the default SIP profile and create a copy that you can edit.
- Select **Add New** and create a new SIP profile.

Step 4 In the new SIP profile, set the following values:

- **Timer Register Delta** = 120
- **Timer Register Expires** = 720
- **Timer Keep Alive Expires** = 720
- **Timer Subscribe Expires** = 21600
- **Timer Subscribe Delta** = 15

Step 5 Select **Save**.

Setting up System SIP Parameters

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

Before you begin

This configuration is only for mobile clients.

Cisco Jabber must be running to receive work calls.

Procedure

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

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

Step 3 Select the node.

Step 4 Select the **Cisco CallManager (Active)** service.

Step 5 Scroll to the **Clusterwide Parameters (System - Mobility)** section.

Step 6 Increase the **SIP Dual Mode Alert Timer** value to 10000 milliseconds.

Step 7 Select **Save**.

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

Configure the Phone Security Profile

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

If you enable secure phone capabilities for users, device connections to Cisco Unified Communications Manager are secure. However, calls with other devices are secure only if both devices have a secure connection.

Before you begin

- Configure the Cisco Unified Communications Manager security mode using the Cisco CTL Client. At minimum, select mixed mode security.

  For instructions on how to configure mixed mode with the Cisco CTL Client, see the Cisco Unified Communications Manager Security Guide.

- For conference calls, ensure that the conferencing bridge supports 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.

- If your deployment uses Unified Communications Manager Release 12.5 or later, we recommend using SIP OAuth with Cisco Jabber. For details, see the chapter on SIP OAuth in the *Feature Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Procedure

Step 1 In **Cisco Unified Communications Manager**, select **System** > **Security** > **Phone Security Profile**.

Step 2 Select **Add New**.

Step 3 From the **Phone Type** drop-down list, select the option that is applicable to the device type you are configuring and then select **Next**.

- **Cisco Unified Client Services Framework**—Select this option to create a CSF device for Cisco Jabber for Mac or Cisco Jabber for Windows.
- **Cisco Dual Mode for iPhone**—Select this option to create a TFT device for an iPhone.
- **Cisco Jabber for Tablet**—Select this option to create a TAB device for an iPad or an Android tablet or for Chromebooks.
- **Cisco Dual Mode for Android**—Select this option to create a BOT device for an Android device.
- **CTI Remote Device**—Select this option to create a CTI remote device.

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

Step 4 In the **Name** field of the **Phone Security Profile Configuration** window, specify a name for the phone security profile.

Step 5 For **Device Security Mode**, select one of the following options:

- **Authenticated**—The SIP connection is over TLS using NULL-SHA encryption.
- **Encrypted**—The SIP connection is over TLS using AES 128/SHA encryption. The client uses Secure Real-time Transport Protocol (SRTP) to offer encrypted media streams.

Step 6 For **Transport Type**, leave the default value of **TLS**.

Step 7 Select the **TFTP Encrypted Config** check box to encrypt the device configuration file that resides on the TFTP server.

Note For a TCT/BOT/Tablet device, do not select the TFTP Encrypted Config check box here. For Authentication Mode, select By Authentication String or Null String.

Step 8 For **Authentication Mode**, select **By Authentication String** or **By Null String**.

Note Using the CAPF Authentication mode **By Null String** with JVDI and Jabber for Windows CSF devices is not supported. It causes Jabber registration with Cisco Unified Communications Manager to fail.

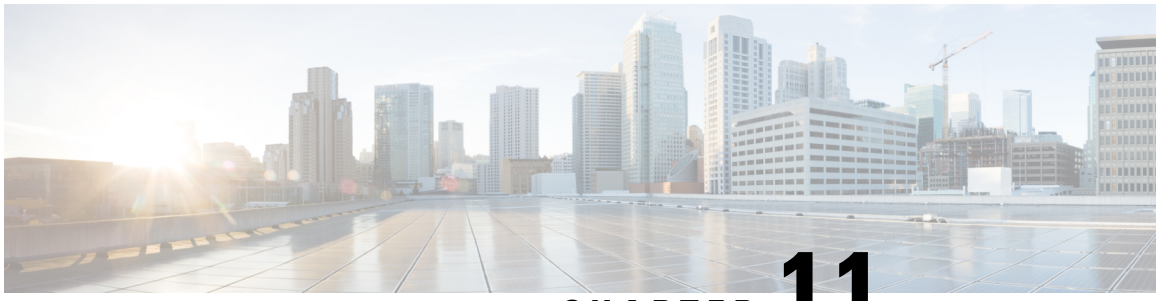
Step 9 For **Key Size (Bits)**, select the appropriate key size for the certificate. Key size refers to the bit length of the public and private keys that the client generates during the CAPF enrollment process.

The Cisco Jabber clients were tested using authentication strings with 1024-bit length keys. The Cisco Jabber clients require more time to generate 2048-bit length keys than 1024-bit length keys. As a result, if you select 2048, expect it to take longer to complete the CAPF enrollment process.

Step 10 For **SIP Phone Port**, leave the default value.

The port that you specify in this field takes effect only if you select **Non Secure** as the value for **Device Security Mode**.

Step 11 Click **Save**.



CHAPTER 11

Configure Deskphone Control

Prerequisites

The Cisco CTIManager service must be running in the Cisco Unified Communications Manager cluster.

Configure Desk Phone Control Workflow

Procedure

	Command or Action	Purpose
Step 1	Create Desk Phone Devices, on page 68	Create a desk phone device.
Step 2	Enable Device for CTI, on page 69	Allows Cisco Jabber desktop clients to control the desk phone of the user.
Step 3	Configure Desk Phone Video, on page 69.	Let users receive video transmitted to their desk phone devices on their computers through the client.
Step 4	Add Directory Number to the Device for Desktop Applications, on page 71.	Assign a Directory number to the device.
Step 5	Enable Video Rate Adaptation, on page 71	The client uses video rate adaptation to negotiate optimum video quality.

Create Desk Phone Devices

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

Before you begin

Create software phone 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 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.

Enable Device for CTI

If you want Cisco Jabber desktop clients to be able to control the desk phone of the user, you must select the **Allow Control of Device from CTI** option when you create the device for the user.

Procedure

Step 1 In Cisco Unified CM Administration, click **Device** > **Phone** and search for the phone.

Step 2 In the **Device Information** section, check **Allow Control of Device from CTI**.

Step 3 Click **Save**.

Configure Desk Phone Video

Desk phone video capabilities let you receive the video signal on your laptop and the audio signal on your desk phone. Physically connect your computer to the desk phone through the computer port for the client to establish a connection to the Jabber client. You cannot use this feature with a wireless connection to your desk phone.

Note If you have both wireless and wired connections available, configure Microsoft Windows to not prioritize wireless connections over wired connections. See Microsoft's *An explanation of the Automatic Metric feature for Internet Protocol routes* for more information.

First, download and install Jabber Desk Phone Video Services Interface from Cisco.com. Jabber Desk Phone Video Services Interface provides the Cisco Discover Protocol (CDP) driver. CDP enables the client to:

- Discover the desk phone.
- Establish and maintain a connection to the desk phone using the Cisco Audio Session Tunnel (CAST) protocol.

Desk Phone Video Considerations

Review the following considerations and limitations before you set up the desk phone video feature:

- You cannot have more than one video device connected with CAST. You cannot use a desk phone with a built-in camera with this feature. If your desk phone has a local USB camera, remove it before using this feature.
- You cannot use this feature with devices that do not support CTI.
- You cannot use both video screen sharing, using the BFCP protocol, and 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 a video signal 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 you start a call from a desk phone's keypad, the call starts as an audio call on the desk phone. Jabber then escalates the call to video. For this reason, you cannot make video calls to devices that do not support the escalation, such as H.323 endpoints. To use this feature with devices that do not support escalation, begin calls from the Jabber client.
- A compatibility issue exists with Cisco Unified IP Phones that use firmware version SCCP45.9-2-1S. Upgrade your firmware to version SCCP45.9-3-1 to use this feature.
- Some antivirus or firewall applications, such as Symantec EndPoint Protection, block inbound CDP packets. This blockage disables desk phone video. Configure your antivirus or firewall application to allow inbound CDP packets.

  See the following Symantec technical document for more details about this issue: *Cisco IP Phone version 7970 and Cisco Unified Video Advantage is Blocked by Network Threat Protection*.
- Do not select the **Media Termination Point Required** check box on the SIP trunk configuration for Cisco Unified Communications Manager (Unified CM). That setting disables desk phone video.

Procedure

Step 1 Physically connect your computer to the computer port on your desk phone.

Step 2 Enable the desk phone for video in Unified CM.

Step 3 Install Jabber Desk Phone Video Services Interface on your computer.

Troubleshooting Desk Phone Video

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 Jabber Desk Phone Video Services Interface from the Services tab of the Windows Task Manager.
6. Restart the client.

Add Directory Number to the Device for Desktop Applications

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

Procedure

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

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

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

Step 4 Specify all other required configuration settings as appropriate.

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

a) Locate the **Users Associated with Line** section.
b) Select **Associate End Users**.
c) Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
d) Select the appropriate users from the list.
e) Select **Add Selected**.

The selected users are added to the voicemail profile.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.

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

Enable Video Rate Adaptation

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

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

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

Enable RTCP on Common Phone Profiles

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

Note RTCP is an integral component of Jabber Telephony services. Jabber will continue to send RTCP packets even when disabled.

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**.

Configure User Associations

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

Before you begin

Create and configure Cisco Jabber devices.

Procedure

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

Step 2 Select **User Management** > **End User**.

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

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

Step 4 Select the appropriate user from the list.

The **End User Configuration** window opens.

Step 5 Locate the **Service Settings** section.

Step 6 Select 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. Jabber only supports a single softphone association per device type. For example, only one TCT, BOT, CSF, and TAB device can be associated with a 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.

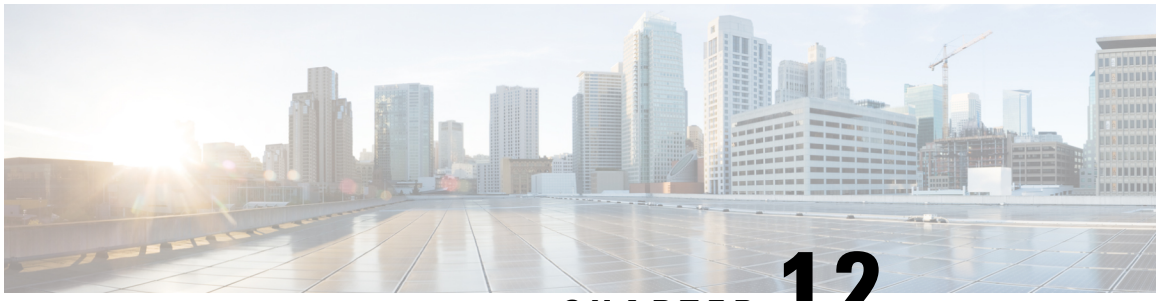
Certain phone models require additional control groups, as follows:

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

Step 16 Select **Add Selected**.

The **Find and List Access Control Groups** window closes.

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



CHAPTER 12

Configure Extend and Connect

Configure Extend and Connect Workflow

Procedure

	Command or Action	Purpose
Step 1	Enable User Mobility, on page 75	Enable users mobility and you can assign users as owners of CTI remote devices.
Step 2	Create CTI Remote Devices, on page 76	Create CTI remote devices, these virtual devices monitor and have call control over a user's remote destination.
Step 3	Add a Remote Destination, on page 77	(Optional) If you plan to provision users with dedicated CTI remote devices, add a remote destination in Cisco Unified Communications Manager.

Enable User Mobility

This task is only for desktop clients.

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

Before you begin

This task is applicable only if:

- You plan to assign Cisco Jabber for Mac or Cisco Jabber for Windows users to CTI remote devices.

- You have Cisco Unified Communication Manager release 9.x and later.

Procedure

Step 1 Select **User Management** > **End User**.

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

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

Step 3 Select the user from the list.

The **End User Configuration** window opens.

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

Step 5 Select **Enable Mobility**.

Step 6 Select **Save**.

Create CTI Remote Devices

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

Procedure

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

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

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

Step 3 Select **Add New**.

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

The **Phone Configuration** window opens.

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

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

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 System Configuration Guide for Cisco Unified Communications Manager documentation for more information.

Step 9 Select **Save**.

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

Add 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.

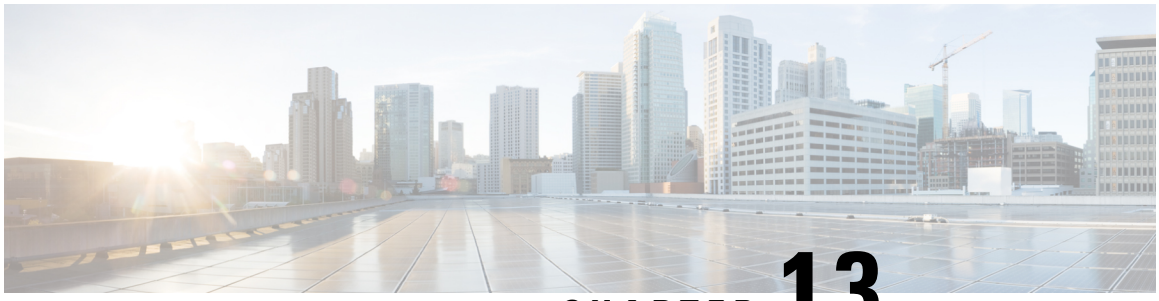
When users select a remote destination in the client, it displays as the value of **Active Remote Destination**.

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.

PART III

Configuration



CHAPTER 13

Configure Service Discovery

Service Discovery Options

Service discovery enables clients to automatically detect and locate services on your enterprise network. You can configure service discovery using one of the following options.

Option	Description
Configure DNS SRV records, on page 81	The client automatically locates and connects to services. This is the recommended option.
Customizations, on page 83	You can customize service discovery by using installation parameters, URL configuration, or Enterprise Mobility Management.
Manual Connection Settings, on page 89	Manual connection settings provide a fallback mechanism when service discovery is not used.

Configure DNS SRV records

Before you begin

Review your SRV record requirements in the *Service Discovery* chapter of the *Planning Guide for Cisco Jabber*.

Procedure

Create the SRV records for your deployment:

Option	Description
_cisco-uds	Provides the location of Cisco Unified Communications Manager. The client can retrieve service profiles from Cisco Unified Communications Manager to determine the authenticator.
_collab-edge	Provides the location of Cisco VCS Expressway or Cisco Expressway-E. The client can retrieve service profiles from Cisco Unified Communications Manager to determine the authenticator.

Example of an SRV record

```
_cisco-uds._tcp.DOMAIN service location:
priority = 0
weight = 0
port = 8443
svr hostname=_cisco-uds._tcp.example.com
```

What to do next

Test SRV records, on page 82

Test SRV records

After creating your SRV records test to see if they are accessible.

Tip You can also use the SRV check tool on the Collaboration Solutions Analyzer site if you prefer a web-based option.

Procedure

Step 1 Open a command prompt.

Step 2 Enter **nslookup**.

The default DNS server and address is displayed. Confirm that this is the expected DNS server.

Step 3 Enter **set type=SRV**.

Step 4 Enter the name for each of your SRV records.

For example, `_cisco-uds._tcp.`*`exampledomain`*

- Displays server and address—SRV record is accessible.

- Displays `_cisco-uds_tcp.exampledomain: Non-existent domain`—There is an issue with your SRV record.

Customizations

Windows Customizations

Installer Switches

Bootstrap files provide a fallback mechanism for service discovery in situations where service discovery has not been deployed and where you do not want users to manually specify their connection settings.

The client only reads the bootstrap file on the initial launch. After the initial launch, the client caches the server addresses and configuration, and then loads from the cache on subsequent launches.

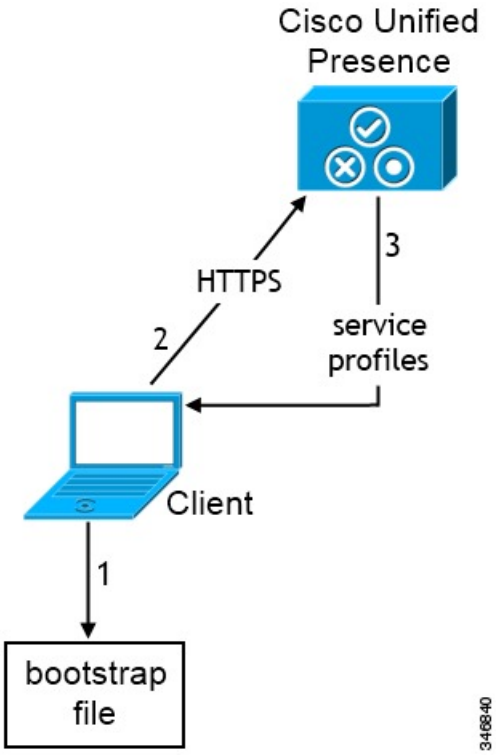
We recommend that you do not use a bootstrap file, and instead use service discovery for your Calling in Webex App (Unified CM) deployment.

Bootstrap Settings for On-Premises Deployments

The following table lists the argument values for various deployment types.

Product Mode	Server Releases	Argument Values
Full UC (Default Mode)	Release 9 and later: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	Use the following installer switches and values: • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=` `<presence_server_address>`
IM Only (Default Mode)	Release 9 and later: Cisco Unified Communications Manager IM and Presence Service	Use the following installer switches and values: • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=` `<presence_server_address>`

The following diagram illustrates how the client uses bootstrap settings in on-premises deployments:



When users start the client for the first time, the following occurs:

1. The client retrieves settings from the bootstrap file.

   The client starts in default mode and determines that Cisco Unified Communications Manager IM and Presence Service is the authenticator. The client also gets the address of the presence server, unless Service Discovery results dictate otherwise.

2. The client authenticates to Cisco Unified Communications Manager IM and Presence Service .
3. The client retrieves service profiles from the presence server.

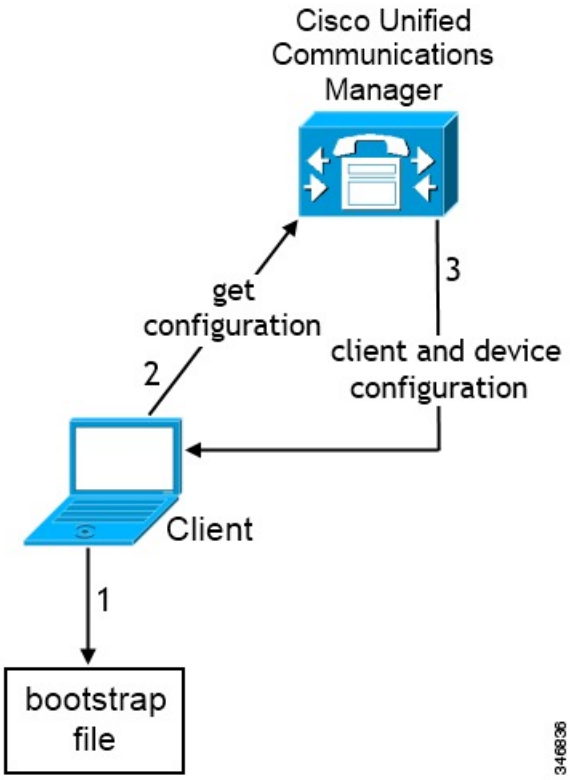
Bootstrap Settings for On-Premises Deployments in Phone Mode

During installation, you set values for arguments as follows:

- Set `CUCM` as the value for AUTHENTICATOR.
- Set `phone_mode` as the value for PRODUCT_MODE.
- Set the TFTP server address as the value for TFTP.
- Set the CTI server address as the value for CTI.
- Set the CCMCIP server address as the value for CCMCIP.

  Cisco Unified Communications Manager release 9.x and earlier—If you enable Cisco Extension Mobility, the `Cisco Extension Mobility` service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the *Feature and Services* guide for your Cisco Unified Communications Manager release.

The following diagram illustrates how the client uses bootstrap settings in phone mode deployments:



When users start the client for the first time, the following process occurs:

1. The client retrieves settings from the bootstrap file.

   The client starts in phone mode and determines that Cisco Unified Communications Manager is the authenticator. The client also gets the addresses for the TFTP server (and CTI servers for Jabber for Windows and Jabber for Mac), unless Service Discovery results dictate otherwise.

2. The client authenticates to Cisco Unified Communications Manager and gets configuration.
3. The client retrieves device and client configuration.

Mac and Mobile Customizations

Configuration URL Workflow

Procedure

	Command or Action	Purpose
Step 1	Configuration URL, on page 86	
Step 2	Provide Users with Configuration URL from a Website, on page 88	

Configuration URL

To enable users to launch Cisco Jabber without manually entering service discovery information, create and distribute a configuration URL to users.

You can provide a configuration URL link to users by emailing the link to the user directly, or by posting the link to a website.

Include the following parameters in the URL:

- ServicesDomain—Required. Every configuration URL must include the domain of the IM and presence server that Cisco Jabber needs for service discovery.
- VoiceServiceDomain—Required only if you deploy a hybrid cloud-based architecture where the domain of the IM and presence server differs from the domain of the voice server. Set this parameter to ensure that Cisco Jabber can discover voice services.
- ServiceDiscoveryExcludedServices—Optional. You can exclude any of the following services from the service discovery process:
  - Webex—When you set this value, the client:
    - Does not perform CAS lookup
    - Looks for:
      - `_cisco-uds`
      - `_cuplogin`
      - `_collab-edge`
  - CUCM—When you set this value, the client:
    - Does not look for `_cisco-uds`
    - Looks for:
      - `_cuplogin`
      - `_collab-edge`
  - CUP—When you set this value, the client:
    - Does not look for `_cuplogin`
    - Looks for:
      - `_cisco-uds`
      - `_collab-edge`

  You can specify multiple, comma-separated values to exclude multiple services.

  If you exclude all three services, the client does not perform service discovery and prompts the user to manually enter connection settings.
- ServicesDomainSsoEmailPrompt—Optional. Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.

- ON
- OFF

- EnablePRTEncryption—Optional. Specifies that the PRT file is encrypted. Applies to Cisco Jabber for Mac.
  - true
  - false
- PRTCertificateName—Optional. Specifies the name of the certificate. Applies to Cisco Jabber for Mac.
- InvalidCertificateBehavior—Optional. Specifies the client behavior for invalid certificates.
  - RejectAndNotify—A warning dialog displays and the client doesn't load.
  - PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate.
- PRTCertificateUrl—Specifies the name of a certificate with a public key in the trusted root certificate store. Applies to Cisco Jabber mobile clients.
- Telephony_Enabled—Specifies whether the user has phone capability or not. The default is true.
  - True
  - False
- ForceLaunchBrowser—Used to force user to use the external browser. Applies to Cisco Jabber mobile clients.
  - True
  - False

Note ForceLaunchBrowser is used for client certificate deployments and for devices with Android OS below 5.0.

- IP_Mode—Specifies the network IP protocol for the Jabber client.
  - IPv4-Only—Jabber will only attempt to make IPv4 connections.
  - IPv6-Only—Jabber will only attempt to make IPv6 connections.
  - Two Stacks (Default)—Jabber can connect with either IPv4 or IPv6.

Create the configuration URL in the following format:

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>
```

Note The parameters are case sensitive.

Examples

- `ciscojabber://provision?ServicesDomain=cisco.com`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

Provide Users with Configuration URL from a Website

You can provide a configuration URL link to users by emailing the link to the user directly, or by posting the link to a website.

Note Due to a limitation of the Android operating system, Cisco Jabber for Android users can encounter an issue if they open the configuration URL directly from an Android application. To work around this issue, we recommend that you distribute your configuration URL link using a website.

If you want to use the website explore option for URL provisioning, we recommended you to use Mozilla Firefox.

Use the following procedure to distribute the link from a website.

Procedure

Step 1 Create an internal web page that includes the configuration URL as an HTML hyperlink.

Step 2 Email the link to the internal web page to users.

In the email message, instruct users to perform the following steps:

a. Install the client.

b. Click the link in the email message to open the internal web page.

c. Click the link on the internal web page to configure the client.

Manual Connection Settings

Manual connection settings provide a fallback mechanism when Service Discovery is not used.

When you start Cisco Jabber, you can specify the authenticator and server address in the **Advanced settings** window. The client caches the server address to the local application configuration that loads on subsequent starts.

Cisco Jabber prompts users to enter these advanced settings on the initial start as follows:

- On-Premises with Cisco Unified Communications Manager release 9.x and Later — If the client cannot get the authenticator and server addresses from the service profile.

Settings that you enter in the **Advanced settings** window take priority over any other sources including SRV records and bootstrap settings.

If you select **Cisco IM & Presence**, the client retrieves UC services from Cisco Unified Communications Manager IM and Presence Service. The client does not use service profiles or SSO discovery.

Note For Cisco Jabber for Windows, service discovery stops after 20 seconds regardless of the number of servers the SRV record resolves to. During service discovery, once Cisco Jabber finds `_cisco-uds`, it attempts to connect to the first 2 servers within 20 seconds. Cisco Jabber doesn't attempt to connect to any servers after it's attempted service discovery for the highest 2 priority servers.

Users can manually point to the working server or re-order SRV priorities to at least one of the top two priority servers available for service discovery.

Automatic Connection Setting for Service Discovery

Users can select the **Automatic** option in the **Advanced settings** window to discover servers automatically.

The Automatic option allows users change from manually setting the service connection details to using service discovery. For example, on the initial launch, you manually set the authenticator and specify a server address in the **Advanced settings** window.

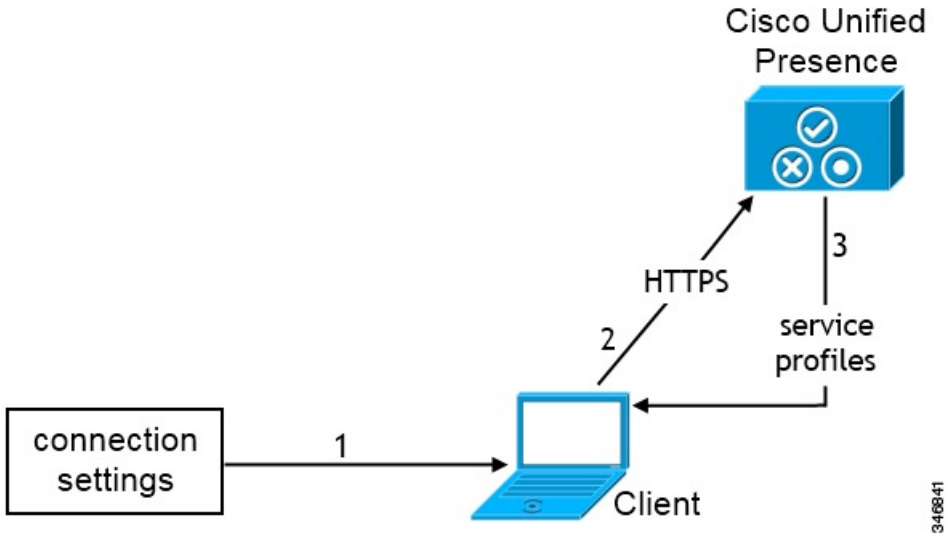
The client always checks the cache for manual settings. The manual settings take higher priority over SRV records, and for Cisco Jabber for Windows, the bootstrap file. For this reason, if you decide to deploy SRV records and use service discovery, you override the manual settings from the initial launch.

Manual Connection Settings for On-Premises Deployments

Users can set Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service as the authenticator and specify the server address in the **Advanced settings** window.

Remember You can automatically set the default server address with the `_cuplogin` SRV record.

The following diagram illustrates how the client uses manual connection settings in on-premises deployments:



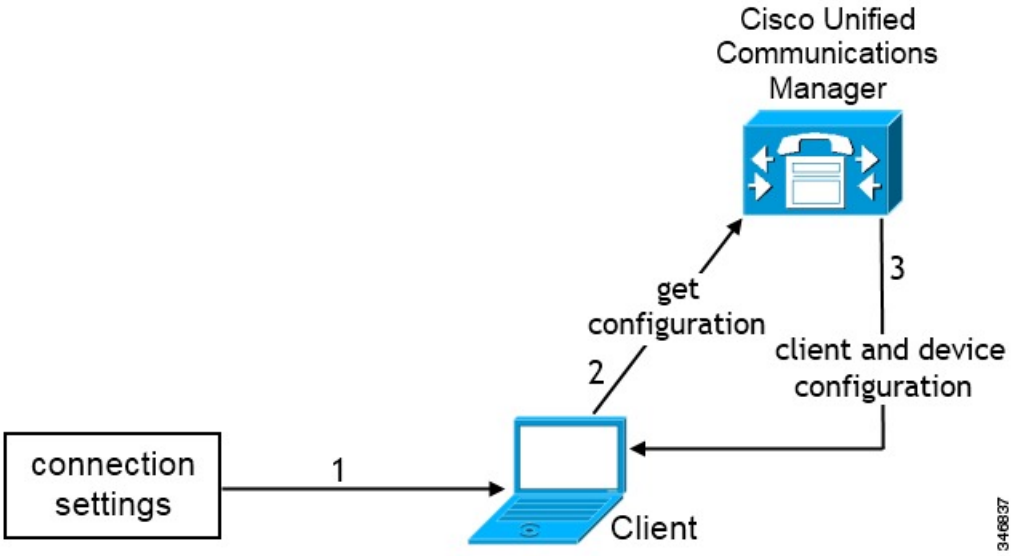
1. Users manually enter connection settings in the **Advanced settings** window.
2. The client authenticates to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.
3. The client retrieves service profiles from the presence server.

Manual Connection Settings for On-Premises Deployments in Phone Mode

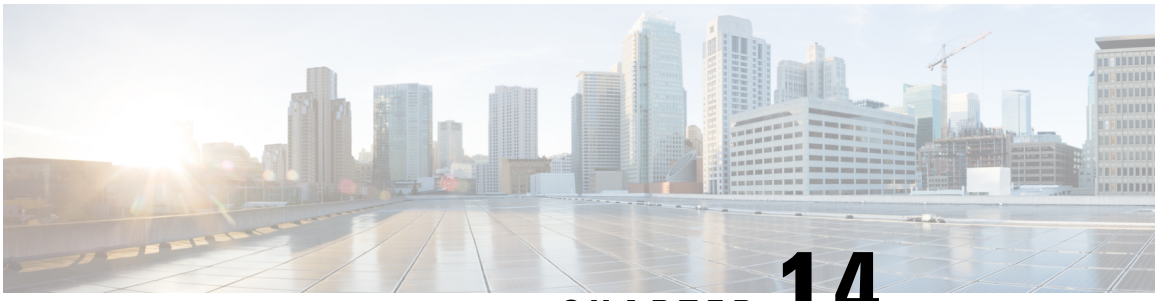
Users can specify the following server addresses in the **Phone Services** window in Webex Teams app settings:

- Username
- TFTP server
- CCMCIP server (Windows)
- CTI server (Windows)
- Password

The following diagram illustrates how the client uses manual connection settings in phone mode deployments:



1. Users manually enter connection settings in the **Calls** window.
2. The client authenticates to Cisco Unified Communications Manager and gets configuration.
3. The client retrieves device and client configuration.



CHAPTER 14

Configure Certificate Validation

Configure Certificates for an On-Premises Deployment

Certificates are required for each service to which the Jabber clients connect.

Procedure

	Command or Action	Purpose
Step 1	If you have Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service, download the applicable HTTP (tomcat) and XMPP certificates.	For more information, see the *Security Configuration on IM and Presence Service* chapter in Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager.
Step 2	Download the HTTPS (tomcat) certificate for Cisco Unified Communications Manager and Cisco Unity Connection.	For more information, see the *Cisco Unified Communications Manager Security Guide* and the *Cisco Unified Communications Operating System Administration Guide* found here.
Step 3	Download the HTTP (tomcat) for Webex Meetings Server.	For more information, see the *Cisco Webex Meetings Server Administration Guide* found here.
Step 4	If you plan to configure remote access, download the Cisco VCS Expressway and Cisco Expressway-E Server certificate. The Server certificate is used for both HTTP and XMPP.	For more information, see Configuring Certificates on Cisco VCS Expressway.
Step 5	Generate a Certificate Signing Request (CSR).	
Step 6	Upload the certificate to the service.	If you use a multiserver SAN, you only need to upload a certificate to the service once per cluster per tomcat certificate and once per cluster per XMPP certificate. If you do not use a multiserver SAN, then you must upload the

	Command or Action	Purpose
		certificate to the service for every Cisco Unified Communications Manager node.
Step 7	Deploy CA Certificates to Clients, on page 94	To ensure that certificate validation occurs without users receiving a prompt to accept or decline certificates, deploy certificates to the local certificate store of the clients.

Deploy CA Certificates to Clients

To ensure that certificate validation occurs without users receiving a prompt to accept or decline certificates, deploy certificates to the local certificate store of the endpoint clients.

If you use a well-known public CA, then the CA certificate may already exist on the client certificate store or keychain. If so, you need not deploy CA certificates to the clients.

If the CA certificate is not already on the client certificate store or keychain, then deploy the CA certificate to the clients.

If your deployment size is	Then we recommend
To a large number of local machines	That you use a certificate deployment tool, such as Group Policy or a certificate deployment management application.
To a smaller number of local machines	That you manually deploy the CA certificates.

Manually Deploy CA Certificates to Cisco Jabber for Windows Clients

Procedure

Step 1 Make the CA certificate available to the Cisco Jabber for Windows client machine.

Step 2 From the Windows machine, open the certificate file.

Step 3 Install the certificate and then select **Next**.

Step 4 Select **Place all certificates in the following store**, then select **Browse**.

Step 5 Select the Trusted Root Certification Authorities store.
When you finish the wizard, a message is displayed to verify successful certificate import.

What to do next

Verify that the certificate is installed in the correct certificate store by opening the Windows Certificate Manager tool. Browse to **Trusted Root Certification Authorites** > **Certificates**. The CA root certificate is listed in the certificate store.

Manually Deploy CA Certificates to Cisco Jabber for Mac Clients

Procedure

Step 1 Make the CA certificate available to the Cisco Jabber for Mac client machine.

Step 2 From the Mac machine, open the certificate file.

Step 3 Add to the login keychain for the current user only, then select **Add**.

What to do next

Verify that the certificate is installed in the correct keychain by opening the Keychain Access Tool and selecting Certificates. The CA root certificate is listed in the keychain.

Manually Deploy CA Certificates to Mobile Clients

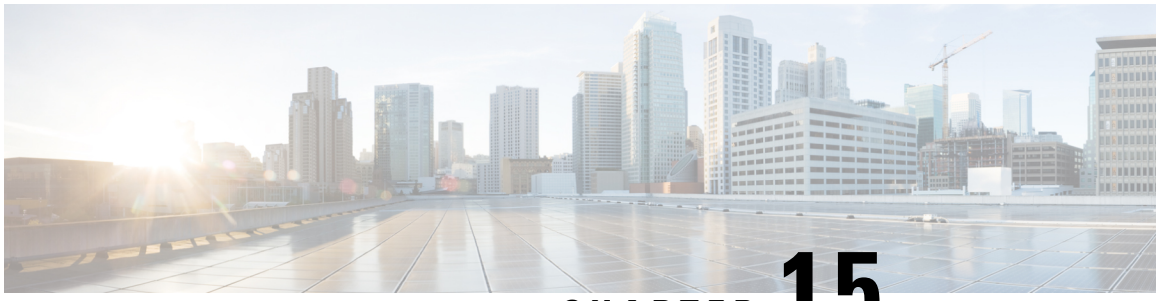
To deploy the CA certificates to an iOS client, you need a certificate deployment management application. You can email the CA certificate to users, or make the certificates available on a web server for users to access. Users can download and install the certificate using the certificate deployment management tool.

However, Jabber for Android does not have a certificate management tool, you must use the following procedure.

Procedure

Step 1 Download the CA certificate to the device.

Step 2 Tap the device **Settings** > **Security** > **Install from device storage** and follow the instructions.



CHAPTER 15

Configure the Clients

Client Configuration Workflow

Procedure

	Command or Action	Purpose
Step 1	*Introduction to Client Configuration*	
Step 2	*Set Client Configuration Parameters in Unified CM* (highest priority) or *Create and Host the Client Configuration Files*	
Step 3	*Set Parameters on Phone Configuration for Desktop Clients*	
Step 4	*Set Parameters on Phone Configuration for Mobile Clients*	
Step 5	*Configure Proxy Setting—Optional*	

Introduction to Client Configuration

Cisco Jabber can retrieve configuration settings from the following sources:

- Service Profiles—You can configure some client settings in UC service profiles on Cisco Unified Communications Manager release 9 and later. When users launch the client, it discovers the Cisco Unified Communications Manager home cluster using a DNS SRV record and automatically retrieves the configuration from the UC service profile.

- Phone Configuration—You can set some client settings in the phone configuration on Cisco Unified Communications Manager release 9 and later. The client retrieves the settings from the phone configuration in addition to the configuration in the UC service profile.
- Cisco Unified Communications Manager IM and Presence Service—You can enable instant messaging and presence capabilities and configure certain settings such as presence subscription requests.

  In the **Advanced settings** window, if you select **Cisco IM & Presence**, the client retrieves UC services from Cisco Unified Communications Manager IM and Presence Service. The client does not use service profiles or SSO discovery.
- Client Configuration—You can set client configuration parameters that are applied when users sign in, by either:
  - Set the client configuration parameters with Unified CM.
  - Create XML files using an XML editor that contain configuration parameters. You then host the XML files on a TFTP server.

Set Client Configuration Parameters in Unified CM

Set client configuration parameters and assign to service profiles in Unified CM.

For Cisco Jabber for iPhone and iPad and Cisco Jabber for Android, you must set the parameters for:

- Directory integration for on-premises deployments.
- Voicemail service credentials for hybrid-cloud deployments.

Note In most environments, Cisco Jabber for Windows and Cisco Jabber for Mac do not require any configuration to connect to services. Set client configuration parameters only if you require custom content such as automatic updates, problem reporting, or user policies and options.

Procedure

Step 1 Define Jabber Configuration Parameters, on page 98

Step 2 Assign Jabber Client Configuration to Service Profile, on page 99

Define Jabber Configuration Parameters

Unified CM allows you to add, search, display, and maintain information about UC Services including Jabber client configuration.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.
Step 2 Select **User Management** > **User Settings** > **UC Service**.
Step 3 Select **Add New**.
Step 4 Select **Jabber Client Configuration (jabber-config.xml)** as the **UC Service Type**.
Step 5 Select **Next**.
Step 6 Enter a name in the **UC Service Information** section, refer to Unified CM Help for more requirements.
Step 7 Enter the parameters in the **Jabber Configuration Parameters** section, for information regarding the parameters see the latest version of the *Parameters Reference Guide for Cisco Jabber*.
Step 8 Select **Save**.

Assign Jabber Client Configuration to Service Profile

Unified CM allows you to assign Jabber client configuration to users through service profiles.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.
Step 2 Select **User Management** > **User Settings** > **Service Profile**.
Step 3 Select **Add New** or select the existing service profile you want to assign the Jabber client configuration to.
Step 4 Select the name of the configuration you want to apply to the profile in the section **Jabber Client Configuration (jabber-config.xml) Profile**.
Step 5 Select **Save**.

Create and Host the Client Configuration Files

Create client configuration files and host them on the Cisco Unified Communications Manager TFTP service.

For Cisco Jabber for iPhone and iPad and Cisco Jabber for Android, you must create a global configuration file to set up:

- Directory integration for on-premises deployments.
- Voicemail service credentials for hybrid-cloud deployments.

Note In most environments, Cisco Jabber for Windows and Cisco Jabber for Mac do not require any configuration to connect to services. Create a configuration file only if you require custom content such as automatic updates, problem reporting, or user policies and options.

Before you begin

Note the following configuration file requirements:

- Configuration filenames are case-sensitive. Use lowercase letters in the filename to prevent errors and to ensure that the client can retrieve the file from the TFTP server.
- Use UTF-8 encoding for the configuration files.
- The client cannot read configuration files that do not have a valid XML structure. Check the structure of your configuration file for closing elements and correct nesting of elements.
- Use only valid XML character entity references in your configuration file. For example, use `&` instead of `&`. If your XML contains invalid characters, the client cannot parse the configuration file.

  To validate your configuration file, open the file in Microsoft Internet Explorer.

  - If Internet Explorer displays the entire XML structure, your configuration file is valid.
  - If Internet Explorer displays only part of the XML structure, your configuration file likely contains invalid characters or entities.

Procedure

	Command or Action	Purpose
Step 1	Specify Your TFTP Server Address, on page 100	Specify your TFTP server address for the client to enable access to your configuration file.
Step 2	Create Global Configurations, on page 101	Configure the clients for users in your deployment.
Step 3	Create Group Configurations, on page 102	Apply different configuration to different set of users.
Step 4	Host Configuration Files, on page 103	Host configuration files on any TFTP server.
Step 5	Restart Your TFTP Server, on page 103	Restart the TFTP server before the client can access the configuration files.

Specify Your TFTP Server Address

The client gets configuration files from a TFTP server.

Procedure

	Command or Action	Purpose
Step 1	Specify your TFTP server address so the client can access your configuration file.	**Attention** If Cisco Jabber 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 TFTP Servers in Phone Mode

Procedure

	Command or Action	Purpose
Step 1	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.	

Create Global Configurations

The client downloads the global configuration file from your TFTP server during the sign in sequence. Configure the client for all users in your deployment.

Before you begin

If the structure of your configuration file is not valid, the client cannot read the values you set. Review the XML samples in this chapter for more information.

Procedure

Step 1 Create a file named `jabber-config.xml` with any text editor.

- Use lowercase letters in the filename.
- Use UTF-8 encoding.

Step 2 Define the required configuration parameters in `jabber-config.xml`.

Step 3 Host the group configuration file on your TFTP server.

If your environment has multiple TFTP servers, ensure that the configuration file is the same on all TFTP servers.

Create Group Configurations

Group configuration files apply to subsets of users and are supported on Cisco Jabber for desktop (CSF devices) and on Cisco Jabber for mobile devices. Group configuration files take priority over global configuration files.

If you provision users with CSF devices, specify the group configuration filenames in the **Cisco Support Field** field on the device configuration. If users do not have CSF devices, set a unique configuration filename for each group during installation with the TFTP_FILE_NAME argument.

Before you begin

If the structure of your configuration file is not valid, the client cannot read the values you set. Review the XML samples in this chapter for more information.

Procedure

Step 1 Create an XML group configuration file with any text editor.

The group configuration file can have any appropriate name; for example, `jabber-groupa-config.xml`.

Step 2 Define the required configuration parameters in the group configuration file.

Step 3 Add the group configuration file to applicable CSF devices.

a) Open the **Cisco Unified CM Administration** interface.
b) Select **Device** > **Phone**.
c) Find and select the appropriate CSF device to which the group configuration applies.
d) In the **Phone Configuration** window, navigate to **Product Specific Configuration Layout** > **Desktop Client Settings**.
e) In the **Cisco Support Field** field, enter `configurationfile=`*`group_configuration_file_name.xml`*. For example, enter `configurationfile=groupa-config.xml`.

Note If you host the group configuration file on your TFTP server in a location other than the default directory, you must specify the path and the filename; for example, `configurationfile=/customFolder/groupa-config.xml`.

Do not add more than one group configuration file. The client uses only the first group configuration in the **Cisco Support Field** field.

f) Select **Save**.

Step 4 Host the group configuration file on your TFTP server.

Host Configuration Files

You can host configuration files on any TFTP server. However, we recommend hosting configuration files on the Cisco Unified Communications Manager TFTP server, which is where the device configuration file resides.

Procedure

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

Step 2 Select **Software Upgrades** > **TFTP File Management**.

Step 3 Select **Upload File**.

Step 4 Select **Browse** in the **Upload File** section.

Step 5 Select the configuration file on the file system.

Step 6 Do not specify a value in the **Directory** text box in the **Upload File** section.

You should leave an empty value in the **Directory** text box so that the configuration file resides in the default directory of the TFTP server.

Step 7 Select **Upload File**.

Restart Your TFTP Server

You must restart your TFTP server before the client can access the configuration files.

Procedure

Step 1 Open the **Cisco Unified Serviceability** interface on Cisco Unified Communications Manager.

Step 2 Select **Tools** > **Control Center - Feature Services**.

Step 3 Select **Cisco Tftp** from the **CM Services** section.

Step 4 Select **Restart**.

A window displays to prompt you to confirm the restart.

Step 5 Select **OK**.

The **Cisco Tftp Service Restart Operation was Successful** status displays.

Step 6 Select **Refresh** to ensure the **Cisco Tftp** service starts successfully.

What to do next

To verify that the configuration file is available on your TFTP server, open the configuration file in any browser. Typically, you can access the global configuration file at the following URL: `http://tftp_server_address:6970/jabber-config.xml`

Configuration File

For detailed information on the *jabber-config.xml* configuration file structure, group elements, parameters, and examples, see the Parameters Reference Guide for Cisco Jabber.

Set parameters on phone configuration for desktop clients

The client can retrieve configuration settings in the phone configuration from the following locations on Cisco Unified Communications Manager:

Enterprise Phone Configuration

Applies to the entire cluster.

Common Phone Profile Configuration

Applies to groups of devices and takes priority over the cluster configuration.

Cisco Unified Client Services Framework (CSF) Phone Configuration

Applies to individual CSF desktop devices and takes priority over the group configuration.

Parameters in Phone Configuration

The following table lists the configuration parameters you can set in the **Product Specific Configuration Layout** section of the phone configuration and maps corresponding parameters from the client configuration file:

Desktop Client Settings Configuration	Description
Video Calling	Enables or disables video capabilities. **Enabled (default)** Users can send and receive video calls. **Disabled** Users cannot send or receive video calls. **Restriction** This parameter is available only on the CSF device configuration.
File Types to Block in File Transfer	Restricts users from transferring specific file types. Set a file extension as the value, for example, `.exe`. Use a semicolon to delimit multiple values, for example, `.exe;.msi;.rar;.zip`

Desktop Client Settings Configuration	Description
Automatically Start in Phone Control	Sets the phone type for users when the client starts for the first time. Users can change their phone type after the initial start. The client then saves the user preference and uses it for subsequent starts. **Enabled** Use the desk phone device for calls. **Disabled (default)** Use the software phone (CSF) device for calls.
Jabber For Windows Software Update Server URL	Specifies the URL to the XML file that holds client update information. The client uses this URL to retrieve the XML file from your web server. In hybrid cloud-based deployments, you should use the WebexAdministration Tool to configure automatic updates.
Problem Report Server URL	Specifies the URL for the custom script that allows users to submit problem reports.

Set Parameters on Phone Configuration for Mobile Clients

The client can retrieve configuration settings in the phone configuration from the following locations on Cisco Unified Communications Manager:

- Cisco Dual Mode for iPhone (TCT) Configuration — Applies to individual TCT devices and takes priority over the group configuration.
- Cisco Jabber for Tablet (TAB) Configuration — Applies to individual TAB devices and takes priority over the group configuration.

Parameters in Phone Configuration

The following table lists the configuration parameters you can set in the **Product Specific Configuration Layout** section of the phone configuration and maps corresponding parameters from the client configuration file:

Desktop Client Settings Configuration	Description
Video Calling	Enables or disables video capabilities. **Enabled (default)** Users can send and receive video calls. **Disabled** Users cannot send or receive video calls. **Restriction** This parameter is available only on the CSF device configuration.

Desktop Client Settings Configuration	Description
File Types to Block in File Transfer	Restricts users from transferring specific file types. Set a file extension as the value, for example, `.exe`. Use a semicolon to delimit multiple values, for example, `.exe;.msi;.rar;.zip`
Automatically Start in Phone Control	Sets the phone type for users when the client starts for the first time. Users can change their phone type after the initial start. The client then saves the user preference and uses it for subsequent starts. **Enabled** Use the desk phone device for calls. **Disabled (default)** Use the software phone (CSF) device for calls.
Jabber For Windows Software Update Server URL	Specifies the URL to the XML file that holds client update information. The client uses this URL to retrieve the XML file from your web server.
Problem Report Server URL	Specifies the URL for the custom script that allows users to submit problem reports.

Optional Configuration of Proxy Settings

Your client might use proxy settings to connect to services.

The following limitations apply when using a proxy for these HTTP requests:

- Proxy Authentication is not supported.
- Wildcards in the bypass list are supported.
- Cisco Jabber supports proxy for HTTP request using HTTP CONNECT, but does not support proxy when using HTTPS CONNECT.
- Web Proxy Auto Discovery (WAPD) is not supported and must be disabled.

If necessary, configure the proxy settings by following the steps for your client type.

Configure Proxy Settings for Cisco Jabber for Windows

Configure proxy settings for Windows in the Local Area Network (LAN) settings for Internet properties.

Procedure

Step 1 In the **Connections** tab select **LAN Settings**.

Step 2 Configure a proxy using one of the following options:

- For automatic configuration, specify a `.pac` file URL.
- For Proxy Server, specify an explicit proxy address.

Configure Proxy Settings for Cisco Jabber for Mac

Configure proxy settings for Mac in **System Preferences**.

Procedure

Step 1 Select **System Preferences** > **Network**

Step 2 Choose your network service from the list and select **Advanced** > **Proxies** .

Step 3 Configure a proxy using one of the following options:

- For automatic configuration, specify a `.pac` file URL.
- For Proxy Server, specify an explicit proxy address.

Configure Proxy Settings for Cisco Jabber iPhone and iPad

Configure proxy settings in the Wi-Fi settings of an iOS device using one of the following methods:

Procedure

Step 1 Select **Wi-Fi** > **HTTP PROXY** > **Auto** and specify a `.pac` file URL as the automatic configuration script.

Step 2 Select **Wi-Fi** > **HTTP PROXY** > **Manual** and specify an explicit proxy address.

Configure Proxy Settings for Cisco Jabber for Android

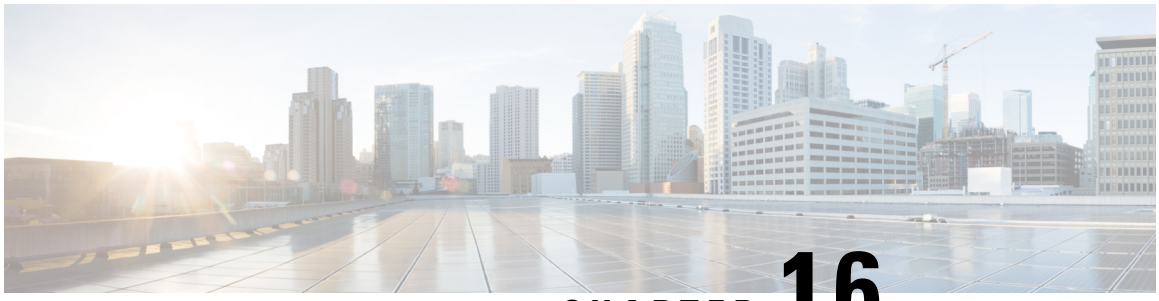
Procedure

Configure proxy settings in the Wi-Fi settings of an Android device using one of the following methods:

- Specify a .pac file URL as the automatic configuration script in the **Wi-Fi** > **Modify Network** > **Show Advanced Options** > **Proxy Settings** > **Auto** tab.

  Note This method is only supported on devices with Android OS 5.0 and later, and Cisco DX series devices.

- Specify an explicit proxy address in the **Wi-Fi Networks** > **Modify Network** > **Show Advanced Options** > **Proxy Settings** > **Auto** tab.



CHAPTER 16

Deploy Cisco Jabber Applications and Jabber Softphone for VDI

Accessories Manager

Accessories Manager

The Jabber desktop clients use the Accessories Manager to enable interaction with accessories like headsets. The Accessories Manager is a component that provides Unified Communication control APIs to accessory device vendors.

Some Cisco headsets and other third-party devices use these APIs to mute audio, answer calls, and end calls from the device. Third-party vendors write plug-ins that the application loads. Standard headsets use the APIs to connect with speaker and microphone support.

Only specific devices interact with Accessories Manager for call control. Contact your devices vendor for more information. The Accessories Manager doesn't support desktop phones.

Accessories manager functionality is enabled by default and configured using the EnableAccessoriesManager parameter. You can disable specific Accessories Manager plugins from third-party vendors using the BlockAccessoriesManager parameter.

Note If you set EnableAccessoriesManager to false in `jabber-config.xml`, call control buttons on some headsets don’t work.

The client installer includes the third-party plug-ins from the vendors. They are installed in the `/Library/Cisco/Jabber/Accessories/` folder.

Supported third-party vendors:

- Logitech
- Sennheiser
- Jabra
- Plantronics

Download the Cisco Jabber Clients

If required, you can add your own Customer signature to the Jabber Installer or Cisco Dynamic Libraries by using the signing tools from the Operating System for that client.

Note For Cisco Jabber for Mac, the installer includes the product installer file. Use the Terminal tool to extract the `pkg` file from the installer and sign the `pkg` file before adding to the installer.

Procedure

Download the client from the applicable source.

- Visit the Cisco Software Center to download the Cisco Jabber for Mac and Cisco Jabber for Windows clients.
- For Cisco Jabber for Android, download the app from Google Play.
- For Cisco Jabber for iPhone and iPad, download the app from the App store.

Install Cisco Jabber for Windows

Cisco Jabber for Windows provides an MSI installation package that you can use in the following ways:

Install Option	Description
Use the Command Line, on page 111	You can specify arguments in a command line window to set installation properties. Choose this option if you plan to install multiple instances.
Run the MSI Manually, on page 127	Run the MSI manually on the file system of the client workstation and then specify connection properties when you start the client. Choose this option if you plan to install a single instance for testing or evaluation purposes.

Install Option	Description
Create a Custom Installer, on page 128	Open the default installation package, specify the required installation properties, and then save a custom installation package. Choose this option if you plan to distribute an installation package with the same installation properties.
Deploy with Group Policy, on page 131	Install the client on multiple computers in the same domain.

Before you begin

You must be logged in with local administrative rights.

Use the Command Line

Specify installation arguments in a command line window.

Procedure

Step 1 Open a command line window.

Step 2 Enter the following command:

```
msiexec.exe /i CiscoJabberSetup.msi
```

Step 3 Specify command line arguments as parameter=value pairs.

```
msiexec.exe /i CiscoJabberSetup.msi argument=value
```

Step 4 Run the command to install Cisco Jabber for Windows.

Example Installation Commands

Review examples of commands to install Cisco Jabber for Windows.

Cisco Unified Communications Manager, Release 9.x

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1
```

Where:

CLEAR=1 — Deletes any existing bootstrap file.
`/quiet` — Specifies a silent installation.

Related Topics

Command Line Arguments, on page 112
LCID for Languages, on page 125

Command Line Arguments

Review the command line arguments you can specify when you install Cisco Jabber for Windows.

Related Topics

Example Installation Commands, on page 111
LCID for Languages, on page 125

Override Argument

The following table describes the parameter you must specify to override any existing bootstrap files from previous installations:

Argument	Value	Description
CLEAR	1	Specifies if the client overrides any existing bootstrap file from previous installations. The client saves the arguments and values you set during installation to a bootstrap file. The client then loads settings from the bootstrap file at startup.

If you specify CLEAR, the following occurs during installation:

1. The client deletes any existing bootstrap file.
2. The client creates a new bootstrap file.

If you do not specify CLEAR, the client checks for existing bootstrap files during installation.

- If no bootstrap file exists, the client creates a bootstrap file during installation.
- If a bootstrap file exists, the client does not override that bootstrap file and preserves the existing settings.

Note If you are reinstalling Cisco Jabber for Windows, you should consider the following:

- The client does not preserve settings from existing bootstrap files. If you specify CLEAR, you must also specify all other installation arguments as appropriate.
- The client does not save your installation arguments to an existing bootstrap file. If you want to change the values for installation arguments, or specify additional installation arguments, you must specify CLEAR to override the existing settings.

To override existing bootstrap files, specify CLEAR in the command line as follows:

```
msiexec.exe /i CiscoJabberSetup.msi CLEAR=1
```

Mode Type Argument

The following table describes the command line argument with which you specify the product mode:

Argument	Value	Description
PRODUCT_MODE	Phone_Mode	Specifies the product mode for the client. You can set the following value: • Phone_Mode — Cisco Unified Communications Manager is the authenticator. Choose this value to provision users with audio devices as base functionality.

When to Set the Product Mode

In phone mode deployments Cisco Unified Communications Manager is the authenticator. When the client gets the authenticator, it determines the product mode is phone mode. However, because the client always starts in the default product mode on the initial launch, users must restart the client to enter phone mode after sign in.

Note Cisco Unified Communications Manager, Release 9.x and Later — You should not set PRODUCT_MODE during installation. The client gets the authenticator from the service profile. After the user signs in, the client requires a restart to enter phone mode.

Change Product Modes

To change the product mode, you must change the authenticator for the client. The client can then determine the product mode from the authenticator.

The method for changing from one product mode to another after installation, depends on your deployment.

Note In all deployments, the user can manually set the authenticator in the Advanced settings window.

In this case, you must instruct the user to change the authenticator in the Advanced settings window to change the product mode. You cannot override the manual settings, even if you uninstall and then reinstall the client.

Change Product Modes with Cisco Unified Communications Manager Version 9.x and Later

To change product modes with Cisco Unified Communications Manager version 9.x and later, you change the authenticator in the service profile.

Procedure

Step 1 Change the authenticator in the service profiles for the appropriate users.

Change Default Mode > Phone Mode

Do not provision users with an IM and Presence service.

If the service profile does not contain an IM and presence service configuration, the authenticator is Cisco Unified Communications Manager.

Change Phone Mode > Default Mode

Provision users with an IM and Presence service.

If you set the value of the **Product type** field in the IM and Presence profile to:

- **Unified CM (IM and Presence)** the authenticator is Cisco Unified Communications Manager IM and Presence Service.
- Webex **(IM and Presence)** the authenticator is the Webex Messenger service.

Step 2 Instruct users to sign out and then sign in again.

When users sign in to the client, it retrieves the changes in the service profile and signs the user in to the authenticator. The client then determines the product mode and prompts the user to restart the client.

After the user restarts the client, the product mode change is complete.

Authentication Arguments

The following table describe the command line arguments you can set to specify the source of authentication:

Argument	Value	Description
AUTHENTICATOR	CUP CUCM	Specifies the source of authentication for the client. This value is used if Service Discovery fails. Set one of the following as the value: • CUP—Cisco Unified Communications Manager IM and Presence Service. On-premises deployments in the default product mode. The default product mode can be either full UC or IM only. • CUCM—Cisco Unified Communications Manager. On-premises deployments in phone mode. In on-premises deployments with Cisco Unified Communications Manager version 9.x and later, you should deploy the `_cisco-uds` SRV record. The client can then automatically determine the authenticator.
CUP_ADDRESS	IP address Hostname FQDN	Specifies the address of Cisco Unified Communications Manager IM and Presence Service. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*)

Argument	Value	Description
TFTP	IP address Hostname FQDN	Specifies the address of your TFTP server. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*) You should specify this argument if you set Cisco Unified Communications Manager as the authenticator. If you deploy: • In phone mode—you should specify the address of the TFTP server that hosts the client configuration. • In default mode—you can specify the address of the Cisco Unified Communications Manager TFTP service that hosts the device configuration.
CTI	IP address Hostname FQDN	Sets the address of your CTI server. Specify this argument if: • You set Cisco Unified Communications Manager as the authenticator. • Users have desk phone devices and require a CTI server.
CCMCIP	IP address Hostname FQDN	Sets the address of your CCMCIP server. Specify this argument if: • You set Cisco Unified Communications Manager as the authenticator. • The address of your CCMCIP server is not the same as the TFTP server address. The client can locate the CCMCIP server with the TFTP server address if both addresses are the same.
SERVICES_DOMAIN	Domain	Sets the value of the domain where the DNS SRV records for Service Discovery reside. This argument can be set to a domain where no DNS SRV records reside if you want the client to use installer settings or manual configuration for this information. If this argument is not specified and Service Discovery fails, the user will be prompted for services domain information.

Argument	Value	Description
VOICE_SERVICES_DOMAIN	Domain	If this setting is specified, the client uses the value of VOICE_SERVICES_DOMAIN to lookup the following DNS records for the purposes of Service Discovery and Edge Detection: • `_cisco-uds` • `_cuplogin` • `_collab-edge` This setting is optional and if not specified, the DNS records are queried on the Services Domain which is obtained from the SERVICES_DOMAIN, email address input by the user, or cached user configuration.
EXCLUDED_SERVICES	One or more of: • Webex • CUCM	Lists the services that you want Jabber to exclude from Service Discovery. For example, suppose that you did a trial with Webex and your company domain is registered on Webex. But, you want Jabber to authenticate with CUCM server, rather than with Webex. In this case set: • EXCLUDED_SERVICES=WEBEX Possible values are CUCM, Webex If you exclude all services, you need to use manual configuration or bootstrap configuration to configure the Jabber client.
UPN_DISCOVERY_ENABLED	true false	Allows you to define whether the client uses the User Principal Name (UPN) of a Windows session to get the User ID and domain for a user when discovering services. • true (default)—The UPN is used to find the User ID and the domain of the user, which is used during service discovery. Only the user discovered from UPN can log in to the client. • false—The UPN is not used to find the User ID and domain of the user. The user is prompted to enter credentials to find the domain for service discovery. Example installation command: `msiexec.exe /i CiscoJabberSetup.msi /quiet UPN_DISCOVERY_ENABLED=false`

TFTP Server Address

Cisco Jabber for Windows retrieves two different configuration files from the TFTP server:

- Client configuration files that you create.
- Device configuration files that reside on the Cisco Unified Communications Manager TFTP service when you provision users with devices.

To minimize effort, you should host your client configuration files on the Cisco Unified Communications Manager TFTP service. You then have only one TFTP server address for all configuration files and can specify that address as required.

You can, however, host your client configuration on a different TFTP server to the one that contains the device configuration. In this case, you have two different TFTP server addresses, one address for the TFTP server that hosts device configuration and another address for the TFTP server that hosts client configuration files.

Default Deployments

This section describes how you should handle two different TFTP server addresses in deployments that have a presence server.

You should do the following:

1. Specify the address of the TFTP server that hosts the client configuration on the presence server.
2. During installation, specify the address of the Cisco Unified Communications Manager TFTP service with the TFTP argument.

When the client starts for the first time, it:

1. Retrieves the address of the Cisco Unified Communications Manager TFTP service from the bootstrap file.
2. Gets device configuration from the Cisco Unified Communications Manager TFTP service.
3. Connects to the presence server.
4. Retrieves the address of the TFTP service that hosts the client configuration from the presence server.
5. Gets client configuration from the TFTP server.

Phone Mode Deployments

This section describes how you should handle two different TFTP server addresses in phone mode deployments.

You should do the following:

1. During installation, specify the address of the TFTP server that hosts the client configuration with the TFTP argument.
2. Specify the address of the TFTP server that hosts the device configuration in your client configuration file with the following parameter: TftpServer1.
3. Host the client configuration file on the TFTP server.

When the client starts for the first time, it:

1. Retrieves the address of the TFTP server from the bootstrap file.
2. Gets client configuration from the TFTP server.

3. Retrieves the address of the Cisco Unified Communications Manager TFTP service from the client configuration.
4. Gets device configuration from the Cisco Unified Communications Manager TFTP service.

Common Installation Arguments

The following table describes some common command line arguments:

Argument	Value	Description
AUTOMATIC_SIGN_IN	true false	Specifies whether the **Sign me in when Cisco Jabber starts** check box is checked when the user installs the client. • true—The **Sign me in when Cisco Jabber starts** check box is checked when the user installs the client. • false (default)—The **Sign me in when Cisco Jabber starts** check box is not checked when the user installs the client.
CC_MODE	true false	Specifies whether Jabber is running in Common Criteria mode. The default value is false.
CLICK2X	DISABLE Click2Call	Disables click-to-x functionality with Cisco Jabber. If you specify this argument during installation, the client does not register as a handler for click-to-x functionality with the operating system. This argument prevents the client from writing to the Microsoft Windows registry during installation. You must re-install the client and omit this argument to enable click-to-x functionality with the client after installation. **Note** Jabber for Windows and Skype for Business can compete for the Windows API. To potentially mitigate this issue, you can install Jabber with `CLICK2X=DISABLE`. **Click2Call function in Browser**—The Click2X parameter can now be configured by using the newly added Click2Call parameter. This enables only the Click to call feature in the browser and disables the Click2X feature.

Argument	Value	Description
DIAGNOSTICSTOOLENABLED	true false	Specifies whether the Cisco Jabber Diagnostics Tool is available to Cisco Jabber for Windows users. • true (default)—Users can display the Cisco Jabber Diagnostics Tool by entering Ctrl + Shift + D. • false—The Cisco Jabber Diagnostics Tool is not available to users.
ENABLE_DPI_AWARE	true false	Enables DPI awareness. DPI awareness enables Cisco Jabber to automatically adjust the display of text and images to suit different screen sizes. • true (default)— • on Windows 8.1 and Windows 10, Cisco Jabber adjusts to different DPI settings on each monitor. • on Windows 7 and Windows 8, Cisco Jabber displays according to the system DPI settings. • false—DPI awareness is not enabled. DPI awareness is enabled by default. To disable DPI awareness, use the following command: `msiexec.exe /i CiscoJabberSetup.msi CLEAR=1 ENABLE_DPI_AWARE=false` **Note** If you are installing Cisco Jabber with the command line, remember to include the CLEAR=1 argument. If you are not installing Cisco Jabber from the command line, you must manually delete the jabber-bootstrap.properties file.

Argument	Value	Description
ENABLE_PRT	true false	• true (default)—The **Report a problem** menu item is enabled in the **Help** menu in the client. • false—The Jabber menu item option **Report a problem** is removed from the **Help** menu in the client. If you set the argument to false, users can still manually use the **Start Menu** > **Cisco Jabber** directory, or the Program files directory and launch the Problem Report Tool manually. If a user manually creates a PRT, and this parameter value is set to false, then the zip file created from the PRT has no content.
ENABLE_PRT_ENCRYPTION	true false	Enables problem report encryption. You must configure this argument with the PRT_CERTIFICATE_NAME argument. • true—PRT files sent by Jabber clients are encrypted. • false (default)—PRT files sent by Jabber clients are not encrypted. PRT encryption requires a public/private key pair to encrypt and decrypt the Cisco Jabber problem report.
FIPS_MODE	true false	Specifies whether Cisco Jabber is in FIPS mode. Cisco Jabber can be in FIPS mode on an operating system that is not FIPS enabled. Only connections with non-Windows APIs are in FIPS mode. If you don't include this setting, Cisco Jabber will determine the FIPS mode from the operating system.
FORGOT_PASSWORD_URL	URL	Specifies the URL where users can reset lost or forgotten passwords. This argument is optional but recommended.
FORWARD_VOICEMAIL	true false	Enables voicemail forwarding in the Voice Messages tab. • true (default)—Users can forward voicemails to contacts. • false—Voicemail forwarding is not enabled.

Argument	Value	Description
INVALID_CERTIFICATE_BEHAVIOR	RejectAndNotify PromptPerSession	Specifies the client behavior for invalid certificates. • RejectAndNotify—A warning dialog displays and the client doesn't load. • PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate. For invalid certificates in FIPS mode, this argument is ignored, the client displays a warning message and doesn't load.
IP_Mode	IPv4-Only IPv6-Only Two Stacks	Specifies the network IP protocol for the Jabber client. • IPv4-Only—Jabber will only attempt to make IPv4 connections. • IPv6-Only—Jabber will only attempt to make IPv6 connections. • Two Stacks (Default)—Jabber can connect with either IPv4 or IPv6. **Note** IPv6-only support is available only for desktop devices on-premise deployment. All Jabber mobile devices must be configured as Two Stacks. For more details about IPv6 deployment, see the IPv6 Deployment Guide for Cisco Collaboration Systems Release. There are a number of factors used to determine the network IP protocol used by Jabber, for more information see the IPv6 Requirements section in the *Planning Guide*.

Argument	Value	Description
LANGUAGE	LCID in decimal	Defines the Locale ID (LCID), in decimal, of the language that Cisco Jabber for Windows uses. The value must be an LCID in decimal that corresponds to a supported language. For example, you can specify one of the following: • 1033 specifies English. • 1036 specifies French. See the *LCID for Languages* topic for a full list of the languages that you can specify. This argument is optional. If you do not specify a value, Cisco Jabber for Windows checks the value for the UseSystemLanguage parameter. If the UseSystemLanguage parameter is set to true, the same language is used as for the operating system. If the UseSystemLanguage parameter is to set to false or not defined, then the client uses the regional language for the current user as the default. The regional language is set at **Control Panel** > **Region and Language** > **Change the date, time, or number format** > **Formats tab** > **Format dropdown**.
LOCATION_MODE	ENABLED DISABLED ENABLEDNOPROMPT	Specifies whether the Location feature is enabled and whether users are notified when new locations are detected. • ENABLED(default)—Location feature is turned on. Users are notified when new locations are detected. • DISABLED—Location feature is turned off. Users are not notified when new locations are detected. • ENABLEDNOPROMPT—Location feature is turned on. Users are not notified when new locations are detected.

Argument	Value	Description
LOG_DIRECTORY	Absolute path on the local filesystem	Defines the directory where the client writes log files. Use quotation marks to escape space characters in the path, as in the following example: `"C:\my_directory\Log Directory"` The path you specify must not contain Windows invalid characters. The default value is `%USER_PROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs`
LOGIN_RESOURCE	WBX MUT	Controls user sign in to multiple client instances. By default, users can sign in to multiple instances of Cisco Jabber at the same time. Set one of the following values to change the default behavior: • WBX—Users can sign in to one instance of Cisco Jabber for Windows at a time. Cisco Jabber for Windows appends the `wbxconnect` suffix to the user's JID. Users cannot sign in to any other Cisco Jabber client that uses the `wbxconnect` suffix. • MUT—Users can sign in to one instance of Cisco Jabber for Windows at a time, but can sign in to other Cisco Jabber clients at the same time. Each instance of Cisco Jabber for Windows appends the user's JID with a unique suffix.
PRT_CERTIFICATE_NAME	Certificate name	Specifies the name of a certificate with a public key in the Enterprise Trust or Trusted Root Certificate Authorities certificate store. The certificate public key is used to encrypt Jabber Problem reports. You must configure this argument with the ENABLE_PRT_ENCRYPTION argument.

Argument	Value	Description
RESET_JABBER	1	Resets the user's local and roaming profile data. These folders are deleted: • `%appdata%\Cisco\Unified Communications\Jabber` • `%localappdata%\Cisco\Unified Communications\Jabber`
SSO_EMAIL_PROMPT	ON OFF	Specifies whether the user is shown the email prompt for determining their home cluster. In order for the email prompt to work defined by ServicesDomainSsoEmailPrompt the installer requirements are: • SSO_EMAIL_PROMPT=ON • UPN_DISCOVERY_ENABLED=False • VOICE_SERVICES_DOMAIN=<domain_name> • SERVICES_DOMAIN=<domain_name> Example: msiexec.exe /i CiscoJabberSetup.msi SSO_EMAIL_PROMPT=ON UPN_DISCOVERY_ENABLED=False VOICE_SERVICES_DOMAIN=example.cisco.com SERVICES_DOMAIN=example.cisco.com CLEAR=1
Telemetry_Enabled	true false	Specifies whether analytics data is gathered. The default value is true. To improve your experience and product performance, Cisco Jabber may collect and send non-personally identifiable usage and performance data to Cisco. The aggregated data is used by Cisco to understand trends in how Jabber clients are being used and how they are performing. Full details on what analytics data Cisco Jabber does and does not collect can be found in the Cisco Jabber Supplement to Cisco's On-Line Privacy Policy at https://www.cisco.com/web/siteassets/legal/privacy_02Jun10.html.

Argument	Value	Description
TFTP_FILE_NAME	Filename	Specifies the unique name of a group configuration file. You can specify either an unqualified or fully qualified filename as the value. The filename you specify as the value for this argument takes priority over any other configuration file on your TFTP server. This argument is optional. **Remember** You can specify group configuration files in the **Cisco Support Field** on the CSF device configuration on Cisco Unified Communications Manager.
UXModel	modern classic	Applies to Cisco Jabber for desktop clients Jabber defaults to the Modern Design in all deployments. But, on-premises deployments also support the Classic Design. Jabber Team Messaging Mode only supports the Modern Design. If you want an on-premises deployment to start the Classic Design, use the UXModel parameter. The allowed values are: • modern (default)—Jabber starts in the Modern Design. • classic—Jabber starts in the Classic Design. Each user can set a personal preference in Jabber, which takes precedence over this parameter.

LCID for Languages

The following table lists the Locale Identifier (LCID) or Language Identifier (LangID) for the languages that the Cisco Jabber clients support.

Supported Languages	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android, Cisco Jabber for iPhone and iPad	LCID/LangID
Arabic - Saudi Arabia	X		X	1025
Bulgarian - Bulgaria	X	X		1026

Supported Languages	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android, Cisco Jabber for iPhone and iPad	LCID/LangID
Catalan - Spain	X	X		1027
Chinese (Simplified) - China	X	X	X	2052
Chinese (Traditional) - Taiwan	X	X	X	1028
Croatian - Croatia	X	X	X	1050
Czech - Czech Republic	X	X		1029
Danish - Denmark	X	X	X	1030
Dutch - Netherlands	X	X	X	1043
English - United States	X	X	X	1033
Finnish - Finland	X	X		1035
French - France	X	X	X	1036
German - Germany	X	X	X	1031
Greek - Greece	X	X		1032
Hebrew - Israel	X			1037
Hungarian - Hungary	X	X	X	1038
Italian - Italy	X	X	X	1040
Japanese - Japan	X	X	X	1041
Korean - Korea	X	X	X	1042
Norwegian - Norway	X	X		2068
Polish - Poland	X	X		1045
Portuguese - Brazil	X	X	X	1046
Portuguese - Portugal	X	X		2070

Supported Languages	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android, Cisco Jabber for iPhone and iPad	LCID/LangID
Romanian - Romania	X	X	X	1048
Russian - Russia	X	X	X	1049
Serbian	X	X		1050
Slovak - Slovakian	X	X	X	1051
Slovenian -Slovenia	X	X		1060
Spanish - Spain (Modern Sort)	X	X	X	3082
Swedish - Sweden	X	X	X	5149
Thai - Thailand	X	X		1054
Turkish	X	X	X	1055

Related Topics

Example Installation Commands, on page 111
Command Line Arguments, on page 112

Run the MSI Manually

You can run the installation program manually to install a single instance of the client and specify connection settings in the Advanced settings window.

Procedure

Step 1 Launch `CiscoJabberSetup.msi`.

The installation program opens a window to guide you through the installation process.

Step 2 Follow the steps to complete the installation process.

Step 3 Start Cisco Jabber for Windows.

Step 4 Select **Manual setup and sign in**.

The Advanced settings window opens.

Step 5 Specify values for the connection settings properties.

Step 6 Select **Save**.

Create a Custom Installer

You can transform the default installation package to create a custom installer.

Note You use Microsoft Orca to create custom installers. Microsoft Orca is available as part of the Microsoft Windows SDK for Windows 7 and .NET Framework 4.

Download and install Microsoft Windows SDK for Windows 7 and .NET Framework 4 from the Microsoft website.

Procedure

	Command or Action	Purpose
Step 1	Get the Default Transform File, on page 128	You must have the default transform file to modify the installation package with Microsoft Orca.
Step 2	Create Custom Transform Files, on page 128	Transform files contain installation properties that you apply to the installer.
Step 3	Transform the Installer, on page 129	Apply a transform file to customize the installer.

Get the Default Transform File

You must have the default transform file to modify the installation package with Microsoft Orca.

Procedure

Step 1 Download the Cisco Jabber administration package from Software Download page.

Step 2 Copy `CiscoJabberProperties.msi` from the Cisco Jabber administration package to your file system.

What to do next

Create Custom Transform Files, on page 128

Create Custom Transform Files

To create a custom installer, you use a transform file. Transform files contain installation properties that you apply to the installer.

The default transform file lets you specify values for properties when you transform the installer. You should use the default transform file if you are creating one custom installer.

You can optionally create custom transform files. You specify values for properties in a custom transform file and then apply it to the installer.

Create custom transform files if you require more than one custom installer with different property values. For example, create one transform file that sets the default language to French and another transform file that

sets the default language to Spanish. You can then apply each transform file to the installation package separately. The result is that you create two installers, one for each language.

Before you begin

Get the Default Transform File, on page 128

Procedure

Step 1 Start Microsoft Orca.

Step 2 Open `CiscoJabberSetup.msi` and then apply `CiscoJabberProperties.msi`.

Step 3 Specify values for the appropriate installer properties.

Step 4 Generate and save the transform file.

a) Select **Transform** > **Generate Transform**.
b) Select a location on your file system to save the transform file.
c) Specify a name for the transform file and select **Save**.

The transform file you created is saved as *`file_name`*`.mst`. You can apply this transform file to modify the properties of `CiscoJabberSetup.msi`.

What to do next

Transform the Installer, on page 129

Transform the Installer

Apply a transform file to customize the installer.

Note Applying transform files will alter the digital signature of `CiscoJabberSetup.msi`. Attempts to modify or rename `CiscoJabberSetup.msi` will remove the signature entirely.

Before you begin

Create Custom Transform Files, on page 128

Procedure

Step 1 Start Microsoft Orca.

Step 2 Open `CiscoJabberSetup.msi` in Microsoft Orca.

a) Select **File** > **Open**.
b) Browse to the location of `CiscoJabberSetup.msi` on your file system.
c) Select `CiscoJabberSetup.msi` and then select **Open**.

The installation package opens in Microsoft Orca. The list of tables for the installer opens in the **Tables** pane.

Step 3 Required: Remove all language codes except for 1033 (English).

Restriction You must remove all language codes from the custom installer except for 1033 (English).

Microsoft Orca does not retain any language files in custom installers except for the default, which is 1033. If you do not remove all language codes from the custom installer, you cannot run the installer on any operating system where the language is other than English.

a) Select **View** > **Summary Information**.

The **Edit Summary Information** window displays.

b) Locate the **Languages** field.
c) Delete all language codes except for 1033.
d) Select **OK**.

English is set as the language for your custom installer.

Step 4 Apply a transform file.

a) Select **Transform** > **Apply Transform**.
b) Browse to the location of the transform file on your file system.
c) Select the transform file and then select **Open**.

Step 5 Select **Property** from the list of tables in the **Tables** pane.

The list of properties for `CiscoJabberSetup.msi` opens in the right panel of the application window.

Step 6 Specify values for the properties you require.

Tip Values are case sensitive. Ensure the value you enter matches the value in this document.

Tip Set the value of the CLEAR property to `1` to override any existing bootstrap file from previous installations. If you do not override existing bootstrap files, the values you set in the custom installer do not take effect.

Step 7 Remove any properties that you do not require.

It is essential to remove any properties that are not being set, otherwise the properties being set will not take effect. Remove each property that is not needed one at a time.

a) Right-click the property you want to remove.
b) Select **Drop Row**.
c) Select **OK** when Microsoft Orca prompts you to continue.

Step 8 Required: Enable your custom installer to save embedded streams.

a) Select **Tools** > **Options**.
b) Select the **Database** tab.
c) Select **Copy embedded streams during 'Save As'**.
d) Select **Apply** and then **OK**.

Step 9 Save your custom installer.

a) Select **File** > **Save Transformed As**.
b) Select a location on your file system to save the installer.
c) Specify a name for the installer and then select **Save**.

Installer Properties

The following are the properties you can modify in a custom installer:

- CLEAR
- PRODUCT_MODE
- AUTHENTICATOR
- CUP_ADDRESS
- TFTP
- CTI
- CCMCIP
- LANGUAGE
- TFTP_FILE_NAME
- FORGOT_PASSWORD_URL
- SSO_ORG_DOMAIN
- LOGIN_RESOURCE
- LOG_DIRECTORY
- CLICK2X
- SERVICES_DOMAIN

These properties correspond to the installation arguments and have the same values.

Deploy with Group Policy

Install Cisco Jabber for Windows with Group Policy using the Microsoft Group Policy Management Console (GPMC) on Microsoft Windows Server.

Note To install Cisco Jabber for Windows with Group Policy, all computers or users to which you plan to deploy Cisco Jabber for Windows must be in the same domain.

Procedure

	Command or Action	Purpose
Step 1	Set a Language Code, on page 132	You must use this procedure and set the Language field to 1033 only if the MSI is to be modified by Orca in any way.
Step 2	Deploy the Client with Group Policy, on page 132	Deploy Cisco Jabber for Windows with Group Policy.

Set a Language Code

Altering the installation language is not necessary in Group Policy deployment scenarios where the exact MSI file provided by Cisco will be used. The installation language will be determined from the Windows User Locale (Format) in these situations. You must use this procedure and set the Language field to 1033 only if the MSI is to be modified by Orca in any way.

For a list of the Locale Identifier (LCID) or Language Identifier (LangID) for languages that Jabber clients support, see LCID for Languages, on page 125.

Procedure

Step 1 Start Microsoft Orca.

Microsoft Orca is available as part of the Microsoft Windows SDK for Windows 7 and ,NET Framework 4 that you can download from the Microsoft website.

Step 2 Open `CiscoJabberSetup.msi`.

a) Select **File** > **Open**.
b) Browse to the location of `CiscoJabberSetup.msi` on your file system.
c) Select `CiscoJabberSetup.msi` and then select **Open**.

Step 3 Select **View** > **Summary Information**.

Step 4 Locate the **Languages** field.

Step 5 Set the **Languages** field to 1033.

Step 6 Select **OK**.

Step 7 Required: Enable your custom installer to save embedded streams.

a) Select **Tools** > **Options**.
b) Select the **Database** tab.
c) Select **Copy embedded streams during 'Save As'**.
d) Select **Apply** and then **OK**.

Step 8 Save your custom installer.

a) Select **File** > **Save Transformed As**.
b) Select a location on your file system to save the installer.
c) Specify a name for the installer and then select **Save**.

What to do next

Deploy the Client with Group Policy, on page 132

Deploy the Client with Group Policy

Complete the steps in this task to deploy Cisco Jabber for Windows with Group Policy.

Before you begin

Set a Language Code, on page 132

Procedure

Step 1 Copy the installation package to a software distribution point for deployment.

All computers or users to which you plan to deploy Cisco Jabber for Windows must be able to access the installation package on the distribution point.

Step 2 Select **Start** > **Run** and then enter the following command:

```
GPMC.msc
```

The **Group Policy Management** console opens.

Step 3 Create a new group policy object.

a) Right-click on the appropriate domain in the left pane.
b) Select **Create a GPO in this Domain, and Link it here**.

The **New GPO** window opens.

c) Enter a name for the group policy object in the **Name** field.
d) Leave the default value or select an appropriate option from the **Source Starter GPO** drop-down list and then select **OK**.

The new group policy displays in the list of group policies for the domain.

Step 4 Set the scope of your deployment.

a) Select the group policy object under the domain in the left pane.

The group policy object displays in the right pane.

b) Select **Add** in the **Security Filtering** section of the **Scope** tab.

The **Select User, Computer, or Group** window opens.

c) Specify the computers and users to which you want to deploy Cisco Jabber for Windows.

Step 5 Specify the installation package.

a) Right-click the group policy object in the left pane and then select **Edit**.

The **Group Policy Management Editor** opens.

b) Select **Computer Configuration** and then select **Policies** > **Software Settings**.
c) Right-click **Software Installation** and then select **New** > **Package**.
d) Enter the location of the installation package next to **File Name**; for example, `\\server\software_distribution`.

Important You must enter a Uniform Naming Convention (UNC) path as the location of the installation package. If you do not enter a UNC path, Group Policy cannot deploy Cisco Jabber for Windows.

e) Select the installation package and then select **Open**.
f) In the **Deploy Software** dialog box, select **Assigned** and then **OK**.

Group Policy installs Cisco Jabber for Windows on each computer the next time each computer starts.

Configure Automatic Updates for Windows

To enable automatic updates, you create an XML file that contains the information for the most recent version, including the URL of the installation package on the HTTP server. The client retrieves the XML file when users sign in, resume their computer from sleep mode, or perform a manual update request from the **Help** menu.

XML File Structure

XML files for automatic updates have the following structure:

```
<JabberUpdate>
          <App name="JabberWin">
               <LatestBuildNum>12345</LatestBuildNum>
               <LatestVersion>11.8.x</LatestVersion>
               <Mandatory>true</Mandatory>
               <Message>
                  <![CDATA[<b>This new version of Cisco Jabber lets you do the
                  following:</b><ul><li>Feature 1</li><li>Feature 2</li></ul>For
                  more information click <a target="_blank"
                  href="http://cisco.com/go/jabber">here</a>.]]>
               </Message>
               <DownloadURL>http://http_server_name/CiscoJabberSetup.msi</DownloadURL>

          </App>
        </JabberUpdate>
```

Before you begin

- Install and configure an HTTP server to host the XML file and installation package.
- Ensure users have permission to install software updates on their workstations.

  Microsoft Windows stops update installations if users do not have administrative rights on their workstations. You must be logged in with administrative rights to complete installation.

Procedure

Step 1 Host the update installation program on your HTTP server.

Step 2 Create an update XML file with any text editor.

Step 3 Specify values in the XML as follows:

- `name`—Specify the following ID as the value of the `name` attribute for the `App` element:
  - JabberWin—The update applies to Cisco Jabber for Windows.
- `LatestBuildNum`—Build number of the update.
- `LatestVersion`—Version number of the update.
- `Mandatory`—(Windows clients only) True or False. Determines whether users must upgrade their client version when prompted.
- `Message`—HTML in the following format:

  `<![CDATA[your_html]]>`

- `DownloadURL`—URL of the installation package on your HTTP server.
- `AllowUpdatesViaExpressway`—(Windows client only). False (default) or True. Determines whether Jabber can carry out automatic updates while connected to the corporate network over the Expressway for Mobile and Remote Access.

  If your update XML file is hosted on a public web server, set this parameter to false. Otherwise the update file tells Jabber that it is hosted on an internal server that must be accessed through the Expressway for Mobile and Remote Access.

Step 4 Save and close your update XML file.

Step 5 Host your update XML file on your HTTP server.

Step 6 Specify the URL of your update XML file as the value of the UpdateUrl parameter in your configuration file.

Uninstall Cisco Jabber for Windows

You can uninstall Cisco Jabber for Windows using either the command line or the Microsoft Windows control panel. This document describes how to uninstall Cisco Jabber for Windows using the command line.

Use the Installer

If the installer is available on the file system, use it to remove Cisco Jabber for Windows.

Procedure

Step 1 Open a command line window.

Step 2 Enter the following command:

`msiexec.exe /x path_to_CiscoJabberSetup.msi`

For example,

`msiexec.exe /x C:\Windows\Installer\CiscoJabberSetup.msi /quiet`

Where `/quiet` specifies a silent uninstall.

The command removes Cisco Jabber for Windows from the computer.

Use the Product Code

If the installer is not available on the file system, use the product code to remove Cisco Jabber for Windows.

Procedure

Step 1 Find the product code.

a) Open the Microsoft Windows registry editor.

b) Locate the following registry key: `HKEY_CLASSES_ROOT\Installer\Products`

c) Select **Edit** > **Find**.
d) Enter Cisco Jabber in the **Find what** text box in the **Find** window and select **Find Next**.
e) Find the value of the **ProductIcon** key.

The product code is the value of the **ProductIcon** key, for example, `C:\Windows\Installer\{product_code}\ARPPRODUCTICON.exe`.

Note The product code changes with each version of Cisco Jabber for Windows.

Step 2 Open a command line window.

Step 3 Enter the following command:

```
msiexec.exe /x product_code
```

For example,

```
msiexec.exe /x 45992224-D2DE-49BB-B085-6524845321C7 /quiet
```

Where `/quiet` specifies a silent uninstall.

The command removes Cisco Jabber for Windows from the computer.

Install Cisco Jabber for Mac

Installer for Cisco Jabber for Mac

Installing the Client

You can choose to install the client using one of the following methods:

- Provide the installer for users to manually install the application. The client is installed in the `Applications` folder. You must remove previous versions of the client.
- Configure automatic updates for users, the installer silently updates the application.

  For automatic updates, the installer always adds the client in the `Applications` folder.

  - If the client existed in a different folder, or a sub folder of the `Applications` folder, then the installer creates a link in that folder to run the client in the Applications folder.
  - If the user previously renamed the client, then the installer renames the new client to match.

The installer prompts users for system credentials during the installation.

Quiet Install—To install the client quietly, in the Terminal tool use the following Mac OS X command:

```
sudo installer -pkg /path_to/Install_Cisco-Jabber-Mac.pkg -target /
```

For more information on the installer command, refer to the installer manual pages on your Mac.

Configuration

Provide configuration information for your users to sign into the client. Choose one of the following:

- Provide your users with a configuration URL with optional server information. For further information, see the *URL Configuration for Cisco Jabber for Mac* section.
- Provide your users with the server information to connect manually. For further information, see the *Manual Connection Settings* section.
- Use service discovery. For more information, see the *Service Discovery* section.

Running Jabber natively on Apple M1 Mac

Before Release 14.1.2, you can only run Jabber on an Intel-based Mac or using Rosetta on an Apple M1 Mac. Now, you can also run Jabber on an Apple M1 Mac without using Rosetta.

To run Jabber natively on an Apple M1 Mac, uncheck **Open using Rosetta** for **Cisco Jabber**.

You can check how you're running Jabber in the **Activity Monitor**. The **Kind** displays **Apple** when you run natively.

Run Installer Manually

You can run the installation program manually to install a single instance of the client and specify connection settings in the **Preferences** settings.

Before you begin

Remove any older versions of the client.

Procedure

Step 1 Launch the `jabber-mac.pkg`.
The installer opens a window to guide you through the installation process.

Step 2 Follow the steps to complete the installation process.
The installer prompts the user to enter the system credentials.

Step 3 Launch the client, using either a configuration URL or running the client directly.
Enter user credentials.

URL Configuration for Cisco Jabber for Mac

To enable users to launch Cisco Jabber without manually entering service discovery information, create and distribute a configuration URL to users.

You can provide a configuration URL link to users by emailing the link to the user directly, or by posting the link to a website.

You can include and specify the following parameters in the URL:

- ServicesDomain—Required. Every configuration URL must include the domain of the IM and presence server that Cisco Jabber needs for service discovery.
- ServiceDiscoveryExcludedServices—Optional. You can exclude any of the following services from the service discovery process:

- Webex—When you set this value, the client:
  - Does not perform CAS lookup
  - Looks for:
    - `_cisco-uds`
    - `_cuplogin`
    - `_collab-edge`
- CUCM—When you set this value, the client:
  - Does not look for `_cisco-uds`
  - Looks for:
    - `_cuplogin`
    - `_collab-edge`
- CUP—When you set this value, the client:
  - Does not look for `_cuplogin`
  - Looks for:
    - `_cisco-uds`
    - `_collab-edge`

You can specify multiple, comma-separated values to exclude multiple services.

If you exclude all three services, the client does not perform service discovery and prompts the user to manually enter connection settings.

- ServicesDomainSsoEmailPrompt—Optional. Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.
  - ON
  - OFF
- EnablePRTEncryption—Optional. Specifies that the PRT file is encrypted. Applies to Cisco Jabber for Mac.
  - true
  - false
- PRTCertificateName—Optional. Specifies the name of the certificate. Applies to Cisco Jabber for Mac.
- InvalidCertificateBehavior—Optional. Specifies the client behavior for invalid certificates.
  - RejectAndNotify—A warning dialog displays and the client doesn't load.
  - PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate.

- Telephony_Enabled—Specifies whether the user has phone capability or not. The default is true.
  - True
  - False
- DiagnosticsToolEnabled—Specifies whether the diagnostics tool is available in the client. The default is true.
  - True
  - False

Create the configuration URL in the following format:

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>
```

Note The parameters are case sensitive.

Examples

- `ciscojabber://provision?ServicesDomain=cisco.com`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

Configure Automatic Updates for Mac

To enable automatic updates, you create an XML file that contains the information for the most recent version, including the URL of the installation package on the HTTP server. The client retrieves the XML file when users sign in, resume their computer from sleep mode, or perform a manual update request from the **Help** menu.

XML File Structure

The following is example XML file for automatic updates:

```
<JabberUpdate>
<App name="JabberMac">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.6.1</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2</li>
  </ul>For more information click <a target="_blank"
```

```
href="http://cisco.com/go/jabber">here</a>.]]>
  </Message>

<DownloadURL>http://http_server_name/Install_Cisco-Jabber-Mac-1.1.1-12345-MrbCdd.zip</DownloadURL>
</App>
</JabberUpdate>
```

Example XML File 2

The following is an example XML file for automatic updates for both Cisco Jabber for Windows and Cisco Jabber for Mac:

```
<JabberUpdate>
 <App name="JabberMac">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.6.1</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2</li>
  </ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
  </Message>

<DownloadURL>http://http_server_name/Install_Cisco-Jabber-Mac-1.1.1-12345-MrbCdd.zip</DownloadURL>

 </App>
 <App name="JabberWin">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.0</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2
  </li></ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
  </Message>
  <DownloadURL>http://http_server_name/CiscoJabberSetup.msi
  </DownloadURL>
</App>
</JabberUpdate>
```

Before you begin

Install and configure an HTTP server to host the XML file and installation package.

Note Configure Web servers to escape special characters to ensure the DSA signature succeeds. For example, on Microsoft IIS the option is: **Allow double spacing**.

Procedure

Step 1 Host the update installation program on your HTTP server.

Step 2 Create an update XML file with any text editor.

Step 3 Specify values in the XML as follows:

- `name`—Specify the following ID as the value of the `name` attribute for the `App` element:
  - JabberWin—The update applies to Cisco Jabber for Windows.
  - JabberMac—The update applies to Cisco Jabber for Mac.

- `LatestBuildNum`—Build number of the update.
- `LatestVersion`—Version number of the update.
- `Mandatory`—True or False. Determines whether users must upgrade their client version when prompted.
- `Message`—HTML in the following format:

  `<![CDATA[`*`your_html`*`]]>`
- `DownloadURL`—URL of the installation package on your HTTP server.

  For Cisco Jabber for Mac the URL file must be in the following format:

  `Install_Cisco-Jabber-Mac-`*`version-size-dsaSignature`*`.zip`

Step 4 Save and close your update XML file.

Step 5 Host your update XML file on your HTTP server.

Step 6 Specify the URL of your update XML file as the value of the UpdateUrl parameter in your configuration file.

Install Cisco Jabber Mobile Clients

Procedure

Step 1 To install Cisco Jabber for Android, download the app from Google Play from your mobile device.

Step 2 To install Cisco Jabber for iPhone and iPad, download the app from the App Store from your mobile device.

URL Configuration for Cisco Jabber for Android, iPhone, and iPad

To enable users to launch Cisco Jabber without manually entering service discovery information, create and distribute a configuration URL to users.

You can provide a configuration URL link to users by emailing the link to the user directly, or by posting the link to a website.

You can include and specify the following parameters in the URL:

- ServicesDomain—Required. Every configuration URL must include the domain of the IM and presence server that Cisco Jabber needs for service discovery.
- ServiceDiscoveryExcludedServices—Optional. You can exclude any of the following services from the service discovery process:
  - Webex—When you set this value, the client:
    - Does not perform CAS lookup
    - Looks for:
      - `_cisco-uds`

- `_cuplogin`
- `_collab-edge`

- CUCM—When you set this value, the client:
  - Does not look for `_cisco-uds`
  - Looks for:
    - `_cuplogin`
    - `_collab-edge`

- CUP—When you set this value, the client:
  - Does not look for `_cuplogin`
  - Looks for:
    - `_cisco-uds`
    - `_collab-edge`

You can specify multiple, comma-separated values to exclude multiple services.

If you exclude all three services, the client does not perform service discovery and prompts the user to manually enter connection settings.

- ServicesDomainSsoEmailPrompt—Optional. Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.
  - ON
  - OFF

- InvalidCertificateBehavior—Optional. Specifies the client behavior for invalid certificates.
  - RejectAndNotify—A warning dialog displays and the client doesn't load.
  - PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate.

- PRTCertificateUrl—Specifies the name of a certificate with a public key in the trusted root certificate store. Applies to Cisco Jabber mobile clients.
- Telephony_Enabled—Specifies whether the user has phone capability or not. The default is true.
  - True
  - False

- ForceLaunchBrowser—Used to force user to use the external browser. Applies to Cisco Jabber mobile clients.
  - True
  - False

Note ForceLaunchBrowser is used for client certificate deployments and for devices with Android OS below 5.0.

Create the configuration URL in the following format:

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>
```

Note The parameters are case sensitive.

Examples

- `ciscojabber://provision?ServicesDomain=cisco.com`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

Mobile Configuration Using Enterprise Mobility Management

Enterprise Mobility Management (EMM) with the AppConfig Standard

Before using Enterprise Mobility Management (EMM), ensure:

- The EMM vendor supports Android for Work or Apple Managed App Configuration.
- That Android devices have OS 5.0 or later.

To allow users to launch Cisco Jabber for Android or Cisco Jabber for iPhone and iPad, you can configure Cisco Jabber using Enterprise Mobility Management (EMM). For more information on setting up EMM, refer to the instructions for administrators provided by the EMM provider.

If you want Jabber to run only on managed devices, then you can deploy certificate-based authentication, and enroll the client certificate through EMM.

You can configure Cisco Jabber for iPhone and iPad as the default dialer for the local contacts that are imported from Microsoft Exchange Server. Configure the profile with the **Exchange ActiveSync** and enter the value `com.cisco.jabberIM` in the **Default Audio Call App** field of the MDM configuration file.

When using EMM, disable URL configuration by setting the AllowUrlProvisioning parameter to False in the EMM application. For more information on configuring the parameter, see the *AllowUrlProvisioning Parameter* section.

EMM by App Wrapping

Another approach to EMM is *app wrapping*. You use a vendor app-wrapping tool to encapsulate Jabber and apply policies to restrict what users can do in Jabber. You then distribute the encapsulated Jabber to your users. You must repeat the encapsulation anytime you upgrade to a new version of Jabber.

We require you to sign a two-way agreement to use app wrapping with Cisco Jabber. Contact us for details at `jabber-mobile-mam@cisco.com`.

EMM by SDK Integration

In Release 12.8, we added support for Microsoft Intune and BlackBerry Dynamics as another approach for EMM. Using the Microsoft and BlackBerry SDKs, we created new clients that are available through the App Store and Google Play Store:

- Jabber for Intune
- Jabber for BlackBerry

With these solutions, you create your management policies in a portal. When users sign in with the new clients, the clients synch with the portal and apply your policies.

EMM with Jabber for Intune

When you use the Jabber for Intune client in your deployment, your administrator configures your management policies in Microsoft Azure. Users download the new client from the App Store or Google Play Store. When the user runs the new client, it synchs with the policies that the administrator created.

Caution Jabber for Intune doesn't support Apple Push Notification (APN) on the iOS platform. When you put Jabber in the background, iOS devices might not receive chat messages and calls.

Note For Android devices, users first install the Intune Company Portal. Then, they run the client through the portal.

The general process for setting up Jabber for Intune is:

1. Create a new Azure AD tenant.
2. Create new AD users or synch your on-premises AD users.
3. Create an Office 365 group or a Security group and add your users.
4. Add the Jabber for Intune client into Microsoft Intune.
5. Create and deploy your policies in Microsoft Intune.
6. Users sign in to the client and synch to receive your policies.

For details on these steps, see the Microsoft documentation.

This table lists the Microsoft Intune restrictions that we support in app protection policies for Cisco Jabber:

Restriction	Android	iPhone and iPad
Send data to other apps	Yes	Yes
Save copies of your organization's data	Yes	Yes
Cut, copy, and paste to other apps	Yes	Yes
Screen captures	Yes	N/A
Maximum PIN attempts	Yes	Yes
Offline grace periods	Yes	Yes
Minimum app versions	Yes	Yes
Use on jailbroken or rooted devices	Yes	Yes
Minimum device OS version	Yes	Yes
Minimum patch version	Yes	N/A
Work (or school) account credentials for access	Yes	Yes
Recheck the access requirements	Yes	Yes

EMM with Jabber for BlackBerry

When you use the Jabber for BlackBerry client in your deployment, your administrator configures your management policies in the BlackBerry Unified Endpoint Management (UEM). Users download the new client from the App Store or Google Play Store. Jabber for BlackBerry is undergoing BlackBerry certification and isn't yet available in BlackBerry Marketplace.

Important Because the client is undergoing BlackBerry certification, we must grant access to your organization. To receive access, contact us (jabber-mobile-mam@cisco.com) and provide the Organization ID of your customer from their BlackBerry UEM server.

The new client has integrated the BlackBerry Dynamics SDK and can directly fetch the policies from BlackBerry UEM. The client bypasses BlackBerry Dynamics for connectivity and storage. The FIPS setting is not supported through the BlackBerry Dynamics SDK.

Your chat, voice, and video traffic bypasses the BlackBerry infrastructure. When the client isn't on-premises, it requires Mobile & Remote Access through a Cisco Expressway for all traffic.

Caution Jabber for BlackBerry doesn't support Apple Push Notification (APN) on the iOS platform. When you put Jabber in the background, iOS devices might not receive chat messages and calls.

Note Jabber for BlackBerry on Android requires Android 6.0 or above.

Jabber for BlackBerry on iOS requires iOS 11.0 or above.

For BlackBerry Dynamics, your administrator sets up policies in to control use of the Jabber for BlackBerry client.

The general process for setting up Jabber for BlackBerry is:

1. Create a server in the UEM.
2. Add the Jabber for BlackBerry client into BlackBerry Dynamics.
3. Create or import your users in BlackBerry Dynamics.

Note For Android users, you can optionally generate access keys in BlackBerry Dynamics.

4. Create and deploy your policies in UEM. Note the behavior of these settings on the Jabber for BlackBerry app configuration:
   - If you enable the optional DLP policy, BlackBerry requires that:
     - Use BlackBerry Works to send emails.
     - Use BlackBerry Access for SSO authentication in iOS devices. Enable **Use native browser** for iOS on Expressway and Unified Communications Manager. Then, add the **`ciscojabber`** scheme to the BlackBerry access policies in the BlackBerry UEM.
   - This list shows the Jabber parameters that are useful to set through app configuration in Jabber for BlackBerry deployments. See the *URL Configuration for Cisco Jabber for Android, iPhone, and iPad* section in the *Deployment Guide* for more details on these parameters:

Field	Supported on iOS	Supported on Android
Disable cross launch Webex Meetings [1]	Yes	Yes
Services Domain	Yes	Yes
Voice Services Domain	Yes	Yes
Service Discovery Excluded Services	Yes	Yes
Services Domain SSO Email Prompt	Yes	Yes
Invalid Certificate Behavior	Yes	Yes
Telephony Enabled	Yes	Yes
Allow Url Provisioning	Yes	Yes
IP Mode	Yes	Yes

[1] Enabling cross launch of Webex Meetings allows it to run as an exception in a BlackBerry Dynamics container that doesn't allow non-Dynamics apps.

5. Users sign in to the client.

For details on these steps, see the BlackBerry documentation.

This table lists the BlackBerry restrictions that we support in app protection policies for Cisco Jabber:

Group	Feature	Android	iPhone and iPad
IT policies	Wipe the device without network connectivity	Yes	Yes
Activation	Allowed Version	Yes	Yes
BlackBerry Dynamics	Password	Yes	Yes
	Data leakage prevention - Don’t allow copying data from BlackBerry Dynamics apps into non-BlackBerry Dynamics apps	Yes	Yes
	Data leakage prevention - Don’t allow copying data from non-BlackBerry Dynamics apps into BlackBerry Dynamics apps	Yes	Yes
	Data leakage prevention - Don’t allow screen captures on Android and Windows 10+ devices	Yes	N/A
	Data leakage prevention - Don’t allow screen recording and sharing on iOS devices	N/A	Yes
	Data leakage prevention - Don’t allow custom keyboards on iOS devices	N/A	Yes
Enterprise Management Agent profile	Allow personal app collection	Yes	Yes
Compliance profile	Rooted OS or failed attestation	Yes	Yes
	Restricted OS version is installed	Yes	Yes
	Required security patch level isn’t installed	Yes	N/A

IdP Connections in Jabber for BlackBerry

In Jabber for Android and iPhone and iPad deployments, the client connects to an Identity Provider (IdP) proxy in the DMZ. The proxy then passes the request to the IdP server behind the inner firewall.

In Jabber for BlackBerry, you have an alternate path available. If you enable the DLP policy in the BlackBerry UEM, clients on iOS devices can securely tunnel directly to the IdP server. To use this setup, configure your deployment as follows:

- Enable **Use native browser** for iOS on Expressway and Unified CM.
- Add the **`ciscojabber`** scheme to the BlackBerry access policies in the BlackBerry UEM.

Jabber for BlackBerry on the Android OS always connects to the IdP proxy for SSO.

If your deployment only contains devices running on iOS, you don't need an IdP proxy in the DMZ. But, if your deployment contains any devices running on Android OS, you require the IdP proxy.

App Transport Security on iOS

iOS includes the App Transport Security (ATS) feature. ATS requires that Jabber for BlackBerry and Jabber for Intune makes secure network connections over TLS with reliable certificates and encryption. ATS blocks connections to servers that don't have an X.509 digital certificate. The certificate must pass these checks:

- An intact digital signature
- A valid expiration date
- A name that matches the DNS name of the server
- A chain of valid certificates to a trusted anchor certificate from a CA

Note For more information on trusted anchor certificates that are part of iOS, see *Lists of available trusted root certificates in iOS* at https://support.apple.com/en-us/HT204132. A system administrator or user can also install their own trusted anchor certificate, as long as it meets the same requirements.

For more information on ATS, see *Preventing Insecure Network Connections* at https://developer.apple.com/documentation/security/preventing_insecure_network_connections.

Useful Parameters for MDM Deployments

EMM vendors might allow you to set different value types in Application Configuration settings, but Jabber only reads String value types. For EMM, you might find the following parameters useful. See the *URL Configuration for Cisco Jabber for Android, iPhone, and iPad* section for more details on these parameters:

- ServicesDomain
- VoiceServicesDomain
- ServiceDiscoveryExcludedServices
- ServicesDomainSsoEmailPrompt
- EnablePRTEncryption
- PRTCertificateURL
- PRTCertificateName
- InvalidCertificateBehavior
- Telephony_Enabled
- ForceLaunchBrowser
- FIPS_MODE
- CC_MODE

- LastLoadedUserProfile
- AllowUrlProvisioning

  When using EMM, disable URL configuration by setting the AllowUrlProvisioning parameter to **`False`** in the EMM application. For more information on configuring the parameter, refer to the topic *AllowUrlProvisioning Parameter*.
- IP_Mode
- AllowTeamsUseEmbeddedSafari—Cisco Jabber for iPhone and iPad only
- AutoLoginUserName
- AutoLoginUserPassword

The following sections discuss the use of some of these parameters in an MDM deployment.

AllowUrlProvisioning Parameter

Use this parameter when migrating users from URL configuration to EMM.

The following values apply to this parameter:

- true (default)—Bootstrap configuration is performed using URL configuration
- false— Bootstrap configuration is not performed using URL configuration

  Example:`<AllowURLProvisioning>`*`false`*`</AllowURLProvisioning>`

AutoLoginUserName

Applies to Cisco Jabber for iPhone and iPad.

In EMM, defines the username on a mobile device. This parameter must be used with the AutoLoginUserPassword parameter and the ServicesDomain parameter. Together, these parameters let you install the Jabber app with the user's sign-in details already entered.

AutoLoginUserPassword

Applies to Cisco Jabber for iPhone and iPad.

In EMM, defines the password on a mobile device. This parameter must be used with the AutoLoginUserName parameter and the ServicesDomain parameter. Together, these parameters let you install the Jabber app with the user's sign-in details already entered.

CC_MODE Parameter

Use this parameter to enable or disable Common Criteria mode on Cisco Jabber mobile clients using EMM.

- *true*—Runs Cisco Jabber in Common Criteria mode.
- *false* (default)—Does not run Cisco Jabber in Common Criteria mode.

  Example:`<CC_MODE>`*`true`*`</CC_MODE>`

Note To enable CC_MODE, the RSA key size must be at least 2048 bits. For more information about how to set up Jabber to run in common criteria mode, read about how to *Deploy Cisco Jabber Applications* in the *On-Premises Deployment Guide for Cisco Jabber 12.5*.

FIPS_MODE Parameter

Use this parameter to enable or disable FIPS mode on Cisco Jabber mobile clients using EMM.

- *true*—Runs Cisco Jabber in FIPS mode.
- *false*—Does not run Cisco Jabber in FIPS mode.

  Example:`<FIPS_MODE>false</FIPS_MODE>`

LastLoadedUserProfile

Applies to Cisco Jabber for iPhone and iPad and Cisco Jabber for Android.

In EMM, defines the username on a mobile device, so that the user only needs to enter their password to log onto the device.

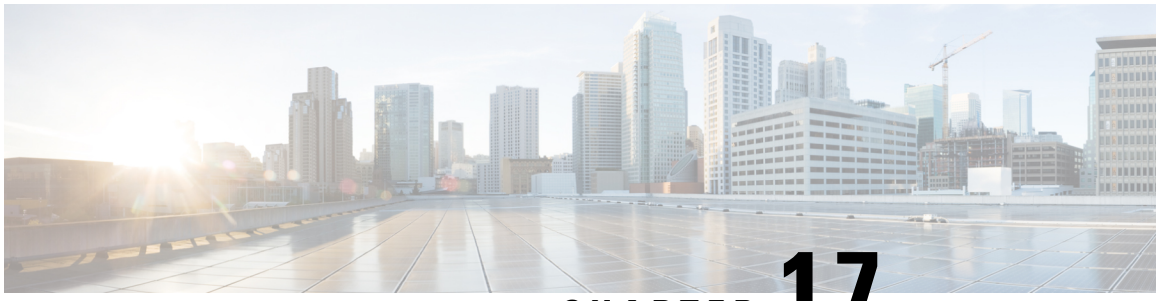
```
<LastLoadedUserProfile>username@example.com<LastLoadedUserProfile>
```

Install Jabber Softphone for VDI

Procedure

Step 1 Complete the workflow for deploying Jabber.

Step 2 To install Jabber Softphone for VDI, follow the instructions in the Deployment and Installation Guide for Cisco Jabber Softphone for VDI for the client you are installing.



CHAPTER 17

Remote Access

Service Discovery Requirements Workflow

Procedure

	Command or Action	Purpose
Step 1	Service Discovery Requirements, on page 151	
Step 2	DNS Requirements, on page 152	
Step 3	Certificate Requirements, on page 152	
Step 4	Test _collab-edge SRV Record, on page 152	

Service Discovery Requirements

Service discovery enables clients to automatically detect and locate services on your enterprise network. Expressway for Mobile and Remote Access allows you to access the services on your enterprise network. You should meet the following requirements to enable the clients to connect through Expressway for Mobile and Remote Access and discover services:

- DNS requirements
- Certificate requirements
- Test external SRV `_collab-edge`.

DNS Requirements

The DNS requirements for service discovery through remote access are:

- Configure a `_collab-edge` DNS SRV record on an external DNS server.
- Configure a `_cisco-uds` DNS SRV record on the internal name server.
- Optionally, for a hybrid cloud-based deployment with different domains for the IM and Presence server and the voice server, configure the Voice Services Domain to locate the DNS server with the `_collab-edge` record.

Certificate Requirements

Before you configure remote access, download the Cisco VCS Expressway and Cisco Expressway-E Server certificate. The Server certificate is used for both HTTP and XMPP.

For more information on configuring Cisco VCS Expressway certificate, see Configuring Certificates on Cisco VCS Expressway.

Test _collab-edge SRV Record

Test SRV records

After creating your SRV records test to see if they are accessible.

Tip You can also use the SRV check tool on the Collaboration Solutions Analyzer site if you prefer a web-based option.

Procedure

Step 1 Open a command prompt.

Step 2 Enter **nslookup**.

The default DNS server and address is displayed. Confirm that this is the expected DNS server.

Step 3 Enter **set type=SRV**.

Step 4 Enter the name for each of your SRV records.

For example, `_cisco-uds._tcp.`*`exampledomain`*

- Displays server and address—SRV record is accessible.
- Displays `_cisco-uds_tcp.`*`exampledomain`*`: Non-existent domain`—There is an issue with your SRV record.

Cisco Anyconnect Deployment Workflow

Procedure

	Command or Action	Purpose
Step 1	Application Profiles, on page 153	
Step 2	Automate VPN Connection, on page 154	
Step 3	AnyConnect Documentation Reference, on page 157	
Step 4	Session Parameters, on page 157	

Cisco AnyConnect Deployment

Application Profiles

After you download the Cisco AnyConnect Secure Mobility Client to their device, the ASA must provision a configuration profile to the application.

The configuration profile for the Cisco AnyConnect Secure Mobility Client includes VPN policy information such as the company ASA VPN gateways, the connection protocol (IPSec or SSL), and on-demand policies.

You can provision application profiles for Cisco Jabber for iPhone and iPad in one of the following ways:

ASDM

We recommend that you use the profile editor on the ASA Device Manager (ASDM) to define the VPN profile for the Cisco AnyConnect Secure Mobility Client.

When you use this method, the VPN profile is automatically downloaded to the Cisco AnyConnect Secure Mobility Client after the client establishes the VPN connection for the first time. You can use this method for all devices and OS types, and you can manage the VPN profile centrally on the ASA.

For more information, see the *Creating and Editing an AnyConnect Profile* topic of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

iPCU

You can provision iOS devices using an Apple configuration profile that you create with the iPhone Configuration Utility (iPCU). Apple configuration profiles are XML files that contain information such as device security policies, VPN configuration information, and Wi-Fi, mail, and calendar settings.

The high-level procedure is as follows:

1. Use iPCU to create an Apple configuration profile.

   For more information, see the iPCU documentation.

2. Export the XML profile as a .mobileconfig file.

3. Email the .mobileconfig file to users.

   After a user opens the file, it installs the AnyConnect VPN profile and the other profile settings to the client application.

MDM

You can provision iOS devices using an Apple configuration profile that you create with third-party Mobile Device Management (MDM) software. Apple configuration profiles are XML files that contain information such as device security policies, VPN configuration information, and Wi-Fi, mail, and calendar settings.

The high-level procedure is as follows:

1. Use MDM to create the Apple configuration profiles.

   For information on using MDM, see the Apple documentation.

2. Push the Apple configuration profiles to the registered devices.

To provision application profiles for Cisco Jabber for Android, use the profile editor on the ASA Device Manager (ASDM) to define the VPN profile for the Cisco AnyConnect Secure Mobility Client. The VPN profile is automatically downloaded to the Cisco AnyConnect Secure Mobility Client after the client establishes the VPN connection for the first time. You can use this method for all devices and OS types, and you can manage the VPN profile centrally on the ASA. For more information, see the *Creating and Editing an AnyConnect Profile* topic of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Automate VPN Connection

When users open Cisco Jabber from outside the corporate Wi-Fi network, Cisco Jabber needs a VPN connection to access the Cisco UC application servers. You can set up the system to allow Cisco AnyConnect Secure Mobility Client to automatically establish a VPN connection in the background, which helps ensure a seamless user experience.

Note Even if VPN is set to automatic connection, VPN is not launched before Expressway Mobile and Remote Access because that has the higher connection priority.

Set Up Trusted Network Connection

The Trusted Network Detection feature enhances the user experience by automating the VPN connection based on the user's location. When the user is inside the corporate Wi-Fi network, Cisco Jabber can reach the Cisco UC infrastructure directly. When the user leaves the corporate Wi-Fi network, Cisco Jabber automatically detects that it is outside the trusted network. After this occurs, Cisco AnyConnect Secure Mobility Client initiates the VPN to ensure connectivity to the UC infrastructure.

Note The Trusted Network Detection feature works with both certificate- and password-based authentication. However, certificate-based authentication provides the most seamless user experience.

Procedure

Step 1 Using ASDM, open the Cisco AnyConnect client profile.

Step 2 Enter the list of Trusted DNS Servers and Trusted DNS Domain Suffixes that an interface can receive when the client is within a corporate Wi-Fi network. The Cisco AnyConnect client compares the current interface DNS servers and domain suffix with the settings in this profile.

Note You must specify all your DNS servers to ensure that the Trusted Network Detection feature works properly. If you set up both the TrustedDNSDomains and TrustedDNSServers, sessions must match both settings to be defined as a trusted network.

For detailed steps for setting up Trusted Network Detection, see the *Trusted Network Detection* section in the *Configuring AnyConnect Features* chapter (Release 2.5) or *Configuring VPN Access* (releases 3.0 or 3.1) of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Set Up Connect On-Demand VPN

The Apple iOS Connect On Demand feature enhances the user experience by automating the VPN connection based on the user's domain.

When the user is inside the corporate Wi-Fi network, Cisco Jabber can reach the Cisco UC infrastructure directly. When the user leaves the corporate Wi-Fi network, Cisco AnyConnect automatically detects if it is connected to a domain that you specify in the AnyConnect client profile. If so, the application initiates the VPN to ensure connectivity to the UC infrastructure. All applications on the device including Cisco Jabber can take advantage of this feature.

Note Connect On Demand supports only certificate-authenticated connections.

The following options are available with this feature:

- **Always Connect** — Apple iOS always attempts to initiate a VPN connection for domains in this list.
- **Connect If Needed** — Apple iOS attempts to initiate a VPN connection to the domains in the list only if it cannot resolve the address using DNS.
- **Never Connect** — Apple iOS never attempts to initiate a VPN connection to domains in this list.

Attention Apple plans to remove the Always Connect option in the near future. After the Always Connect option is removed, users can select the Connect If Needed option. In some cases, Cisco Jabber users may have issues when using the Connect If Needed option. For example, if the hostname for the Cisco Unified Communications Manager is resolvable outside the corporate network, iOS will not trigger a VPN connection. The user can work around this issue by manually launching Cisco AnyConnect Secure Mobility Client before making a call.

Procedure

Step 1 Use the ASDM profile editor, iPCU, or MDM software to open the AnyConnect client profile.

Step 2 In the AnyConnect client profile, under the Connect if Needed section, enter your list of on-demand domains.

The domain list can include wild-card options (for example, cucm.cisco.com, cisco.com, and *.webex.com).

Set Up Automatic VPN Access on Cisco Unified Communications Manager

Before you begin

- The mobile device must be set up for on-demand access to VPN with certificate-based authentication. For assistance with setting up VPN access, contact the providers of your VPN client and head end.
- For requirements for Cisco AnyConnect Secure Mobility Client and Cisco Adaptive Security Appliance, see the *Software Requirements* topic.
- For information about setting up Cisco AnyConnect, see the *Cisco AnyConnect VPN Client Maintain and Operate Guides*.

Procedure

Step 1 Identify a URL that will cause the client to launch VPN on Demand.

a) Use one of the following methods to identify a URL that causes the client to launch VPN on Demand.

- Connect if Needed
  - Configure Cisco Unified Communications Manager for access through a domain name (not an IP address) and ensure that this domain name is not resolvable outside the firewall.
  - Include this domain in the “Connect If Needed” list in the Connect On Demand Domain List of the Cisco AnyConnect client connection.
- Always Connect
  - Set the parameter in step 4 to a nonexistent domain. A nonexistent domain causes a DNS query to fail when the user is inside or outside the firewall.
  - Include this domain to the “Always Connect” list in the Connect On Demand Domain List of the Cisco AnyConnect client connection.

    The URL must include only the domain name. Do not include a protocol or a path (for example, use “cm8ondemand.company.com” instead of “https://cm8ondemand.company.com/vpn”.

b) Enter the URL in Cisco AnyConnect and verify that a DNS query on this domain fails.

Step 2 Open the **Cisco Unified CM Administration** interface.

Step 3 Navigate to the device page for the user.

Step 4 In the **Product Specific Configuration Layout** section, in the **On-Demand VPN URL** field, enter the URL that you identified and used in Cisco AnyConnect in Step 1.

The URL must be a domain name only, without a protocol or path.

Step 5 Select **Save**.

When Cisco Jabber opens, it initiates a DNS query to the URL. If this URL matches the On-Demand domain list entry that you defined in this procedure (for example, cisco.com), Cisco Jabber indirectly initiates the AnyConnect VPN connection.

What to do next

- Test this feature.
  - Enter the URL into the Internet browser on the iOS device and verify that VPN launches automatically. You should see a VPN icon in the status bar.
  - Verify that the iOS device can connect to the corporate network using VPN. For example, access a web page on your corporate intranet. If the iOS device cannot connect, contact the provider of your VPN technology.
  - Verify with your IT department that your VPN does not restrict access to certain types of traffic (for example, if the administrator set the system to allow only email and calendar traffic).
- Verify that you set up the client to connect directly to the corporate network.

AnyConnect Documentation Reference

For detailed information on AnyConnect requirements and deployments review the documentation for your release at the following: https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-user-guide-list.html

Session Parameters

You can configure ASA session parameters to improve performance for secure connections. For the best user experience, you should configure the following ASA session parameters:

- Datagram Transport Layer Security (DTLS) — DTLS is an SSL protocol that provides a data path that prevents latency and data loss.
- Auto Reconnect — Auto reconnect, or session persistence, lets Cisco AnyConnect Secure Mobility Client recover from session disruptions and re-establish sessions.
- Session Persistence — This parameter allows the VPN session to recover from service disruptions and re-establish the connection.
- Idle Timeout — Idle timeout defines a period of time after which ASA terminates secure connections, if no communication activity occurs.
- Dead-Peer Detection (DTD) — DTD ensures that ASA and Cisco AnyConnect Secure Mobility Client can quickly detect failed connections.

Set ASA Session Parameters

We recommend that you set up the ASA session parameters as follows to optimize the end user experience for Cisco AnyConnect Secure Mobility Client.

Procedure

Step 1 Set up Cisco AnyConnect to use DTLS.

For more information, see the *Enabling Datagram Transport Layer Security (DTLS) with AnyConnect (SSL) Connections* topic in the *Configuring AnyConnect Features Using ASDM* chapter of the *Cisco AnyConnect VPN Client Administrator Guide, Version 2.0*.

Step 2 Set up session persistence (auto-reconnect).

a) Use ASDM to open the VPN client profile.
b) Set the **Auto Reconnect Behavior** parameter to **Reconnect After Resume**.

For more information, see the *Configuring Auto Reconnect* topic in the *Configuring AnyConnect Features* chapter (Release 2.5) or *Configuring VPN Access* chapter (releases 3.0 or 3.1) of the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Step 3 Set the idle timeout value.

a) Create a group policy that is specific to Cisco Jabber clients.
b) Set the idle timeout value to 30 minutes.

For more information, see the *vpn-idle-timeout* section of the *Cisco ASA 5580 Adaptive Security Appliance Command Reference* for your release

Step 4 Set up Dead Peer Detection (DPD).

a) Disable server-side DPD.
b) Enable client-side DPD.

For more information, see the *Enabling and Adjusting Dead Peer Detection* topic of the *Configuring VPN* chapter of the *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6*.

Define Mobile and Remote Access Policies for User Profiles

When your users are working outside your corporate network, you can add Mobile and Remote Access (MRA) access policies in Cisco Unified Communications Manager, and control what services in Cisco Jabber they can access. The MRA access policies are assigned to user profiles and you can allocate different MRA access policies to users in your organization.

Before you begin

Mobile and Remote Access policies is supported on Cisco Unified Communications Manager Release 12.0 or later, Cisco Expressway X8.10 or later, and in an OAuth enabled environment.

Procedure

Step 1 In **Cisco Unified CM Administration**, go to **User Management** and select **End User**.

Step 2 Click **Find** to search for end-users, and select an end-user.

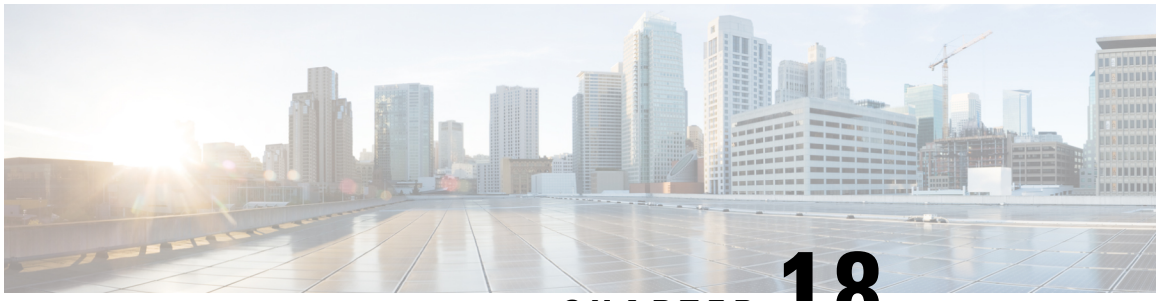
Step 3 In the **End User Configuration** window, click **View Details** for a **User Profile**.

Step 4 In the **Mobile and Remote Access Policy** section, select **Enable Mobile and Remote Access**.

Step 5 In the **Jabber Policies** drop-down, choose a policy:

- **No Service**—Users cannot access any Cisco Jabber service.
- **IM & Presence only**—Users can access only IM, presence, voicemail, and contact search.
- **IM & Presence, Voice and Video calls**—Users can access all Cisco Jabber services.

Step 6 Select **Save**.



CHAPTER 18

Quality of Service

Quality of Service Options

Use the following options to configure the quality of service for Cisco Jabber:

Option	Description
Enable Media Assure, on page 161	Configure Media Assure in Cisco Unified Communications Manager.
Supported Codecs, on page 163	Review the supported Codecs for each client.
Define a port range on the SIP profile, on page 164	Configure Port Ranges in Cisco Unified Communications Manager
Define a Port Range in Jabber-config.xml, on page 164	Configure Port Ranges in the jabber-config.xml file.
Set DSCP Values, on page 164	Configure Differentiated Services Code Point (DSCP) values.

Enable Media Assure

Media Assure enhances the quality of real-time media on all network types so that your meetings aren't interrupted because of poor media quality.

Before you begin

Media Assure is supported for video on Cisco Unified Communications Manager Release 10.x or later and for audio and video on Cisco Unified Communications Manager Release 11.5 or later.

Procedure

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

Step 2 Select **Device** > **Device Settings** > **Sip Profile**.

Step 3 Select your profile from the available list.

Step 4 In the **SDP Information** section, select **Pass all unknown SDP attributes** value for **SDP Transparency Profile**.

Step 5 Select **Apply Config.**
All SIP devices using this profile must restart before any changes are applied.

Supported Codecs

Type	Codec	Codec Type	Cisco Jabber for Android	Cisco Jabber for iPhone and iPad	Cisco Jabber for Mac	Cisco Jabber for Windows
Audio	G.711	A-law	Yes Supports normal mode.		Yes	Yes
		µ-law/Mu-law	Yes Supports normal mode.		Yes	Yes
	G.722		Yes		Yes	Yes
	G.722.1	24 kb/s and 32 kb/s	Yes Supports normal mode.		Yes	Yes
	G.729		Does not support Visual Voicemail with G.729; however, you can access voice messages using G.729 and the **Call Voicemail** feature.		No	No
	G.729a		Yes Minimum requirement for low-bandwidth availability. Only codec that supports low-bandwidth mode. Supports normal mode.		Yes	Yes
	Opus		Yes		Yes	Yes
Video	H.264/AVC	Baseline profile	Yes		Yes	Yes
		High profile	No		Yes	Yes
Voicemail	G.711	A-law	Yes		Yes	Yes
		µ-law / Mu-law (default)	Yes		Yes	Yes
	PCM linear		Yes		Yes	Yes

If users have issues with voice quality when using Cisco Jabber for Android or Cisco Jabber for iPhone and iPad, they can turn low-bandwidth mode on and off in the client settings.

Define a port range on the SIP profile

The client uses the port range to send RTP traffic across the network. The client divides the port range equally and uses the lower half for audio calls and the upper half for video calls. As a result of splitting the port range for audio media and video media, the client creates identifiable media streams. You can then classify and prioritize those media streams by setting DSCP values in the IP packet headers.

Procedure

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

Step 2 Select **Device** > **Device Settings** > **SIP Profile**.

Step 3 Find the appropriate SIP profile or create a new SIP profile.

The **SIP Profile Configuration** window opens.

Step 4 Specify whether you want common or separate port ranges for audio and video. If you are separating your audio and video port ranges, provide audio and video ports. Specify the port range in the following fields:

- **Start Media Port** — Defines the start port for media streams. This field sets the lowest port in the range.
- **Stop Media Port** — Defines the stop port for media streams. This field sets the highest port in the range.

Step 5 Select **Apply Config** and then **OK**.

Define a Port Range in Jabber-config.xml

This topics applies to Cisco Jabber for Windows.

Procedure

To specify a port range to use when users share their screen from a chat window in Cisco Jabber for Windows, see "SharePortRangeStart" in the *Cisco Jabber Parameters Reference Guide*.

Set DSCP Values

Set Differentiated Services Code Point (DSCP) values in RTP media packet headers to prioritize Cisco Jabber traffic as it traverses the network.

Set DSCP Values on Cisco Unified Communications Manager

You can set DSCP values for audio media and video media on Cisco Unified Communications Manager. Cisco Jabber can then retrieve the DSCP values from the device configuration and apply them directly to the IP headers of RTP media packets.

Restriction For later operating systems such as Microsoft Windows 7, Microsoft implements a security feature that prevents applications from setting DSCP values on IP packet headers. For this reason, you should use an alternate method for marking DSCP values, such as Microsoft Group Policy.

For more information on configuring flexible DSCP values, refer to Configure Flexible DSCP Marking and Video Promotion Service Parameters.

Procedure

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

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

The **Service Parameter Configuration** window opens.

Step 3 Select the appropriate server and then select the **Cisco CallManager** service.

Step 4 Locate the **Clusterwide Parameters (System - QOS)** section.

Step 5 Specify DSCP values as appropriate and then select **Save**.

Set DSCP Values with Group Policy

If you deploy Cisco Jabber for Windows on a later operating system such as Microsoft Windows 7, you can use Microsoft Group Policy to apply DSCP values.

Complete the steps in the following Microsoft support article to create a group policy: http://technet.microsoft.com/en-us/library/cc771283%28v=ws.10%29.aspx

You should create separate policies for audio media and video media with the following attributes:

Attributes	Audio Policy	Video Policy	Signaling Policy
Application name	`CiscoJabber.exe`	`CiscoJabber.exe`	`CiscoJabber.exe`
Protocol	UDP	UDP	TCP
Port number or range	Corresponding port number or range from the SIP profile on Cisco Unified Communications Manager.	Corresponding port number or range from the SIP profile on Cisco Unified Communications Manager.	5060 for SIP 5061 for secure SIP
DSCP value	46	34	24

Set DSCP Values on the Client

For some configurations, there is an option to enable differentiated services for calls in the Cisco Jabber for Mac client and Cisco Jabber for mobile clients.

Important This option is enabled by default. Cisco recommends not disabling this option unless you are experiencing issues in the following scenarios:

- You can hear or see other parties, but you cannot be heard or seen
- You are experiencing unexpected Wi-Fi disconnection issues

Disabling differentiated service for calls may degrade audio and video quality.

Note If EnableDSCPPacketMarking is configured as true or false, then the user cannot see **Enable Differentiated Service for Calls** in the Cisco Jabber clients.

Procedure

Step 1 In Cisco Jabber for Mac, go to **Jabber > Preferences > Calls > Advanced** and select **Enable Differentiated Service for Calls**.

Step 2 In Cisco Jabber for mobile clients, go to **Jabber > Settings > Audio and Video** and select **Enable Differentiated Service for Calls**.

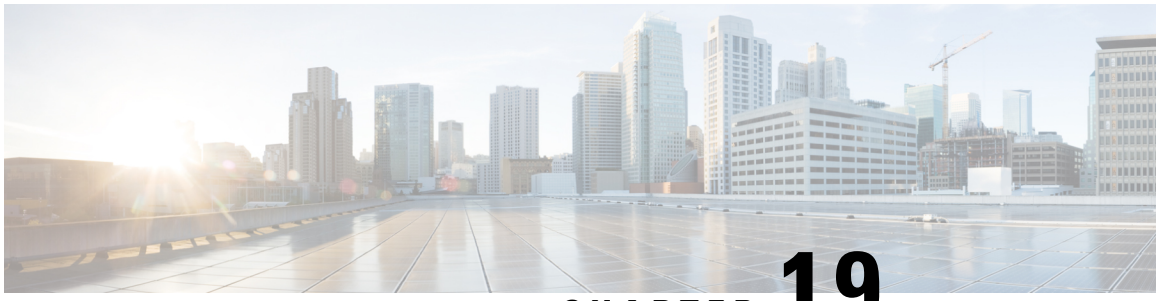
Set DSCP Values on the Network

You can configure switches and routers to mark DSCP values in the IP headers of RTP media.

To set DSCP values on the network, you must identify the different streams from the client application.

- Media Streams — Because the client uses different port ranges for audio streams and video streams, you can differentiate audio media and video media based on those port range. Using the default port ranges in the SIP profile, you should mark media packets as follows:
  - Audio media streams in ports from 16384 to 24574 as EF
  - Video media streams in ports from 24575 to 32766 as AF41
- Signaling Streams—You can identify signaling between the client and servers based on the various ports required for SIP, CTI QBE, and XMPP. For example, SIP signaling between Cisco Jabber and Cisco Unified Communications Manager occurs through port 5060.

  You should mark signaling packets as AF31.



CHAPTER 19

Integrate Cisco Jabber with Applications

Configure Presence in Microsoft SharePoint 2010 and 2013

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

Before you begin

- For Cisco Jabber for Windows clients only.
- Ensure that all sites are in sync with Microsoft SharePoint Central Administration (CA).
- Ensure that synchronization between Microsoft SharePoint and Active Directory is set up.

Procedure

Step 1 If you have Microsoft SharePoint 2013, update the SharePoint CA profile pages for users with the following information:

a) For the **SIP Address** profile field, leave it blank.
b) In the **Work email** profile field, enter the user profile. For example, `john4mail@example.pst`.

Step 2 If you have Microsoft SharePoint 2010, update the SharePoint CA profile pages for users with the following information:

a) For the **SIP Address** profile field, enter the user profile. For example, `john4mail@example.pst`
b) In the **Work email** profile field, leave it blank.

Client Availability

Users can define whether their availability reflects their calendar events by setting an option to let others know they are in a meeting from the **Status** tab of the **Options** window from the client. This option synchronizes events in your calendar with your availability. The client only displays **In a meeting** availability for supported integrated calendars.

The client supports using two sources for the **In a meeting** availability:

Note Cisco Jabber for mobile clients support this meeting integration feature from Cisco Jabber 11.7 release.

- Microsoft Exchange and Cisco Unified Communication Manager IM and Presence Integration — Applies to on-premises deployments. The **Include Calendar information in my Presence Status** field in Cisco Unified Presence is the same as the **In a meeting** option in the client. Both fields update the same value in the Cisco Unified Communication Manager IM and Presence database.

  If users set both fields to different values, then the last field that the user sets takes priority. If users change the value of the **Include Calendar information in my Presence Status** field while the client is running, the users must restart the client for those changes to apply.

- Cisco Jabber Client — Applies to on-premises and cloud-based deployments. You must disable Cisco Unified Communication Manager IM and Presence and Microsoft Exchange integration for the client to set the **In a meeting** availability. The client checks if integration between Cisco Unified Communication Manager IM and Presence and Microsoft Exchange is on or off. The client can only set availability if integration is off.

The following deployment scenarios describe how availability is created:

Deployment Scenario	You select In a meeting (according to my calendar)	You do not select In a meeting (according to my calendar)
You enable integration between Cisco Unified Communication Manager IM and Presence and Microsoft Exchange.	Cisco Unified Communication Manager IM and Presence sets availability status	Availability status does not change
You do not enable integration between Cisco Unified Communication Manager IM and Presence and Microsoft Exchange.	Client sets availability status	Availability status does not change
Cloud-based deployments	Client sets availability status	Availability status does not change

Additionally, the following table describes availability that is supported differently by each deployment scenarios:

Availability Enabled in the Client	Availability Enabled by Integrating Cisco Unified Communication Manager IM and Presence with Microsoft Exchange
Offline in a meeting availability is not supported.	**Offline in a meeting** availability is supported.
In a meeting availability is supported for non-calendar events.	**In a meeting** availability is not supported for non-calendar events.

Note Offline in a meeting availability refers to when the user is not logged in to the client but an event exists in the user's calendar.

Non-calendar events refer to events that do not appear in the user's calendar, such as instant meetings, **Offline**, or **On a call**.

Protocol Handlers

Cisco Jabber registers the following protocol handlers with the operating system to enable click-to-call or click-to-IM functionality from web browsers or other applications:

- XMPP: or XMPP://

  Starts an instant message and opens a chat window in Cisco Jabber.

- IM: or IM://

  Starts an instant message and opens a chat window in Cisco Jabber.

- TEL: or TEL://

  Starts an audio or video call with Cisco Jabber.

Note TEL is registered by Apple native phone. It cannot be used to cross launch Cisco Jabber for iPhone and iPad.

- CISCOTEL: or CISCOTEL://

  Starts an audio or video call with Cisco Jabber.

- SIP: or SIP://

  Starts an audio or video call with Cisco Jabber.

- CLICKTOCALL: or CLICKTOCALL://

  Starts an audio or video call with Cisco Jabber.

Registry Entries for Protocol Handlers

To register as a protocol handler, the client writes to the following locations in the Microsoft Windows registry:

- `HKEY_CLASSES_ROOT\tel\shell\open\command`

- HKEY_CLASSES_ROOT\xmpp\shell\open\command
- HKEY_CLASSES_ROOT\im\shell\open\command

In the case where two or more applications register as handlers for the same protocol, the last application to write to the registry takes precedence. For example, if Cisco Jabber registers as a protocol handler for XMPP: and then a different application registers as a protocol handler for XMPP:, the other application takes precedence over Cisco Jabber.

Protocol Handlers on HTML Pages

You can add protocol handlers on HTML pages as part of the `href` attribute. When users click the hyperlinks that your HTML pages expose, the client performs the appropriate action for the protocol.

TEL and IM Protocol Handlers

Example of the TEL: and IM: protocol handlers on an HTML page:

```
<html>
  <body>
    <a href="TEL:1234">Call 1234</a><br/>
    <a href="IM:msmith@domain">Send an instant message to Mary Smith</a>
  </body>
</html>
```

In the preceding example, when users click the hyperlink to call 1234, the client starts an audio call to that phone number. When users click the hyperlink to send an instant message to Mary Smith, the client opens a chat window with Mary.

CISCOTEL and SIP Protocol Handlers

Example of the CISCOTEL and SIP protocol handlers on an HTML page:

```
<html>
  <body>
    <a href="CISCOTEL:1234">Call 1234</a><br/>
    <a href="SIP:msmith@domain">Call Mary</a><br/>
    <a href="CISCOTELCONF:msmith@domain;amckenzi@domain">Weekly conference call</a>
  </body>
</html>
```

In the preceding example, when users click the *Call 1234* or *Call Mary* hyperlinks, the client starts an audio call to that phone number.

XMPP Protocol Handlers

Example of a group chat using the XMPP: protocol handler on an HTML page:

```
<html>
  <body>
    <a href="XMPP:msmith@domain;amckenzi@domain">Create a group chat with Mary Smith and
Adam McKenzie</a>
  </body>
</html>
```

In the preceding example, when users click the hyperlink to create a group chat with Mary Smith and Adam McKenzie, the client opens a group chat window with Mary and Adam.

Tip Add lists of contacts for the XMPP: and IM: handlers to create group chats. Use a semi-colon to delimit contacts, as in the following example:

```
XMPP:user_a@domain.com;user_b@domain.com;user_c@domain.com;user_d@domain.com
```

Add Subject Lines and Body Text

You can add subject lines and body text to any of the protocol handlers so that when users click on the hyperlink to create a person-to-person or group chat, the client opens a chat window with pre-populated subject line and body text.

Subject and body text can be added in any of the following scenarios:

- Using any supported protocol handler for instant messaging on the client
- For either person-to-person chats or for group chats
- Including a subject and body text, or one or the other

In this example, when users click on the link below it opens a person-to-person chat window with a pre-populated body text of **`I.T Desk`**:

```
xmpp:msmith@domain?message;subject=I.T.%20Desk
```

In this example, when users click on the link below it opens a **Start Group Chat** dialog box with a topic of **I.T Desk**, and the input box for the chat window is pre-populated with the text **`Jabber 10.5 Query`**:

```
im:user_a@domain.com;user_b@domain.com;user_c@domain.com?message;subject=I.T%20Desk;body=Jabber%2010.5%20Query
```

Protocol Handler Supported Parameters

Cross Launch for Mobile Clients

The Cisco Jabber for mobile clients provide you with the ability to return to a specified application. For example if you create a ciscotel URI link that dials a number, you can add in the application name as a parameter and when the call has completed the user is prompted to return to that application.

```
ciscotel://1234567?CrossLaunchBackSchema=SomeAppSchema&CrossLaunchBackAppName=SomeAppName
```

- CrossLaunchBackAppName—Users are prompted with the name of an application that Cisco Jabber cross launches back to when a call ends.
  - none (default)—No application in the dialog box.
  - *app_name*—The application name that is displayed in the dialog box.
- CrossLaunchBackSchema—Specifies the schema used when a call is ended.
  - none(default)—You stay in Cisco Jabber.
  - *schema*—The schema used to cross launch back the application.

Supported Separators

When creating a URI link for HTML pages, you can use a semi-colon to separate the characters. This is supported with the SIP, Tel, CiscoTel and ClickToCall protocol handlers. In the following example, the link will create a conference call with the two numbers:

```
tel:123;123
```

The IM protocol supports the semi-colon separator. In the following example, the link will create a group chat with the two participants:

```
im:participant1@example.com,participant2@example.com
```

DTMF Support

Enter DTMF in the IM Window

In the conversation window of the client, you can enter a protocol handler including DTMF digits and the client will create a link that participants can use. The supported protocols are TEL, CISCOTEL, SIP, CLICKTOCALL, CISCOIM, IM, and XMPP. The supported parameters are numbers or SIP URIs.

In the following example, the number is 1800123456, the PIN for entry is 5678#, using the TEL URI link this example creates a meeting link:

```
tel:1800123456,,,5678#
```

Enter DTMF in an Active Call

During a call, users can copy and paste DTMF digits into the call window of the client. Users can easily enter Meeting IDs, Attendee IDs, and PINs from their meeting invitation. If you enter alphanumeric strings during an active call, they are interpreted as the corresponding numbers on the keypad, and commas represent a one second pause between DTMF signals.

Supported DTMF Signals

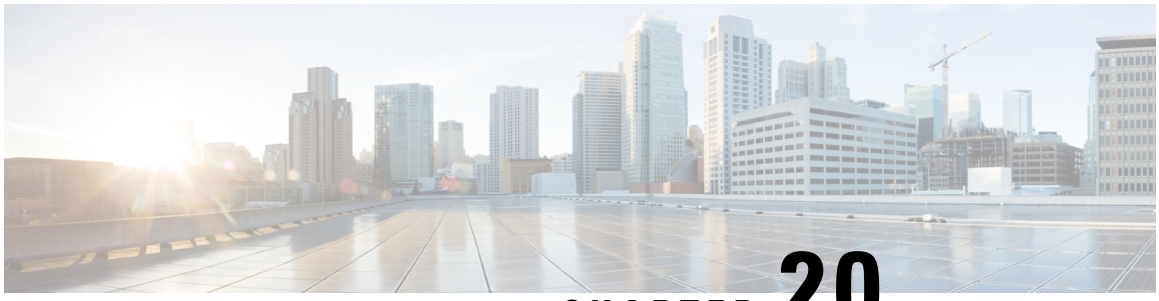
If a user enters a DTMF signal that isn't supported by the system that Jabber is calling, then Jabber will not send the input from the user.

Cisco Jabber for Windows and mobiles support the following DTMF signals:

- 0 to 9
- #
- *
- A to D

PART IV

Troubleshooting



CHAPTER 20

Troubleshooting

Cisco Jabber Diagnostic Tool

Windows and Mac

The Cisco Jabber Diagnostics tool provides configuration and diagnostic information for the following services:

- Service Discovery
- Webex
- Cisco Unified Communications Manager Summary
- Cisco Unified Communications Manager Configuration
- Voicemail
- Certificate Validation
- Active Directory
- DNS Records

To access the tool, users must bring the hub, call, or chat window into focus and select **Ctrl + Shift + D**.

Users can update the data by selecting **Reload** . Users can also save the information to an html file by selecting **Save**.

The tool is available by default. To disable this tool:

- For Jabber for Windows set the DIAGNOSTICSTOOLENABLED installation parameter to FALSE.
- For Jabber for Mac include the DiagnosticsToolEnabled parameter in the configuration URL with the value set to FALSE.

For more information about these parameters, see *On-Premises Deployment for Cisco Jabber*, or *Cloud and Hybrid Deployments for Cisco Jabber*, depending on your deployment.

Android, iPhone, and iPad

If users are unable to sign into Cisco Jabber or your Cisco Jabber IM and Phone services aren't connected, they can use the **Diagnose Error** option to check what's causing the issue.

Users can tap **Diagnose Error** option either from the **Sign In** page or from the warning notification they get when connecting to Cisco Jabber services. Cisco Jabber then verifies:

- If there are any network issues
- If Cisco Jabber servers are reachable
- If Cisco Jabber can reconnect

If any of these checks fail, Cisco Jabber displays an error report with the possible solution. If the issue persists, they can send a problem report.

Contact Resolution Tool

Applies to Cisco Jabber for Windows.

The Contact Resolution tool provides information for the available directory sources and a search tool to display contact search results.

To access the Contact Resolution tool, users must bring the hub, call, or chat window into focus and select **`Ctrl + Shift + C`**.

The tool is available by default and can be disabled by setting the ContactsDiagnosticsToolEnabled installation parameter to FALSE.

The tool provides the following search options:

- Predictive—The search takes the entered string and displays the matching records. This is the same search that is used when a user searches for a contact in the client.
- Equivalence—This search type includes further options to resolve the search string:
  - URI or JID
  - Phone number
  - SIP URI
  - Email

  The search will return the records matching the specified values.

For more information about the ContactsDiagnosticsToolEnabled installation parameter, see *On-Premises Deployment for Cisco Jabber*, or *Cloud and Hybrid Deployments for Cisco Jabber*, depending on your deployment.