



Cisco Jabber 10.6 Deployment and Installation Guide

First Published: January 27, 2015

Americas Headquarters

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

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

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

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

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

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

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

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

© 2015 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Cisco Jabber Overview 1

Purpose of this Guide 1

About Cisco Jabber 1

CHAPTER 2

Configuration and Installation Workflows 3

Deployment and Installation Workflow for an On-Premises Deployment 3

Deployment and Installation Workflow for Phone Mode 4

Deployment and Installation Workflow for a Cloud-Based Deployment 5

CHAPTER 3

Configure Directory Integration 7

Configure Directory Integration for an On-Premises Deployment 7

Enable Synchronization 7

Configure IM Address Scheme 8

Populate User ID and Directory URI 9

Specify an LDAP Attribute for the User ID 10

Specify an LDAP Attribute for the Directory URI 10

Perform Synchronization 11

Authenticate with the Directory Server 11

Configure Directory Integration for Cloud-Based Deployments 12

Add Directory Groups 12

CHAPTER 4

Set Up Certificate Validation 13

Configure Certificates for an On-Premises Deployment 13

Deploy CA Certificates to Clients 14

Manually Deploy CA Certificates to Cisco Jabber for Windows Clients 14

Manually Deploy CA Certificates to Cisco Jabber for Mac Clients 15

Manually Deploy CA Certificates to Mobile Clients 15

Certificate Validation for Cloud Deployments 15

Update Profile Photo URLs 16

CHAPTER 5**Configure Service Discovery 17**

Configuration URL Workflow 17

Create Configuration URL 17

Provide Users with Configuration URL from a Website 19

Manual Connection Settings 20

Automatic Connection Setting for Service Discovery 20

Manual Connection Settings for On-Premises Deployments 20

Manual Connection Settings for On-Premises Deployments in Phone Mode 21

Manual Connection Settings for Cloud-Based Deployments 22

Installer Switches: Cisco Jabber for Windows 23

Bootstrap Settings for On-Premises Deployments 23

Bootstrap Settings for On-Premises Deployments in Phone Mode 25

Bootstrap Settings for Cloud-Based Deployments 26

CHAPTER 6**Configure a Service Profile 27**

Activate and Start Essential Services 27

Create a Service Profile 28

CHAPTER 7**Configure IM and Presence Service 29**

Configure IM and Presence Service for an On-Premises Deployment 29

IM and Presence Service Workflow for an On-Premises Deployment with CUCM 9.x and
Later 29

IM and Presence Service Workflow for an On-Premises Deployment with CUCM 8.6 30

Pre-Populate Contact Lists in Bulk 30

Enable Message Settings 30

Specify Capabilities Assignments 31

Add an IM and Presence Service 32

Apply an IM and Presence Service 32

Configure Presence in Microsoft SharePoint 2010 and 2013 33

Configure Users 34

Configure Users Individually 34

Configure Users in Bulk 35

Configure IM and Presence Service for Cloud-Based Deployments 35

Configure IM and Presence Service 36

Configure Privacy Options 36

CHAPTER 8**Configure Voice and Video Communication 39**

Configure Voice and Video Communications for On-Premises Deployments 39

Install Cisco Options Package File for Devices 40

Apply COP File for BFCP Capabilities 41

Create SIP Profiles 42

 Increase SIP Dual Mode Alert Timer Value 43

Configure the Phone Security Profile 43

Enable User Mobility 45

Add a CTI Service 45

 Apply a CTI Service 46

Add a CTI Gateway Server 47

 Create a CTI Gateway Profile 47

Video Desktop Sharing 48

Create and Configure Cisco Jabber Devices 48

 Add a Directory Number to the Device 50

 Add a Remote Destination 51

Provide Users with Authentication Strings 52

Desk Phone Video Configuration 53

Enable Video Rate Adaptation 55

 Enable RTCP on Common Phone Profiles 55

 Enable RTCP on Device Configurations 55

Configure User Associations 56

Reset Devices 57

Create a CCMCIP Profile 58

Dial Plan Mapping 59

 Publish Dial Rules 59

Configure Voice and Video Communication for Cloud-Based Deployments 60

Configure Audio and Video Services 60

Add Teleconferencing Service Name Accounts 61

CHAPTER 9**Configure Voicemail 63**

Configure Voicemail for an On-Premises Deployment with CUCM 9.x and Later 63

Configure Voicemail for an On-Premises Deployment with CUCM 8.6	64
Configure Cisco Unity Connection for Use with Cisco Jabber	65
Configure Voicemail Accounts on Cisco Unity Connection	66
Add a Voicemail Service	66
Apply a Voicemail Service	67
Add a Mailstore Service	68
Apply Mailstore Service	69
Add a Voicemail Server	70
Create a Mailstore	71
Create a Voicemail Profile	72
Configure Retrieval and Redirection	73
Set a Voicemail Credentials Source	74
Enable Enhanced Message Waiting Indicator	75
Configure Voicemail for Cloud-Based Deployments	75
Configure Voicemail	75
Allow Users to Set Voicemail Server Settings	76

CHAPTER 10
Configure Conferencing 77

Configure Conferencing for an On-Premises Deployment	77
Configure On-Premises Conferencing using WebEx Meetings Server	77
Authenticate Cisco WebEx Meetings Server	77
Add Cisco WebEx Meetings Server on Cisco Unified Communications Manager	78
Add the Cisco WebEx Meetings Server to a Service Profile	79
Add Cisco WebEx Meetings Server on Cisco Unified Presence	80
Add Cisco WebEx Meetings Server to a Profile	80
Configure Cloud-Based Conferencing Using WebEx Meeting Center	81
Integration with Cisco WebEx Meeting Center	82
Authentication with Cisco WebEx Meeting Center	82
Provide Conferencing Credentials	82
Add Cisco WebEx Meeting Center	83
Add Cisco WebEx Meeting Center to a Profile	83
Set Up Cisco WebEx Meeting Center on Cisco Unified Presence	84
Add Cisco WebEx Meeting Center	85
Add Cisco WebEx Meeting Center to a Profile	85

Configure Conferencing for a Cloud-Based Deployment using Cisco WebEx Meeting Center	86
Authentication with Cisco WebEx Meeting Center	87
Specify Conferencing Credentials in the Client	87

CHAPTER 11**Configure the Clients 89**

Introduction to Client Configuration	89
Configure Service Profiles	90
Set Parameters on Service Profile	90
Parameters in Service Profiles	91
Add Cisco Unified Communications Manager Services	93
Create Service Profiles	93
Apply Service Profiles	94
Associate Users with Devices	94
Set Parameters on Phone Configuration for Desktop Clients	95
Parameters in Phone Configuration	96
Set Parameters on Phone Configuration for Mobile Clients	97
Parameters in Phone Configuration	97
Create and Host Client Configuration Files	98
Specify Your TFTP Server Address	99
Specify Your TFTP Server on Cisco Unified Presence	100
Specify Your TFTP Server on Cisco Unified Communications Manager IM and Presence Service	100
Specify TFTP Servers in Phone Mode	101
Specify TFTP Servers with the Cisco WebEx Administration Tool	101
Create Global Configurations	101
Create Group Configurations	102
Host Configuration Files	103
Restart Your TFTP Server	103
Configuration File Structure	104
XML Structure	104
Group Elements and Parameters	105
Client Parameters	105
Options Parameters	108
Phone Parameters	111
Policies Parameters	113

On-Premises Policies	114
Common Policies	115
Cisco WebEx Policies	126
Presence Parameters	126
Voicemail Parameters	127
Service Credentials Parameters	127
Example Configuration	128
Configure Problem Reporting	129
Configure Automatic Updates	129
Custom Embedded Tabs for Cisco Jabber for Windows	132
Custom Embedded Tab Definitions	132
User Custom Tabs	134
Custom Icons	134
Chats and Calls from Custom Tabs	134
UserID Tokens	135
JavaScript Notifications	135
Show Call Events in Custom Tabs	137
Custom Embedded Tab Example	139
<hr/>	
CHAPTER 12	Integrate with Directory Sources 141
	Integrate with Directory Sources for an On-Premises Deployment 141
	Configure Contact Sources 141
	Enhanced Directory Integration 142
	Domain Name Retrieval 143
	Directory Server Discovery 143
	Basic Directory Integration 144
	Authentication with Contact Sources 145
	Specify LDAP Directory Configuration on Cisco Unified Presence 145
	Specify LDAP Directory Configuration on Cisco Unified Communications Manager 146
	Set Credentials in the Client Configuration 147
	Use Anonymous Binds 147
	Cisco Unified Communications Manager User Data Service 148
	Enable Integration with UDS 148
	Set UDS Service Parameters 149

UDS Service Parameters	149
Contact Resolution with Multiple Clusters	150
Federation	150
Interdomain Federation	150
Intradomain Federation	151
Configure Intradomain Federation for BDI or EDI	151
Client Configuration for Directory Integration	153
When to Configure Directory Integration	153
Configure Directory Integration in a Service Profile	153
Add a Directory Service	154
Directory Profile Parameters	154
Apply Directory Service to a Service Profile	157
Configure Directory Integration in the Configuration File	157
Summary of Directory Integration Configuration Parameters	157
Directory Server Type Parameter	160
EDI and BDI Directory Integration Parameters	161
Attribute Mapping Parameters	161
Attributes on the Directory Server	162
Directory Connection Parameters	163
IM Address Scheme Parameters	170
Directory Query Parameters	171
Base Filter Examples	175
Phone Number Masks Parameter	175
Contact Photo Parameters	177
Contact Photo Retrieval	179
UDS Parameters	180
Contact Photo Retrieval with UDS	181
Directory Server Configuration Examples	182
Domain Controller Connection	182
Manual Server Connections for Cisco Jabber for Windows	182
UDS Integration	183
LDAP Integration with Expressway for Mobile and Remote Access	183
Simple Authentication for Cisco Jabber for Windows	184
Simple Authentication for Mobile Clients and Cisco Jabber for Mac	184
Simple Authentication with SSL for Cisco Jabber for Windows	185

Simple Authentication with SSL for Mobile Clients	185
OpenLDAP Integration	185
Anonymous Binds for Cisco Jabber for Windows	185
Anonymous Binds for Mobile Clients and Cisco Jabber for Mac	186
Authenticated Binds for Cisco Jabber for Windows	187
Authenticated Binds for Mobile Clients and Cisco Jabber for Mac	188
AD LDS Integration	188
Anonymous Binds for Cisco Jabber for Windows	188
Anonymous Binds for Mobile Clients and Cisco Jabber for Mac	189
Windows Principal User Authentication	189
AD LDS Principal User Authentication for Cisco Jabber for Windows	190
AD LDS Principal User Authentication for Mobile Clients and Cisco Jabber for Mac	191

CHAPTER 13**Install the Clients 193**

Install Cisco Jabber for Windows	193
Use the Command Line	193
Example Installation Commands	194
Command Line Arguments	195
Override Argument	195
Mode Type Argument	196
When to Set the Product Mode	196
Change Product Modes	196
Change Product Modes with Cisco Unified Communications Manager Version 9.x and Later	197
Change Product Modes with Cisco Unified Communications Manager Version 8.x	197
Authentication Arguments	198
TFTP Server Address	201
Common Installation Arguments	202
SSO Arguments	205
Cloud-Based SSO Arguments	205
Run the MSI Manually	205
Create a Custom Installer	205
Get the Default Transform File	206
Create Custom Transform Files	206

Transform the Installer	207
Installer Properties	208
Deploy with Group Policy	209
Set a Language Code	209
Deploy the Client with Group Policy	210
Supported Languages	211
Cisco Media Services Interface	211
Desk Phone Video Capabilities	212
Install Cisco Media Services Interface	212
Uninstall Cisco Jabber for Windows	212
Use the Installer	212
Use the Product Code	213
Install Cisco Jabber for Mac	213
Prepare Your Network	213
Distribute the Cisco Jabber for Mac client	214
Install Cisco Jabber Mobile Clients	214
<hr/>	
CHAPTER 14	Remote Access 215
Expressway for Mobile and Remote Access Deployments	215
Supported Services	217
Cisco AnyConnect Deployments	223
Cisco AnyConnect Deployment Considerations	224
Application Profiles	225
Automate VPN Connection	227
Set Up Trusted Network Connection	227
Set Up Connect On-Demand VPN	228
Set Up Automatic VPN Access on Cisco Unified Communications Manager	229
Set Up Certificate-Based Authentication	230
Distribute Certificates with SCEP	231
Distribute Client Certificate with Mobileconfig File	231
Session Parameters	231
Set ASA Session Parameters	232
Group Policies and Profiles	233
Trusted Network Detection	233
Tunnel Policies	233

Survivable Remote Site Telephony 234

CHAPTER 15**Cisco Jabber Features and Options 235**

Cisco Jabber Features 235

Cisco Jabber Features for Windows, Mac, iOS and Android 237

Telemetry 237

Call Preservation 238

Configure Prompts for Presence Subscription Requests 238

Disable Temporary Presence in Cisco Unified Communications Manager IM and Presence 239

Disable Temporary Presence in Cisco Unified Presence 240

Enable URI Dialing 240

 Associate URIs to Directory Numbers 241

 Automatically Populate Directory Numbers with URIs 241

 Configure Directory Numbers with URIs 241

 Associate the Directory URI Partition 242

 Enable FQDN in SIP Requests for Contact Resolution 242

Set Up Voicemail Avoidance 243

 Set Up Timer-Controlled Voicemail Avoidance 243

 Set Up User-Controlled Voicemail Avoidance 243

 Set Up Cisco Unified Communications Manager to Support Voicemail Avoidance 244

 Enable Voicemail Avoidance on Mobility Identity 244

 Enable Voicemail Avoidance on Remote Destination 245

Enable File Transfers and Screen Captures 246

 Enable File Transfers and Screen Captures 247

 Enable File Transfer and Screen Captures for Group Chats and Chat Rooms 247

 Enable File Transfer and Screen Captures for Peer to Peer Chats Only 248

 Configuring Maximum File Transfer Size 248

Cisco Jabber Features for Windows 249

 Call Pickup 249

 Configure Call Pickup Group 251

 Assign Directory Number 252

 Configure Other Call Pickup 252

 Configure Directed Call Pickup 253

Auto Call Pickup	253
Configure Auto Call Pickup	254
Configure Silent Monitoring and Call Recording	254
Configure Persistent Chat	255
Administer and Moderate Persistent Chat Rooms	258
Enable Persistent Chat Room Passwords	259
Integrate with Microsoft Products	260
Calendar Integration	261
Enable Calendar Events from Microsoft Outlook	261
Enable Presence Integration with Microsoft Outlook	262
Enable Presence with the Active Directory User and Computers Tool	262
Add Local Contacts from Microsoft Outlook	263
Save Chat History to an Outlook Folder	263
Limitations for Saving Chat History to an Outlook Folder	263
Authentication Modes	263
Authenticate Using Single Sign On for the Operating System	264
Authenticate by Synching Credentials	264
Specify Server Addresses	264
Detect Server Addresses Automatically	264
Define Server Addresses	265
Add Custom Emoticons	265
Emoticon Definitions	266
Cisco Jabber Features for Mac	269
Local Contacts in Mac Address Book	269
Cisco Jabber for Android and iOS	269
Configure Call Park	269
Set Up Cisco Unified Communications Manager to Support Dial via Office	270
Set Up Enterprise Feature Access Number	270
Set Up Mobility Profile	271
Verify Device COP File Version	271
Prerequisite for All Clients	272
Set Up Dial via Office	272
Set Up Dial via Office for Each Device	273
Add Mobility Identity	274
Enable Dial via Office on Each Device	275

Set Up Mobile Connect	276
Enable Mobile Connect	277
Add Remote Destination (Optional)	278
Transfer Active VoIP Call to the Mobile Network	279
Enable Handoff from VoIP to Mobile Network	280
Set Up Handoff DN	280
Match Caller ID with Mobility Identity	281
Set Up User and Device Settings for Handoff	282
Enable Transfer from VoIP to Mobile Network	282
Cisco Jabber for iOS, Android and Windows	283
Hunt Group	283
Line Group	284
Configure Line Group	284
Hunt List	285
Configure Hunt List	285
Add Line Group to Hunt List	286
Hunt Pilot	286
Configure Hunt Pilot	286

APPENDIX A

Cisco Jabber Reference Information	289
Client Availability	289
Multiple Resource Login	290
Protocol Handlers	291
Registry Entries for Protocol Handlers	291
Protocol Handlers on HTML Pages	292
Audio and Video Performance Reference	293
Audio Bit Rates for Cisco Jabber Desktop Clients	293
Audio Bit Rates for Cisco Jabber Mobile Clients	293
Video Bit Rates for Cisco Jabber Desktop Clients	294
Video Bit Rates for Cisco Jabber for Android	294
Video Bit Rates for Cisco Jabber for iPhone and iPad	295
Presentation Video Bit Rates	295
Maximum Negotiated Bit Rate	295
Bandwidth Performance Expectations for Cisco Jabber for Windows and Cisco Jabber for Mac	296

Bandwidth Performance Expectations for Cisco Jabber for Android	297
Bandwidth Performance Expectations for Cisco Jabber for iPhone and iPad	297
Video Rate Adaptation	298
Define a Port Range on the SIP Profile	298
Set DSCP Values	299
Set DSCP Values on Cisco Unified Communications Manager	299
Set DSCP Values with Group Policy	299
Set DSCP Values on the Client	300
Set DSCP Values on the Network	300



Cisco Jabber Overview

- [Purpose of this Guide, page 1](#)
- [About Cisco Jabber, page 1](#)

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 or cloud 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 Android
- Cisco Jabber for iPhone and iPad
- Cisco Jabber for Mac
- Cisco Jabber for Windows

For more information about the Cisco Jabber suite of products, see <http://www.cisco.com/go/jabber>.



CHAPTER 2

Configuration and Installation Workflows

- [Deployment and Installation Workflow for an On-Premises Deployment, page 3](#)
- [Deployment and Installation Workflow for Phone Mode, page 4](#)
- [Deployment and Installation Workflow for a Cloud-Based Deployment, page 5](#)

Deployment and Installation Workflow for an On-Premises 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 .	<ul style="list-style-type: none"> • 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	Configure Directory Integration for an On-Premises Deployment, on page 7.	
Step 3	Configure Certificates for an On-Premises Deployment, on page 13.	Certificates are required for each service to which the Jabber clients connect.
Step 4	Configure Service Discovery, on page 17.	
Step 5	Configure a Service Profile, on page 27	

	Command or Action	Purpose
Step 6	Configure IM and Presence Service for an On-Premises Deployment, on page 29.	
Step 7	Configure Voice and Video Communications for On-Premises Deployments, on page 39.	
Step 8	Complete one of the following: <ul style="list-style-type: none"> • Configure Voicemail for an On-Premises Deployment with CUCM 9.x and Later, on page 63. • Configure Voicemail for an On-Premises Deployment with CUCM 8.6, on page 64. 	
Step 9	Configure Conferencing for an On-Premises Deployment, on page 77.	
Step 10	Configure the Clients, on page 89	
Step 11	Install the Clients, on page 193	

Deployment and Installation Workflow for Phone Mode

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 .	<ul style="list-style-type: none"> • 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	Configure Directory Integration for an On-Premises Deployment, on page 7.	
Step 3	Configure Certificates for an On-Premises Deployment, on page 13.	Certificates are required for each service to which the Jabber clients connect.
Step 4	Configure Service Discovery, on page 17.	
Step 5	Configure a Service Profile, on page 27	

	Command or Action	Purpose
Step 6	Configure Voice and Video Communications for On-Premises Deployments, on page 39.	
Step 7	Complete one of the following: <ul style="list-style-type: none"> • Configure Voicemail for an On-Premises Deployment with CUCM 9.x and Later, on page 63. • Configure Voicemail for an On-Premises Deployment with CUCM 8.6, on page 64. 	
Step 8	Configure Conferencing for an On-Premises Deployment, on page 77.	
Step 9	Configure Conferencing, on page 77	
Step 10	Configure the Clients, on page 89	
Step 11	Install the Clients, on page 193	

Deployment and Installation Workflow for a Cloud-Based 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 .	<ul style="list-style-type: none"> • 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	Configure Directory Integration, on page 7	
Step 3	Set Up Certificate Validation, on page 13	
Step 4	Configure Service Discovery, on page 17	
Step 5	Configure a Service Profile, on page 27	
Step 6	Configure IM and Presence Service for Cloud-Based Deployments, on page 35	

	Command or Action	Purpose
Step 7	Configure Voice and Video Communication for Cloud-Based Deployments, on page 60	
Step 8	Configure Voicemail for Cloud-Based Deployments, on page 75	
Step 9	Configure Conferencing for a Cloud-Based Deployment using Cisco WebEx Meeting Center, on page 86	
Step 10	Configure the Clients, on page 89	
Step 11	Install the Clients, on page 193	



Configure Directory Integration

- [Configure Directory Integration for an On-Premises Deployment, page 7](#)
- [Configure Directory Integration for Cloud-Based Deployments, page 12](#)

Configure Directory Integration for an On-Premises Deployment

Procedure

	Command or Action	Purpose
Step 1	Enable Synchronization, on page 7.	To replicate contact data to Cisco Unified Communications Manager.
Step 2	Configure IM Address Scheme, on page 8	Only for Cisco Unified Communications Manager IM & Presence 10.x or later.
Step 3	Populate User ID and Directory URI, on page 9	Populate the user ID and directory URI from an attribute in the directory.
Step 4	Perform Synchronization, on page 11	Synchronize Cisco Unified Communications Manager with the directory server.
Step 5	Authenticate with the Directory Server, on page 11.	Configure Cisco Unified Communications Manager to authenticate with the directory server

Enable Synchronization

To ensure that contact data in your directory server is replicated to Cisco Unified Communications Manager, you must synchronize with the directory server. Before you can synchronize with the directory server, you must enable synchronization.

Procedure

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

What to Do Next

Specify an LDAP attribute for the user ID.

Configure IM Address Scheme

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

Procedure

- Step 1** Select the **IM Address Scheme** in the **Advanced Presence Settings** section of Cisco Unified Communications Manager IM & Presence Administration.
- UserID@[Default Domain]
 - Directory URI

For more information on configuring the *IM Address Scheme*, see the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* guide.

- Step 2** Select the required mapping in the **Standard User Fields to Be Synchronized** section of the Cisco Unified Communications Manager Administration.
- User ID mapped to an LDAP field, the default is **sAMAccountName**
 - Directory URI mapped to either **mailor msRTCSIP-primaryuseraddress**

For more information on mapping the fields, see the *Populate User ID and Directory URI* section.

Populate User ID and Directory URI

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

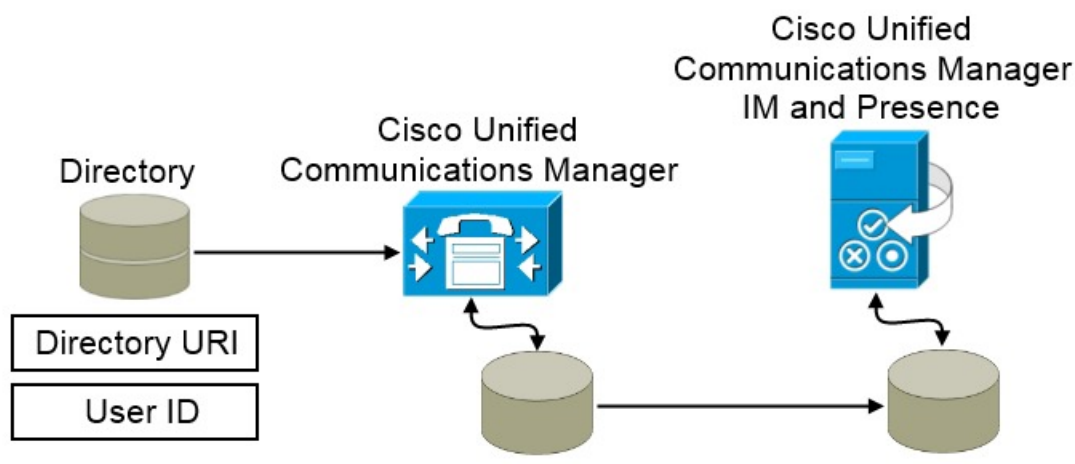
User ID

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

Directory URI

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

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



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

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

Specify an LDAP Attribute for the User ID

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

Procedure

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

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

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

The EDI parameter is `UserAccountName`.

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

The BDI parameter is `BDIUserAccountName`.

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

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

Specify an LDAP Attribute for the Directory URI

On Cisco Unified Communications Manager version 9.0(1) and later, you can populate the directory URI from an attribute in the directory.

Before You Begin

[Enable Synchronization.](#)

Procedure

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

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

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

Step 4 Select 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 5 Select **Save**.

Perform Synchronization

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

Before You Begin

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

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

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

Procedure

- Step 1** Select **System > LDAP > LDAP Directory**.
 - Step 2** Select **Add New**.
The **LDAP Directory** window opens.
 - Step 3** Specify the required details on the **LDAP Directory** window.
See the *Cisco Unified Communications Manager Administration Guide* for more information about the values and formats you can specify.
 - Step 4** Create an LDAP Directory Synchronization Schedule to ensure that your information is synchronized regularly.
 - Step 5** Select **Save**.
 - Step 6** Select **Perform Full Sync Now**.
Note The amount of time it takes for the synchronization process to complete depends on the number of users that exist in your directory. If you synchronize a large directory with thousands of users, you should expect the process to take some time.
-

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

Authenticate with the Directory Server

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

Procedure

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

Configure Directory Integration for Cloud-Based Deployments

Procedure

	Command or Action	Purpose
Step 1	Review Directory Integration .	Review the topics.
Step 2	See Understanding the Configuration Tab .	Configure your organization information.
Step 3	See Overview of User Management .	Create and provision users.
Step 4	Add Directory Groups , on page 12.	

Add Directory Groups

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

Procedure

-
- Step 1** Set up directory integration.
 - Step 2** Define your directory groups in a comma-separated values (.csv) file.
 - Step 3** Import your directory groups using the Cisco WebEx Administration Tool.
-

Related Topics

[Directory Integration](#)



CHAPTER 4

Set Up Certificate Validation

- [Configure Certificates for an On-Premises Deployment](#), page 13
- [Certificate Validation for Cloud Deployments](#), page 15

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 <i>Security Configuration on IM and Presence Service</i> 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 <i>Cisco Unified Communications Manager Security Guide</i> and the <i>Cisco Unified Communications Operating System Administration Guide</i> found here .
Step 3	Download the HTTP (tomcat) for Cisco WebEx Meetings Server.	For more information, see the <i>Cisco WebEx Meetings Server Administration Guide</i> 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

	Command or Action	Purpose
		certificate and once per cluster per XMPP certificate. If you do not use a multiserver SAN, then you must upload the certificate to the service for every Cisco Unified Communications Manager node.
Step 7	Deploy CA Certificates to Clients, on page 14	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 Authorities > 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.
-

Certificate Validation for Cloud Deployments

Cisco WebEx Messenger and Cisco WebEx Meeting Center present the following certificates to the client by default:

- CAS
- WAPI



Note

Cisco WebEx certificates are signed by a public Certificate Authority (CA). Cisco Jabber validates these certificates to establish secure connections with cloud-based services.

Cisco Jabber validates the following XMPP certificates received from Cisco WebEx Messenger. If these certificates are not included in your operating system, you must provide them.

- **VeriSign Class 3 Public Primary Certification Authority - G5**—This certificate is stored in the Trusted Root Certificate Authority
- **VeriSign Class 3 Secure Server CA - G3**—This certificate validates the Webex Messenger server identity and is stored in the Intermediate Certificate Authority.

For more information about root certificates for Cisco Jabber for Windows, see <http://www.identrust.co.uk/certificates/trustid/install-nes36.html>.

For more information about root certificates for Cisco Jabber for Mac, see <http://support.apple.com>.

Update Profile Photo URLs

In cloud-based deployments, Cisco WebEx assigns unique URLs to profile photos when you add or import users. When Cisco Jabber resolves contact information, it retrieves the profile photo from Cisco WebEx at the URL where the photo is hosted.

Profile photo URLs use HTTP Secure (`https://server_name/`) and present certificates to the client. If the server name in the URL is:

- A fully qualified domain name (FQDN) that contains the Cisco WebEx domain — The client can validate the web server that is hosting the profile photo against the Cisco WebEx certificate.
- An IP address — The client cannot validate the web server that is hosting the profile photo against the Cisco WebEx certificate. In this case, the client prompts users to accept certificates whenever they look up contacts with an IP address in their profile photo URLs.



Important

- We recommend that you update all profile photo URLs that contain an IP address as the server name. Replace the IP address with the FQDN that contains the Cisco WebEx domain to ensure that the client does not prompt users to accept certificates.
- When you update a photo, the photo can take up to 24 hours to refresh in the client.

The following steps describe how to update profile photo URLs. Refer to the appropriate Cisco WebEx documentation for detailed instructions.

Procedure

-
- Step 1** Export user contact data in CSV file format with the Cisco WebEx Administration Tool.
 - Step 2** In the **userProfilePhotoURL** field, replace IP addresses with the Cisco WebEx domain.
 - Step 3** Save the CSV file.
 - Step 4** Import the CSV file with the Cisco WebEx Administration Tool.
-



Configure Service Discovery

- [Configuration URL Workflow, page 17](#)
- [Manual Connection Settings, page 20](#)
- [Installer Switches: Cisco Jabber for Windows, page 23](#)

Configuration URL Workflow

Procedure

	Command or Action	Purpose
Step 1	Create Configuration URL, on page 17	
Step 2	Provide Users with Configuration URL from a Website, on page 19	

Create Configuration URL

To enable users to launch Cisco Jabber without having to manually enter 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.
- **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. You must 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`
- **ServicesDomainSsoEmailPrompt** — Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.
 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.

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. When you create the configuration URL, you must use the following capitalization:

- ServicesDomain
- VoiceServicesDomain
- ServiceDiscoveryExcludedServices
- ServicesDomainSsoEmailPrompt

Examples

- `ciscojabber://provision?ServicesDomain=cisco.com`
- `ciscojabber://provision?ServicesDomain=cisco.com
&VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain
&VoiceServicesDomain=voicesservice_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.

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:

- 1 Install the client.
- 2 Click the link in the email message to open the internal web page.
- 3 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 Version 9.x and Later

If the client cannot get the authenticator and server addresses from the service profile.

Cloud-Based or On-Premises with Cisco Unified Communications Manager Version 8.x

The client also prompts users to enter server addresses in the **Advanced settings** window if you do not set server addresses with SRV records.

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

Automatic Connection Setting for Service Discovery

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

This option lets 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 also 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 must override the manual settings from the initial launch.

Manual Connection Settings for On-Premises Deployments

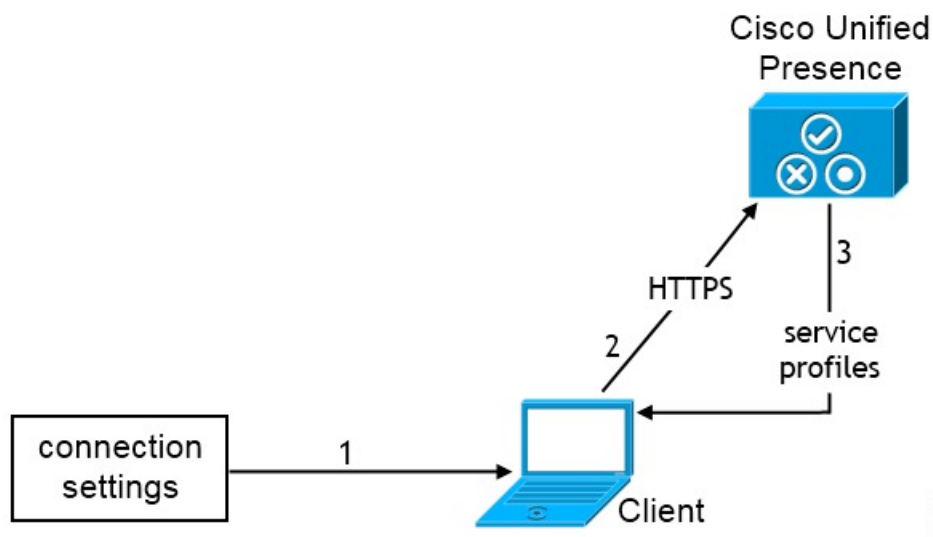
Users can set Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service as the authenticator and specify the server address in the **Advanced settings** window.



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:



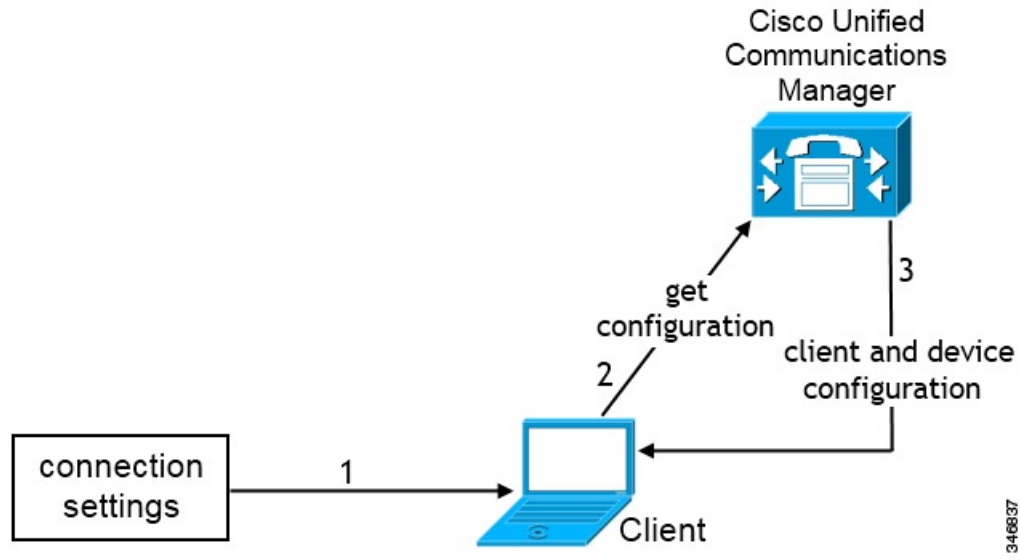
- 1 Users manually enter connection settings in the **Advanced settings** window.
- 2 The client authenticates to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.
- 3 The client retrieves service profiles from the presence server.

Manual Connection Settings for On-Premises Deployments in Phone Mode

Users can set Cisco Unified Communications Manager as the authenticator and specify the following server addresses in the **Advanced settings** window:

- TFTP server
- CCMCIP server
- CTI server (Cisco Jabber for Windows and Cisco Jabber for Mac)

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

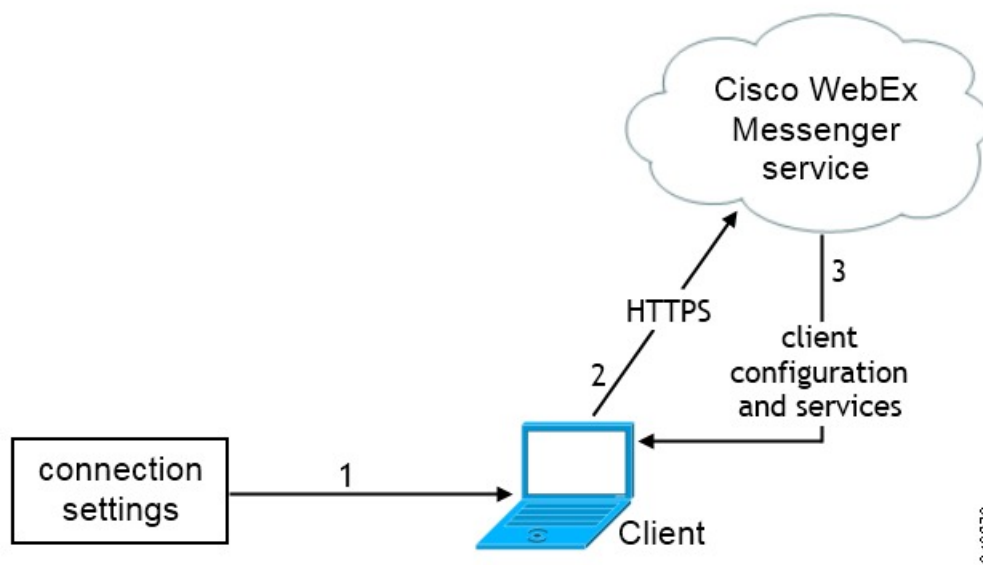


- 1 Users manually enter connection settings in the **Advanced settings** window.
- 2 The client authenticates to Cisco Unified Communications Manager and gets configuration.
- 3 The client retrieves device and client configuration.

Manual Connection Settings for Cloud-Based Deployments

Users can set the Cisco WebEx Messenger service as the authenticator and specify the CAS URL for login in the **Advanced settings** window.

The following diagram illustrates how the client uses manual connection settings in cloud-based deployments:



- 1 Users manually enter connection settings in the **Advanced settings** window.
- 2 The client authenticates to the Cisco WebEx Messenger service.
- 3 The client retrieves configuration and services.

Installer Switches: Cisco Jabber for Windows

When you install Cisco Jabber, you can specify the authenticator and server addresses. The installer saves these details to a bootstrap file. When users launch the client for the first time, it reads the bootstrap file. The bootstrap file is ignored if service discovery is deployed.

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, in on-premises deployments with Cisco Unified Communications Manager version 9.x and later.

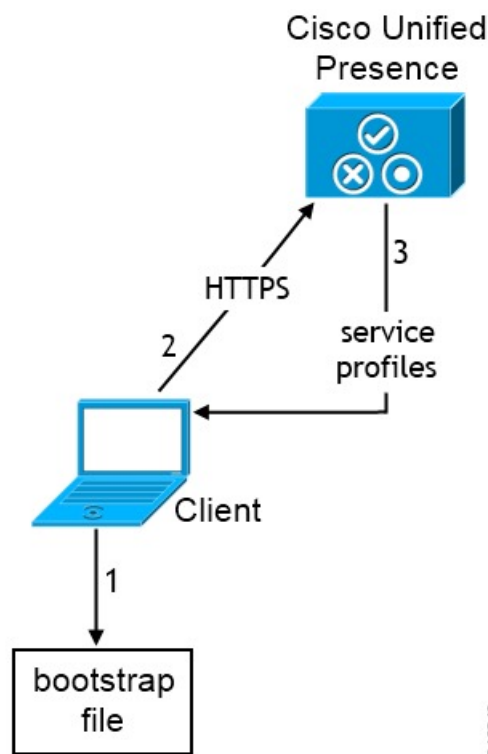
Bootstrap Settings for On-Premises Deployments

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

Product Mode	Server Versions	Argument Values
Full UC (Default Mode)	Version 9 and later: <ul style="list-style-type: none"> • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service 	Use the following installer switches and values: <ul style="list-style-type: none"> • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>
Full UC (Default Mode)	Version 8.x: <ul style="list-style-type: none"> • Cisco Unified Communications Manager • Cisco Unified Presence 	Use the following installer switches and values: <ul style="list-style-type: none"> • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>
IM Only (Default Mode)	Version 9 and later: <ul style="list-style-type: none"> • Cisco Unified Communications Manager IM and Presence Service 	Use the following installer switches and values: <ul style="list-style-type: none"> • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>

Product Mode	Server Versions	Argument Values
IM Only (Default Mode)	Version 8.x: Cisco Unified Presence	Use the following installer switches and values: <ul style="list-style-type: none"> • 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:

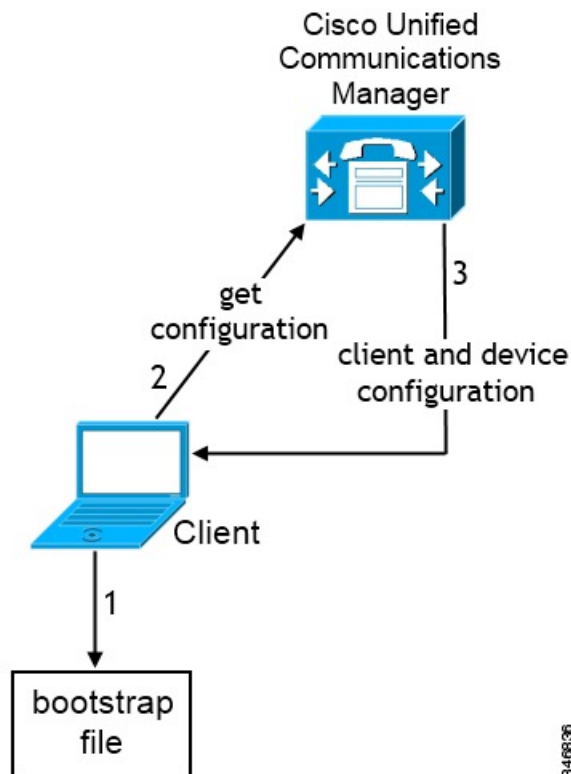
- 1 The client retrieves settings from the bootstrap file.
The client starts in default mode and determines that Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service is the authenticator. The client also gets the address of the presence server, unless Service Discovery results dictate otherwise.
- 2 The client authenticates to Cisco Unified Presence or 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`.

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:

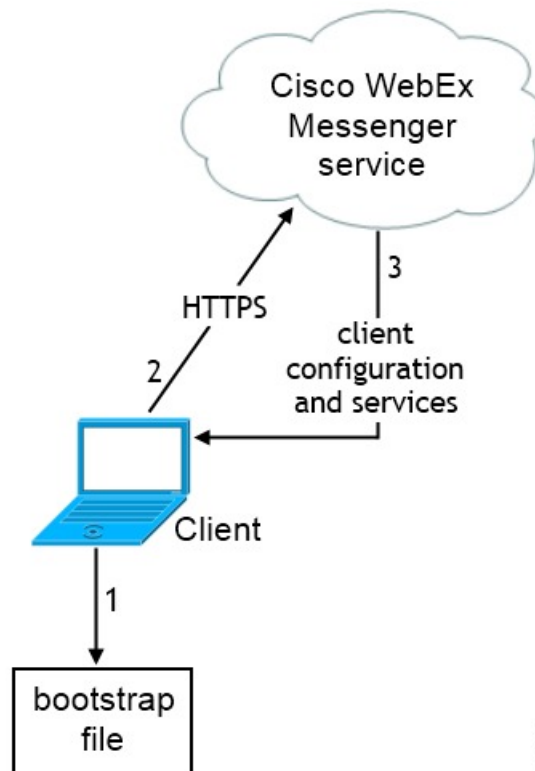
- 1 The client retrieves settings from the bootstrap file.
The client starts in phone mode and determines that Cisco Unified Communications Manager is the authenticator. The client also gets the addresses for the TFTP server (and CTI servers for Jabber for Windows and Jabber for Mac), unless Service Discovery results dictate otherwise.
- 2 The client authenticates to Cisco Unified Communications Manager and gets configuration.
- 3 The client retrieves device and client configuration.

Bootstrap Settings for Cloud-Based Deployments

During installation, you set values for arguments as follows:

- Set WEBEX as the value for AUTHENTICATOR.

The following diagram illustrates how the client uses bootstrap settings in cloud-based 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 the Cisco WebEx Messenger service is the authenticator, unless Service Discovery results dictate otherwise.
- 2 The client authenticates to the Cisco WebEx Messenger service.
- 3 The client retrieves configuration and services.



Configure a Service Profile

- [Activate and Start Essential Services, page 27](#)
- [Create a Service Profile, page 28](#)

Activate and Start Essential Services

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

Procedure

- Step 1** Open the **Cisco Unified IM and Presence Serviceability** interface.
 - Step 2** Select **Tools > Control Center - Feature Services**.
 - Step 3** Select the appropriate server from the **Server** drop-down list.
 - Step 4** Ensure the following services are started and activated:
 - **Cisco SIP Proxy**
 - **Cisco Sync Agent**
 - **Cisco XCP Authentication Service**
 - **Cisco XCP Connection Manager**
 - **Cisco XCP Text Conference Manager**
 - **Cisco Presence Engine**
 - Step 5** Select **Tools > Control Center - Network Services**.
 - Step 6** Select the appropriate server from the **Server** drop-down list.
 - Step 7** Ensure **Cisco XCP Router Service** is running.
-

What to Do Next

- If you have Cisco Unified Communications Manager IM & Presence 9.x and later, [Create a Service Profile](#), on page 28.
- If you have Cisco Unified Presence 8.6, [Pre-Populate Contact Lists in Bulk](#), on page 30.

Create a Service Profile

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

Before You Begin

[Activate and Start Essential Services](#), on page 27

Procedure

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

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

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

Step 4 Enter settings on the **Service Profile Configuration** window as follows:

- a) Specify a unique name for the service profile in the **Name** field.
- b) Specify an optional description in the **Description** field.
- c) Select **Make this the default service profile for the system**, if appropriate.

Note For phone mode, in the **IM and Presence Profile** section ensure that the **Primary** field has **<None>** selected.

Step 5 Select **Save**.



CHAPTER 7

Configure IM and Presence Service

- [Configure IM and Presence Service for an On-Premises Deployment, page 29](#)
- [Configure IM and Presence Service for Cloud-Based Deployments, page 35](#)

Configure IM and Presence Service for an On-Premises Deployment

IM and Presence Service Workflow for an On-Premises Deployment with CUCM 9.x and Later

Procedure

	Command or Action	Purpose
Step 1	Pre-Populate Contact Lists in Bulk, on page 30	
Step 2	Enable Message Settings, on page 30	
Step 3	Add an IM and Presence Service, on page 32	
Step 4	Apply an IM and Presence Service, on page 32	
Step 5	Configure Presence in Microsoft SharePoint 2010 and 2013, on page 33	
Step 6	Configure Users, on page 34	

IM and Presence Service Workflow for an On-Premises Deployment with CUCM 8.6

Procedure

	Command or Action	Purpose
Step 1	Pre-Populate Contact Lists in Bulk, on page 30	
Step 2	Enable Message Settings, on page 30	
Step 3	Specify Capabilities Assignments, on page 31	
Step 4	Configure Presence in Microsoft SharePoint 2010 and 2013, on page 33	

Pre-Populate Contact Lists in Bulk

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

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

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

Procedure

	Command or Action	Purpose
Step 1	Create a CSV file that defines the contact list you want to provide to users.	
Step 2	Use the BAT to import the contact list in bulk to a set of users.	For more information about using BAT and the format of the CSV file, see the <i>Deployment Guide for Cisco Unified Presence</i> for your release.

Enable Message Settings

Enable and configure instant messaging capabilities.

Before You Begin

[Pre-Populate Contact Lists in Bulk, on page 30.](#)

Procedure

- Step 1** Open the **Cisco Unified CM IM and Presence Administration** interface.
- Step 2** Select **Messaging > Settings**.
- Step 3** Select the following options:
- **Enable instant messaging**
 - **Allow clients to log instant message history**
- Step 4** Select other messaging settings as appropriate.
- Step 5** Select **Save**.
- Important** Cisco Jabber does not support the following settings on the **Presence Settings** window on Cisco Unified Communications Manager IM and Presence Service version 9.0.x:
- **Use DND status when user is on the phone**
 - **Use DND status when user is in a meeting**
-

What to Do Next

- If you have Cisco Unified Communications Manager IM & Presence 9.x and later, [Add an IM and Presence Service](#), on page 32.
- If you have Cisco Unified Presence 8.6, [Specify Capabilities Assignments](#), on page 31.

Specify Capabilities Assignments

Complete the steps in this task to provide users with instant messaging and presence capabilities when using Cisco Unified Presence.

Before You Begin

[Enable Message Settings](#), on page 30

Procedure

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

- Enable CUP
- Enable CUPC

Step 6 Select **Save**.

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:

- Select **Unified CM (IM and Presence)** from the **Product Type** drop-down list.
- 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.
- Specify an optional description in the **Description** field.
- 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 32

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**.
- Step 6** Add users to the service profile.
- a) Select **User Management > End User**.
The **Find and List Users** dialog box opens.
 - b) Specify the appropriate filters in the **Find User where** field and then select **Find** to find a user.
 - c) Click the user in the list.
The **End User Configuration** window appears.
 - d) Under the **Service Settings** area, check the **Home Cluster** check box.
 - e) Check the **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)** check box.
 - f) Select your service profile from the **UC Service Profile** drop-down list.
- Step 7** Click **Save**.
-

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:
- For the **SIP Address** profile field, leave it blank.
 - 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:
- For the **SIP Address** profile field, enter the user profile. For example, john4mail@example.pst
 - In the **Work email** profile field, leave it blank.
-

Configure Users

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

Before You Begin

[Configure Presence in Microsoft SharePoint 2010 and 2013, on page 33](#)

Configure Users Individually

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

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **User Management > End User**.
The **Find and List Users** window opens.
- Step 3** Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
- Step 4** Select the appropriate username from the list.
The **End User Configuration** window opens.
- Step 5** Locate the **Service Settings** section and do the following:
- Select **Enable User for Unified CM IM and Presence**.
 - Select your service profile from the **UC Service Profile** drop-down list.
- Important** **Cisco Unified Communications Manager version 9.x only:** If the user has only instant messaging and presence capabilities (IM only), you must select **Use Default**. Cisco Unified Communications Manager version 9.x always applies the default service profile regardless of what you select from the **UC Service Profile** drop-down list.
- Step 6** Select **Save**.
-

Configure Users in Bulk

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

Procedure

-
- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Bulk Administration > Users > Update Users > Query**.
The **Find and List Users To Update** window opens.
- Step 3** Specify the appropriate filters in the **Find User where** field and then select **Find** to retrieve a list of users.
- Step 4** Select **Next**.
The **Update Users Configuration** window opens.
- Step 5** Select both of the **Enable User for Unified CM IM and Presence** check boxes.
Important There are two check boxes for **Enable User for Unified CM IM and Presence**. To disable instant messaging and presence, you select one check box. To enable instant messaging and presence, you select both check boxes.
- Step 6** Select the **UC Service Profile** check box and then select your service profile from the drop-down list.
Important **Cisco Unified Communications Manager version 9.x only:** If the user has only instant messaging and presence capabilities (IM only), you must select **Use Default**.

For IM only users, Cisco Unified Communications Manager version 9.x always applies the default service profile regardless of what you select from the **UC Service Profile** drop-down list.
- Step 7** In the **Job Information** section, specify if you want to run the job immediately or at a later time.
- Step 8** Select **Submit**.
-

Configure IM and Presence Service for Cloud-Based Deployments

Procedure

	Command or Action	Purpose
Step 1	Configure IM and Presence Service, on page 36	
Step 2	Configure Presence in Microsoft SharePoint 2010 and 2013	
Step 3	Configure Privacy Options, on page 36	

Configure IM and Presence Service

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

Configure Privacy Options

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

Procedure

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

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

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

- **Accept requests automatically from all contacts** — The client automatically accepts presence subscription requests from any domain. If you specify this setting, users from any domain can automatically add users to their contact list and view their availability status.
- **Accept requests automatically from contacts in my organization** — The client automatically accepts presence subscription requests only from users in the domains you specify. To specify a domain, select **Domain(s)** in the **System Settings** section on the **Configuration** tab.

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

- Prompt me for each request — The client prompts users to accept each presence subscription request.

Step 5 Select **Save**.



Configure Voice and Video Communication

- [Configure Voice and Video Communications for On-Premises Deployments, page 39](#)
- [Configure Voice and Video Communication for Cloud-Based Deployments, page 60](#)

Configure Voice and Video Communications for On-Premises Deployments

Procedure

	Command or Action	Purpose
Step 1	Install Cisco Options Package File for Devices, on page 40.	Complete this task to make Cisco Jabber available as a device in Cisco Unified Communications Manager. This is applicable for Cisco Unified Communications Manager 9.x and later only.
Step 2	Apply COP File for BFCP Capabilities, on page 41.	Complete this task if you have Cisco Unified Communications Manager 8.6 and you plan to enable video desktop sharing.
Step 3	Create SIP Profiles, on page 42.	Complete this task if you have Cisco Unified Communications Manager Version 9 or earlier and plan to configure devices for mobile clients.
Step 4	Configure the Phone Security Profile, on page 43	Complete this task to setup secure phone capabilities for all devices.
Step 5	Enable User Mobility, on page 45.	Complete this task if you plan to assign Cisco Jabber for Mac or Cisco Jabber for Windows users to CTI remote devices.

	Command or Action	Purpose
Step 6	Add a CTI Service, on page 45.	Complete this task if you plan to assign Cisco Jabber for Mac or Cisco Jabber for Windows users to CTI remote devices.
Step 7	Add a CTI Gateway Server, on page 47.	Complete this only if you have CUCM 8.6 with CUP.
Step 8	Video Desktop Sharing, on page 48	
Step 9	Create and Configure Cisco Jabber Devices, on page 48	Create at least one device for every user that will access Cisco Jabber.
Step 10	Provide Users with Authentication Strings, on page 52	
Step 11	Desk Phone Video Configuration, on page 53	
Step 12	Enable Video Rate Adaptation, on page 55	
Step 13	Configure User Associations, on page 56	
Step 14	Reset Devices, on page 57	Only if installing Cisco Jabber for Mac
Step 15	Create a CCMCIP Profile, on page 58	
Step 16	Dial Plan Mapping, on page 59	

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.

Apply COP File for BFCP Capabilities

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



Note

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

Procedure

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

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

Create SIP Profiles

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

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

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

Before You Begin

[Install Cisco Options Package File for Devices](#), on page 40

Procedure

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

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

Step 5 Select **Save**.

What to Do Next

[Increase SIP Dual Mode Alert Timer Value](#), on page 43

Increase SIP Dual Mode Alert Timer Value

Increase the SIP Dual Mode Alert Timer value to ensure that calls to the Cisco Jabber extension are not prematurely routed to the mobile-network phone number.

Before You Begin

This configuration is only for mobile clients.

Cisco Jabber must be running to receive work calls.

[Create SIP Profiles](#), on page 42

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 you must use mixed mode security.

For instructions on how to configure mixed mode with the Cisco CTL Client, see the Cisco Unified Communications Manager Security Guide at <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>.

- 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.

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.
 - **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 Realtime 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** checkbox to encrypt the device configuration file that resides on the TFTP server.
- Step 8** For **Authentication Mode**, select **By Authentication String**.
- 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, you should 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**.
-

Enable User Mobility

This task is applicable only for desktop

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 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**.
-

Add a CTI Service

The CTI service lets users control devices.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **User Management > User Settings > UC Service**.
The **Find and List UC Services** window opens.
- Step 3** Select **Add New**.

The **UC Service Configuration** window opens.

- Step 4** In the **Add a UC Service** section, select **CTI** from the **UC Service Type** drop-down list.
- Step 5** Select **Next**.
- Step 6** Provide details for the instant messaging and presence service as follows:
- 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.
 - Specify an optional description in the **Description** field.
 - Specify the CTI service address in the **Host Name/IP Address** field.
 - Specify the port number for the CTI service in the **Port** field.
- Step 7** Select **Save**.
-

What to Do Next

Add the CTI service to your service profile.

Apply a CTI Service

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

Before You Begin

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

Procedure

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

Add a CTI Gateway Server

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

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

Procedure

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

What to Do Next

[Create a CTI Gateway Profile, on page 47](#)

Create a CTI Gateway Profile

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

Before You Begin

[Add a CTI Gateway Server, on page 47](#)

Procedure

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

Video Desktop Sharing

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



Note Cisco Jabber for mobile clients can only receive BFCP.



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



Tip

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

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

Create and Configure Cisco Jabber Devices

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

Before You Begin

- Install COP files.
- Enable mobility for each user for whom you plan to assign to a CTI remote device.

- Create SIP profiles if you have Cisco Unified Communications Manager Version 9 or earlier and plan to configure devices for mobile clients.
- Create the Phone Security Profile if you plan to setup secure phone capabilities for all devices.

Procedure

- Step 1** Log into the **Cisco Unified CM Administration** interface.
- Step 2** Select **Device > Phone**.
- 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**.
- **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.
 - **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 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 **User** is selected.
- Step 6** In the **Device Name** field, use the applicable format to specify a name for the device:

If you select	Then
CTI Remote Device	The device name auto-populates as <i>CTIRD<username></i> . For example, if you create a CTI remote device for user, Tanya Adams, whose username is tadams, the device name auto-populates as CTIRDtadams.
Cisco Unified Client Services Framework	Enter <i>CSF<USERNAME></i> . For example, if you create a CSF device for user, Tanya Adams, whose username is tadams, enter CSFTADAMS.
Cisco Dual Mode for iPhone	Enter <i>TFT<USERNAME></i> . For example, if you create a TFT device for user, Tanya Adams, whose username is tadams, enter TFTTADAMS.
Cisco Jabber for Tablet	Enter <i>TAB<USERNAME></i> . For example, if you create a TAB device for user, Tanya Adams, whose username is tadams, enter TABTADAMS.

If you select	Then
Cisco Dual Mode for Android	Enter <i>BOT<USERNAME></i> . For example, if you create a BOT device for user, Tanya Adams, whose username is tadams, enter BOTTADAMS.

- Step 7** If you are creating a CTI Remote Device, in the **Protocol Specific Information** section, select an appropriate option from the **Rerouting Calling Search Space** drop-down list.
The Rerouting Calling Search Space defines the calling search space for re-routing and ensures that users can send and receive calls from the CTI remote device.
- Step 8** To generate an authentication string that you can provide to end users to access their devices and securely register to Cisco Unified Communications Manager, navigate to the **Certification Authority Proxy Function (CAPF) Information** section.
- Step 9** From the **Certificate Operation** drop-down list, select **Install/Upgrade**.
- Step 10** From the **Authentication Mode** drop-down list, select **By Authentication String**.
- Step 11** Click **Generate String**.
The Authentication String auto-populates with a string value. This is the string that you will provide to end users.
- Step 12** From the **Key Size (Bits)** drop-down list, select the same key size that you set in the phone security profile.
- Step 13** In the **Operation Completes By** fields, specify an expiration value for the authentication string or leave as default.
- Step 14** Specify remaining configuration settings in the **Phone Configuration** window as appropriate.
For more information about the remaining configuration settings, on the menu bar, click **Help > This Page**, and then select the **Phone settings** topic. For detailed information about the settings in the **Product Specific Configuration Layout** section, click the question mark icon.
- Step 15** Select **Save**.
- Step 16** Click **Apply Config**.

What to Do Next

Add a Directory Number to the device.

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**.
-

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.

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.

Desk Phone Video Configuration

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

Set Up Desk Phone Video

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

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

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

**Tip**

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

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

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

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

**Note**

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

Desk Phone Video Considerations

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

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

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

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

- 1 Ensure you enable the desk phone device for video in Cisco Unified Communications Manager.

- 2 Reset the physical desk phone.
- 3 Exit the client.
- 4 Run services.msc on the computer where you installed the client.
- 5 Restart Cisco Media Services Interface.
- 6 Restart the client.

Enable Video Rate Adaptation

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

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

**Note**

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

Enable RTCP on Common Phone Profiles

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

Procedure

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

Enable RTCP on Device Configurations

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

Procedure

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

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.
- 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.

Reset Devices

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

Procedure

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

Step 2 Select **Device > Phone**.

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

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

Step 4 Select the appropriate device from the list.

The **Phone Configuration** window opens.

Step 5 Locate the **Association Information** section.

Step 6 Select the appropriate directory number configuration.

The **Directory Number Configuration** window opens.

Step 7 Select **Reset**.

The **Device Reset** dialog box opens.

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

What to Do Next

[Create a CCMCIP Profile, on page 58](#)

Create a CCMCIP Profile

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



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

Before You Begin

[Reset Devices, on page 57](#)

Procedure

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

What to Do Next

[Dial Plan Mapping](#), on page 59

Dial Plan Mapping

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

Application Dial Rules

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

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

Directory Lookup Dial Rules

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

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

Publish Dial Rules

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



Remember

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

Before You Begin

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

Procedure

-
- Step 1** Open the **Cisco Unified OS Administration** interface.
- Step 2** Select **Software Upgrades > Install/Upgrade**.
- Step 3** Specify the location of `cmterm-cupc-dialrule-wizard-0.1.cop.sgn` in the **Software Installation/Upgrade** window.
- Step 4** Specify the location of `cmterm-cupc-dialrule-wizard-0.1.cop.sgn` in the **Software Installation/Upgrade** window.
- Step 5** Select **Next**.
- Step 6** Select `cmterm-cupc-dialrule-wizard-0.1.cop.sgn` from the **Available Software** list.
- Step 7** Select `cmterm-cupc-dialrule-wizard-0.1.cop.sgn` from the Available Software list.
- Step 8** Select **Next** and then select **Install**.
- Step 9** Restart the TFTP service.
- Step 10** Open the dial rules XML files in a browser to verify that they are available on your TFTP server.
- Navigate to `http://tftp_server_address:6970/CUPC/AppDialRules.xml`.
 - Navigate to `http://tftp_server_address:6970/CUPC/DirLookupDialRules.xml`.
- If you can access `AppDialRules.xml` and `DirLookupDialRules.xml` with your browser, the client can download your dial rules.
- Step 11** Repeat the preceding steps for each Cisco Unified Communications Manager instance that runs a TFTP service.
-

What to Do Next

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

Configure Voice and Video Communication for Cloud-Based Deployments

Procedure

	Command or Action	Purpose
Step 1	Configure Audio and Video Services, on page 60	
Step 2	Add Teleconferencing Service Name Accounts, on page 61	

Configure Audio and Video Services

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

- *Getting started with Cisco Unified Communications Manager for Click to Call*
- *Creating unified communications clusters*

What to Do Next

[Add Teleconferencing Service Name Accounts, on page 61](#)

Add Teleconferencing Service Name Accounts

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

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

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

Before You Begin

[Configure Audio and Video Services, on page 60](#)



CHAPTER 9

Configure Voicemail

- [Configure Voicemail for an On-Premises Deployment with CUCM 9.x and Later, page 63](#)
- [Configure Voicemail for an On-Premises Deployment with CUCM 8.6, page 64](#)
- [Configure Cisco Unity Connection for Use with Cisco Jabber, page 65](#)
- [Configure Voicemail Accounts on Cisco Unity Connection, page 66](#)
- [Add a Voicemail Service, page 66](#)
- [Add a Mailstore Service, page 68](#)
- [Add a Voicemail Server, page 70](#)
- [Create a Mailstore, page 71](#)
- [Create a Voicemail Profile, page 72](#)
- [Configure Retrieval and Redirection, page 73](#)
- [Set a Voicemail Credentials Source, page 74](#)
- [Enable Enhanced Message Waiting Indicator, page 75](#)
- [Configure Voicemail for Cloud-Based Deployments, page 75](#)

Configure Voicemail for an On-Premises Deployment with CUCM 9.x and Later

Procedure

	Command or Action	Purpose
Step 1	Configure Cisco Unity Connection for Use with Cisco Jabber, on page 65	Configure Cisco Unity Connection so that Cisco Jabber can access voicemail services.
Step 2	Add a Voicemail Service, on page 66	

	Command or Action	Purpose
Step 3	Configure Voicemail Accounts on Cisco Unity Connection, on page 66	To configure Cisco Unity Connection, you must create user profiles and then provide users with IMAP access.
Step 4	Apply a Voicemail Service, on page 67	After you add a voicemail service, you must apply it to a service profile so that the client can retrieve the settings.
Step 5	Add a Mailstore Service, on page 68	
Step 6	Apply Mailstore Service, on page 69	After you add a mailstore service, you must apply it to a service profile so that the client can retrieve the settings.
Step 7	Configure Retrieval and Redirection, on page 73	Configure retrieval so that users can access voice mail messages. Configure redirection so that users can send incoming calls to voicemail.
Step 8	Set a Voicemail Credentials Source, on page 74	
Step 9	Enable Enhanced Message Waiting Indicator, on page 75	This procedure applies only if you want to set up a basic voicemail account that allows users to dial in to their voice mailbox. This procedure is not required if you want to set up visual voicemail.

Configure Voicemail for an On-Premises Deployment with CUCM 8.6

Procedure

	Command or Action	Purpose
Step 1	Configure Cisco Unity Connection for Use with Cisco Jabber, on page 65	
Step 2	Add a Voicemail Server, on page 70	
Step 3	Create a Mailstore, on page 71	
Step 4	Create a Voicemail Profile, on page 72	
Step 5	Configure Retrieval and Redirection, on page 73	
Step 6	Set a Voicemail Credentials Source, on page 74	

Configure Cisco Unity Connection for Use with Cisco Jabber

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



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

Procedure

- Step 1** Ensure the **Connection Jetty** and **Connection REST Service** services are started.
- Open the **Cisco Unity Connection Serviceability** interface.
 - Select **Tools > Service Management**.
 - Locate the following services in the **Optional Services** section:
 - **Connection Jetty**
 - **Connection REST Service**
 - Start the services if required.
- Step 2** Open the **Cisco Unity Connection Administration** interface.
- Step 3** Edit user password settings.
- Select **Users**.
 - Select the appropriate user.
 - Select **Edit > Password Settings**.
 - Select **Web Application** from the **Choose Password** menu.
 - Uncheck **User Must Change at Next Sign-In**.
 - Select **Save**.
- Step 4** Provide users with access to the web inbox.
- Select **Class of Service**.
The **Search Class of Service** window opens.
 - Select the appropriate class of service or add a new class of service.
 - Select **Allow Users to Use the Web Inbox and RSS Feeds**.
 - In the **Features** section, select **Allow Users to Use Unified Client to Access Voice Mail**.
 - Select all other options as appropriate.
 - Select **Save**.
- Step 5** Select API configuration settings.
- Select **System Settings > Advanced > API Settings**.
The **API Configuration** window opens.
 - Select the following options:

- **Allow Access to Secure Message Recordings through CUMI**
- **Display Message Header Information of Secure Messages through CUMI**
- **Allow Message Attachments through CUMI**

c) Select **Save**.

What to Do Next

- If you have Cisco Unified Communications Manager 9.x and later, [Add a Voicemail Service](#), on page 66.
- If you have Cisco Unified Communications Manager 8.x, [Add a Voicemail Server](#), on page 70.

Configure Voicemail Accounts on Cisco Unity Connection

To configure Cisco Unity Connection, you must create user profiles and then provide users with IMAP access. See the Cisco Unity Connection documentation for specific configuration tasks.

Before You Begin

[Add a Voicemail Service](#), on page 66

Procedure

Step 1 Create user profiles on Cisco Unity Connection.

Step 2 Provide users with IMAP access.

- a) Open the Cisco Unity Connection administrative interface.
 - b) Select **Class of Service**.
The **Edit Class of Service** window opens.
 - c) Locate the **Licensed Features** section.
 - d) Select **Allow Users to Access Voice Mail Using an IMAP Client and/or Single Inbox**.
 - e) Select **Allow IMAP Users to Access Message Bodies**.
 - f) Select **Save**.
-

What to Do Next

[Apply a Voicemail Service](#), on page 67

Add a Voicemail Service

Allow users to receive voice messages.

Before You Begin

[Configure Cisco Unity Connection for Use with Cisco Jabber, on page 65](#)

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **User Management > User Settings > UC Service**.
The **Find and List UC Services** window opens.
- Step 3** In the **Find and List UC Services** window, select **Add New**.
- Step 4** In the **Add a UC Service** section, select **Voicemail** from the **UC Service Type** drop-down list and select **Next**.
- Step 5** Specify details for the voicemail service as follows:
- **Product Type** — Select **Unity Connection**.
 - **Name** — Enter a descriptive name for the server, for example, **PrimaryVoicemailServer**.
 - **Description** — Enter an optional description.
 - **Hostname/IP Address** — Enter the IP address or the fully qualified domain name (FQDN) of the voicemail server.
 - **Port**—You do not need to specify a port number. By default, the client always uses port 443 to connect to the voicemail server. For this reason, any value you specify does not take effect.
 - **Protocol Type**—You do not need to specify a value. By default, the client always uses HTTPS to connect to the voicemail server. For this reason, any value you specify does not take effect.
- Step 6** Select **Save**.
-

What to Do Next

[Configure Voicemail Accounts on Cisco Unity Connection, on page 66](#)

Apply a Voicemail Service

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

Before You Begin

[Configure Voicemail Accounts on Cisco Unity Connection, on page 66](#)

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**.

Step 6 Add users to the service profile.

- a) Select **User Management > End User**.
The **Find and List Users** window opens.
 - b) Specify the appropriate filters in the **Find User where** field and then select **Find** to find a user.
 - c) Click the user in the list.
The **End User Configuration** window opens.
 - d) Under the **Service Settings** area, check the **Home Cluster** check box.
 - e) Check the **Enable User for Unified CM IM and Presence (Configure IM and Presence in the associated UC Service Profile)** check box.
Note 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.
 - f) Select your service profile from the **UC Service Profile** drop-down list.
 - g) Click **Save**.
-

What to Do Next

[Add a Mailstore Service](#), on page 68

Add a Mailstore Service

The mailstore service provides users with visual voicemail capabilities.

Before You Begin

[Apply a Voicemail Service, on page 67](#)

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **User Management > User Settings > UC Service**.
The **Find and List UC Services** window opens.
- Step 3** Select **Add New**.
- Step 4** In the **Add a UC Service** section, from the **UC Service Type** drop-down list, select **MailStore** and then click **Next**.
- Step 5** Provide details for the mailstore service as follows:
- **Name**—Enter a descriptive name for the server, for example, PrimaryMailStoreServer.
 - **Description**—Enter an optional description.
 - **Hostname/IP Address**—Enter the IP address or the Fully Qualified Domain Name (FQDN) of the mailstore server.
 -
 - **Port**—You do not need to specify a port number. By default, the client always uses port 443 to connect to the mailstore server. For this reason, any value you specify does not take effect.
 -
 - **Protocol Type**—You do not need to specify a value. By default, the client always uses HTTPS to connect to the mailstore server. For this reason, any value you specify does not take effect.
- Step 6** Select **Save**.
-

What to Do Next

[Apply Mailstore Service, on page 69](#)

Apply Mailstore Service

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

Before You Begin

[Add a Mailstore Service, on page 68](#)

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **User Management > User Settings > Service Profile**.

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

- Step 3** Find and select your service profile.
The **Service Profile Configuration** window opens.
- Step 4** Configure the **MailStore Profile** section as follows:
- a) Select up to three services from the following drop-down lists:
 - **Primary**
 - **Secondary**
 - **Tertiary**
 - b) Specify appropriate values for the following fields:
 - **Inbox Folder**
 - **Trash Folder**
 - **Polling Interval**
- Step 5** Select **Save**.

What to Do Next

[Configure Retrieval and Redirection, on page 73](#)

Add a Voicemail Server

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

Before You Begin

[Configure Cisco Unity Connection for Use with Cisco Jabber, on page 65](#)

Procedure

- Step 1** Open the **Cisco Unified Presence Administration** interface.
- Step 2** Select **Application > Cisco Jabber > Voicemail Server**.
- Note** In some versions of Cisco Unified Presence, this path is as follows: **Application > Cisco Unified Personal Communicator > Voicemail Server**.
The **Find and List Voicemail Servers** window opens.
- Step 3** Select **Add New**.
- Step 4** Select **Unity Connection** from the **Server Type** drop-down list.
- Step 5** Specify details in the **Voicemail Server Configuration** section as follows:
- **Name**—Enter a descriptive name for the server, for example, PrimaryVoicemailServer.
 - **Description**—Enter an optional description.

- **Hostname/IP Address**—Enter the IP address or the fully qualified domain name (FQDN) of the voicemail server.
- **Port**—You do not need to specify a port number. By default, the client always uses port 443 to connect to the voicemail server. For this reason, any value you specify does not take effect.
- **Protocol Type**—You do not need to specify a value. By default, the client always uses HTTPS to connect to the voicemail server. For this reason, any value you specify does not take effect.

Step 6 Select **Save**.

What to Do Next

[Create a Mailstore](#), on page 71

Related Topics

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

Create a Mailstore

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

Before You Begin

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

If you have Cisco Unified Communications Manager 9.x or later, see [Add a Mailstore Service](#), on page 68.

Procedure

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

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

- **Application > Cisco Jabber > Mailstore**
- **Application > Cisco Unified Personal Communicator > Mailstore**

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

Step 3 Select **Add New**.

The **Mailstore Configuration** window opens.

Step 4 Specify details as follows:

- **Name**—Enter a descriptive name for the server, for example, PrimaryMailStoreServer.
- **Description**—Enter an optional description.
- **Hostname/IP Address**—Enter the hostname, IP Address, or Fully Qualified Domain Name (FQDN) of the mailstore server.
-

- **Port**—You do not need to specify a port number. By default, the client always uses port 443 to connect to the mailstore server. For this reason, any value you specify does not take effect.
-
- **Protocol Type**—You do not need to specify a value. By default, the client always uses HTTPS to connect to the mailstore server. For this reason, any value you specify does not take effect.

Step 5 Select **Save**.

Create a Voicemail Profile

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

Before You Begin

[Create a Mailstore](#), on page 71

Procedure

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

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

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

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

Step 3 Select **Add New**.

The **Voicemail Profile Configuration** window opens.

Step 4 Specify the required details.

Step 5 Add users to the voicemail profile as follows:

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

The selected users are added to the voicemail profile.

Step 6 Select **Save**.

What to Do Next

[Configure Retrieval and Redirection](#), on page 73

Configure Retrieval and Redirection

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

Before You Begin

If you have Cisco Unified Communications Manager 9.x and later, [Apply Mailstore Service, on page 69](#).

If you have Cisco Unified Communications Manager 8.x, [Create a Voicemail Profile, on page 72](#).

Procedure

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

h) Select **Save**.

What to Do Next

[Set a Voicemail Credentials Source](#), on page 74

Set a Voicemail Credentials Source

You can specify a voicemail credentials source for users.



Tip

In hybrid cloud-based deployments, you can set a voicemail credentials source as part of your configuration file with the `VoiceMailService_UseCredentialsFrom` parameter.

Before You Begin

[Configure Retrieval and Redirection](#), on page 73

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.

If you have Cisco Unified Communications Manager 9.x and later, [Enable Enhanced Message Waiting Indicator](#), on page 75.

Enable Enhanced Message Waiting Indicator

This procedure applies only if you want to set up a basic Voicemail account that allows users to dial in to their voice mailbox. This procedure is not required if you want to set up visual voicemail.

A Message Waiting Indicator alerts users to the presence of new voice messages. Enhanced Message Waiting Indicator provides a count of new voice messages on systems that support this feature. Users can call the voice messaging system to retrieve the messages.



Note

To enable the basic Message Waiting Indicator, follow the instructions in the Cisco Unified Communications Manager documentation for your release. There are no unique configurations for this client.

If your deployment supports Enhanced Message Waiting Indicator, enable this option in the Cisco Unity Connection Administration portal.

Before You Begin

[Set a Voicemail Credentials Source](#), on page 74

Procedure

- Step 1** Open the **Cisco Unity Connection Administration** interface.
- Step 2** In the left pane, navigate to **Telephony Integrations > Phone System**.
- Step 3** Select the link for the desired phone system.
- Step 4** In the Message Waiting Indicators section, select the **Send Message Counts** check box.

Configure Voicemail for Cloud-Based Deployments

Procedure

	Command or Action	Purpose
Step 1	Configure Voicemail , on page 75	
Step 2	Allow Users to Set Voicemail Server Settings , on page 76	

Configure Voicemail

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

What to Do Next

[Allow Users to Set Voicemail Server Settings](#), on page 76

Allow Users to Set Voicemail Server Settings

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

Before You Begin

[Configure Voicemail](#), on page 75

Procedure

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

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

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



CHAPTER 10

Configure Conferencing

- [Configure Conferencing for an On-Premises Deployment, page 77](#)
- [Configure Conferencing for a Cloud-Based Deployment using Cisco WebEx Meeting Center, page 86](#)

Configure Conferencing for an On-Premises Deployment

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

Configure On-Premises Conferencing using WebEx Meetings Server

Procedure

	Command or Action	Purpose
Step 1	Authenticate Cisco WebEx Meetings Server, on page 77.	
Step 2	Add Cisco WebEx Meetings Server on Cisco Unified Communications Manager, on page 78.	Complete this task if you have CUCM 9.x and later.
Step 3	Add Cisco WebEx Meetings Server on Cisco Unified Presence, on page 80.	Complete this task if you have CUCM 8.6 and CUP.

Authenticate Cisco WebEx Meetings Server

Procedure

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

- Configure single sign-on (SSO) with Cisco WebEx Meetings Server to integrate with the SSO environment. In this case, you do not need to specify credentials for users to authenticate with Cisco WebEx Meetings Server
- Set a credentials source on Cisco Unified Communications Manager. If the users' credentials for Cisco WebEx Meetings Server match their credentials for Cisco Unified Communications Manager IM and Presence Service or Cisco Unity Connection, you can set a credentials source. The client then automatically authenticates to Cisco WebEx Meetings Server with the users' credential source.
- Instruct users to manually enter credentials in the client.

What to Do Next

[Add Cisco WebEx Meetings Server on Cisco Unified Communications Manager, on page 78](#)

Add Cisco WebEx Meetings Server on Cisco Unified Communications Manager

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

Before You Begin

[Authenticate Cisco WebEx Meetings Server, on page 77](#)

Procedure

-
- Step 1** Open the **Cisco Unified CM Administration** interface and select **User Management > User Settings > UC Service**.
The **Find and List UC Services** window opens.
- Step 2** Select **Add New**.
- Step 3** In the **Add a UC Service** section, from the **UC Service Type** drop-down list, select **Conferencing** and then select **Next**.
- Step 4** Complete the following fields:
- **Product Type** — Select **WebEx (Conferencing)**.
 - **Name** — Enter a name for the configuration. The name you specify is displayed when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.
 - **Description** — Enter an optional description.
 - **Hostname/IP Address** — Enter the site URL for Cisco WebEx Meetings Server. This URL is case sensitive and must match the case that was configured for the site URL in Cisco WebEx Meetings Server.
 - **Port** — Leave the default value.
 - **Protocol** — Select **HTTPS**.
- Step 5** To use Cisco WebEx as the single sign-on (SSO) identity provider, check **User web conference server as SSO identity provider**.
- Note** This field is available only if you select **WebEx (Conferencing)** from the **Product Type** drop-down list.

Step 6 Select **Save**.

What to Do Next

[Add the Cisco WebEx Meetings Server to a Service Profile](#), on page 79

Add the Cisco WebEx Meetings Server to a Service Profile

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

Before You Begin

Create a service profile.

[Add Cisco WebEx Meetings Server on Cisco Unified Communications Manager](#), on page 78

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface and select **User Management > User Settings > Service Profile**
- Step 2** Find and select your service profile.
- Step 3** In the **Conferencing Profile** section, from the **Primary**, **Secondary**, and **Tertiary** drop-down lists, select up to three instances of Cisco WebEx Meetings Server.
- Step 4** From the **Server Certificate Verification** drop-down list, select the appropriate value.
- Step 5** From the **Credentials source for web conference service** drop-down list, select one of the following:
- **Not set** — Select this option if the user does not have a credentials source that matches their Cisco WebEx Meetings Server credentials or if you use SSO at the meeting site.
 - **Unified CM - IM and Presence** — Select this option if the Cisco Unified Communications Manager IM and Presence Service credentials for the user match their Cisco WebEx Meetings Server credentials.
 - **Voicemail** — Select this option if the Cisco Unity Connection credentials for the user match their Cisco WebEx Meetings Server credentials.
- Note** You cannot synchronize the credentials you specify in Cisco Unified Communications Manager with credentials you specify in Cisco WebEx Meetings Server. For example, if you specify that instant messaging and presence credentials for a user are synchronized with their Cisco WebEx Meetings Server credentials, the instant messaging and presence credentials for that user change. You must update the Cisco WebEx Meetings Server credentials for that user to match that change.
- Step 6** Select **Save**.
-

What to Do Next

[Add Cisco WebEx Meetings Server on Cisco Unified Presence](#), on page 80

Add Cisco WebEx Meetings Server on Cisco Unified Presence

Before You Begin

[Add the Cisco WebEx Meetings Server to a Service Profile, on page 79](#)

Procedure

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

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

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

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

Step 4 Complete the following fields:

- **Name** — Enter a name for the configuration. The name is displayed when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.
- **Description** — Enter an optional description.
- **Hostname/IP Address** — Enter the site URL for Cisco WebEx Meetings Server.
- **Port** — Accept the default value.
- **Protocol** — Select **HTTPS**.
- **Server Type** — Select **WebEx**.
- **Site ID** — You do not need to specify a value for this field.
- **Partner ID** — You do not need to specify a value for this field.

Step 5 Select **Save**.

What to Do Next

[Add Cisco WebEx Meetings Server to a Profile, on page 80](#)

Add Cisco WebEx Meetings Server to a Profile

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

Before You Begin

[Add Cisco WebEx Meetings Server on Cisco Unified Presence, on page 80](#)

Procedure

-
- Step 1** Open the **Cisco Unified Presence Administration** interface.
- Step 2** Depending on your version of Cisco Unified Presence, select one of the following:
- **Application > Cisco Jabber > Conferencing Profile**
 - **Application > Cisco Unified Personal Communicator > Conferencing Profile**
- Step 3** Select **Add New**.
The **Conferencing Profile Configuration** window opens.
- Step 4** Complete the following fields:
- **Name** — Enter a name for the configuration.
 - **Description** — Enter an optional description.
 - **Primary Conferencing Server** — Select the primary instance of Cisco WebEx Meetings Server.
 - **Backup Conferencing Server** — Select the backup instance of Cisco WebEx Meetings Server.
- Step 5** From the **Server Certificate Verification** drop-down list, select one of the following:
- **Any Certificate**
 - **Self Signed or Keystore**
 - **Keystore Only**
- Step 6** To set this profile as the system default, check **Make this the default Conferencing Profile for the system**.
- Step 7** In the **Users in Profile** section, select **Add Users to Profile**.
- Step 8** In the **Find and List Users** window, select **Find** to retrieve a list of users.
- Step 9** Select the appropriate users from the list and then select **Add Selected**.
The selected users are added to the profile.
- Step 10** Select **Save**.
-

Configure Cloud-Based Conferencing Using WebEx Meeting Center

Procedure

	Command or Action	Purpose
Step 1	Integration with Cisco WebEx Meeting Center, on page 82.	
Step 2	Authentication with Cisco WebEx Meeting Center, on page 82.	Authenticate the client with Cisco WebEx Meeting Center using tightly coupled integration.

	Command or Action	Purpose
Step 3	Provide Conferencing Credentials, on page 82.	Provide conferencing credentials to the client.
Step 4	<p>Depending on your version of Cisco Unified Communications Manager, select one of the following:</p> <ul style="list-style-type: none"> • If you have Cisco Unified Communications Manager 9.x and later with Cisco Unified Communications Manager IM and Presence Service, Add Cisco WebEx Meeting Center, on page 83. • If you have Cisco Unified Communications Manager 8.6 with Cisco Unified Presence, Set Up Cisco WebEx Meeting Center on Cisco Unified Presence, on page 84. 	

Integration with Cisco WebEx Meeting Center

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

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

Authentication with Cisco WebEx Meeting Center

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

Provide Conferencing Credentials

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

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

Add Cisco WebEx Meeting Center

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

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **User Management > User Settings > UC Service**.
The **Find and List UC Services** window opens.
- Step 3** Select **Add New**.
- Step 4** In the **Add a UC Service** section, from the **UC Service Type** drop-down list, select **Conferencing** and then select **Next**.
- Step 5** Complete the following fields:
- **Product Type** — Select **WebEx (Conferencing)**.
 - **Name** — Enter a name for the configuration. The name is displayed when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.
 - **Description** — Enter an optional description.
 - **Host Name/IP Address** — Enter the Cisco WebEx Meeting Center site hostname. Do not enter an IP address.
 - **Port** — Enter the Cisco WebEx Meeting Center site port number.
 - **Protocol** — Select **HTTPS**.
- Step 6** To use Cisco WebEx as the single sign-on (SSO) identity provider, check **User web conference server as SSO identity provider**.
- Note** This field is available only if you select **WebEx (Conferencing)** as the **Product Type**.
- Step 7** Select **Save**.
-

What to Do Next

Add Cisco WebEx Meeting Center to a service profile.

Add Cisco WebEx Meeting Center to a Profile

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

Before You Begin

Create a service profile.

Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **User Management > User Settings > Service Profile**.
The **Find and List Service Profiles** window opens.
- Step 3** Find and select your service profile.
The **Service Profile Configuration** window opens.
- Step 4** Configure the **Conferencing Profile** section as follows:
- Select your service from the **Primary** drop-down list.

Note The client uses only the service you select from the **Primary** drop-down list. You do not need to select services from the **Secondary** or **Tertiary** drop-down lists.
 - Select the appropriate value from the **Server Certificate Verification** drop-down list.
 - Select one of the following from the **Credentials source for web conference service** drop-down list:
 - Not set — The user does not have a credentials source that matches their Cisco WebEx Meeting Center credentials.
 - Unified CM - IM and Presence — The user's Cisco Unified Communications Manager IM and Presence Service credentials match their Cisco WebEx Meeting Center credentials.
 - Voicemail — The user's Cisco Unity Connection credentials match their Cisco WebEx Meeting Center credentials.
- Restriction** You cannot specify a credentials source if you use an identity provider for authentication with Cisco WebEx Meeting Center.
- Important** If you select a credentials source, you must ensure that those credentials match the user's Cisco WebEx Meeting Center credentials.
- There is no mechanism to synchronize the credentials you specify in Cisco Unified Communications Manager with credentials you specify in Cisco WebEx Meeting Center. For example, you specify that a user's instant messaging and presence credentials are synchronized with the user's Cisco WebEx Meeting Center credentials. The user's instant messaging and presence credentials then change. You must update the user's Cisco WebEx Meeting Center credentials to match that change.
- Step 5** Select **Save**.
-

Set Up Cisco WebEx Meeting Center on Cisco Unified Presence

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

Add Cisco WebEx Meeting Center

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

Procedure

- Step 1** Open the **Cisco Unified Presence Administration** interface.
- Step 2** Select **Application > Cisco Jabber > Conferencing Server**.
In some versions of Cisco Unified Presence, this path is as follows: **Application > Cisco Unified Personal Communicator > Conferencing Server**.
- Step 3** Select **Add New**.
The **Conferencing Server Configuration** window opens.
- Step 4** Specify details for Cisco WebEx Meeting Center in the following fields:
- Name — Enter a name for the configuration. The name you specify displays when you add services to profiles. Ensure the name you specify is unique, meaningful, and easy to identify.
 - Description — Enter an optional description.
 - Hostname/IP Address — Specify the hostname of the Cisco WebEx Meeting Center site.
Note You must specify a hostname, not an IP address.
 - Port — Specify a port number for the Cisco WebEx Meeting Center site.
 - Protocol — Select **HTTPS** from the drop-down list.
 - Server Type — Select **WebEx** from the drop-down list.
 - Site ID — Specify the optional primary site ID for Cisco WebEx Meeting Center.
 - Partner ID — Specify the optional appropriate partner ID for Cisco WebEx Meeting Center.
- Step 5** Select **Save**.
-

Add Cisco WebEx Meeting Center to a Profile

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

Procedure

- Step 1** Open the **Cisco Unified Presence Administration** interface.
- Step 2** Select **Application > Cisco Jabber > Conferencing Profile**.

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

Step 3 Select **Add New**.

The **Conferencing Profile Configuration** window opens.

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

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

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

- **Server Certificate Verification** — Select one of the following from the drop-down list:
 - **Any Certificate**
 - **Self Signed or Keystore**
 - **Keystore Only**

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

Step 6 Add users to the conferencing profile as follows:

- a) Select **Add Users to Profile** in the **Users in Profile** section.
The **Find and List Users** dialog box opens.
- b) Select **Find** to retrieve a list of users.
- c) Select the appropriate users from the list.
- d) Select **Add Selected**.

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

Step 7 Select **Save**.

Configure Conferencing for a Cloud-Based Deployment using Cisco WebEx Meeting Center

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

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

Authentication with Cisco WebEx Meeting Center

- **Tightly Coupled Integration with the Cisco WebEx Messenger Service** — Tightly coupled integration refers to a configuration that you set up between Cisco WebEx Messenger and Cisco WebEx Meeting Center.

When users authenticate with Cisco WebEx Messenger, it passes an authentication token back to the client. The client then passes that authentication token to Cisco WebEx Meeting Center.

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

- **Authentication with an Identity Provider** — The client can redirect authentication from Cisco WebEx Meeting Center to an identity provider.

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

- 1 Set up your identity provider as appropriate.

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

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

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

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

Specify Conferencing Credentials in the Client

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

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

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

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

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



Configure the Clients

- [Introduction to Client Configuration, page 89](#)
- [Configure Service Profiles, page 90](#)
- [Create and Host Client Configuration Files, page 98](#)
- [Configure Problem Reporting, page 129](#)
- [Configure Automatic Updates, page 129](#)
- [Custom Embedded Tabs for Cisco Jabber for Windows, page 132](#)

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 version 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.

Applies to on-premises deployments only.

Phone Configuration

You can set some client settings in the phone configuration on Cisco Unified Communications Manager version 9 and later. The client retrieves the settings from the phone configuration in addition to the configuration in the UC service profile.

Applies to on-premises deployments only.

Cisco Unified Presence or 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.

If you do not use service discovery with Cisco Unified Communications Manager version 9 and later, the client retrieves UC services from Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.

Applies to on-premises deployments only.

Client Configuration Files

You can create XML files that contain configuration parameters. You then host the XML files on a TFTP server. When users sign in, the client retrieves the XML file from the TFTP server and applies the configuration.

Applies to on-premises and cloud-based deployments.

Cisco WebEx Administration Tool

You can configure some client settings with the Cisco WebEx Administration Tool.

Applies to cloud-based deployments only.

Configure Service Profiles

You can configure some client settings in UC service profiles on Cisco Unified Communications Manager version 9 and later.



Important

- Cisco Jabber only retrieves configuration from service profiles on Cisco Unified Communications Manager if the client gets the `_cisco-uds` SRV record from a DNS query.
In a hybrid environment, if the CAS URL lookup is successful Cisco Jabber retrieves the configurations from Cisco WebEx Messenger service and the `_cisco-uds` SRV record is ignored.
- In an environment with multiple Cisco Unified Communications Manager clusters, you can configure the Intercluster Lookup Service (ILS). ILS enables the client to find the user's home cluster and discover services.
If you do not configure ILS, then you must manually configure remote cluster information, similar to the EMCC remote cluster set up. For more information on Remote Cluster Configuration, see the *Cisco Unified Communications Manager Features and Services Guide*.

Related Topics

[Remote Cluster Configuration on Cisco Unified Communications Manager 10.0](#)

Set Parameters on Service Profile

The client can retrieve UC service configuration and other settings from service profiles.

Parameters in Service Profiles

Learn which configuration parameters you can set in service profiles. Review the corresponding parameters in the client configuration file.

IM and Presence Service Profile

The following table lists the configuration parameters you can set in the IM and Presence Service profile:

IM and Presence Service Configuration	Description
<p>Product type</p>	<p>Provides the source of authentication to Cisco Jabber and has the following values:</p> <p>Unified CM (IM and Presence Service)</p> <p>Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service is the authenticator.</p> <p>WebEx (IM and Presence Service)</p> <p>The Cisco WebEx Messenger service is the authenticator.</p> <p>Note As of this release, the client issues an HTTP query in addition to the query for SRV records. The HTTP query allows the client to determine if it should authenticate to the Cisco WebEx Messenger service.</p> <p>As a result of the HTTP query, the client connects to the Cisco WebEx Messenger service in cloud-based deployments before getting the <code>_cisco-uds</code> SRV record. Setting the value of the Product type field to WebEx may have no practical effect if the WebEx service has already been discovered by a CAS lookup.</p> <p>Not set</p> <p>If the service profile does not contain an IM and presence service configuration, the authenticator is Cisco Unified Communications Manager.</p>

IM and Presence Service Configuration	Description
<p>Primary server</p>	<p>Specifies the address of your primary presence server.</p> <p>On-Premises Deployments</p> <p>You should specify the fully qualified domain name (FQDN) of Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.</p> <p>Cloud-Based Deployments</p> <p>The client uses the following URL as default when you select WebEx as the value for the Product type parameter:</p> <p><code>https://loginp.webexconnect.com/cas/auth.do</code></p> <p>This default URL overrides any value that you set.</p>

Voicemail Profile

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

Voicemail Service Configuration	Description
<p>Voicemail server</p>	<p>Specifies connection settings for the voicemail server.</p>
<p>Credentials source for voicemail service</p>	<p>Specifies that the client uses the credentials for the instant messaging and presence or conferencing service to authenticate with the voicemail service.</p> <p>Ensure that the credentials source that you set match the user's voicemail credentials. If you set a value for this parameter, users cannot specify their voicemail service credentials in the client user interface.</p>

Conferencing Profile

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

Conferencing Service Configuration	Description
<p>Conferencing server</p>	<p>Specifies connection settings for the conferencing server.</p>
<p>Credentials source for web conference service</p>	<p>Specifies that the client uses the credentials for the instant messaging and presence or voicemail service to authenticate with the conferencing service.</p> <p>Ensure that the credentials source that you set match the user's conferencing credentials.</p>

Directory Profile

See the *Client Configuration for Directory Integration* chapter for information about configuring directory integration in a service profile.

CTI Profile

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

CTI Service Configuration	Description
CTI server	Specifies connection settings for the CTI server.

Add Cisco Unified Communications Manager Services

Add Cisco Unified Communications Manager services to specify the address, ports, protocols, and other settings for services such as IM and Presence Service, voicemail, conferencing, and directory.

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 the UC service type you want to add and then select **Next**.
 - Step 5** Configure the UC service as appropriate and then select **Save**.
-

What to Do Next

Add your UC services to service profiles.

Create Service Profiles

After you add and configure Cisco Unified Communications Manager services, you add them to a service profile. You can apply additional configuration in the service profile.

Procedure

-
- Step 1** Open the **Cisco Unified CM Administration** interface.
 - Step 2** Select **User Management > User Settings > Service Profile**.

The **Find and List UC Services** 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.
- Note** On Cisco Unified Communications Manager version 9.x only, users who have only instant messaging capabilities (IM only) must use the default service profile. For this reason, you should set the service profile as the default if you plan to apply the service profile to IM only users.
- Step 6** Add your UC services, apply any additional configuration, and then select **Save**.
-

What to Do Next

Apply service profiles to end user configuration.

Apply Service Profiles

After you add UC services and create a service profile, you apply the service profile to users. When users sign in to Cisco Jabber, the client can then retrieve the service profile for that user from Cisco Unified Communications Manager.

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** Enter the appropriate search criteria to find existing users and then select a user from the list.
The **End User Configuration** window opens.
- Step 4** Locate the **Service Settings** section.
- Step 5** Select a service profile to apply to the user from the **UC Service Profile** drop-down list.
- Important** **Cisco Unified Communications Manager version 9.x only:** If the user has only IIM and Presence Service capabilities (IM only), you must select **Use Default**. For IM only users, Cisco Unified Communications Manager version 9.x always applies the default service profile regardless of what you select from the **UC Service Profile** drop-down list.
- Step 6** Apply any other configuration as appropriate and then 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.

**Note**

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

Procedure

-
- Step 1** Associate users with devices.
- Open the **Unified CM Administration** interface.
 - Select **User Management > End User**.
 - Find and select the appropriate user.
The **End User Configuration** window opens.
 - Select **Device Association** in the **Device Information** section.
 - Associate the user with devices as appropriate.
 - Return to the **End User Configuration** window and then select **Save**.
- Step 2** Set the **User Owner ID** field in the device configuration.
- Select **Device > Phone**.
 - Find and select the appropriate device.
The **Phone Configuration** window opens.
 - Locate the **Device Information** section.
 - Select **User** as the value for the **Owner** field.
 - Select the appropriate user ID from the **Owner User ID** field.
 - Select **Save**.
-

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.



Note For users with only IM and Presence Service capabilities (IM only), you must set phone configuration parameters in the **Enterprise Phone Configuration** window.

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

Desktop Client Settings Configuration	Description
Automatically Start in Phone Control	<p>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.</p> <p>Enabled</p> <p>Use the desk phone device for calls.</p> <p>Disabled (default)</p> <p>Use the software phone (CSF) device for calls.</p>
Jabber For Windows Software Update Server URL	<p>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.</p> <p>In hybrid cloud-based deployments, you should use the Cisco WebEx Administration Tool to configure automatic updates.</p>
Problem Report Server URL	<p>Specifies the URL for the custom script that allows users to submit problem reports.</p>

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:

Mobile Client Settings Configuration	Description
On-Demand VPN URL	<p>URL for initiating on-demand VPN.</p> <p>Note Applicable for iOS only.</p>

Mobile Client Settings Configuration	Description
Preset Wi-fi Networks	Enter the SSIDs for Wi-Fi networks (SSIDs) approved by your organization. Separate SSIDs with a forward slash (/). Devices do not connect to secure connect if connected to one of the entered Wi-Fi networks.
Default Ringtone	Sets the default ringtone to Normal or Loud .
Video Capabilities	Enables or disables video capabilities. Enabled (default) Users can send and receive video calls. Disabled Users cannot send or receive video calls.
Dial via Office Note TCT and BOT devices only.	Enables or disables Dial via Office. Enabled Users can dial via office. Disabled (default) Users cannot dial via office.

Create and Host Client Configuration Files

For on-premises and hybrid cloud-based deployments, create client configuration files and host them on the Cisco Unified Communications Manager TFTP service.

For cloud-based deployments, configure the client with the Cisco WebEx Administration Tool. However, you can optionally set up a TFTP server to configure the client with settings that are not available in Cisco WebEx Administration Tool.

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 the client can retrieve the file from the TFTP server.
- You must 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 confirm that elements are nested correctly.
- Valid XML character entity references only are permitted 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 does is valid.
- If Internet Explorer displays only part of the XML structure, it is likely that your configuration file contains invalid characters or entities.

Procedure

	Command or Action	Purpose
Step 1	Specify Your TFTP Server Address, on page 99	Specify your TFTP server address for 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. The first step in configuring the client is to 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 Your TFTP Server on Cisco Unified Presence

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

Procedure

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

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

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

The **Cisco Jabber Settings** window opens.

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

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

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

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

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

Step 5 Select **Save**.

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

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

Procedure

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

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

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

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

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

Step 5 Select **Save**.

Specify TFTP Servers in Phone Mode

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

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

Specify TFTP Servers with the Cisco WebEx Administration Tool

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

Procedure

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

Create Global Configurations

The client downloads the global configuration file from your TFTP server during the login 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 Windows (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 file names in the **Cisco Support Field** field on the device configuration. If users do not have CSF devices, set a unique configuration file name for each group during installation with the `TFTP_FILE_NAME` argument.

Before You Begin

- If you have Cisco Unified Communications Manager, 8.6, the **Cisco Support Field** field does not exist.. Download the `cisco.cm.addcsfsupportfield.cop` COP file from the Cisco Jabber administration package to your file system and deploy to Cisco Unified Communications Manager. For more information about deploying COP files, see the Cisco Unified Communications Manager documentation.

The COP file adds the **Cisco Support Field** field to CSF devices in the **Desktop Client Settings** section on the **Phone Configuration** window.

- 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, Cisco recommends hosting configuration files on the Cisco Unified Communications Manager TFTP server, which is the same as that 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 Structure

You create client configuration files in an XML format that contains the following elements

XML Declaration

The configuration file must conform to XML standards and contain the following declaration:

```
<?xml version="1.0" encoding="utf-8"?>
```

Root Element

The root element `config`, contains all group elements. You must also add the version attribute to the root element as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
</config>
```

Group Elements

Group elements contain configuration parameters and values. You must nest group elements within the root element.

XML Structure

The following snippet shows the XML structure of a client configuration file:

```
<Client>
  <parameter>value</parameter>
</Client>
<Directory>
  <parameter>value</parameter>
</Directory>
<Options>
  <parameter>value</parameter>
```



```

</Options>
<Phone>
  <parameter>value</parameter>
</Phone>
<Policies>
  <parameter>value</parameter>
</Policies>
<Presence>
  <parameter>value</parameter>
</Presence>
<Voicemail>
  <parameter>value</parameter>
</Voicemail>

```

Group Elements and Parameters

The following table describes the group elements you can specify in a client configuration file:

Element	Description
Client	Contains configuration parameters for the client.
Directory	Contains configuration parameters for directory integration.
Options	Contains configuration parameters for user options.
Phone	Contains configuration parameters for phone services.
Policies	Contains configuration parameters for policies.
Presence	Contains configuration parameters for presence options.
Voicemail	Contains configuration parameters for the voicemail service.

Client Parameters

The following table describes the parameters you can specify within the Client element:

Parameter	Value	Description
PrtLogServerURL	URL	Specifies the custom script for submitting problem reports.
UpdateURL	URL	Specifies the URL to the automatic updates XML definition file on your HTTP server. The client uses this URL to retrieve the update XML file.
jabber-plugin-config	Plug-in definition	Contains plug-in definitions such as custom embedded tabs that display HTML content.

Parameter	Value	Description
Forgot_Password_URL	URL	Specifies the URL of your web page for users to reset or retrieve forgotten passwords. In hybrid cloud-based deployments, use the Cisco WebEx Administration Tool to direct users to the web page to reset or retrieve forgotten passwords.
Persistent_Chat_Enabled	true false	Specifies whether the Persistent Chat feature is available in the client. <ul style="list-style-type: none"> • true — The Persistent Chat interface is shown in the client. • false (default) — The default value is assumed if the setting is not present in the configuration file.
MaxNumberOfBookmarks	30	Specifies the maximum number of bookmarks allowed in persistent chat rooms. <ul style="list-style-type: none"> • 30 (default) - sets a maximum of 30 bookmarks.
Mention_P2Pchat	true false	Specifies whether mentions are enabled in person to person chat. <ul style="list-style-type: none"> • true (default) — Enables mentions in person to person chat. • false — Disables mentions in person to person chat.
Mention_GroupChat	true false	Specifies whether mentions are enabled in group chat. <ul style="list-style-type: none"> • true (default) — Enables mentions in group chat. • false — Disables mentions in group chat.
Mention_PersistentChat	true false	Specifies whether mentions are enabled in persistent chat. <ul style="list-style-type: none"> • true (default) — Enables mentions in persistent chat. • false — Disables mentions in persistent chat.

Parameter	Value	Description
spell_check_enabled	true false	Specifies whether spell check is enabled in the client. Spell check supports autocorrect, allows users to select the correct word from a list of suggestions, and add the word to a dictionary. <ul style="list-style-type: none"> • true — Spell check is enabled. • false (default) — Spell check is disabled.
spell_check_language	Language code	Specifies the default spell check language for users. By default, the client uses the Jabber language as the default spell check language. You can define the default language dictionary that you want to set the client to use. From the conversation windows, users may select different default languages for each user they IM with. <pre><spell_check_language>1031</spell_check_language></pre> defines German as the default spell check language.
Disable_IM_History	true false	Specifies whether to retain chat history after participants close the chat window. <p>Note This parameter is not available for IM-only deployments.</p> <ul style="list-style-type: none"> • true — Do not retain chat history after participants close the chat window. • false (default) — Retain chat history: <ul style="list-style-type: none"> ◦ After participants close the chat window. ◦ Until the participants sign out. <p>If the participants re-open the chat window, the last 99 messages show.</p> <p>Message archiving should be disabled on the server.</p>
EnableAutosave	true false	Specifies whether users can save instant messages automatically each time they close a conversation. Enables the option in the client under File > Options > Chats > Autosave each chat when closing the conversation . <ul style="list-style-type: none"> • true — The check box is available. • false (default) — The check box is unavailable.
AutosaveChatsLocation	C:\Users\ username\ My Documents\ 	Defines the path where instant messages are saved automatically each time a user closes a conversation. Use the absolute path on the local file system.

Parameter	Value	Description
Location_Enabled	true false	Specifies whether the Location feature is available in the client. <ul style="list-style-type: none"> • true (default)—The Location feature is shown in the client. • false—The Location feature is not shown in the client.
LOCATION_MATCHING_MODE	MacAddress Only MacAddress WithSubnet	Determines how the client detects the current network locations for the Location feature. <ul style="list-style-type: none"> • MacAddressOnly (default) - The client uses the Mac address of the network default gateway. • MacAddressWithSubnet - The client uses a unique pair of subnet addresses and Mac address of the default gateway.

Options Parameters

The following table describes the parameters you can specify within the Options element:

Parameter	Value	Description
Set_Status_Away_On_Inactive	true false	Specifies if the availability status changes to Away when users are inactive. <ul style="list-style-type: none"> • true (default) — Availability status changes to Away when users are inactive. • false — Availability status does not change to Away when users are inactive.
Set_Status_Inactive_Timeout	Number of minutes	Sets the amount of time, in minutes, before the availability status changes to Away if users are inactive. The default value is 15.
Set_Status_Away_On_Lock_OS	true false	Specifies if the availability status changes to Away when users lock their operating systems. <ul style="list-style-type: none"> • true (default) — Availability status changes to Away when users lock their operating systems. • false — Availability status does not change to Away when users lock their operating systems.

Parameter	Value	Description
StartCallWithVideo	true false	<p>Specifies how calls start when users place calls. Calls can start with audio only or audio and video.</p> <ul style="list-style-type: none"> • true (default) — Calls always start with audio and video. • false — Calls always start with audio only. <p>Important Server settings take priority over this parameter in the client configuration file. However, if users change the default option in the client user interface, that setting takes priority over both the server and client configurations.</p> <p>Configure this setting on the Cisco Unified Presence node:</p> <ol style="list-style-type: none"> 1 Open the Cisco Unified Presence Administration interface. 2 Select Application > Cisco Jabber > Settings. 3 Select or clear the Always begin calls with video muted parameter and then select Save. <p>For Cisco Unified Communications Manager version 9.x and later</p> <ol style="list-style-type: none"> 1 Open the Cisco Unified CM Administration interface. 2 Select System > Enterprise Parameters. 3 Set a value for the Never Start Call with Video parameter and then select Save.
Start_Client_On_Start_OS	true false	<p>Specifies if the client starts automatically when the operating system starts.</p> <ul style="list-style-type: none"> • true — The client starts automatically. • false (default) — The client does not start automatically.
AllowUserCustomTabs	true false	<p>Specifies if users can create their own custom embedded tabs.</p> <ul style="list-style-type: none"> • true (default) — Users can create custom embedded tabs. • false — Users cannot create custom embedded tabs.

Parameter	Value	Description
ShowContactPictures	true false	Specifies if contact pictures display in the contact list. <ul style="list-style-type: none"> • true (default) — Contact pictures display in the contact list. • false — Contact pictures do not display in the contact list.
ShowOfflineContacts	true false	Specifies if offline contacts display in the contact list. <ul style="list-style-type: none"> • true (default) — Offline contacts display in the contact list. • false — Offline contacts do not display in the contact list.
Location_Mode	ENABLED DISABLED ENABLED NOPROMPT	Specifies whether the Location feature is turned on and whether users are notified when new locations are detected. <ul style="list-style-type: none"> • 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.
DockedWindowVisible	true false	Specifies if the docked window displays when the client starts. <ul style="list-style-type: none"> • true (default) — The docked window displays when the client starts. • false — The docked window does not display when the client starts.
DockedWindowPosition	TopCenter TopLeft TopRight	Sets the position of the docked window on the user's screen. <ul style="list-style-type: none"> • TopCenter (default) — The position of the docked window is at the top center of the screen. • TopLeft — The position of the docked window is at the top left of the screen. • TopRight — The position of the docked window is at the top right of the screen.

Parameter	Value	Description
Callhistory_Expire_Days	Number of days	Sets the number of days before the call history is deleted. If the value is 0 or not specified in the configuration file the call history is not deleted until the count exceeds the maximum number of stored calls.

Phone Parameters

The following table describes the parameters you can specify within the Phone element:

Parameter	Value	Description
CcmcipServer1	Hostname IP address FQDN	Specifies the address of the primary CCMCIP server. This parameter is required: <ul style="list-style-type: none"> Only if the address of your CCMCIP server is not the same as the TFTP server address. If the address of the CCMCIP server is the same as the TFTP server address, the client can use the TFTP server address to connect to the CCMCIP server. In deployments with Cisco Unified Communications Manager version 8. In deployments with Cisco Unified Communications Manager version 9 and later, the client can discover the CCMCIP server if you provision the <code>_cisco-uds</code> SRV record.
CcmcipServer2	Hostname IP address FQDN	Specifies the address of the secondary CCMCIP server. This parameter is optional.
CtiServer1	Hostname IP address FQDN	Specifies the address of the primary CTI server. You should specify a CTI server address in the client configuration if users have desk phone devices.
CtiServer2	Hostname IP address FQDN	Specifies the address of the secondary CTI server. This parameter is optional.

Parameter	Value	Description
EnableCallPark	true false	Specifies whether the call park feature is available in the client. To access the call park feature, choose the More option in the call window. <ul style="list-style-type: none"> • true (default) — Call park is enabled. • false — Call park is disabled. There is no call park option under the More button.
EnableDSCPPacketMarking	true false	Applicable to Jabber for Mac only. Specifies if DSCP marking is applied to the packets: <ul style="list-style-type: none"> • true (default) — DSCP marking is enabled and the checkbox in the client is not shown. • false — DSCP marking is not made to packets and the checkbox in the client is not shown.
Meeting_Server_Address	Cisco WebEx meetings site URL	Specifies the primary Cisco WebEx meeting site URL for users. The Jabber for Windows client populates the meeting site in the user's host account on the Options window. The Jabber for Mac client populates the meeting site in the user's host account on the Preferences > Meetings window. Users can enter their credentials to set up the host account and access their Cisco WebEx meetings, if the meeting site requires credentials. Important If you specify an invalid meeting site, users cannot add, or edit, any meetings sites in the client user interface. This parameter is optional.
Meeting_Server_Address_Backup	Cisco WebEx meetings site URL	Specifies the secondary Cisco WebEx meeting site URL for users. This parameter is optional.
Meeting_Server_Address_Backup2	Cisco WebEx meetings site URL	Specifies the tertiary Cisco WebEx meeting site URL for users. This parameter is optional.

Parameter	Value	Description
TftpServer1	Hostname IP address FQDN	<p>Specifies the address of the primary Cisco Unified Communications Manager TFTP service where device configuration files reside. Set one of the following as the value:</p> <ul style="list-style-type: none"> • Hostname (<i>hostname</i>) • IP address (<i>123.45.254.1</i>) • FQDN (<i>hostname.domain.com</i>) <p>You should set this parameter in the client configuration only if:</p> <ul style="list-style-type: none"> • You deploy the client in phone mode. • The TFTP server address for the device configuration is different to the TFTP server address for the client configuration. <p>During installation, you should set the address of the TFTP server where the client configuration file resides with the following argument: TFTP.</p>
TftpServer2	Hostname IP address FQDN	<p>Specifies the address of the secondary Cisco Unified Communications Manager TFTP service.</p> <p>This parameter is optional.</p>
useCUCMGroupForCti	true false	<p>Specifies if the Cisco Unified CM Group handles load balancing for CTI servers. Set one of the following values:</p> <ul style="list-style-type: none"> • true — The Cisco Unified CM Group handles CTI load balancing. You should set this value in phone mode deployments only. In full UC mode, the presence server automatically handles CTI load balancing. • false (default) — The Cisco Unified CM Group does not handle CTI load balancing.

Policies Parameters

Policies parameters let you control specific client functionality.

On-Premises Policies

The following table describes the parameters you can specify within the Policies element in on-premises deployments:

Parameter	Value	Description
Screen_Capture_Enabled	true false	Specifies if users can take screen captures. <ul style="list-style-type: none"> • true (default) — Users can take screen captures. • false — Users cannot take screen captures.
File_Transfer_Enabled	true false	Specifies if users can transfer files to each other. <ul style="list-style-type: none"> • true (default) — Users can transfer files to each other. • false — Users cannot transfer files to each other.
Disallowed_File_Transfer_Types	File extension	Restricts users from transferring specific file types. Set file extensions as the value, for example, <code>.exe</code> . Use a semicolon to delimit multiple file extensions, for example, <code>.exe;.msi;.rar;.zip</code> .
PreferredFT	MFT P2P	When Cisco Unified Communications Manager IM & Presence server provides both Managed File Transfer and Peer-to-Peer File Transfer , this parameter specifies the preferred method of transferring files in the client. <ul style="list-style-type: none"> • MFT — Files are transferred using the managed file transfer option. • P2P — Files are transferred using peer to peer file transfer. <p>If the parameter is not defined, the client checks Cisco Unified Communications Manager IM & Presence Server and when managed file transfer is available the client uses this option, otherwise it uses peer to peer file transfer.</p>
DisableMFTForConversationTypes	P2P GroupChat PersistentChat	When the Managed File Transfer option is available, this parameter specifies the conversation types that disable the setting. Use a semicolon to delimit multiple conversation types, for example <code>P2P;GroupChat;PersistentChat</code> .

Parameter	Value	Description
Customize_Phone_Server	true false	<p>Allows users to change their phone server settings in the client in on-premises deployments. Do not set this parameter to true if you are deploying SAML SSO, as changing phone server settings could interfere with SSO working properly.</p> <ul style="list-style-type: none"> • true — Users can change their phone server settings. • false (default) — Users cannot change their phone server settings.
Customize_Voicemail_Server	true false	<p>Allows users to change their voicemail server settings in the client in on-premises deployments. Do not set this parameter to true if you are deploying SAML SSO, as changing voicemail server settings could interfere with SSO working properly.</p> <ul style="list-style-type: none"> • true — Users can change their voicemail server settings. • false (default) — Users cannot change their voicemail server settings.

Common Policies

The following table describes the parameters you can specify within the Policies element in both on-premises deployments and hybrid cloud-based deployments:

Parameter	Value	Description
Disallow_File_Transfer_On_Mobile	true false	<p>Specifies whether the user can send or receive files on mobile.</p> <ul style="list-style-type: none"> • true — Users cannot send or receive files on mobile. • false (default) — Users can send or receive files on mobile.
EnableVideo	true false	<p>Enables or disables video capabilities.</p> <ul style="list-style-type: none"> • true (default) — Users can make and receive video calls. • false — Users cannot make or receive video calls.

Parameter	Value	Description
InitialPhoneSelection	deskphone softphone	<p>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.</p> <ul style="list-style-type: none"> • deskphone — Use the desk phone device for calls. • softphone (default) — Use the software phone (CSF) device for calls. <p>The client selects devices in the following order:</p> <ol style="list-style-type: none"> 1 Software phone devices 2 Desk phone devices <p>If you do not provision users with software phone devices, the client automatically selects desk phone devices.</p>
UserDefinedRemoteDestinations	true false	<p>Lets users add, edit, and delete remote destinations through the client interface. Use this parameter to change the default behavior when you provision Extend and Connect capabilities.</p> <p>By default, if a user's device list contains only a CTI remote device, the client does not let that user add, edit, or delete remote destinations. This occurs to prevent users from modifying dedicated remote devices that you assign. However, if the user's device list contains a software device or a desk phone device, the client lets users add, edit, and delete remote destinations.</p> <ul style="list-style-type: none"> • true — Users can add, edit, and delete remote destinations. • false (default) — Users cannot add, edit, and delete remote destinations.
enableLocalAddressBookSearch	true false	<p>Lets users search for and add local Microsoft Outlook contacts to their contact lists.</p> <ul style="list-style-type: none"> • true (default) — Users can search for and add local contacts to their contact lists. • false — Users cannot search for or add local contacts to their contact lists.

Parameter	Value	Description
EnableAccessoriesManager	true false	Enables the accessories API in the client. This API lets accessory vendors create plugins to enable call management functionality for devices such as headsets. <ul style="list-style-type: none"> • true (default) — Enable the accessories API. • false — Disable the accessories API.
BlockAccessoriesManagerPlugins	Plugin library	Disables specific Accessories Manager plugins from third party vendors such as Jabra or Logitech. You should set the name of the plugin DLL file as the value. Use a comma to separate multiple values, for example, on Microsoft Windows: <pre><BlockAccessoriesManagerPlugins> JabraJabberPlugin.dll,lucpcisco.dll </BlockAccessoriesManagerPlugins></pre>
ForceFontSmoothing	true false	Specifies if the client applies anti-aliasing to smooth text. <ul style="list-style-type: none"> • true (default) — The client applies anti-aliasing to text. • false — The operating system applies anti-aliasing to text.
EnableBFCPVideoDesktopShare	true false	Enables BFCP video desktop sharing capabilities. <ul style="list-style-type: none"> • true (default) — Enables BFCP video desktop sharing on the client. • false — Disables BFCP video desktop sharing.
Meetings_Enabled	true false	Enables meetings capabilities in the client. Works in conjunction with the CalendarIntegrationType parameter. <ul style="list-style-type: none"> • true (default) — Enables meetings capabilities, allowing you to create meetings and get reminders to join meetings. • false — Disables meetings capabilities.
CalendarIntegrationType	0 1	This parameter works in conjunction with the Meetings_Enabled parameter. <ul style="list-style-type: none"> • 0 — Disables calendar integration in the Meetings tab of the client user interface. If you disable this parameter, the Meetings tab in the client is empty, but the Meetings tab remains on the hub window. • 1 — Enables calendar integration in the Meetings tab of the client user interface.

Parameter	Value	Description
Telephony_Enabled	true false	<p>Enables audio and video capabilities and user interface in the client.</p> <ul style="list-style-type: none"> • true (default) — Enables audio and video capabilities and user interface. • false — Disables audio and video capabilities and user interface. <p>If your client is enabled for IM-only mode, then you must set this parameter to false. If you do not set this parameter in IM-only mode deployments, then users may see disabled telephony capabilities on their user interface.</p>
Voicemail_Enabled	true false	<p>Enables voicemail capabilities and user interface in the client.</p> <ul style="list-style-type: none"> • true (default) — Enables voicemail capabilities and user interface. • false — Disables voicemail capabilities and user interface.
EnableTelProtocolHandler	true false	<p>Specifies if the client registers as the protocol handler for the <code>tel:</code> URI.</p> <ul style="list-style-type: none"> • true (default) — The client registers as the protocol handler for the <code>tel:</code> URI. • false — The client does not register as the protocol handler for the <code>tel:</code> URI.
EnableIMProtocolHandler	true false	<p>Specifies if the client registers as the protocol handler for the <code>im:</code> URI.</p> <ul style="list-style-type: none"> • true (default) — The client registers as the protocol handler for the <code>im:</code> URI. • false — The client does not register as the protocol handler for the <code>im:</code> URI.
EnableSIPProtocolHandler	true false	<p>Specifies if the client registers as the protocol handler for the <code>sip:</code> URI.</p> <ul style="list-style-type: none"> • true (default) — The client registers as the protocol handler for the <code>sip:</code> URI. • false — The client does not register as the protocol handler for the <code>sip:</code> URI.

Parameter	Value	Description
EnableSaveChatToFile	true false	<p>Allows users to save their chats to the file system as HTML.</p> <ul style="list-style-type: none"> • true (default) — Users can save their chats to file. • false — Users cannot save their chats to file.
InstantMessageLabels	Security label	<p>Defines a catalog of security labels, such as SECRET and CONFIDENTIAL, that users must apply before they send an instant message. The label appears before each message that is sent. For example, SECRET: <i>message text</i>.</p> <p>You can specify a maximum of 20 labels.</p> <p>Jabber does not control message distribution based on these labels. Any such control requires the use of a third-party product, such as a Compliance server, which supports XEP-256 label headers.</p> <p>XEP-0258 is used to implement security labels. For more information, refer to <i>XEP-0258: Security Labels in XMPP</i>.</p> <p>Sample <code>jabber-config-user.xml</code> for security labels:</p> <pre><InstantMessageLabels> <item selector="Classified SECRET"> <securitylabel xmlns='urn:xmpp: sec-label:0'> <displaymarking fgcolor='black' bgcolor='red'>SECRET </displaymarking> </securitylabel> </item> <item...> ... </item> </InstantMessageLabels></pre>
EnableSIPURIDialling	true false	<p>Enables URI dialing with Cisco Jabber and allows users to make calls with URIs.</p> <ul style="list-style-type: none"> • true — Users can make calls with URIs. • false (default) — Users cannot make calls with URIs.

Parameter	Value	Description
DirectoryURI BDIDirectoryURI	Directory attribute	<p>Specifies the directory attribute that holds the SIP URI for users.</p> <ul style="list-style-type: none"> • On-Premises Deployments — Set one of the following as the value: <ul style="list-style-type: none"> • mail • msRTCSIP-PrimaryUserAddress • Cloud-Based Deployments — Set one of the following as the value: <ul style="list-style-type: none"> • mail • imaddress • workphone • homephone • mobilephone <p>The mail attribute is used by default.</p> <p>Important The value you specify must match the directory URI setting for users in Cisco Unified Communications Manager or the Cisco WebEx Administration Tool.</p>
ForceC2XDirectoryResolution	true false	<p>Specifies if the client queries the directory to resolve contact information when users perform click-to-x actions.</p> <ul style="list-style-type: none"> • true (default) — The client queries the directory when users perform click-to-x actions. • false — The client does not query the directory for click-to-x actions. <p>Note This parameter does not take effect when users connect to the corporate network through Expressway for Mobile and remote Access. In this case, UDS provides contact resolution and the client cannot query the directory.</p>
AlertOnAvailableEnabled	true false	<p>Enables users to add contacts to their availability watch list.</p> <ul style="list-style-type: none"> • true (default) — Users can add contacts to their availability watch list. • false — Users cannot add contacts to their availability watch list.

Parameter	Value	Description
ServiceDiscoveryExcludedServices	WEBEX CUCM CUP	<p>Specifies whether to exclude certain services from Service Discovery.</p> <ul style="list-style-type: none"> • WEBEX — When you set this value, the client: <ul style="list-style-type: none"> ◦ Does not perform CAS lookup ◦ Looks for <code>_cisco-uds</code>, <code>_cuplogin</code>, and <code>_collab-edge</code>. • CUCM — When you set this value, the client: <ul style="list-style-type: none"> ◦ Does not look for <code>_cisco_uds</code> ◦ Looks for <code>_cuplogin</code> and <code>_collab-edge</code>. • CUP — When you set this value, the client: <ul style="list-style-type: none"> ◦ Does not look for <code>_cuplogin</code> ◦ Looks for <code>_cisco-uds_collab-edge</code> <p>You can specify multiple, comma-separated values to exclude multiple services. For example:</p> <pre><ServiceDiscoveryExcludedServices> WEBEX, CUCM </ServiceDiscoveryExcludedServices></pre>
VoiceServicesDomain	FQDN	<p>Specifies the Fully Qualified Domain Name that represents the DNS domain where the DNS SRV records for <code>_collab-edge</code> and <code>_cisco-uds</code> are configured.</p> <p>Example — Given the following DNS SRV records:</p> <ul style="list-style-type: none"> • <code>_collab-edge._tls.voice.example.com</code> • <code>_cisco-uds._tcp.voice.example.com</code> <p>The <code>VoiceServicesDomain</code> value would be <code>voice.example.com</code>.</p>
ctiwindowbehaviour	OnVideo OnCall Never	<p>Specifies the behavior of the notification window that is displayed for incoming calls when the user is in deskphone control mode (CTI mode).</p> <ul style="list-style-type: none"> • OnVideo — Notification window is only displayed for incoming video calls. This option is not supported on Cisco Jabber for Mac. • OnCall (default) — Notification window is always displayed for incoming calls. • Never — Notification window is never displayed for incoming calls.

Parameter	Value	Description
EnableCallPickup	true false	Specifies if a user can pickup a call in their call pickup group. <ul style="list-style-type: none"> • true — Enables call pickup. • false (default) — Disables call pickup.
EnableGroupCallPickup	true false	Specifies if a user can pickup incoming calls in another call pickup group, by entering the call pickup group number. <ul style="list-style-type: none"> • true — Enables group call pickup. • false (default) — Disables group call pickup.
EnableOtherGroupPickup	true false	Specifies if a user can pickup an incoming call in a group that is associated with their own call pickup group. <ul style="list-style-type: none"> • true — Enables other group call pickup. • false (default) — Disables other group call pickup.
EnableHuntGroup	true false	Specifies if a user can log into a hunt group. <ul style="list-style-type: none"> • true — Users can log into their hunt group. • false (default) — Users cannot log into their hunt group.
PreventDeclineOnHuntCall	true false	Specifies if the Decline button is displayed for an incoming call in a hunt group. <ul style="list-style-type: none"> • true — Decline button is not displayed for an incoming call in a hunt group. • false (default) — Decline button is displayed for an incoming call in a hunt group.
TelemetryEnabled	true false	Specifies whether analytics data will be gathered. <ul style="list-style-type: none"> • true (default) — Analytics data will be gathered. • false — Analytics data will not be gathered.

Parameter	Value	Description
TelemetryCustomerID	String	<p>Specifies the source of analytic information. This can be a string that explicitly identifies an individual customer or a string that identifies a common source without identifying the customer. Cisco recommends using a Global Unique Identifier (GUID) generating utility to generate a 36 character unique identifier or to use a reverse domain name. The following utilities are available for generating a GUID:</p> <ul style="list-style-type: none"> • Mac OS X - uuidgen • Linux - uuidgen • Microsoft Windows - [guid]::NewGuid().ToString() or (from cmd.exe) powershell -command "[guid]::NewGuid().ToString()" • Online - guid.us <p>This identifier should be globally unique regardless of the method used to create the GUID.</p>
TelemetryEnabledOverCellularData	true false	<p>Specifies whether analytics data will be sent over Wi-Fi only.</p> <ul style="list-style-type: none"> • true (default) — Analytics data will be sent over Wi-Fi and mobile data connections. • false — Analytics data will be sent over Wi-Fi connections only. <p>This parameter is optional.</p>
EnableMediaStatistics	ON OFF	<p>Allows viewing of real-time audio and video statistics when on a call.</p> <ul style="list-style-type: none"> • ON (default) — EnableMediaStatistics=ON • OFF — EnableMediaStatistics=OFF <p>This parameter is optional.</p>

Parameter	Value	Description
EnableTelProtocolPopupWindow CiscoTelProtocolPermissionEnabled	true false	<p>Specifies whether the dialog box is enabled or disabled which asks users to confirm if they want to make a call after they click on a ciscotel:uri enabled number.</p> <ul style="list-style-type: none"> • true (default) — Dialog box is enabled and users are asked to confirm that they want to place the call. • false — Dialog box is disabled and the call is made without requesting confirmation first. This may cause accidental or unwanted calls. <p>Note The CiscoTelProtocolPermissionEnabled parameter replaces the EnableTelProtocolPopupWindow parameter. Both parameters are supported in the client, however the dialog box is disabled if either parameter is set to false.</p>
CiscoTelProtocolCrossLaunchBackNotificationEnabled	true false	<p>Added to jabber-config.xml — Specifies that a dialog box is enabled that provides a choice for you to go back to another application when a call ends, or to stay in Jabber.</p> <ul style="list-style-type: none"> • true (default) — Dialog box is enabled. • false — Dialog box is disabled, and: <ul style="list-style-type: none"> • If CiscoTelProtocolCrossLaunchBackSchema contains the parameter CrossLaunchBackSchema, you cross launch back directly to the previous application. • If CiscoTelProtocolCrossLaunchBackSchema does not contain the parameter CrossLaunchBackSchema, you stay in Jabber.
CiscoTelProtocolCrossLaunchBackSchema	none <i>schema_names</i>	<p>Added to jabber-config.xml — Specifies a white list of applications that can be cross launched back to when a call is ended.</p> <ul style="list-style-type: none"> • none (default) — No list. • <i>schema_names</i> — Contains the schema white list.
CrossLaunchBackAppName	none <i>app_name</i>	<p>In the URI — Specifies the name of an application, displayed in a dialog box, that Jabber cross launches back to when a call is ended.</p> <ul style="list-style-type: none"> • none (default) — No application in the dialog box. • <i>app_name</i> — The application name that is displayed in the dialog box.

Parameter	Value	Description
CrossLaunchBackSchema	none <i>app_name</i>	In the URI — Specifies the name of the application that Jabber cross launches back to when a call is ended. <ul style="list-style-type: none"> • none (default) — You stay in Jabber. • <i>app_name</i> — The application you cross launch back to.
SSO_Enabled	TRUE FALSE	Specifies whether users sign in by using single sign-on (SSO). <ul style="list-style-type: none"> • TRUE (default) — Users sign in by using SSO. • FALSE — Users do not use SSO to sign in.
ServicesDomainSsoEmailPrompt	ON OFF	Specifies whether the user is shown the email prompt for the purposes of determining their home cluster. <ul style="list-style-type: none"> • ON — The prompt is shown. • OFF (default) — The prompt is not shown.
EnableP2PDesktopShare	true false	Allows users to share their screen if not on a call. <ul style="list-style-type: none"> • true (default) — Allows users to share their screens. • false — Users cannot do peer to peer screen sharing.
EnableForensicsContactData	true false	Specifies whether users' Contacts folder is collected by the Problem Reporting Tool (PRT) when reporting a problem that is related to their contacts. <ul style="list-style-type: none"> • true (default) — Contacts folder is collected by the PRT tool. • false — Contacts folder is not collected by the PRT tool.
SharePortRangeStart	<i>Start of port range</i>	Defines a specific port range for the Cisco Jabber for Windows client to use when users share their screen from a chat window when used with the SharePortRangeSize parameter. If you do not configure these parameters, the client uses the default port range for IM screen share. The value you enter specifies the start of the port range. For example: <pre><Policies> <SharePortRangeStart>45130</SharePortRangeStart> <SharePortRangeSize>100</SharePortRangeSize> </Policies></pre>

Parameter	Value	Description
SharePortRangeSize	<i>Size of port range</i>	Specifies the size of the port range, when used with the SharePortRangeStart parameter. For more information on port ranges, see the topic on <i>Ports and Protocols for Cisco Jabber for Windows and Cisco Jabber for Mac</i> in the <i>Cisco Jabber 10.5 Deployment and Installation Guide</i> or the <i>Cisco Jabber 10.6 Planning Guide</i> .

Cisco WebEx Policies

If you use the Cisco WebEx Messenger service for instant messaging and presence capabilities, you can set policies for the client through the Cisco WebEx Administration Tool. See *Using policy actions available in Cisco WebEx* for a list of available policies and descriptions.



Note

All settings in the service profile obtained via UDS will overwrite the configuration in Cisco WebEx Administration Tool.

Related Topics

[Using policy actions available in Cisco WebEx](#)

Presence Parameters

The following table describes the parameters you can specify within the Presence element:

Parameter	Value	Description
LoginResource	multiResource wbxconnect	Controls user sign in to multiple client instances. <ul style="list-style-type: none"> • multiResource (default) — Users can sign in to multiple instances of the client at the same time. • wbxconnect — Users can sign in to one instance of the client at a time. <p>The client appends the <code>wbxconnect</code> suffix to the user's JID. Users cannot sign in to any other Cisco Jabber client that uses the <code>wbxconnect</code> suffix.</p>
PresenceServerAddress	Hostname IP address FQDN	Specifies the address of a presence server for on-premises deployments. Set one of the following as the value: <ul style="list-style-type: none"> • Hostname (<i>hostname</i>) • IP address (<i>123.45.254.1</i>) • FQDN (<i>hostname.domain.com</i>)

Parameter	Value	Description
PresenceServerURL	CAS URL	Specifies the Central Authentication Service (CAS) URL for the Cisco WebEx Messenger service. The following is an example of a URL you can set as the value: <code>https://loginp.webexconnect.com/cas/sso/ex_org/orgadmin.app</code>
CalendarWebExMeetingPresence	true false	Enables users' presence to change to "In a WebEx meeting" even if they do not join the WebEx session link but the meeting is in their Microsoft Outlook calendar. <ul style="list-style-type: none"> • true - Users' presence changes to "In a WebEx meeting" even if they do not join the WebEx session link. • false (default) - Users must join the WebEx session link for their presence to change to "In a WebEx meeting". Otherwise, their presence remains "Available", even if the meeting is in their Microsoft Outlook calendar.

Voicemail Parameters

The following table describes the voicemail service configuration parameters you can specify within the Voicemail element:

Key	Value	Description
VoicemailPrimaryServer	Hostname IP address FQDN	Specifies the address of your voicemail server. Set one of the following as the value: <ul style="list-style-type: none"> • Hostname (<i>hostname</i>) • IP address (<i>123.45.254.1</i>) • FQDN (<i>hostname.domain.com</i>)

Service Credentials Parameters

You can specify service credentials parameters so that users do not need to authenticate with certain services.

Voicemail Service Credentials

You can specify the following parameter to configure voicemail service credentials within the Voicemail element:

Parameter	Value	Description
VoiceMailService_UseCredentialsFrom	phone	<p>Specifies that the client uses the phone service credentials to access voicemail services.</p> <p>Ensure the user's phone service credentials match their voicemail service credentials. If you set this configuration, users cannot specify voicemail service credentials in the client interface.</p> <p>This parameter is not set by default.</p> <p>You should set this parameter in the following deployments only:</p> <ul style="list-style-type: none"> • Hybrid cloud-based deployments. • Phone mode deployments. <p>In on-premises deployments, you should set the credentials source for voicemail services on the presence server.</p>

The following is an example of the voicemail service credentials parameter:

```
<?xml version="1.0" encoding="utf-8"?> <config version="1.0"> <Voicemail>
<VoiceMailService_UseCredentialsFrom>phone</VoiceMailService_UseCredentialsFrom> </Voicemail>
</config>
```

Example Configuration

The following is an example of a configuration file used in an on-premises deployment for all clients:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Client>
    <PrtLogServerUrl>http://server_name:port/path/prt_script.php</PrtLogServerUrl>
    <jabber-plugin-config>
      <browser-plugin>
        <page refresh="true" preload="true">
          <tooltip>Cisco</tooltip>
          <icon>http://www.cisco.com/web/fw/i/logo.gif</icon>
          <url>www.cisco.com</url>
        </page>
      </browser-plugin>
    </jabber-plugin-config>
  </Client>
  <Options>
    <Set_Status_Inactive_Timeout>20</Set_Status_Inactive_Timeout>
    <StartCallWithVideo>>false</StartCallWithVideo>
  </Options>
  <Policies>
    <Disallowed_File_Transfer_Types>.exe;.msi</Disallowed_File_Transfer_Types>
  </Policies>
  <Directory>
    <BDIPresenceDomain>example.com</BDIPresenceDomain>
    <BDIPrimaryServerName>dir.example.com</BDIPrimaryServerName>
    <BDISearchBase1>ou=staff,dc=example,dc=com</BDISearchBase1>
    <BDIConnectionUsername>ad_jabber_access@example.com</BDIConnectionUsername>
    <BDIConnectionPassword>jabber</BDIConnectionPassword>
    <BDIPhotoUriSubstitutionEnabled>True</BDIPhotoUriSubstitutionEnabled>
    <BDIPhotoUriSubstitutionToken>sAMAccountName</BDIPhotoUriSubstitutionToken>
    <BDIPhotoUriWithToken>http://example.com/photo/sAMAccountName.jpg
```



```

        </BDIPhotoUriWithToken>
    </Directory>
</config>

```

Configure Problem Reporting

Setting up problem reporting enables users to send a summary of issues that they encounter with the client. There are two methods for submitting problem reports as follows:

- Users submit the problem report directly through the client interface.
- Users save the problem report locally and then upload it at a later time.

The client uses an HTTP POST method to submit problem reports. Create a custom script to accept the POST request and specify the URL of the script on your HTTP server as a configuration parameter. Because users can save problem reports locally, you should also create an HTML page with a form to enable users to upload problem reports.

Before You Begin

Complete the following steps to prepare your environment:

- 1 Install and configure an HTTP server.
- 2 Create a custom script to accept the HTTP POST request.
- 3 Create an HTML page that enables users to upload problem reports that are saved locally. Your HTML page should contain a form that accepts the problem report saved as a .ZIP archive and contains an action to post the problem report using your custom script.

The following is an example form that accepts problem reports:

```

<form name="uploadPrt" action="http://server_name.com/scripts/UploadPrt.php" method="post"
  enctype="multipart/form-data">
  <input type="file" name="zipFileName" id="zipFileName" /><br />
  <input type="submit" name="submitBtn" id="submitBtn" value="Upload File" />
</form>

```

Procedure

-
- Step 1** Host your custom script on your HTTP server.
 - Step 2** Specify the URL of your script as the value of the PrtLogServerUrl parameter in your configuration file.
-

Configure Automatic Updates

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.

**Note**

If you use the Cisco WebEx Messenger service for instant messaging and presence capabilities, you should use the Cisco WebEx Administration Tool to configure automatic updates.

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.
XML files for automatic updates have the following structure:

```
<JabberUpdate>
  <App name="JabberWin">
    <LatestBuildNum>12345</LatestBuildNum>
    <LatestVersion>10.5.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>
```

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 (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.

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

```
Cisco-Jabber-Mac-version-size-dsaSignature.zip
```

Example:

The following is example XML for automatic updates:

```
<JabberUpdate>
<App name="JabberWin">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.x</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>
```

Example:

The following is an example XML 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/Cisco-Jabber-Mac-9.6.1-12345-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>
```

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.

Custom Embedded Tabs for Cisco Jabber for Windows

Custom embedded tabs display HTML content in the client interface. Learn how to create custom embedded tab definitions for Cisco Jabber.

Custom Embedded Tab Definitions

The following XML snippet shows the structure for custom tab definitions:

```
<jabber-plugin-config>
  <browser-plugin>
    <page refresh="" preload="">
      <tooltip></tooltip>
      <icon></icon>
      <url></url>
    </page>
  </browser-plugin>
</jabber-plugin-config>
```

The following table describes the parameters for custom embedded tab definitions:

Parameter	Value	Description
browser-plugin	All custom tab definitions	Contains all definitions for custom embedded tabs.
page	One custom tab definition	Contains one custom embedded tab definition.
refresh	true false	Controls when the content refreshes. <ul style="list-style-type: none"> • true — Content refreshes each time users select the tab. • false (default) — Content refreshes when users restart the client or sign in. <p>This parameter is optional and is an attribute of the page element.</p>

Parameter	Value	Description
preload	true false	<p>Controls when the content loads.</p> <ul style="list-style-type: none"> • true — Content loads when the client starts. • false (default) — Content loads when users select the tab. <p>This parameter is optional and is an attribute of the page element.</p>
tooltip	String of unicode characters	<p>Defines hover text for the custom embedded tab.</p> <p>This parameter is optional. If you do not specify the hover text, the client will use <i>Custom tab</i>.</p>
icon	URL	<p>Specifies an icon for the tab. You can specify a local or hosted icon as follows:</p> <ul style="list-style-type: none"> • Local icon — Specify the URL as follows: <code>file://file_path/icon_name</code> • Hosted icon — Specify the URL as follows: <code>http://path/icon_name</code> <p>Local icon</p> <p>Specify the URL as follows: <code>file://file_path/icon_name</code></p> <p>Hosted icon</p> <p>Specify the URL as follows: <code>http://path/icon_name</code></p> <p>You can use any icon that Microsoft Internet Explorer can render, including .JPG, .PNG, and .GIF formats.</p> <p>This parameter is optional. If you do not specify an icon, the client loads the favicon from the HTML page. If no favicon is available, the client loads the default icon.</p>

Parameter	Value	Description
url	URL	<p>Specifies the URL where the content for the embedded tab resides.</p> <p>The client uses the Internet Explorer rendering engine to display the content of the embedded tab. For this reason, you can specify any content that Internet Explorer supports.</p> <p>Note Cisco Jabber for Windows supports Internet Explorer version 9 or earlier. The client uses Internet Explorer in version 9 mode if a later version is on the workstation.</p> <p>This parameter is required.</p>

User Custom Tabs

Users can create their own custom embedded tabs through the client user interface.

You must enable users to create custom embedded tabs. Set true as the value for the AllowUserCustomTabs parameter in your configuration file as follows:

```
<Options>
  <AllowUserCustomTabs>true</AllowUserCustomTabs>
</Options>
```



Note

User custom embedded tabs are set to true by default.

Custom Icons

To achieve optimal results, your custom icon should conform to the following guidelines:

- Dimensions: 20 x 20 pixels
- Transparent background
- PNG file format

Chats and Calls from Custom Tabs

You can use protocol handlers to start chats and calls from custom embedded tabs.

Use the `XMPP:` or `IM:` protocol handler to start chats.

Use the `TEL:` protocol handler to start audio and video calls.

Related Topics

[Protocol Handlers](#), on page 291

UserID Tokens

You can specify the `${UserID}` token as part of the value for the url parameter. When users sign in, the client replaces the `${UserID}` token with the username of the logged in user.

**Tip**

You can also specify the `${UserID}` token in query strings; for example, `www.cisco.com/mywebapp.op?url=${UserID}`.

The following is an example of how you can use the `${UserID}` token:

- 1 You specify the following in your custom embedded tab:

```
<url>www.cisco.com/${UserID}/profile</url>
```
- 2 Mary Smith signs in. Her username is msmith.
- 3 The client replaces the `${UserID}` token with Mary's username as follows:

```
<url>www.cisco.com/msmith/profile</url>
```

JavaScript Notifications

You can implement JavaScript notifications in custom embedded tabs. This topic describes the methods the client provides for JavaScript notifications. This topic also gives you an example JavaScript form that you can use to test notifications. It is beyond the scope of this documentation to describe how to implement JavaScript notifications for asynchronous server calls and other custom implementations. You should refer to the appropriate JavaScript documentation for more information.

Notification Methods

Cisco Jabber includes an interface that exposes the following methods for JavaScript notifications:

- `SetNotificationBadge` — You call this method from the client in your JavaScript. This method takes a string value that can have any of the following values:
 - Empty — An empty value removes any existing notification badge.
 - A number from 0 to 999
 - Two digit alphanumeric combinations, for example, A1
- `onPageSelected()` — The client invokes this method when users select the custom embedded tab.
- `onPageDeselected()` — The client invokes this method when users select another tab.
- `onHubResized()` — The client invokes this method when users resize or move the client hub window.
- `onHubActivated()` — The client invokes this method when the client hub windows is activated.
- `onHubDeActivated()` — The client invokes this method when the client hub window is deactivated.

Subscribe to Presence in Custom Tabs

You can use the following JavaScript functions to subscribe to the presence of a contact and receive presence updates from the client:

- `SubscribePresence()` — Specify a string value using the IM address of a user for this method.
- `OnPresenceStateChanged` — This method enables users to receive updates from the client on the presence of a contact. You can specify one of the following values as the string:
 - IM address
 - Basic presence (Available, Away, Offline, Do Not Disturb)
 - Rich presence (In a meeting, On a call, or a custom presence state)



Note

If you subscribe to the presence of a person who is not on your contact list (also called *temporary presence subscription*), the subscription expires after 68 minutes. After the subscription expires, you must re-subscribe to the person's presence in order to continue to receive presence updates.

Get Locale Information in Custom Tabs

You can use the following JavaScript functions to retrieve the current locale information of a contact from the client:

- `GetUserLocale()` — This method enables users to request locale information from the client.
- `OnLocaleInfoAvailable` — This method enables users to receive locale information from client. You can use a string value that contains the client locale information.

Example JavaScript

The following code is an example of an HTML page that uses JavaScript to display a form into which you can input a number from 1 to 999:

```
<html>
  <head>
    <script type="text/javascript">
      function OnPresenceStateChanged(jid, basicPresence,
localizedPresence)
      {
        var cell = document.getElementById(jid);
        cell.innerHTML = basicPresence.concat(",
", localizedPresence);
      }

      function GetUserLocale()
      {
        window.external.GetUserLocale();
      }

      function SubscribePresence()
      {
        window.external.SubscribePresence('johndoe@example.com');
      }

      function OnLocaleInfoAvailable(currentLocale)
      {
        var cell = document.getElementById("JabberLocale");
```



```

        cell.innerText = currentLocale;
    }
    function onHubActivated()
    {
        var cell = document.getElementById("hubActive");
        cell.innerText = "TRUE";
    }
    function onHubDeActivated()
    {
        var cell = document.getElementById("hubActive");
        cell.innerText = "FALSE";
    }
    function onHubResized()
    {
        alert("Hub Resized or Moved");
    }
    function OnLoadMethods()
    {
        SubscribePresence();
        GetUserLocale();
    }
</script>
</head>
<body onload="OnLoadMethods()">
    <table>
        <tr>
            <td>John Doe</td>
            <td id="johndoe@example.com">unknown</td>
        </tr>
    </table>
    <table>
        <tr>
            <td>Jabber Locale: </td>
            <td id="JabberLocale">Null</td>
        </tr>
        <tr>
            <td>Hub Activated: </td>
            <td id="hubActive">---</td>
        </tr>
    </table>
</body>
</html>

```

To test this example JavaScript form, copy the preceding example into an HTML page and then specify that page as a custom embedded tab.

Show Call Events in Custom Tabs

You can use the following JavaScript function to show call events in a custom tab:

OnTelephonyConversationStateChanged

An API in the telephony service enables the client to show call events in a custom embedded tab. Custom tabs can implement the `OnTelephonyConversationStateChanged` JavaScript function. The client calls this function every time a telephony conversation state changes. The function accepts a JSON string that the client parses to get call events.

The following snippet shows the JSON that holds the call events:

```
{
  "conversationId": string,
  "acceptanceState": "Pending" | "Accepted" | "Rejected",
  "state": "Started" | "Ending" | "Ended",
  "callType": "Missed" | "Placed" | "Received" | "Passive" | "Unknown",
  "remoteParticipants": [{participant1}, {participant2}, ..., {participantN}],
  "localParticipant": {
  }
}
```

Each participant object in the JSON can have the following properties:

```
{
  "voiceMediaDisplayName": "<displayName>",
  "voiceMediaNumber": "<phoneNumber>",
  "translatedNumber": "<phoneNumber>",
  "voiceMediaPhoneType": "Business" | "Home" | "Mobile" | "Other" | "Unknown",
  "voiceMediaState": "Active" | "Inactive" | "Pending" | "Passive" | "Unknown",
}
```

The following is an example implementation of this function in a custom embedded tab. This example gets the values for the state and acceptanceState properties and shows them in the custom tab.

```
function OnTelephonyConversationStateChanged(json) {
  console.log("OnTelephonyConversationStateChanged");

  try {
    var conversation = JSON.parse(json);

    console.log("conversation id=" + conversation.conversationId);
    console.log("conversation state=" + conversation.state);
    console.log("conversation acceptanceState=" + conversation.acceptanceState);
    console.log("conversation callType=" + conversation.callType);
  }
  catch(e) {
    console.log("cannot parse conversation:" + e.message);
  }
}
```

The following is an example implementation of this function with all possible fields:

```
function OnTelephonyConversationStateChanged(json) {
  console.log("OnTelephonyConversationStateChanged");

  try {
    var conversation = JSON.parse(json);

    console.log("conversation state=" + conversation.state);
    console.log("conversation acceptanceState=" + conversation.acceptanceState);
    console.log("conversation callType=" + conversation.callType);

    for (var i=0; i<conversation.remoteParticipants.length; i++) {
      console.log("conversation remoteParticipants[" + i + "]=");
      console.log("voiceMediaDisplayName=" +
conversation.remoteParticipants[i].voiceMediaDisplayName);
      console.log("voiceMediaNumber=" +
conversation.remoteParticipants[i].voiceMediaNumber);
      console.log("translatedNumber=" +
conversation.remoteParticipants[i].translatedNumber);
      console.log("voiceMediaPhoneType=" +
conversation.remoteParticipants[i].voiceMediaPhoneType);
      console.log("voiceMediaState=" +
conversation.remoteParticipants[i].voiceMediaState);
    }

    console.log("conversation localParticipant=");
    console.log(" voiceMediaDisplayName=" +
conversation.localParticipant.voiceMediaDisplayName);
    console.log(" voiceMediaNumber=" + conversation.localParticipant.voiceMediaNumber);

    console.log(" translatedNumber=" + conversation.localParticipant.translatedNumber);
  }
}
```

```
        console.log("  voiceMediaPhoneType=" +
conversation.localParticipant.voiceMediaPhoneType);
        console.log("  voiceMediaState=" + conversation.localParticipant.voiceMediaState);
    }
    catch(e) {
        console.log("cannot parse conversation:" + e.message);
    }
}
```

Custom Embedded Tab Example

The following is an example of a configuration file with one embedded tab:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Client>
    <jabber-plugin-config>
      <browser-plugin>
        <page refresh="true" preload="true">
          <tooltip>Cisco</tooltip>
          <icon>http://www.cisco.com/web/fw/i/logo.gif</icon>
          <url>www.cisco.com</url>
        </page>
      </browser-plugin>
    </jabber-plugin-config>
  </Client>
</config>
```




Integrate with Directory Sources

- [Integrate with Directory Sources for an On-Premises Deployment, page 141](#)
- [Configure Contact Sources, page 141](#)
- [Federation, page 150](#)
- [Client Configuration for Directory Integration, page 153](#)

Integrate with Directory Sources for an On-Premises Deployment

Before You Begin

[Configure Directory Integration for an On-Premises Deployment, on page 7.](#)

Procedure

	Command or Action	Purpose
Step 1	Configure Contact Sources, on page 141	
Step 2	Client Configuration for Directory Integration, on page 153	

Configure Contact Sources

The client requires a contact source to search for users and to support contact resolution.

You can configure Enhanced Directory Integration (EDI), Basic Directory Integration (BDI), and Cisco Unified Communications Manager User Data Service (UDS) as contact sources.

Procedure

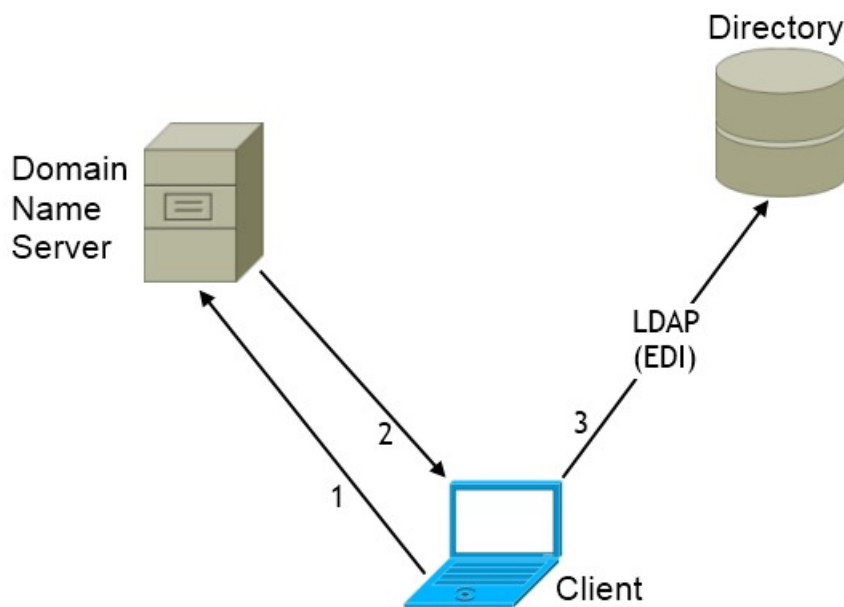
	Command or Action	Purpose
Step 1	To configure EDI as a contact source, see Domain Name Retrieval, on page 143 and Directory Server Discovery, on page 143 .	EDI is an LDAP-based contact source and is the default contact source used by Cisco Jabber for Windows.
Step 2	To configure BDI as a contact source, see Authentication with Contact Sources, on page 145 .	BDI is an LDAP-based contact source and is the default contact source used by Cisco Jabber for Mac, iOS, and Android clients.
Step 3	To configure UDS as a contact source, see Enable Integration with UDS, on page 148 and Set UDS Service Parameters, on page 149	Cisco Unified Communications Manager UDS is a Cisco Unified Communications Manager contact source and is available as a contact source for all Cisco Jabber clients. UDS is the contact source used for Expressway Mobile and Remote Access.

Enhanced Directory Integration

EDI uses native Microsoft Windows APIs to retrieve contact data from the directory service.

The following are the default settings for on-premises deployments with EDI:

- Cisco Jabber integrates with Active Directory as the contact source.
- Cisco Jabber automatically discovers and connects to a Global Catalog.



In the preceding diagram, the client does the following by default:

- 1 Gets the DNS domain from the workstation and looks up the SRV record for the Global Catalog.
- 2 Retrieves the address of the Global Catalog from the SRV record.
- 3 Connects to the Global Catalog with the logged in user's credentials.

Domain Name Retrieval

Cisco Jabber for Windows retrieves the fully qualified DNS domain from the `USERDNSDOMAIN` environment variable on the client workstation.

After the client gets the DNS domain, it can locate the Domain Name Server and retrieve SRV records.

In some instances, the value of the `USERDNSDOMAIN` environment variable does not resolve to the DNS domain that corresponds to the domain of the entire forest. For example, when an organization uses a sub-domain or resource domain. In this case, the `USERDNSDOMAIN` environment variable resolves to a child domain, not the parent domain. As a result, the client cannot access information for all users in the organization.

If the `USERDNSDOMAIN` environment variable resolves to a child domain, you can use one of the following options to enable Cisco Jabber for Windows to connect to a service in the parent domain:

- Ensure that the Global Catalog or LDAP directory server can access all users in the organization.
- Configure your DNS server to direct the client to a server that can access all users in the organization when Cisco Jabber for Windows requests a Global Catalog or LDAP directory server.
- Configure Cisco Jabber for Windows to use the FQDN of the parent domain.

Specify the FQDN of the parent domain as the value of the `PrimaryServerName` parameter in your client configuration as follows:

```
<PrimaryServerName>parent-domain-fqdn</PrimaryServerName>
```

Related Topics

- [Directory Connection Parameters](#)
- [Configuring DNS for the Forest Root Domain](#)
- [Assigning the Forest Root Domain Name](#)
- [Deploying a GlobalNames Zone](#)
- [Support for DNS Namespace planning in Microsoft server products](#)

Directory Server Discovery

Cisco Jabber can automatically discover and connect to the directory server if:

- The workstation on which you install Cisco Jabber is on the Microsoft Windows domain.
- The client can retrieve the address of the directory server from a DNS SRV record.

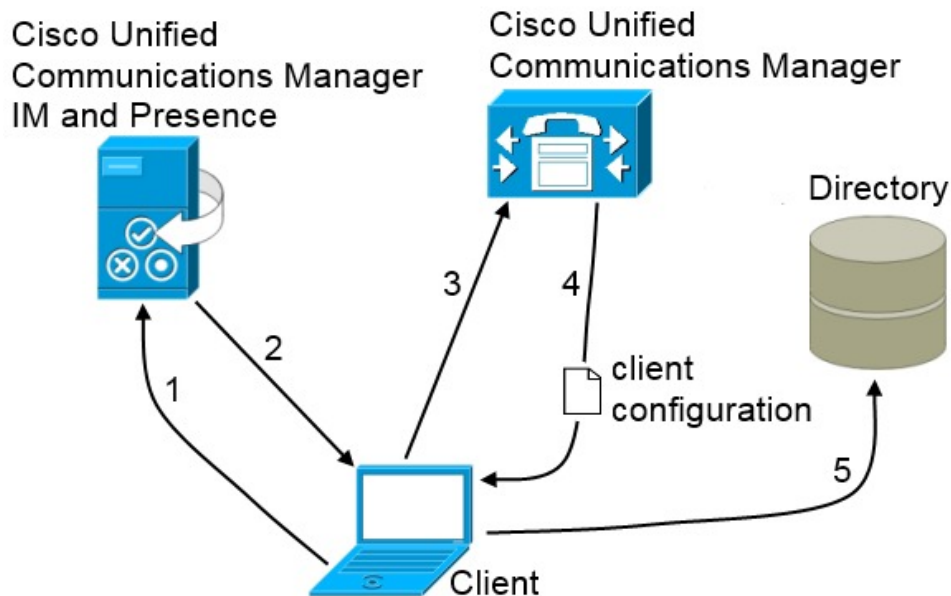
Directory Server	SRV Record
Global Catalog	<code>_gc._msdcs._tcp.domain.com</code>

Directory Server	SRV Record
Domain Controller LDAP-based directory servers	<code>_ldap._msdcs._tcp.domain.com</code>

Basic Directory Integration

When using Basic Directory Integration (BDI), the client retrieves contact data from the directory service as follows.

- 1 The client connects to the Cisco Unified Presence or Cisco Unified Communication Manager IM and Presence Service node.
- 2 The client gets the LDAP profile configuration section in the service profile from the Cisco Unified Presence or Cisco Unified Communication Manager IM and Presence Service node.
The service profile contains the location of Cisco Unified Communication Manager (TFTP) node. Depending on your configuration, the service profile can also contain the credentials to authenticate with the directory.
- 3 The client connects to the Cisco Unified Communication Manager node.
- 4 The client downloads the client configuration file from the Cisco Unified Communication Manager node.
The client configuration file contains the location of the directory. Depending on your configuration, the client configuration file can also contain the credentials to authenticate with the directory.
- 5 The client uses the directory location and the authentication credentials to connect to the directory.



380408

Authentication with Contact Sources

BDI requires users to authenticate with the directory source to resolve contacts. You can use the following methods to authenticate with the contact source, in order of priority:

- Specify credentials in Cisco Unified Presence or Cisco Unified Communications Manager — Specify credentials in a profile on the server. The client can then retrieve the credentials from the server to authenticate with the directory. This method is the most secure option for storing and transmitting credentials.
- Set common credentials in the client configuration file — Specify a shared username and password in the client configuration file. The client can then authenticate with the directory server.



Important

The client transmits and stores these credentials as plain text.

Use a well-known or public set of credentials for an account that has read-only permissions.

- Use anonymous binds — Configure the client to connect to the directory source with anonymous binds.

Specify LDAP Directory Configuration on Cisco Unified Presence

If your environment includes Cisco Unified Presence version 8.x, you can specify directory configuration in the LDAP profile. The client can then get the directory configuration from the server to authenticate with the directory source.

Complete the steps to create an LDAP profile that contains authentication credentials, and then assign that profile to users.

Procedure

- Step 1** Open the **Cisco Unified Presence Administration** interface.
 - Step 2** Select **Application > Cisco Unified Personal Communicator > LDAP Profile**.
 - Step 3** Select **Add New**.
 - Step 4** Specify a name and optional description for the profile.
 - Step 5** Specify a distinguished name for a user ID that is authorized to run queries on the LDAP server. Cisco Unified Presence uses this name for authenticated bind with the LDAP server.
 - Step 6** Specify a password that the client can use to authenticate with the LDAP server.
 - Step 7** Select **Add Users to Profile** and add the appropriate users to the profile.
 - Step 8** Select **Save**.
-

What to Do Next

Specify any additional BDI information in the client configuration file.

Specify LDAP Directory Configuration on Cisco Unified Communications Manager

If your environment includes Cisco Unified Communications Manager version 9.x and later, you can specify credentials when you add a directory service. The client can then get the configuration from the server to authenticate with the directory source.

Complete the steps to add a directory service, apply the directory service to the service profile, and specify the LDAP authentication configuration for the 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** In the **Add a UC Service** section, select **Directory** from the **UC Service Type** drop-down list.
- Step 5** Select **Next**.
- Step 6** Enter details for the directory service:
- Product Type — Select **Directory**
 - Name — Enter a unique name for the directory service
 - Hostname/IP Address — Enter the Hostname, IP Address, or FQDN of the directory server.
 - Protocol Type — From the drop-down list, select:
 - TCP or UDP for Cisco Jabber for Windows
 - TLS for Cisco Jabber for iPhone or iPad
 - TCP for Cisco Jabber for Android
- Step 7** Select **Save**.
- Step 8** Apply the directory service to your service profile as follows:
- a) Select **User Management > User Settings > Service Profile**.
The **Find and List Service Profiles** window opens.
 - b) Find and select your service profile.
The **Service Profile Configuration** window opens.
 - c) In the **Directory Profile** section, select up to three services from the **Primary**, **Secondary**, and **Tertiary** drop-down lists:
 - d) Specify the **Username** and **Password** that the client can use to authenticate with the LDAP server in the following fields:
 - e) Select **Save**.
-

Set Credentials in the Client Configuration

You can set credentials in the client configuration with the following parameters:

- BDIConnectionUsername
- BDIConnectionPassword



Important

The client transmits and stores these credentials as plain text.

Use a well-known or public set of credentials for an account that has read-only permissions.

The following is an example configuration:

```
<Directory>
  <BDIConnectionUsername>admin@example.com</BDIConnectionUsername>
  <BDIConnectionPassword>password</BDIConnectionPassword>
</Directory>
```

Use Anonymous Binds

To use anonymous binds, you set the following parameters in the client configuration file:

Parameter	Value
DirectoryServerType	BDI
BDIPrimaryServerName	IP address FQDN
BDIEnableTLS	True
BDISearchBase1	Searchable organizational unit (OU) in the directory tree
BDIBaseFilter	Object class that your directory service uses; for example, inetOrgPerson
BDIPredictiveSearchFilter	uid or other search filter A search filter is optional.

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>BDI</DirectoryServerType>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIEnableTLS>True</BDIEnableTLS>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
  <BDIBaseFilter>(&objectClass=inetOrgPerson)</BDIBaseFilter>
  <BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>
</Directory>
```

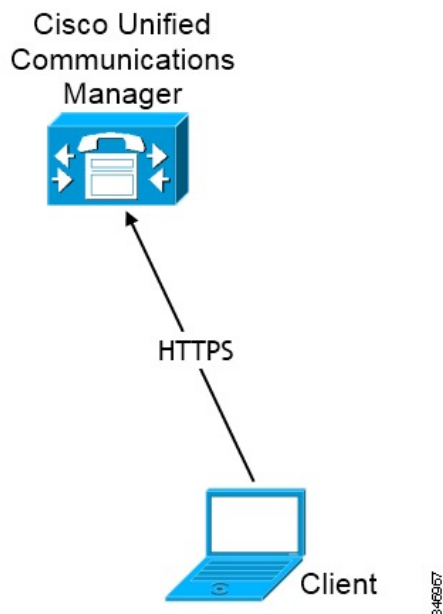
Cisco Unified Communications Manager User Data Service

User Data Service (UDS) is a REST interface on Cisco Unified Communications Manager that provides contact resolution.

UDS is used for contact resolution in the following cases:

- If you set the `DirectoryServerType` parameter to use a value of UDS in the client configuration file.
With this configuration, the client uses UDS for contact resolution when it is inside or outside of the corporate firewall.
- If you deploy Expressway for Remote and Mobile Access.
With this configuration, the client automatically uses UDS for contact resolution when it is outside of the corporate firewall.

You synchronize contact data into Cisco Unified Communications Manager from a directory server. Cisco Jabber then automatically retrieves that contact data from UDS.



Enable Integration with UDS

To enable integration with UDS, perform the following steps:

Procedure

-
- Step 1** Create your directory source in Cisco Unified Communications Manager.
 - Step 2** Synchronize the contact data to Cisco Unified Communications Manager.

After the synchronization occurs, your contact data resides in Cisco Unified Communications Manager.

Step 3 Specify UDS as the value of the `DirectoryServerType` parameter in your configuration file.

The following is an example configuration where UDS is the directory server type:

```
<Directory>
  <DirectoryServerType>UDS</DirectoryServerType>
</Directory>
```

Important This step is required only if you want to use UDS for all contact resolution (that is, both inside and outside the firewall). If you configure Expressway for Mobile and Remote Access, the client automatically uses UDS when outside the firewall, regardless of the value of the `DirectoryServerType` parameter. When using Expressway for Mobile and Remote Access, you can set the value of the `DirectoryServerType` parameter to either UDS or an LDAP-based contact source for use inside the firewall.

Step 4 For manual connections, specify the IP address of the Cisco Unified Communications Manager User Data Service server to ensure that the client can discover the server.

The following is an example configuration for the Cisco Unified Communications Manager User Data Service server:

```
<UdsServer>11.22.33.444</UdsServer>
```

Step 5 Configure the client to retrieve contact photos with UDS.

The following is an example configuration for contact photo retrieval:

```
<UdsPhotoUriWithToken>http://server_name.domain/%uid%.jpg</UdsPhotoUriWithToken>
```

Set UDS Service Parameters

You can set service parameters for UDS on Cisco Unified Communications Manager.

Procedure

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

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

Step 3 Locate the **User Data Service Parameters** section.

UDS Service Parameters

Set values for the following service parameters to configure UDS:

Parameter	Description
Enable All User Search	Allows searches for all users in the directory (search with no last name, first name, or directory number specified). The default value is true.

Parameter	Description
User Search Limit	Limits the number of users returned in a query. The default value is 64.
Number of Digits to Match	Specifies the number of digits to match when users search for phone numbers. Tip To resolve PSTN numbers, set the value equal to the number of digits in the PSTN numbers. For example, if the PSTN numbers have 10 digits, set the value to 10.

Contact Resolution with Multiple Clusters

For contact resolution with multiple Cisco Unified Communications Manager clusters, synchronize all users on the corporate directory to each cluster. Provision a subset of those users on the appropriate cluster.

For example, your organization has 40,000 users. 20,000 users reside in North America. 20,000 users reside in Europe. Your organization has the following Cisco Unified Communications Manager clusters for each location:

- `cucm-cluster-na` for North America
- `cucm-cluster-eu` for Europe

In this example, synchronize all 40,000 users to both clusters. Provision the 20,000 users in North America on `cucm-cluster-na` and the 20,000 users in Europe on `cucm-cluster-eu`.

When users in Europe call users in North America, Cisco Jabber retrieves the contact details for the user in Europe from `cucm-cluster-na`.

When users in North America call users in Europe, Cisco Jabber retrieves the contact details for the user in North America from `cucm-cluster-eu`.

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.

Interdomain Federation

Interdomain federation enables Cisco Jabber users in an enterprise domain to share availability and send instant messages with users in another domain.

- Cisco Jabber users must manually enter contacts from another domain.
- Cisco Jabber supports federation with the following:
 - Microsoft Office Communications Server

- Microsoft Lync
- IBM Sametime
- XMPP standard-based environments such as Google Talk
- AOL Instant Messenger

You configure interdomain federation for Cisco Jabber on Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service. See the appropriate server documentation for more information.

Related Topics

[Integration Guide for Configuring Cisco Unified Presence Release 8.6 for Interdomain Federation](#)
[Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager](#)

Intradomain Federation

Intradomain federation enables users within the same domain to share availability and send instant messages between Cisco Unified Presence and Microsoft Office Communications Server, Microsoft Live Communications Server, or other presence server.

Intradomain federation allows you to migrate users to Cisco Unified Presence or Cisco Unified Communications IM and Presence from a different presence server. For this reason, you configure intradomain federation for Cisco Jabber on the presence server. See the following documents for more information:

- Cisco Unified Presence: *Integration Guide for Configuring Partitioned Intradomain Federation for Cisco Unified Presence Release 8.6 and Microsoft LCS/OCS*
- Cisco Unified Communications IM and Presence: *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*

Configure Intradomain Federation for BDI or EDI

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 Presence 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.

The parameters that you use to configure intradomain federation depend on whether you use *Enhanced Directory Integration* (EDI) or *Basic Directory Integration* (BDI). EDI uses native Microsoft Windows APIs to retrieve contact data from the directory service and is only used by Cisco Jabber for Windows. For BDI, the client retrieves contact data from the directory service and is used by Cisco Jabber for Mac, Cisco Jabber for Android, and Cisco Jabber for iPhone and iPad.

Procedure

-
- Step 1** Set the value of the relevant parameter to true:

- For BDI: `BDISipUriToResolveContacts`
- For EDI: `UseSIPURIToResolveContacts`

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 relevant parameter:

- For BDI: `BDISipUri`
- For EDI: `SipUri`

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`
- `UserPrincipalName (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 relevant `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.`

- For BDI: `BDIUriPrefix`
- For EDI: `UriPrefix`

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

```
<Directory>
  <BDIUseSIPURIToResolveContacts>true</BDIUseSIPURIToResolveContacts>
  <BDISipUri>non-default-attribute</BDISipUri>
  <BDIUriPrefix>sip:</BDIUriPrefix>
</Directory>
```

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

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


Client Configuration for Directory Integration

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



Note In instances where a Service Profile and the configuration file are present, settings in the Service Profile take priority.



Note Cisco Unified Presence 8 profiles cannot be used for directory integration.

When to Configure Directory Integration



Note Install Cisco Jabber for Windows on a workstation that is registered to an Active Directory domain. In this environment, you do not need to configure Cisco Jabber for Windows to connect to the directory. The client automatically discovers the directory and connects to a Global Catalog server in that domain.

Configure Cisco Jabber to connect to a directory if you plan to use one of the following as the contact source:

- Domain Controller
- Cisco Unified Communications Manager User Data Service
- OpenLDAP
- Active Directory Lightweight Directory Service
- Active Directory Application Mode

You can optionally configure directory integration to:

- Change the default attribute mappings.
- Adjust directory query settings.
- Specify how the client retrieves contact photos.
- Perform intradomain federation.

Configure Directory Integration in a Service Profile

With Cisco Unified Communications Manager version 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. For information about service discovery, see [Configure Service Discovery](#), on page 17.

Procedure

	Command or Action	Purpose
Step 1	Add a Directory Service , on page 154	
Step 2	Apply Directory Service to a Service Profile , on page 157	

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 and then select **Save**.
-

What to Do Next

Apply Directory Service.

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.
Tertiary Server	Specifies the address of the tertiary directory server.

Directory Service Configuration	Description
Use UDS for Contact Resolution	<p>Specifies if the client uses UDS as a contact source.</p> <p>Important When this option is selected the following parameters are not used.</p> <p>Note By default, UDS provides contact resolution when users connect to the corporate network through Expressway for Mobile and Remote Access.</p>
Use Logged On User Credential	<p>Specifies if the client uses the logged on username and password.</p> <p>True Use credentials. This is the default value.</p> <p>False Do not use credentials. Specify credentials with the BDIConnectionUsername and BDIConnectionPassword parameters.</p>
Username	<p>Lets you manually specify a shared username that the client can use to authenticate with the directory server.</p> <p>By default, the client uses Integrated Windows Authentication when connecting to the directory server. This parameter lets you manually specify a username in scenarios where it is not possible to authenticate with the directory server with the user's Microsoft Windows credentials.</p> <p>Use only a well-known or public set of credentials for an account that has read-only permissions.</p>
Password	<p>Lets you manually specify a shared password that the client can use to authenticate with the directory server.</p> <p>By default, the client uses Integrated Windows Authentication when connecting to the directory server. This parameter lets you manually specify a password in scenarios where it is not possible to authenticate with the directory server with the user's Microsoft Windows credentials.</p> <p>Use only a well-known or public set of credentials for an account that has read-only permissions.</p>

Directory Service Configuration	Description
<p>Search Base 1</p> <p>Search Base 2</p> <p>Search Base 3</p>	<p>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.</p> <p>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.</p> <p>Active Directory does not typically require a search base. Specify search bases for Active Directory only for specific performance requirements.</p> <p>Specify a search base for directory servers other than Active Directory to create bindings to specific locations in the directory.</p> <p>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.</p>
<p>Recursive Search on All Search Bases</p>	<p>Select this option to perform a recursive search of the directory starting at the search base. Use recursive searches to allow the Cisco JabberCisco 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.</p> <p>This is a required field.</p> <p>The default value is True.</p>
<p>Base Filter</p>	<p>Specifies a base filter for Active Directory queries.</p> <p>Specify a directory subkey name only to retrieve objects other than user objects when you query the directory.</p> <p>The default value is (&amp; ; (objectCategory=person) .</p>
<p>Predictive Search Filter</p>	<p>Defines filters to apply to predictive search queries.</p> <p>You can define multiple, comma-separated values to filter search queries.</p> <p>The default value is Ambiguous Name Resolution (ANR).</p> <p>When Cisco Jabber for Windows 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.</p> <p>Important You must configure your directory server to set attributes for ANR if you want the client to search for those attributes.</p>

Service Discovery will use UDS search when the **Use UDS for Contact Resolution** option is selected, otherwise it uses BDI or EDI search. During service discovery the **Username**, **Password**, **SearchBase1**, **PrimaryServerName**, **ServerPort1**, **UriPrefix**, **UseJabberCredentials**, **BaseFilter**, **PredictiveSearchFilter**, and **DirectoryServerType** in the directory profile will be used to connect to LDAP server for contact search.

Manual sign on uses the **Username** and **Password** from the directory profile to connect to the LDAP server for contact search.

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.

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**.
-

Configure Directory Integration in the Configuration File

You can configure directory integration in the Cisco Jabber configuration file. The following sections show the parameters that can be configured and also includes a section covering examples of the configuration..



Important

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

Summary of Directory Integration Configuration Parameters

The following tables are a summary of all directory integration parameters.

Attribute Mapping

These parameters are used for attribute mapping with LDAP directory servers.

BDI Parameters	EDI Parameters
<ul style="list-style-type: none"> • BDICommonName • BDIDisplayName • BDIFirstname • BDILastname • BDIEmailAddress • BDISipUri • BDIPhotoSource • BDIBusinessPhone • BDIMobilePhone • BDIHomePhone • BDIOtherPhone • BDIDirectoryUri • BDITitle • BDICompanyName • BDIUserAccountName • BDIDomainName • BDICountry • BDILocation • BDINickname • BDIPostalCode • BDICity • BDIState • BDIStreetAddress 	<ul style="list-style-type: none"> • CommonName • DisplayName • Firstname • Lastname • EmailAddress • SipUri • PhotoSource • BusinessPhone • MobilePhone • HomePhone • OtherPhone • DirectoryUri • Title • CompanyName • UserAccountName • DomainName • Country • Location • Nickname • PostalCode • City • State • StreetAddress

Directory Server Connection

These parameters are used for connecting to LDAP directory servers.

BDI Parameters	EDI Parameters
<ul style="list-style-type: none">• BDILDAPServerType• BDIPresenceDomain• BDIPrimaryServerName• BDIserverPort1• BDIUseJabberCredentials• BDIConnectionUsername• BDIConnectionPassword• BDIEnableTLS	<ul style="list-style-type: none">• DirectoryServerType• ConnectionType• PrimaryServerName• SecondaryServerName• ServerPort1• ServerPort2• UseWindowsCredentials• ConnectionUsername• ConnectionPassword• UseSSL• UseSecureConnection

Contact Resolution and Directory Query

These parameters are used for contact resolution and directory queries with LDAP directory servers.

BDI Parameters	EDI Parameters
<ul style="list-style-type: none"> • BDIBaseFilter • BDIUseANR • BDIPredictiveSearchFilter • BDIsearchBase1 • BDIphotoUriSubstitutionEnabled • BDIphotoUriSubstitutionToken • BDIphotoUriWithToken • BDIUseSIPURIToResolveContacts • BDIUriPrefix • BDIDirectoryUri • BDIDirectoryUriPrefix 	<ul style="list-style-type: none"> • BaseFilter • PredictiveSearchFilter • DisableSecondaryNumberLookups • PhoneNumberMasks • SearchTimeout • UseWildcards • MinimumCharacterQuery • SearchBase1, SearchBase2, SearchBase3, SearchBase4, and SearchBase5 • PhotoUriSubstitutionEnabled • PhotoUriSubstitutionToken • PhotoUriWithToken • UseSIPURIToResolveContacts • UriPrefix • DirectoryUri • DirectoryUriPrefix

UDS

These parameters are used for interacting with UDS as a contact source.

- DirectoryServerType
- PresenceDomain
- UdsServer
- UdsPhotoUriWithToken

Directory Server Type Parameter

You specify the directory server type with the following parameter in the `jabber-config.xml` file:

Parameter	Value	Description
DirectoryServerType	BDI EDI UDS	Specifies the type of directory server to use. <ul style="list-style-type: none"> • BDI — Connect to a LDAP server. • EDI — Connect to a LDAP server. • UDS — Connect to UDS.

EDI and BDI Directory Integration Parameters

The following sections lists details about the EDI and BDI parameters you can configure for LDAP-based directory integration.

Attribute Mapping Parameters

The following table describes the parameters for mapping LDAP directory attributes.

BDI Parameter	EDI Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
BDICommonName	CommonName	cn	Yes	Yes	No
BDIDisplayName	DisplayName	displayName	Yes	Yes	Yes
BDIFirstname	Firstname	givenName	Yes	Yes	Yes
BDILastname	Lastname	sn	Yes	Yes	Yes
BDIEmailAddress	EmailAddress	mail	Yes	Yes	Yes
BDISipUri Note The client uses this parameter for intradomain federation, not URI dialing.	SipUri Note The client uses this parameter for intradomain federation, not URI dialing.	msRCSIPPrimaryUserAddress	Yes	Yes	Yes
BDIPhotoSource	PhotoSource	thumbnailPhoto	No	No	No
BDIBusinessPhone	BusinessPhone	telephoneNumber	Yes	No	No
BDIMobilePhone	MobilePhone	mobile	Yes	No	No
BDIHomePhone	HomePhone	homePhone	Yes	No	No
BDIOtherPhone	OtherPhone	otherTelephone	Yes	No	No

BDI Parameter	EDI Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
BDIDirectoryUri Note The client uses this parameter for URI dialing.	DirectoryUri Note The client uses this parameter for URI dialing.	mail	Yes	No	No
BDITitle	Title	title	Yes	No	No
BDICompanyName	CompanyName	company	Yes	Yes	No
BDIUserAccountName	UserAccountName	sAMAccountName	Yes	Yes	Yes
BDIDomainName	DomainName	EDI - userPrincipalName BDI - dn	Yes	Yes	No
BDICountry		co	Yes	No	No
BDILocation	Location	EDI - co BDI - location	Yes	No	No
BDINickname	Nickname	displayName	Yes	Yes	Yes
BDIPostalCode	PostalCode	postalCode	Yes	No	No
BDICity	City	l	Yes	Yes	No
BDIState	State	st	Yes	Yes	No
BDIStreetAddress	StreetAddress	streetAddress	Yes	No	No

Attributes on the Directory Server

You must index attributes on your LDAP directory server so that the client can resolve contacts.

If you use the default attribute mappings, ensure the following attributes are indexed:

- sAMAccountName
- displayName
- sn
- name

- proxyAddresses
- mail
- department
- givenName
- telephoneNumber

Additionally, ensure you index the following attributes for secondary number queries:

- otherTelephone
- mobile
- homePhone



Note By default secondary number queries are enabled in Cisco Jabber for Windows. You can disable secondary number queries with the `DisableSecondaryNumberLookups` parameter.

- msRTCSIP-PrimaryUserAddress

Index `msRTCSIP-PrimaryUserAddress` for intradomain federation only.

Because Cisco Jabber for Windows connects to a Global Catalog server by default, you must ensure that all attributes reside on your Global Catalog server. You can replicate attributes to a Global Catalog server using an appropriate tool such as the Microsoft Active Directory Schema snap-in

- Replicating attributes to your Global Catalog server generates traffic between Active Directory servers in the domain. For this reason, replicate attributes to your Global Catalog server at a time when network traffic can handle extra load.
- If you do not want to replicate attributes to a Global Catalog server, configure Cisco Jabber to connect to a Domain Controller. However, the client queries single domains only when it connects to a Domain Controller.

Directory Connection Parameters

The following table describes parameters for configuring your LDAP directory connection:

BDI Parameter	EDI Parameter	Value	Description
	ConnectionType	0 1	<p>Specifies if the client connects to a Global Catalog or a Domain Controller.</p> <ul style="list-style-type: none"> • 0 (default) — Connect to a Global Catalog. • 1 — Connect to a Domain Controller. <p>Note Default ports are as follows:</p> <ul style="list-style-type: none"> • Global Catalog: 3268 • Domain Controller: 389
BDILDAPServerType		AD OpenLDAP	<p>Specifies the type of LDAP directory server to which the client connects.</p> <ul style="list-style-type: none"> • AD (default) — Connect to Active Directory. • OpenLDAP — Connect to OpenLDAP.
BDIPresenceDomain		Domain of the presence node.	<p>Required parameter. Specifies the domain of the presence node.</p> <p>The client appends this domain to the user ID to create an IM address. For example, a user named Adam McKenzie has the user ID <i>amckenzie</i>. You specify <i>example.com</i> as the presence node domain.</p> <p>When the user logs in, the client constructs the IM address <i>amckenzie@example.com</i> for Adam McKenzie.</p>

BDI Parameter	EDI Parameter	Value	Description
BDIPrimaryServerName	PrimaryServerName	IP address FQDN	<p>Required parameter. Specifies the address of the primary directory server.</p> <p>This parameter is required for manual connections where the client cannot automatically discover the directory server.</p> <p>Note Each time the client starts, it attempts to connect to the primary server. The client attempts to connect to the secondary server if:</p> <ul style="list-style-type: none"> • The primary server is not available. • The primary server fails after the client connects to it. <p>If the connection to the secondary server is successful, the client keeps the connection to the secondary server until the next restart.</p> <p>If the secondary server fails while the client is connected to it, the client attempts to connect to the primary server.</p>
	SecondaryServerName	IP address FQDN	<p>Specifies the address of the backup directory server.</p> <p>This parameter is required for manual connections where the client cannot automatically discover the directory server.</p>
BDIServerPort1	ServerPort1	Port number	Specifies the port for the primary directory server.

BDI Parameter	EDI Parameter	Value	Description
ServerPort2	ServerPort2	Port number	Specifies the port for the backup directory server.
	UseWindowsCredentials	0 1	<p>Specifies if the client uses Microsoft Windows usernames and passwords.</p> <ul style="list-style-type: none"> • 0 — Do not use Windows credentials. <p>Specify credentials with the ConnectionUsername and ConnectionPassword parameters.</p> <ul style="list-style-type: none"> • 1 (default) — Use Windows credentials.
BDIUseJabberCredentials		true false	<p>Specifies whether the client can use the presence server credentials to sign in to the directory server.</p> <ul style="list-style-type: none"> • true — The client searches for the username and password in this order: <ol style="list-style-type: none"> 1 Client configuration file (BDIConnectionUsername and BDIConnectionPassword) 2 Presence server <p>If the credentials are not present, the client tries to sign in anonymously.</p> • false (default) — The client tries to sign in using the values of BDIConnectionUsername and BDIConnectionPassword in the client configuration file. <p>If the parameters are not present, the client tries to sign in anonymously.</p>

BDI Parameter	EDI Parameter	Value	Description
BDIConnectionUsername	ConnectionUsername	Username	<p>Lets you manually specify a shared username that the client can use to authenticate with the directory server.</p> <p>Important The client transmits and stores this username as plain text.</p> <p>By default, Cisco Jabber for Windows uses Integrated Windows Authentication when connecting to the directory server. This parameter lets you manually specify a username in scenarios where it is not possible to authenticate with the directory server with the user's Microsoft Windows credentials.</p> <p>Use only a well-known or public set of credentials for an account with read-only permissions to the directory.</p>

BDI Parameter	EDI Parameter	Value	Description
BDIConnectionPassword	ConnectionPassword	Password	<p>Lets you manually specify a shared password that the client can use to authenticate with the directory server.</p> <p>Important The client transmits and stores this password as plain text.</p> <p>By default, Cisco Jabber for Windows uses Integrated Windows Authentication when connecting to the directory server. This parameter lets you manually specify a password in scenarios where it is not possible to authenticate with the directory server with the user's Microsoft Windows credentials.</p> <p>Use a well-known or public set of credentials for an account with read-only permissions to the directory.</p>
BDIEnableTLS		true false	<p>Use TLS to secure directory connections.</p> <ul style="list-style-type: none"> • true — Use TLS. • false (default) — Do not use TLS.

BDI Parameter	EDI Parameter	Value	Description
	UseSSL	0 1	<p>Use SSL for secure connections to the directory.</p> <ul style="list-style-type: none"> • 0 (default) — Do not use SSL. • 1 — Use SSL. <p>The SSL connection certificate must be present:</p> <ul style="list-style-type: none"> • In the Microsoft Windows certificate store. • On the directory server to which the client connects. <p>To establish an SSL connection, the server presents the client with the certificate. The client then validates the certificate from the server against the certificate in the store on the client computer.</p> <p>Default protocols and ports for SSL connections are as follows:</p> <ul style="list-style-type: none"> • Global Catalog <ul style="list-style-type: none"> • Protocol: TCP • Port number: 3269 • Domain Controller <ul style="list-style-type: none"> • Protocol: TCP • Port number: 636

BDI Parameter	EDI Parameter	Value	Description
	UseSecureConnection	0 1	<p>Specifies the mechanism for authentication with the directory server.</p> <ul style="list-style-type: none"> • 0 — Use simple authentication. <p>Set this value to connect to the directory server using simple binds. With simple authentication, the client transmits credentials in plain text. You can enable SSL to encrypt credentials with the UseSSL parameter.</p> <ul style="list-style-type: none"> • 1 (default) — Use Generic Security Service API (GSS-API). GSS-API leverages the system authentication mechanism. In a Microsoft Windows environment, GSS-API lets you connect to the directory server using Kerberos-based Windows authentication.

IM Address Scheme Parameters

The following table describes parameters for configuring the IM address scheme.

BDI Parameter	EDI Parameter	Value	Description
BDIUseSipUriToResolveContacts	UseSipUriToResolveContacts	true false	<p>Specifies the IM Address scheme to use.</p> <ul style="list-style-type: none"> • true — Use the Directory URI scheme. • false (default) — Use the User ID @[Default Domain] scheme.

BDI Parameter	EDI Parameter	Value	Description
BDIUriPrefix	UriPrefix	prefix string	Specifies a prefix to remove from the SipUri or BDISipUri parameter. For example, sip: may prefix the msRTCSIP-PrimaryUserAddress directory attribute.
BDISipUri	SipUri	mail msRTCSIP PrimaryUser Address	Specifies the directory attribute field that the IM Address scheme field is mapped to.

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

```
<Directory>
  <BDIUseSIPURIToResolveContacts>true</BDIUseSIPURIToResolveContacts>
  <BDISipUri>non-default-attribute</BDISipUri>
  <BDIUriPrefix>sip:</BDIUriPrefix>
</Directory>
```

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

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

Directory Query Parameters

The following table describes parameters for configuring how the client queries your LDAP directory:

BDI Parameter	EDI Parameter	Value	Description
BDIBaseFilter	BaseFilter	Base filter	<p>Specifies a base filter for Active Directory queries.</p> <p>Specify a directory subkey name only to retrieve objects other than user objects when you query the directory.</p> <p>The default value in Cisco Jabber for iPhone and iPad is <code>(&(objectCategory=person))</code>.</p> <p>The default value for all other clients is <code>(&;(objectCategory=person))</code>.</p> <p>Configuration files can contain only valid XML character entity references. Use <code>&amp;;</code> instead of <code>&</code> if you specify a custom base filter.</p>
BDIUseANR		true false	<p>Specifies if Cisco Jabber issues a query using Ambiguous Name Resolution (ANR) when it performs a predictive search.</p> <ul style="list-style-type: none"> • true (default) — Use ANR for predictive search. If you use OpenLDAP, the default value is false. • false — Do not use ANR for predictive search. Set the value to false if you integrate with a directory source other than Active Directory. <p>Important Configure your directory server to set attributes for ANR if you want the client to search for those attributes.</p>

BDI Parameter	EDI Parameter	Value	Description
BDIPredictiveSearchFilter	PredictiveSearchFilter	Search filter	<p>Defines filters to apply to predictive search queries.</p> <p>You can define multiple, comma-separated values to filter search queries.</p> <p>Note This key is only used by Cisco Jabber for iPhone and iPad when BDIUseANR is set to false. And if BDI PredictiveSearchFilter is not set, the default search filter is used.</p> <p>The default EDI value is anr</p> <p>When Cisco Jabber for Windows performs a predictive search, it issues a query using ANR. This query disambiguates the search string and returns results that match the attributes that are set for ANR on your directory server.</p> <p>Important Configure your directory server to set attributes for ANR if you want the client to search for those attributes.</p>
	DisableSecondaryNumberLookups	0 1	<p>Specifies whether users can search for alternative contact numbers if the work number is not available, such as the mobile, home, or other number.</p> <ul style="list-style-type: none"> • 0 (default) — Users can search for alternative contact numbers. • 1 — Users cannot search for alternative contact numbers.
	SearchTimeout	Number of seconds	<p>Specifies the timeout period for queries in seconds.</p> <p>The default value is 5.</p>

BDI Parameter	EDI Parameter	Value	Description
	UseWildcards	0 1	<p>Enables wildcard searches.</p> <ul style="list-style-type: none"> • 0 (default) — Do not use wildcards. • 1 — Use wildcards. <p>If you use wildcards, it might take longer to search the directory.</p>
	MinimumCharacterQuery	Numerical value	<p>Sets the minimum number of characters in a contact name to query the directory.</p> <p>For example, if you set 2 as the value of this parameter, the client searches the directory when users enter at least two characters in the search field.</p> <p>The default value is 3.</p>

BDI Parameter	EDI Parameter	Value	Description
BDISearchBase1	SearchBase1 SearchBase2 SearchBase3 SearchBase4 SearchBase5	Searchable organizational unit (OU) in the directory tree	<p>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.</p> <p>By default, the client searches from the root of the directory tree. You can specify the value of up to five search bases in your OU to override the default behavior.</p> <p>Active Directory does not typically require a search base. Specify search bases for Active Directory only for specific performance requirements.</p> <p>Specify a search base for directory servers other than Active Directory to create bindings to specific locations in the directory.</p> <p>Tip Specify an OU to restrict searches to certain user groups.</p> <p>For example, a subset of your users have IM capabilities only. Include those users in an OU and then specify that as a search base.</p>

Base Filter Examples

The following are example base filters you can use to look up specific locations or objects.

Find only specific groups:

```
(&objectClass=user)(memberOf=cn=group-name,ou=Groups,dc=example,dc=com)
```

Find a nested group within a group:

```
(&objectClass=user)(memberOf:search-oid:=cn=group-name,ou=Groups,dc=example,dc=com)
```

Find only enabled accounts and non-administrator accounts:

```
(&objectCategory=person)(objectClass=user)(!(userAccountControl:search-oid:=2))
(!(sAMAccountName=*_dbo))(!(sAMAccountName=*-admin))
```

Phone Number Masks Parameter

Phone number masks parameter only applies to EDI. The following table describes the parameter to configure masks for phone number resolution:

Parameter	Value	Description
PhoneNumberMasks	Mask string	<p>Specifies masks to use when users search for phone numbers.</p> <p>For example, a user receives a call from +14085550100. In the directory, this number is +(1) 408 555 0100.</p> <p>The following mask resolves the number: +14081+(#) ### ### ####</p> <p>The length of mask strings cannot exceed the size restriction for registry subkey names.</p>

Phone masks apply to phone numbers before the client searches your directory. If you configure phone masks correctly, directory searches succeed as exact query matches and prevent any impact to performance of your directory server.

The following table describes the elements you can include in a phone mask:

Element	Description
Phone number pattern	<p>Provides a number pattern to retrieve phone numbers from your directory.</p> <p>To add a phone mask, you specify a number pattern that applies to the mask.</p> <p>For example, to specify a mask for searches that begin with +1408, you can use the following mask: +1408 +(#) ### ### ####</p> <p>To enable a mask to process phone numbers that have the same number of digits, but different patterns, use multiple masks with the same number of digits.</p> <p>For example, your company has site A and site B. Each site maintains a separate directory in which the phone numbers have different formats, such as the following:</p> <p style="padding-left: 40px;">+(1) 408 555 0100 +1-510-5550101</p> <p>The following mask ensures you can use both numbers correctly: +1408 +(#) ### ### #### +1510 +#-###-#####.</p>
Pipe symbol ()	<p>Separates number patterns and masks.</p> <p>For example, +1408 +(#) ### ### #### +34 +(##) ### ####.</p>
Wildcard character	<p>Substitutes one or more characters for a subset of possible matching characters.</p> <p>Any wildcard character can exist in a phone mask.</p> <p>For example, an asterisk (*) represents one or more characters and can apply to a mask as follows: +3498 +##*###*#####. Using this mask with the wildcard, a phone number search can match any of the following formats:</p> <p style="padding-left: 40px;">+34(98)555 0199 +34 98 555-0199 +34-(98)-555.0199</p>

Element	Description
Reverse mask	<p>Applies a number pattern from right to left.</p> <p>For example, a mask of +3498 R+34 (98) 559 ##### applied to +34985590199 results in +34 (98) 559 0199.</p> <p>You can use both forward and reverse masks.</p>

Contact Photo Parameters

The following table describes parameters for configuring how the client retrieves contact photos from an LDAP directory.

BDI Parameter	EDI Parameter	Value	Description
BDIPhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled	true false	<p>Specifies if photo URI substitution is enabled.</p> <ul style="list-style-type: none"> • true — Photo URI substitution is enabled. • false (default) — Specifies if photo URI substitution is disabled.

BDI Parameter	EDI Parameter	Value	Description
BDIPhotoUriSubstitutionToken	PhotoUriSubstitutionToken	Directory attribute	<p>Specifies a directory attribute to insert in the photo URI; for example, sAMAccountName.</p> <p>Only the following attributes are supported for use with the PhotoURISubstitutionToken parameter:</p> <ul style="list-style-type: none"> • Common Name • Display Name • First Name • Last Name • Nickname • Email Address • Photo Source • Business Phone • Mobile Phone • Home Phone • Preferred Phone • Other Phone • Title • Company Name • User Account Name • Domain Name • Location • Post Code • State • City • Street

BDI Parameter	EDI Parameter	Value	Description
BDIPhotoUriWithToken	PhotoUriWithToken	URI	<p>Specifies a photo URI with a directory attribute as a variable value. For example:</p> <p><code>http://staffphoto.example.com/sAMAccountName.jpg</code></p> <p>The parameter applies to LDAP directory integrations.</p> <p>To configure photo URI substitution, you set the directory attribute as the value of <code>BDIPhotoUriSubstitutionToken</code>.</p> <p>Restriction The client must be able to retrieve the photos from the web server without credentials.</p>
BDIPhotoSource	PhotoSource	Directory attribute	The name of a directory attribute that stores a contact photo as a binary object or a URI to a contact photo.

Contact Photo Retrieval

Cisco Jabber retrieves and displays contact photos with the following methods.



Note

When you change a photo in the Active Directory, the photo can take up to 24 hours to refresh in Cisco Jabber.

URI substitution

Cisco Jabber dynamically builds a URL to contact photos with a directory attribute and a URL template.

To use this method, set the following values in your configuration file:

- 1 Specify `true` as the value of the `BDIPhotoUriSubstitutionEnabled` or `PhotoUriSubstitutionEnabled` parameter.
- 2 Specify a directory attribute to use as a dynamic token as the value of the `BDIPhotoUriSubstitutionToken` or `PhotoUriSubstitutionToken` parameter. For example,


```
<BDIPhotoUriSubstitutionToken>sAMAccountName</BDIPhotoUriSubstitutionToken>
<PhotoUriSubstitutionToken>sAMAccountName</PhotoUriSubstitutionToken>
```
- 3 Specify the URL and the dynamic token as the value of the `BDIPhotoUriWithToken` or `PhotoUriWithToken` parameter. For example,


```
<BDIPhotoUriWithToken>http://staffphoto.example.com/sAMAccountName.jpg</BDIPhotoUriWithToken>
<PhotoUriWithToken>http://staffphoto.example.com/sAMAccountName.jpg</PhotoUriWithToken>
```

With the example values in the preceding steps, the `sAMAccountName` attribute might resolve to `msmith` in your directory. Cisco Jabber then takes this value and replaces the token to build the following URL: `http://staffphoto.example.com/msmith.jpg`.

Binary objects

Cisco Jabber retrieves the binary data for the photo from your database.

If you are using binary objects from Active Directory do not set `BDIPhotoUriWithToken` or `PhotoUriWithToken`.

To use this method to retrieve contact photos, specify the attribute that contains the binary data as the value of the `BDIPhotoSource` or `PhotoSource` parameter in the configuration. For example,

```
<BDIPhotoSource>jpegPhoto</BDIPhotoSource>
<PhotoSource>thumbnailPhoto</PhotoSource>
```

PhotoURL attribute

Cisco Jabber retrieves a URL from a directory attribute.

To use this method to retrieve contact photos, specify the attribute that contains the photo URL as the value of the `BDIPhotoSource` or `PhotoSource` parameter in the configuration. For example,

```
<BDIPhotoSource>photoUri</BDIPhotoSource>
<PhotoSource>photoUri</PhotoSource>
```

UDS Parameters

The following table provides details about the parameters you can use in the configuration file to connect to UDS and perform contact resolution and directory queries.

Parameter	Value	Description
PresenceDomain	Domain of the presence node.	Required parameter. Specifies the domain of the presence server. The client appends this domain to the user ID to create an IM address. For example, a user named Adam McKenzie has the following user ID: <code>amckenzie</code> . You specify <code>example.com</code> as the presence server domain. When the user logs in, the client constructs the following IM address for Adam McKenzie: <code>amckenzie@example.com</code> .
UdsServer	IP address FQDN	Specifies the address of the Cisco Unified Communications Manager User Data Service (UDS) server. This parameter is required for manual connections where the client cannot automatically discover the UDS server.

Parameter	Value	Description
UdsPhotoUriWithToken	URI	<p>Specifies a photo URI with a directory attribute as a variable value; for example, <code>http://www.photo/url/path/%%uid%%.jpg.</code></p> <p>This parameter applies to UDS directory integrations. You must specify this parameter to download contact photos in either of the following cases:</p> <ul style="list-style-type: none"> • If you configure the <code>DirectoryServerType</code> parameter to use UDS. With this configuration, the client uses UDS for contact resolution when it is inside or outside of the corporate firewall. • If you deploy Expressway for Mobile and Remote Access. With this configuration, the client automatically uses UDS for contact resolution when it is outside of the corporate firewall. <p>Restriction The client must be able to retrieve the photos from the web server without credentials.</p>

Contact Photo Retrieval with UDS

Cisco Unified Communications Manager User Data Service (UDS) dynamically builds a URL for contact photos with a directory attribute and a URL template.

To resolve contact photos with UDS, you specify the format of the contact photo URL as the value of the `UdsPhotoUriWithToken` parameter. You also include a `%%uid%%` token to replace the contact username in the URL, for example,

```
<UdsPhotoUriWithToken>http://server_name/%%uid%%.jpg</UdsPhotoUriWithToken>
```

UDS substitutes the `%%uid%%` token with the value of the `userName` attribute in UDS. For example, a user named Mary Smith exists in your directory. The value of the `userName` attribute for Mary Smith is `msmith`. To resolve the contact photo for Mary Smith, Cisco Jabber takes the value of the `userName` attribute and replaces the `%%uid%%` token to build the following URL: `http://staffphoto.example.com/msmith.jpg`



Note

When you change a photo in the Active Directory, the photo can take up to 24 hours to refresh in Cisco Jabber.

**Important**

- If you deploy Expressway for Mobile and Remote Access, the client automatically uses UDS for contact resolution when users connect to services from outside the corporate network. When you set up UDS contact resolution for Expressway for Mobile and Remote Access, you must add the web server on which you host the contact photos to the HTTP server allow list in your Cisco Expressway-C server configuration. The HTTP server allow list enables the client to access web services inside the corporate network.
- All contact photos must follow the format of the URL you specify as the value of UdsPhotoUriWithToken.

Directory Server Configuration Examples

This section describes supported integration scenarios and provides example configurations.

Domain Controller Connection

To connect to a Domain Controller, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
ConnectionType	1

The following is an example configuration:

```
<Directory><DirectoryServerType>EDI</DirectoryServerType>
<ConnectionType>1</ConnectionType></Directory>
```

Manual Server Connections for Cisco Jabber for Windows

To manually connect to a directory server, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
PrimaryServerName	FQDN IP address
ServerPort1	Port number
SecondaryServerName	FQDN IP address
ServerPort2	Port number

The following is an example configuration:

```
<Directory>
<DirectoryServerType>EDI</DirectoryServerType>
<PrimaryServerName>primary-server-name.domain.com</PrimaryServerName>
<ServerPort1>1234</ServerPort1>
<SecondaryServerName>secondary-server-name.domain.com</SecondaryServerName>
<ServerPort2>5678</ServerPort2></Directory>
```

UDS Integration

To integrate with UDS, set the following parameters.

Parameter	Value
DirectoryServerType	UDS
UdsServer	IP address of the UDS server
UdsPhotoUriWithToken	Contact photo URL
PresenceDomain	Server address of your presence domain
Note This parameter is only applicable to Phone Mode.	



Note

Configure the DirectoryServerType parameter to UDS only if you want to use UDS for all contact resolution (that is, from inside and outside the corporate firewall).

The following is an example configuration:

```
<Directory>
<DirectoryServerType>UDS</DirectoryServerType>
<UdsServer>11.22.33.444</UdsServer>
<UdsPhotoUriWithToken>http://server-name/%%uid%.jpg</UdsPhotoUriWithToken>
</Directory>
```

LDAP Integration with Expressway for Mobile and Remote Access

When you deploy Expressway for Mobile and Remote Access with an LDAP directory integration, the client uses:

- LDAP when inside the corporate firewall
- UDS when outside the corporate firewall



Note

LDAP is the default configuration, so it is not necessary to include the DirectoryServerType parameter in your client configuration file.

To ensure that the client can resolve contact photos from both inside and outside your corporate firewall, set the following parameters.

Parameter	Value
BDIPhotoUriWithToken	Contact photo URL when inside the corporate firewall
UdsPhotoUriWithToken	Contact photo URL when outside the corporate firewall

The following is an example configuration:

```
<Directory>
  <BDIPhotoUriWithToken>http://photo.example.com/sAMAccountName.jpg</BDIPhotoUriWithToken>
  <UdsPhotoUriWithToken>http://server-name/%%uid%%.jpg</UdsPhotoUriWithToken>
</Directory>
```

Simple Authentication for Cisco Jabber for Windows

Simple authentication lets you connect to a directory server using simple binds, as in the following example configuration:

```
<UseWindowsCredentials>0</UseWindowsCredentials>
<UseSSL>0</UseSSL>
<UseSecureConnection>0</UseSecureConnection>
<ConnectionUsername>username</ConnectionUsername>
<ConnectionPassword>password</ConnectionPassword>
```

This configuration specifies that the client:

- Does not use Microsoft Windows credentials.
- Does not use SSL.
- Uses simple authentication.
- Uses custom credentials.

As a result of the simple bind, the client transmits the credentials in the payload of the bind request in plain text.

Simple Authentication for Mobile Clients and Cisco Jabber for Mac

Simple authentication lets you connect to a directory server using simple binds, as in the following example configuration:

```
<BDIEnableTLS>False</BDIEnableTLS>
<BDIConnectionUsername>username</BDIConnectionUsername>
<BDIConnectionPassword>password</BDIConnectionPassword>
<BDIServerPort1>389/3268</BDIServerPort1>
```

This configuration specifies that the client:

- Does not use SSL.
- Uses simple authentication.
- Uses custom credentials.
- Uses port 389/3268 for non-TLS.

As a result of the simple bind, the client transmits the credentials in the payload of the bind request in plain text.

Simple Authentication with SSL for Cisco Jabber for Windows

Enable SSL in directory server connections with the UseSSL parameter. You can use SSL to encrypt credentials when you use simple authentication, as in the following example configuration:

```
<UseWindowsCredentials>0</UseWindowsCredentials>
<UseSSL>1</UseSSL>
<UseSecureConnection>0</UseSecureConnection>
<ConnectionUsername>username</ConnectionUsername>
<ConnectionPassword>password</ConnectionPassword>
```

This configuration specifies that the client:

- Does not use Microsoft Windows credentials.
- Uses SSL.
- Uses simple authentication.
- Uses custom credentials.

As a result, the client uses SSL to encrypt the credentials in the client configuration.

Simple Authentication with SSL for Mobile Clients

Enable SSL in directory server connections with the BDIEnableTLS parameter. You can use SSL to encrypt credentials when you use simple authentication, as in the following example configuration:

```
<BDIEnableTLS>True</BDIEnableTLS>
<BDIConnectionUsername>username</BDIConnectionUsername>
<BDIConnectionPassword>password</BDIConnectionPassword>
<BDIServerPort1>636/3269</BDIServerPort1>
```

This configuration specifies that the client:

- Uses SSL.
- Uses simple authentication.
- Uses custom credentials.
- Uses port 636/3269 for TLS.

As a result, the client uses SSL to encrypt the credentials in the client configuration.

OpenLDAP Integration

You can integrate with OpenLDAP using anonymous binds or authenticated binds.

Anonymous Binds for Cisco Jabber for Windows

To integrate with OpenLDAP using anonymous binds, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
ConnectionType	1
PrimaryServerName	IP address Hostname

Parameter	Value
UseWindowsCredentials	0
UseSecureConnection	1
SearchBase1	Root of the directory service or the organizational unit (OU)
UserAccountName	Unique identifier such as uid or cn
BaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
PredictiveSearchFilter	uid or other search filter

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>EDI</DirectoryServerType>
  <ConnectionType>1</ConnectionType>
  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <UseWindowsCredentials>0</UseWindowsCredentials>
  <UseSecureConnection>1</UseSecureConnection>
  <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
  <UserAccountName>uid</UserAccountName>
  <BaseFilter>(&!(objectClass=inetOrgPerson))</BaseFilter>
  <PredictiveSearchFilter>uid</PredictiveSearchFilter>
</Directory>
```

Anonymous Binds for Mobile Clients and Cisco Jabber for Mac

To integrate with OpenLDAP using anonymous binds, set the following parameters:

Parameter	Value
DirectoryServerType	BDI
BDILDAPServerType	OpenLDAP
BDIPrimaryServerName	IP address Hostname
BDIEnableTLS	True
BDISearchBase1	Root of the directory service or the organizational unit (OU)
BDIServerPort1	The port for the primary directory server
BDIUserAccountName	Unique identifier such as uid or cn
BDI BaseFilter	Object class that your directory service uses; for example, inetOrgPerson.

Parameter	Value
(Optional) BDIPredictiveSearchFilter	uid or other search filter

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>BDI</DirectoryServerType>
  <BDILDAPServerType>OpenLDAP</BDILDAPServerType>
  BDI<PrimaryServerName>11.22.33.456BDI</PrimaryServerName>
  BDI<BDIEnableTLS>True</BDIEnableTLS>
  BDI<SearchBase1>ou=people,dc=cisco,dc=comBDI</SearchBase1>
  BDI<ServerPort1>636/3269BDI</ServerPort1>
  BDI<UserAccountName>uidBDI</UserAccountName>
  BDI<BaseFilter>(&objectClass=inetOrgPerson)BDI</BaseFilter>
  BDI<PredictiveSearchFilter>uidBDI</PredictiveSearchFilter>
</Directory>
```

Authenticated Binds for Cisco Jabber for Windows

To integrate with OpenLDAP using authenticated binds, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
ConnectionType	1
PrimaryServerName	IP address Hostname
UseWindowsCredentials	0
UseSecureConnection	0
SearchBase1	Root of the directory service or the organizational unit (OU)
UserAccountName	Unique identifier such as uid or cn
BaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
PredictiveSearchFilter	uid or other search filter
ConnectionUsername	Username
ConnectionPassword	Password

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>EDI</DirectoryServerType>
  <ConnectionType>1</ConnectionType>
  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <UseWindowsCredentials>0</UseWindowsCredentials>
  <UseSecureConnection>0</UseSecureConnection>
  <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
  <UserAccountName>uid</UserAccountName>
  <BaseFilter>(&objectClass=inetOrgPerson)</BaseFilter>
  <PredictiveSearchFilter>uid</PredictiveSearchFilter>
  <ConnectionUsername>cn=lds-read-only-user,dc=cisco,dc=com</ConnectionUsername>
```

```
<ConnectionPassword>password</ConnectionPassword>
</Directory>
```

Authenticated Binds for Mobile Clients and Cisco Jabber for Mac

To integrate with OpenLDAP using authenticated binds, set the following parameters:

Parameter	Value
DirectoryServerType	BDI
BDILDAPServerType	OpenLDAP
BDIPrimaryServerName	IP address Hostname
BDIEnableTLS	False
BDISearchBase1	Root of the directory service or the organizational unit (OU)
BDIServerPort1	The port for the primary directory server
BDIUserName	Unique identifier such as uid or cn
BDIBaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
(Optional) BDIPredictiveSearchFilter	uid or other search filter
BDIConnectionUsername	Username
BDIConnectionPassword	Password

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>BDI</DirectoryServerType>
  <BDILDAPServerType>OpenLDAP</BDILDAPServerType>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIEnableTLS>False</BDIEnableTLS>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
  <BDIServerPort1>389/3268</BDIServerPort1>
  <BDIUserName>uid</BDIUserName>
  <BDIBaseFilter>(&!(objectClass=inetOrgPerson)</BDIBaseFilter>
  <BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>
  <BDIConnectionUsername>cn=administrator,dc=cisco,dc=com</BDIConnectionUsername>
  <BDIConnectionPassword>password</BDIConnectionPassword>
</Directory>
```

AD LDS Integration

You can integrate with AD LDS or ADAM using specific configurations.

Anonymous Binds for Cisco Jabber for Windows

To integrate with AD LDS or ADAM using anonymous binds, set the following parameters:

Parameter	Value
DirectoryServerType	EDI

Parameter	Value
PrimaryServerName	IP address Hostname
ServerPort1	Port number
UseWindowsCredentials	0
UseSecureConnection	1
SearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>EDI</DirectoryServerType>
  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <ServerPort1>50000</ServerPort1>
  <UseWindowsCredentials>0</UseWindowsCredentials>
  <UseSecureConnection>1</UseSecureConnection>
  <SearchBase1>dc=adam,dc=test</SearchBase1>
</Directory>
```

Anonymous Binds for Mobile Clients and Cisco Jabber for Mac

To integrate with AD LDS or ADAM using anonymous binds, set the following parameters:

Parameter	Value
BDIPrimaryServerName	IP address Hostname
BDIServerPort1	Port number
BDISearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIServerPort1>50000</BDIServerPort1>
  <BDISearchBase1>dc=adam,dc=test</BDISearchBase1>
</Directory>
```

Windows Principal User Authentication

To integrate with AD LDS or ADAM using authentication with the Microsoft Windows principal user, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
PrimaryServerName	IP address Hostname

Parameter	Value
ServerPort1	Port number
UseWindowsCredentials	0
UseSecureConnection	1
ConnectionUsername	Username
ConnectionPassword	Password
UserAccountName	Unique identifier such as uid or cn
SearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>EDI</DirectoryServerType>
  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <ServerPort1>50000</ServerPort1>
  <UseWindowsCredentials>0</UseWindowsCredentials>
  <UseSecureConnection>1</UseSecureConnection>
  <ConnectionUsername>cn=adminstrator,dc=cisco,dc=com</ConnectionUsername>
  <ConnectionPassword>password</ConnectionPassword>
  <UserAccountName>cn</UserAccountName>
  <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
</Directory>
```

AD LDS Principal User Authentication for Cisco Jabber for Windows

To integrate with AD LDS or ADAM using authentication with the AD LDS principal user, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
PrimaryServer	IP address Hostname
ServerPort1	Port number
UseWindowsCredentials	0
UseSecureConnection	0
ConnectionUsername	Username
ConnectionPassword	Password
UserAccountName	Unique identifier such as UID or CN
SearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>EDI</DirectoryServerType>
  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <ServerPort1>50000</ServerPort1>
  <UseWindowsCredentials>0</UseWindowsCredentials>
  <UseSecureConnection>0</UseSecureConnection>
  <ConnectionUsername>cn=administrator,dc=cisco,dc=com</ConnectionUsername>
  <ConnectionPassword>password</ConnectionPassword>
  <UserAccountName>cn</UserAccountName>
  <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
</Directory>
```

AD LDS Principal User Authentication for Mobile Clients and Cisco Jabber for Mac

To integrate with AD LDS or ADAM using authentication with the AD LDS principal user, set the following parameters:

Parameter	Value
BDIPrimaryServerName	IP address Hostname
BDIServerPort1	Port number
BDIConnectionUsername	Username
BDIConnectionPassword	Password
BDIUserAccountName	Unique identifier such as uid or cn
BDISearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIServerPort1>50000</BDIServerPort1>
  <BDIConnectionUsername>cn=administrator,dc=cisco,dc=com</BDIConnectionUsername>
  <BDIConnectionPassword>password</BDIConnectionPassword>
  <BDIUserAccountName>cn</BDIUserAccountName>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
</Directory>
```




Install the Clients

- [Install Cisco Jabber for Windows, page 193](#)
- [Install Cisco Jabber for Mac, page 213](#)
- [Install Cisco Jabber Mobile Clients, page 214](#)

Install Cisco Jabber for Windows

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

- **Use the Command Line**—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**—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.
- **Create a Custom Installer**—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**—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 9.x

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

Where:

`CLEAR=1` deletes any existing bootstrap file.
`/quiet` specifies a silent installation.

Cisco Unified Communications Manager 8.x in Default Mode

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP CUP_ADDRESS=1.2.3.4
```

Where:

`CLEAR=1` deletes any existing bootstrap file.
`AUTHENTICATOR=CUP` sets Cisco Unified Presence as the authenticator.
`CUP_ADDRESS=1.2.3.4` sets 1.2.3.4 as the IP address of the presence server.
`/quiet` specifies a silent installation.

Cisco Unified Communications Manager 8.x in Phone Mode

If you are integrating with UDS when you are installing in phone mode, you must first define the `<PresenceDomain>Domain address of your Presence server</PresenceDomain>` parameter.

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 PRODUCT_MODE=Phone_Mode AUTHENTICATOR=CUCM  
TFTP=1.2.3.4 CTI=5.6.7.8
```

Where:

`CLEAR=1` deletes any existing bootstrap file.
`PRODUCT_MODE=Phone_Mode` sets the client to phone mode.
`AUTHENTICATOR=CUCM` sets Cisco Unified Communications Manager as the authenticator.
`TFTP=1.2.3.4` sets 1.2.3.4 as the IP address of the TFTP server that hosts the client configuration.
`CTI=5.6.7.8` sets 5.6.7.8 as the IP address of the CTI server.
`/quiet` specifies a silent installation.

Cisco WebEx Messenger Service

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

Where:

CLEAR=1 deletes any existing bootstrap file.

AUTHENTICATOR=WEBEX sets the Cisco WebEx Messenger service as the authenticator.

/quiet specifies a silent installation.

Cisco WebEx Messenger Service with SSO

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=WEBEX
SSO_ORG_DOMAIN=example.com
```

Where:

CLEAR=1 deletes any existing bootstrap file.

AUTHENTICATOR=WEBEX sets the Cisco WebEx Messenger service as the authenticator.

SSO_ORG_DOMAIN=example.com sets example.com as the single sign-on (SSO) domain.

/quiet specifies a silent installation.

Command Line Arguments

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

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.

Cisco Unified Communications Manager Version 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.

Cisco Unified Communications Manager Version 8.x

You can specify phone mode during installation if you set Cisco Unified Communications Manager as the authenticator. The client reads the bootstrap file on the initial launch and determines it should start in phone mode. The client then gets Cisco Unified Communications Manager as the authenticator from the bootstrap file or manual settings. After the user signs in, the client does not require a restart.

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 Presence or Cisco Unified Communications Manager IM and Presence Service.
- **WebEx (IM and Presence)** the authenticator is the Cisco 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.

Change Product Modes with Cisco Unified Communications Manager Version 8.x

To change product modes with Cisco Unified Communications Manager version 8.x, you must reinstall Cisco Jabber for Windows to change the authenticator.

Change Default Mode > Phone Mode

Set the following arguments, at a minimum:

- CLEAR=1 to delete any existing bootstrap file.
- AUTHENTICATOR=CUCM to set the authenticator to Cisco Unified Communications Manager.
- PRODUCT_MODE=Phone_Mode to set phone mode as the product mode.

Change Phone Mode > Default Mode

Set the following arguments, at a minimum:

- CLEAR=1 to delete any existing bootstrap file.
- AUTHENTICATOR= one of the following:
 - CUP to set the authenticator to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.
 - WEBEX to set the authenticator to the Cisco WebEx Messenger service.

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 WEBEX	<p>Specifies the source of authentication for the client. This value is used if Service Discovery fails. Set one of the following as the value:</p> <ul style="list-style-type: none"> • CUP - Cisco Unified Presence. 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. • WEBEX - Cisco WebEx Messenger Service. Cloud-based or hybrid cloud-based deployments. <p>In on-premises deployments with Cisco Unified Communications Manager version 9.x and later, you should deploy the <code>_cisco-uds</code> SRV record. The client can then automatically determine the authenticator.</p>

Argument	Value	Description
CUP_ADDRESS	IP address Hostname FQDN	Specifies the address of Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service. Set one of the following as the value: <ul style="list-style-type: none"> • Hostname (<i>hostname</i>) • IP address (<i>123.45.254.1</i>) • FQDN (<i>hostname.domain.com</i>)
TFTP	IP address Hostname FQDN	Specifies the address of your TFTP server. Set one of the following as the value: <ul style="list-style-type: none"> • Hostname (<i>hostname</i>) • IP address (<i>123.45.254.1</i>) • FQDN (<i>hostname.domain.com</i>) <p>You should specify this argument if you set Cisco Unified Communications Manager as the authenticator.</p> <p>If you deploy:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • You set Cisco Unified Communications Manager as the authenticator. • The address of your CCMCIP server is not the same as the TFTP server address. <p>The client can locate the CCMCIP server with the TFTP server address if both addresses are the same.</p>

Argument	Value	Description
SERVICES_DOMAIN	Domain	<p>Sets the value of the domain where the DNS SRV records for Service Discovery reside.</p> <p>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.</p>
VOICE_SERVICES_DOMAIN	Domain	<p>In Hybrid Deployments the domain required to discover Webex via CAS lookup may be a different domain than where the DNS records are deployed. If this is the case then set the SERVICES_DOMAIN to be the domain used for Webex discovery (or let the user enter an email address) and set the VOICE_SERVICES_DOMAIN to be the domain where DNS records are deployed. If this setting is specified, the client will use the value of VOICE_SERVICES_DOMAIN to lookup the following DNS records for the purposes of Service Discovery and Edge Detection:</p> <ul style="list-style-type: none"> • _cisco-uds • _cuplogin • _collab-edge <p>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.</p>

Argument	Value	Description
EXCLUDED_SERVICES	One or more of: <ul style="list-style-type: none"> • CUP • WEBEX • CUCM 	<p>Lists the services that you want Jabber to exclude from Service Discovery. For example, you may have done a trial with WebEx which means that your company domain is registered on WebEx, but you do not want Jabber users to authenticate using WebEx. You want Jabber to authenticate with an on-premises CUP server. In this case set:</p> <ul style="list-style-type: none"> • EXCLUDED_SERVICES=WEBEX <p>Possible values are CUP, CUCM, WEBEX.</p> <p>To exclude more than one service, use comma separated values. For example, to exclude CUP and CUCM, specify: EXCLUDED_SERVICES=CUP,CUCM. To exclude all services, specify: EXCLUDED_SERVICES=CUP,CUCM,WEBEX</p> <p>If you exclude all services, you need to use manual configuration or bootstrap configuration to configure the Jabber client.</p>
UPN_DISCOVERY_ENABLED	true false	<p>Cisco Jabber for Windows only.</p> <p>Allows you to define whether the client uses the User Principal Name (UPN) of a Windows session to get the domain for a user when discovering services.</p> <ul style="list-style-type: none"> • true (default) - The UPN is used to find the domain of the user, which is used during service discovery. • false - The UPN is not used to find the domain of the user. The user is prompted to enter credentials to find the domain for service discovery. <p>Example installation command: <code>msiexec.exe /i CiscoJabberSetup.msi /quiet UPN_DISCOVERY_ENABLED=false</code></p>

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 command line arguments that are common to all deployments:

Argument	Value	Description
LANGUAGE	LCID in decimal	<p>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.</p> <p>For example, you can specify one of the following:</p> <ul style="list-style-type: none"> • 1033 specifies English. • 1036 specifies French. <p>This argument is optional. If you do not specify a value, Cisco Jabber for Windows uses the system locale language as the default.</p> <p>See the <i>Supported Languages</i> topic for a full list of the languages you can specify.</p>
FORGOT_PASSWORD_URL	URL	<p>Specifies the URL where users can reset lost or forgotten passwords.</p> <p>This argument is optional but recommended.</p> <p>Note In cloud-based deployments, you can specify a forgot password URL using the Cisco WebEx Administration Tool. However, the client cannot retrieve that forgot password URL until users sign in.</p>
TFTP_FILE_NAME	Filename	<p>Specifies the unique name of a group configuration file.</p> <p>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.</p> <p>This argument is optional.</p> <p>Remember You can specify group configuration files in the Cisco Support Field on the CSF device configuration on Cisco Unified Communications Manager.</p>

Argument	Value	Description
LOGIN_RESOURCE	WBX MUT	<p>Controls user sign in to multiple client instances.</p> <p>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:</p> <p>WBX</p> <p>Users can sign in to one instance of Cisco Jabber for Windows at a time.</p> <p>Cisco Jabber for Windows appends the <code>wbxconnect</code> suffix to the user's JID. Users cannot sign in to any other Cisco Jabber client that uses the <code>wbxconnect</code> suffix.</p> <p>MUT</p> <p>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.</p> <p>Each instance of Cisco Jabber for Windows appends the user's JID with a unique suffix.</p>
LOG_DIRECTORY	Absolute path on the local filesystem	<p>Defines the directory where the client writes log files.</p> <p>Use quotation marks to escape space characters in the path, as in the following example:</p> <pre>"C:\my_directory\Log Directory"</pre> <p>The path you specify must not contain Windows invalid characters.</p> <p>The default value is</p> <pre>%USER_PROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs</pre>
CLICK2X	DISABLE	<p>Disables click-to-x functionality with Cisco Jabber.</p> <p>If you specify this argument during installation,</p> <ul style="list-style-type: none"> • The client does not register as a handler for click-to-x functionality with the operating system. <p>In effect, this argument prevents the client from writing to the Microsoft Windows registry during installation.</p> <ul style="list-style-type: none"> • You must re-install the client and omit this argument to enable click-to-x functionality with the client after installation.

SSO Arguments

This section describes the command line arguments you can use to deploy Cisco Jabber for Windows with single sign on (SSO) capabilities.

Cloud-Based SSO Arguments

The arguments in the following table apply to cloud-based deployments only:

Argument	Value	Description
SSO_ORG_DOMAIN	Domain name	<p>Specifies the domain name for the Cisco WebEx Org that contains the URL for the SSO service.</p> <p>Cisco Jabber for Windows uses this argument to retrieve the URL of the SSO service from the Org. When Cisco Jabber for Windows gets the SSO service URL, it can request login tokens to authenticate with Cisco WebEx Messenger.</p> <p>Note You specify the URL for the SSO service as the value of the Customer SSO Service Login URL in the Cisco WebEx Administration Tool.</p>

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.

Related Topics

[Microsoft Windows SDK for Windows 7 and .NET Framework 4](#)

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 Cisco.com.
 - Step 2** Copy `CiscoJabberProperties.mst` from the Cisco Jabber administration package to your file system.
-

Related Topics

[Software Downloads](#)

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.

Procedure

-
- Step 1** Start Microsoft Orca.
 - Step 2** Open `CiscoJabberSetup.msi` and then apply `CiscoJabberProperties.mst`.
 - 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*.

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.

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 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.

- Step 7** Drop any properties that you do not require.
It is essential to drop any properties that are not being set, otherwise the properties being set will not take effect. Drop each property that is not needed one at a time.
- Right-click the property you want to drop.
 - Select **Drop Row**.
 - Select **OK** when Microsoft Orca prompts you to continue.
- Step 8** Enable your custom installer to save embedded streams.
- Select **Tools > Options**.
 - Select the **Database** tab.
 - Select **Copy embedded streams during 'Save As'**.
 - Select **Apply** and then **OK**.
- Step 9** Save your custom installer.
- Select **File > Save Transformed As**.
 - Select a location on your file system to save the installer.
 - Specify a name for the installer and then select **Save**.
-

Related Topics

[Installer Properties, on page 208](#)

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.

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.

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** 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**.
-

Related Topics

[Supported Languages](#), on page 211

Deploy the Client with Group Policy

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

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.
- Right-click on the appropriate domain in the left pane.
 - Select **Create a GPO in this Domain, and Link it here**.
The **New GPO** window opens.
 - Enter a name for the group policy object in the **Name** field.
 - 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.
- Select the group policy object under the domain in the left pane.
The group policy object displays in the right pane.
 - Select **Add** in the **Security Filtering** section of the **Scope** tab.
The **Select User, Computer, or Group** window opens.
 - Specify the computers and users to which you want to deploy Cisco Jabber for Windows.
- Step 5** Specify the installation package.
- Right-click the group policy object in the left pane and then select **Edit**.
The **Group Policy Management Editor** opens.
 - Select **Computer Configuration** and then select **Policies > Software Settings**.
 - Right-click **Software Installation** and then select **New > Package**.
 - 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.
 - 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.

Supported Languages

The following table lists the languages that Cisco Jabber for Windows supports. You can change the language that your client uses by changing the language setting in your operating system Control Panel. After you select the language, restart your computer, and the Cisco Jabber client will automatically update its language settings to match your system language selection.

Arabic	French	Romanian
Bulgarian	Hebrew	Russian
Catalan	Hungarian	Serbian
Croatian	Italian	Slovak
Czech	Japanese	Slovenian
Danish	Korean	Swedish
German	Norwegian	Thai
Greek	Dutch	Turkish
English	Polish	Chinese - China
Spanish	Portuguese - Brazil	Chinese - Taiwan
Finnish	Portuguese - Portugal	



Note

Cisco Jabber for Windows does not support Locale IDs for all sub-languages. For example, if you specify French - Canada, Cisco Jabber for Windows uses French - France.

See the following documentation for more information about Locale IDs:

- *Microsoft Windows Locale Code Identifier (LCID) Reference*
- *Locale IDs Assigned by Microsoft*

Related Topics

- [Microsoft Windows Locale Code Identifier \(LCID\) Reference](#)
- [Locale IDs Assigned by Microsoft](#)

Cisco Media Services Interface

Cisco Jabber for Windows supports Cisco Media Services Interface version 4.1.2 for Microsoft Windows 7 and later.

Desk Phone Video Capabilities

You must install Cisco Media Services Interface to enable desk phone video capabilities. Cisco Media Services Interface provides a driver that enables Cisco Jabber for Windows to do the following:

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

Install Cisco Media Services Interface

Procedure

- Step 1** Download the **Cisco Media Services Interface** installation program from the download site on Cisco.com.
- Step 2** Install Cisco Media Services Interface on each computer on which you install Cisco Jabber. See the appropriate Cisco Medianet documentation for installing Cisco Media Services Interface.
-

Related Topics

- [Download software](#)
- [Medianet Knowledge Base Portal](#)

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.
- Open the Microsoft Windows registry editor.
  - Locate the following registry key: `HKEY_CLASSES_ROOT\Installer\Products`
  - Select **Edit > Find**.
  - Enter Cisco Jabber in the **Find what** text box in the **Find** window and select **Find Next**.
  - 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

## Prepare Your Network

To install Cisco Media Services Interface for traffic marking, you must prepare your network.

### Procedure

---

- Step 1** Install Cisco Prime Collaboration Manager.
- Step 2** Install routers or switches enabled for Cisco Medianet where appropriate.
- Step 3** Configure your network to handle the metadata attributes that Cisco Media Services Interface applies to applications.  
Not all devices on your network must support Cisco Medianet.

The first hop should prioritize traffic based on the metadata attributes from Cisco Media Services Interface. As the traffic traverses the network, all other devices should also prioritize that traffic unless you configure policies on those devices to handle the traffic differently.

---

## Distribute the Cisco Jabber for Mac client

Visit the [Cisco Software Center](#) to download the Cisco Jabber for Mac client.

Upgrading in the Mac OS X environment is performed automatically by the application, with permission from the user.

## 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.
-



## Remote Access

- [Expressway for Mobile and Remote Access Deployments](#), page 215
- [Cisco AnyConnect Deployments](#), page 223
- [Survivable Remote Site Telephony](#), page 234

### Expressway for Mobile and Remote Access Deployments

Expressway for Mobile and Remote Access for Cisco Unified Communications Manager allows users to access their collaboration tools from outside the corporate firewall without a VPN client. Using Cisco collaboration gateways, the client can connect securely to your corporate network from remote locations such as public Wi-Fi networks or mobile data networks.

You must do the following to set up the Expressway for Mobile and Remote Access feature:

- 1 Set up servers to support Expressway for Mobile and Remote Access using Cisco Expressway-E and Cisco Expressway-C.\*
  - a See the following documents to set up the Cisco Expressway servers:
    - *Cisco Expressway Basic Configuration Deployment Guide*
    - *Mobile and Remote Access via Cisco Expressway Deployment Guide*

\* If you currently deploy a Cisco TelePresence Video Communications Server (VCS) environment, you can set up Expressway for Mobile and Remote Access. For more information, see *Cisco VCS Basic Configuration (Control with Expressway) Deployment Guide* and *Mobile and Remote Access via Cisco VCS Deployment Guide*.

- b Add any relevant servers to the whitelist for your Cisco Expressway-C server to ensure that the client can access services that are located inside the corporate network.

To add a server to the Cisco Expressway-C whitelist, use the **HTTP server allow** setting.

This list can include the servers on which you host voicemail or contact photos.

- 2 Configure an external DNS server that contains the `_collab-edge` DNS SRV record to allow the client locate the Expressway for Mobile and Remote Access server.

- 3 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, ensure that you configure the Voice Services Domain.

The Voice Services Domain allows the client to locate the DNS server that contains the `_collab-edge` record.

You can configure the voice services domain using one of the following methods:

- Client configuration file (all Cisco Jabber clients)
- Configuration URL (all Cisco Jabber clients except Cisco Jabber for Windows)
- Installer options (Cisco Jabber for Windows only)



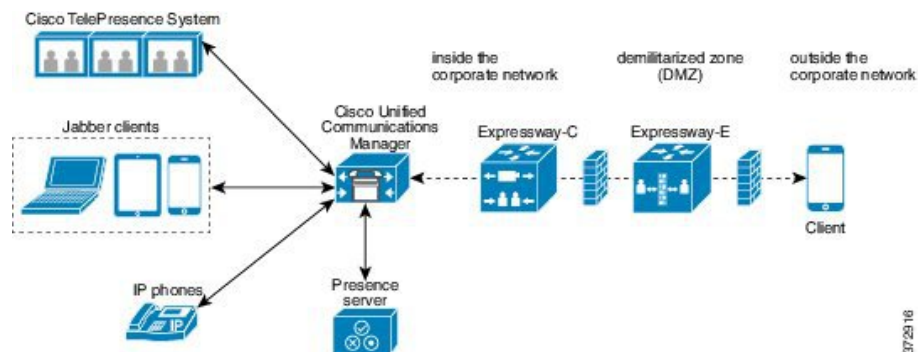
### Important

In most cases, users can sign in to the client for the first time using Expressway for Mobile and Remote Access to connect to services from outside the corporate firewall. In the following cases, however, users must perform initial sign in while on the corporate network:

- If the voice services domain is different from the services domain. In this case, users must be inside the corporate network to get the correct voice services domain from the `jabber-config.xml` file.
- If the client needs to complete the CAPF enrollment process, which is required when using a secure or mixed mode cluster.

The following diagram illustrates the architecture of an Expressway for Mobile and Remote Access environment for Cisco Jabber for Android.

**Figure 1: Cisco Jabber for Android Architecture Diagram**

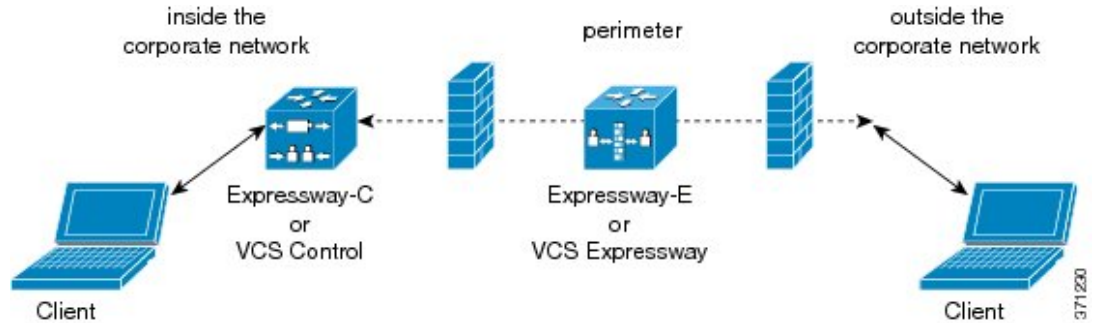


37/23/16



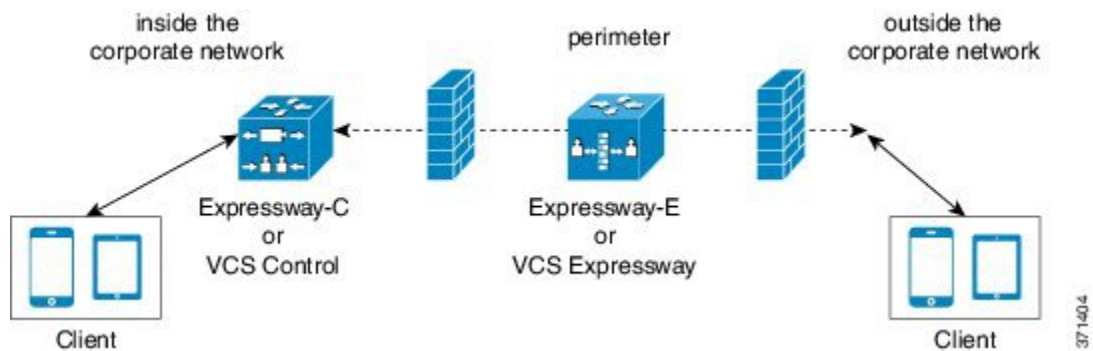
The following diagram illustrates the architecture of an Expressway for Mobile and Remote Access environment for Cisco Jabber for Windows and Mac.

**Figure 2: Cisco Jabber for Windows and Mac Architecture Diagram**



The following diagram illustrates the architecture of an Expressway for Mobile and Remote Access environment for Cisco Jabber for iPhone and iPad.

**Figure 3: Cisco Jabber for iPhone and iPad Architecture Diagram**



**Related Topics**

- [Cisco Expressway Configuration Guides](#)
- [Cisco VCS Configuration Guides](#)

## Supported Services

The following table summarizes the services and functionality that are supported when the client uses Expressway for Mobile and Remote Access to remotely connect to Cisco Unified Communications Manager.

**Table 1: Summary of supported services for Expressway for Mobile and Remote Access**

| Service              | Supported | Unsupported |
|----------------------|-----------|-------------|
| <b>Directory</b>     |           |             |
| UDS directory search | X         |             |

| Service                               |                                                               | Supported                                                                                                                                                  | Unsupported |
|---------------------------------------|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
|                                       | LDAP directory search                                         |                                                                                                                                                            | X           |
|                                       | Directory photo resolution                                    | X<br>* Using HTTP white list on Cisco Expressway-C                                                                                                         |             |
|                                       | Intradomain federation                                        | X<br>* Contact search support depends of the format of your contact IDs. For more information, see the note below.                                         |             |
|                                       | Interdomain federation                                        | X                                                                                                                                                          |             |
| <b>Instant Messaging and Presence</b> |                                                               |                                                                                                                                                            |             |
|                                       | On-premises                                                   | X                                                                                                                                                          |             |
|                                       | Cloud                                                         | X                                                                                                                                                          |             |
|                                       | Chat                                                          | X                                                                                                                                                          |             |
|                                       | Group chat                                                    | X                                                                                                                                                          |             |
|                                       | High Availability: On-premises deployments                    | X                                                                                                                                                          |             |
|                                       | File transfer: On-premises deployments (desktop clients only) | X<br>Advanced options available for file transfer using Cisco Unified Communications Manager IM and Presence Service 10.5(2) or later, see the note below. | X           |
|                                       | File transfer: Cloud deployments (desktop clients only)       | X<br>Desktop clients, some file transfer features are supported for mobile clients.                                                                        |             |

| Service                                         |                                                     | Supported                                                      | Unsupported                                |
|-------------------------------------------------|-----------------------------------------------------|----------------------------------------------------------------|--------------------------------------------|
|                                                 | Video screen share - BFCP                           | X (Cisco Jabber for mobile clients only support BFCP receive.) |                                            |
| <b>Audio and Video</b>                          |                                                     |                                                                |                                            |
|                                                 | Audio and video calls                               | X<br>* Cisco Unified Communications Manager 9.1(2) and later   |                                            |
|                                                 | Deskphone control mode (CTI) (desktop clients only) |                                                                | X                                          |
|                                                 | Extend and connect (desktop clients only)           |                                                                | X                                          |
|                                                 | Dial via Office - Reverse (mobile clients only)     |                                                                | X                                          |
|                                                 | Session persistency                                 |                                                                | X                                          |
|                                                 | Early media                                         |                                                                | X                                          |
|                                                 | Self Care Portal access                             |                                                                | X                                          |
| <b>Voicemail</b>                                |                                                     |                                                                |                                            |
|                                                 | Visual voicemail                                    | X<br>* Using HTTP white list on Cisco Expressway-C             |                                            |
| <b>Cisco WebEx Meetings</b>                     |                                                     |                                                                |                                            |
|                                                 | On-premises                                         |                                                                | X                                          |
|                                                 | Cloud                                               | X                                                              |                                            |
|                                                 | Cisco WebEx screen share (desktop clients only)     | X                                                              |                                            |
| <b>Installation (Desktop clients)</b>           |                                                     |                                                                |                                            |
|                                                 | Installer update                                    | X<br>* Using HTTP white list on Cisco Expressway-C             | X<br>Not supported on Cisco Jabber for Mac |
| <b>Customization (Cisco Jabber for Windows)</b> |                                                     |                                                                |                                            |

| Service                                       |                           | Supported                                          | Unsupported |
|-----------------------------------------------|---------------------------|----------------------------------------------------|-------------|
|                                               | Custom HTML tabs          | X<br>* Using HTTP white list on Cisco Expressway-C |             |
| <b>Security</b>                               |                           |                                                    |             |
|                                               | End-to-end encryption     |                                                    | X           |
|                                               | CAPF enrollment           |                                                    | X           |
| <b>Troubleshooting (Desktop clients only)</b> |                           |                                                    |             |
|                                               | Problem report generation | X                                                  |             |
|                                               | Problem report upload     |                                                    | X           |
| <b>High Availability (failover)</b>           |                           |                                                    |             |
|                                               | Audio and Video services  |                                                    | X           |
|                                               | Voicemail services        |                                                    | X           |
|                                               | IM and Presence services  | X                                                  |             |

## Directory

When the client connects to services using Expressway for Mobile and Remote Access, it supports directory integration with the following limitations.

- LDAP contact resolution — The client cannot use LDAP for contact resolution when outside of the corporate firewall. Instead, the client must use UDS for contact resolution.  
When users are inside the corporate firewall, the client can use either UDS or LDAP for contact resolution. If you deploy LDAP within the corporate firewall, Cisco recommends that you synchronize your LDAP directory server with Cisco Unified Communications Manager to allow the client to connect with UDS when users are outside the corporate firewall.
- Directory photo resolution — To ensure that the client can download contact photos, you must add the server on which you host contact photos to the white list of your Cisco Expressway-C server. To add a server to Cisco Expressway-C white list, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.
- Intradomain federation — 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
  - UserPrincipalName (UPN)@domain
  - EmailAddress@domain

- employeeNumber@domain
- telephoneNumber@domain

### Instant Messaging and Presence

When the client connects to services using Expressway for Mobile and Remote Access, it supports instant messaging and presence with the following limitations:

File transfer has the following limitations for desktop clients:

- For Cisco WebEx cloud deployments, file transfer is supported.
- For on-premises deployments with Cisco Unified Communication IM and Presence Service 10.5(2) or later, the **Managed File Transfer** selection is supported, however the **Peer-to-Peer** option is not supported.
- For on-premises deployments with Cisco Unified Communications Manager IM and Presence Service 10.0(1) or earlier deployments, file transfer is not supported.

### Audio and Video Calling

When the client connects to services using Expressway for Mobile and Remote Access, it supports voice and video calling with the following limitations.

- Cisco Unified Communications Manager — Expressway for Mobile and Remote Access supports video and voice calling with Cisco Unified Communications Manager Version 9.1.2 and later. Expressway for Mobile and Remote Access is not supported with Cisco Unified Communications Manager Version 8.x.
- Deskphone control mode (CTI) (Desktop clients only) — The client does not support deskphone control mode (CTI), including extension mobility.
- Extend and connect (Desktop clients only) — The client cannot be used to:
  - Make and receive calls on a Cisco IP Phone in the office.
  - Perform mid-call control such as hold and resume on a home phone, hotel phone, or Cisco IP Phone in the office.
- Dial via Office - Reverse (Mobile clients only) — The client cannot make Dial via Office - Reverse calls from outside the firewall.
- Session Persistency — The client cannot recover from audio and video calls drop when a network transition occurs. For example, if a users start a Cisco Jabber call inside their office and then they walk outside their building and lose Wi-Fi connectivity, the call drops as the client switches to use Expressway for Mobile and Remote Access.
- Early Media — Early Media allows the client to exchange data between endpoints before a connection is established. For example, if a user makes a call to a party that is not part of the same organization, and the other party declines or does not answer the call, Early Media ensures that the user hears the busy tone or is sent to voicemail.

When using Expressway for Mobile and Remote Access, the user does not hear a busy tone if the other party declines or does not answer the call. Instead, the user hears approximately one minute of silence before the call is terminated.

- Self care portal access (Desktop clients only) — Users cannot access the Cisco Unified Communications Manager Self Care Portal when outside the firewall. The Cisco Unified Communications Manager user page cannot be accessed externally.

Cisco Expressway-E proxies all communications between the client and unified communications services inside the firewall. However, the Cisco Expressway-E does not proxy services that are accessed from a browser that is not part of the Cisco Jabber application.

### Voicemail

Voicemail service is supported when the client connects to services using Expressway for Mobile and Remote Access.



#### Note

To ensure that the client can access voicemail services, you must add the voicemail server to the white list of your Cisco Expressway-C server. To add a server to Cisco Expressway-C white list, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.

### Cisco WebEx Meetings

When the client connects to services using Expressway for Mobile and Remote Access, it supports only cloud-based conferencing using Cisco WebEx Meetings Center.

The client cannot access the Cisco WebEx Meetings Server or join or start on-premises Cisco WebEx meetings.

### Installation

Cisco Jabber for Mac — When the client connects to services using Expressway for Mobile and Remote Access, it doesn't support installer updates.

Cisco Jabber for Windows — When the client connects to services using Expressway for Mobile and Remote Access, it supports installer updates.



#### Note

To ensure that the client can download installer updates, you must add the server that hosts the installer updates to the white list of your Cisco Expressway-C server. To add a server to the Cisco Expressway-C white list, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.

### Customization

Cisco Jabber for Windows only. When the client connects to services using Expressway for Mobile and Remote Access, it supports custom HTML tab configuration for desktop clients.



#### Note

To ensure that the client can download the custom HTML tab configuration, you must add the server that hosts the custom HTML tab configuration to the white list of your Cisco Expressway-C server. To add a server to the Cisco Expressway-C whitelist, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.

## Security

When the client connects to services using Expressway for Mobile and Remote Access, it supports most security features with the following limitations.

- Initial CAPF enrollment — Certificate Authority Proxy Function (CAPF) enrollment is a security service that runs on the Cisco Unified Communications Manager Publisher that issues certificates to Cisco Jabber (or other clients). To successfully enrol for CAPF, the client must connect from inside the firewall or using VPN.
- End-to-end encryption — When users connect through Expressway for Mobile and Remote Access and participate in a call:
  - Media is encrypted on the call path between the Cisco Expressway-C and devices that are registered to the Cisco Unified Communications Manager using Expressway for Mobile and Remote Access.
  - Media is not encrypted on the call path between the Cisco Expressway-C and devices that are registered locally to Cisco Unified Communications Manager, if either Cisco Jabber or an internal device is not configured with Encrypted security mode.
  - Media is encrypted on the call path between the Expressway-C and devices that are registered locally to Cisco Unified Communication Manager, if both Cisco Jabber and internal device are configured with Encrypted security mode.

## Troubleshooting

Cisco Jabber for Windows only. Problem report upload — When the desktop client connects to services using Expressway for Mobile and Remote Access, it cannot send problem reports because the client uploads problem reports over HTTPS to a specified internal server.

To work around this issue, users can save the report locally and send the report in another manner.

## High Availability (failover)

High Availability means that if the client fails to connect to the primary server, it fails over to a secondary server with little or no interruption to the service. In relation to high availability being supported on the Expressway for Mobile and Remote Access, high availability refers to the server for the specific service failing over to a secondary server (such as Instant Messaging and Presence), and not the Cisco Expressway-E server itself failing over.

Some services are available on the Expressway for Mobile and Remote Access that are not supported for high availability. This means that if users are connected to the client from outside the corporate network and the instant messaging and presence server fails over, the services will continue to work as normal. However, if the audio and video server or voicemail server fails over, those services will not work as the relevant servers do not support high availability.

# Cisco AnyConnect Deployments

Cisco AnyConnect refers to a server-client infrastructure that enables the client to connect securely to your corporate network from remote locations such as Wi-Fi networks or mobile data networks.

The Cisco AnyConnect environment includes the following components:

### Cisco Adaptive Security Appliance

Provides a service to secure remote access.

### Cisco AnyConnect Secure Mobility Client

Establishes a secure connection to Cisco Adaptive Security Appliance from the user's device.

For information about requirements for Cisco Adaptive Security Appliance and Cisco AnyConnect Secure Mobility Client, see the *Software Requirements* topic.

## Cisco AnyConnect Deployment Considerations

Cisco Adaptive Security Appliance provides a flexible architecture that can meet the needs of many different deployments. It is beyond the scope of this document to provide end-to-end deployment procedures. Rather, the purpose of this section is to provide information that you should consider when deploying Cisco Adaptive Security Appliance and Cisco AnyConnect Secure Mobility Client for Cisco Jabber for iPhone.

Cisco Adaptive Security Appliance provides a flexible architecture that can meet the needs of many different deployments. It is beyond the scope of this document to provide end-to-end deployment procedures. Rather, the purpose of this section is to provide information that you should consider when deploying Cisco Adaptive Security Appliance and Cisco AnyConnect Secure Mobility Client for Cisco Jabber for Android.

Cisco Adaptive Security Appliance provides a flexible architecture that can meet the needs of many different deployments. It is beyond the scope of this document to provide end-to-end deployment procedures. Rather, the purpose of this section is to provide information that you should consider when deploying Cisco Adaptive Security Appliance and Cisco AnyConnect Secure Mobility Client for Cisco Jabber for iPhone and iPad .

You should refer to the configuration guides for Cisco Adaptive Security Appliance to obtain task-based information on installing and configuring Cisco Adaptive Security Appliance.



---

**Note**

Cisco supports Cisco Jabber for iPhone with Cisco AnyConnect Secure Mobility Client. Although other VPN clients are not officially supported, you may be able to use Cisco Jabber for iPhone with other VPN clients. If you use another VPN client, set up VPN as follows:

- 1 Install and configure the VPN client using the relevant third-party documentation.
- 2 Set up On-Demand VPN using the *Set Up Automatic VPN Access on the Cisco Unified Communications Manager* topic.

**Note**

Cisco supports Cisco Jabber for Android with Cisco AnyConnect Secure Mobility Client. Although other VPN clients are not officially supported, you may be able to use Cisco Jabber for Android with other VPN clients. If you use another VPN client, install and configure the VPN client using the relevant third-party documentation.

---



**Note**

Cisco supports Cisco Jabber for iPhone and iPad with Cisco AnyConnect Secure Mobility Client. Although other VPN clients are not officially supported, you may be able to use Cisco Jabber for iPhone and iPad with other VPN clients. If you use another VPN client, set up VPN as follows:

- 1 Install and configure the VPN client using the relevant third-party documentation.
- 2 Set up On-Demand VPN using the *Set Up Automatic VPN Access on the Cisco Unified Communications Manager* topic.

## Application Profiles

After users 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 in one of the following ways:

### ASDM

Cisco recommends 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.

You can provision application profiles for Cisco Jabber for iPhone and iPad in one of the following ways:

## ASDM

Cisco recommends 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**

---

VPN will not be launched because Expressway for Mobile and Remote Access has the higher connection priority even if VPN is set to automatic connection.

---

## 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 will cause the client to launch VPN on Demand.

### Connect if Needed

- Configure Cisco Unified Communications Manager to be accessed 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 (for example, ccm-sjc-111.cisco.com). 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 this 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.

## Set Up Certificate-Based Authentication

Cisco recommends that you use certificate-based authentication for negotiating a secure connection to Cisco Adaptive Security Appliance from Cisco AnyConnect Secure Mobility Client.

ASA supports certificates issued by standard Certificate Authority (CA) servers such as Cisco IOS CA, Microsoft Windows 2003, Windows 2008R2, Entrust, VeriSign, and RSA Keon. This topic gives you a high-level procedure for setting up ASA for certificate-based authentication. See the *Configuring Digital Certificates* topic in the appropriate ASA configuration guide for step-by-step instructions.

### Procedure

---

**Step 1** Import a root certificate from the CA to the ASA.

**Step 2** Generate an identity certificate for the ASA.

**Step 3** Use the ASA identity certificate for SSL authentication.

**Step 4** Configure a Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP).

**Step 5** Configure the ASA to request client certificates for authentication.

---

## What to Do Next

After you set up certificate-based authentication on ASA, you must distribute certificates to your users. You can use one of the following methods:

- *Distribute Certificates with SCEP*
- *Distribute Client Certificate with Mobileconfig File*

After you set up certificate-based authentication on ASA, you must distribute certificates to your users. See the *Distribute Certificates with SCEP* topic.

After you set up certificate-based authentication on ASA, you must distribute certificates to your users. You can use one of the following methods:

- *Distribute Certificates with SCEP*
- *Distribute Client Certificate with Mobileconfig File*

## Distribute Certificates with SCEP

You can use Simple Certificate Enrollment Protocol (SCEP) on Microsoft Windows Server to securely issue and renew certificates for client authentication.

To distribute certificates with SCEP, you must install the SCEP module on Microsoft Windows Server. See the following topics for more information:

- *ASA 8.X: AnyConnect SCEP Enrollment Configuration Example*
- *Simple Certificate Enrollment Protocol (SCEP) Add-on for Certificate Services*

## Distribute Client Certificate with Mobileconfig File

Use this procedure to create a mobile configuration file that includes a certificate. You can use this file to distribute the certificate to users.

### Procedure

- 
- Step 1** Use the iPCU software to create a mobileconfig file and include the certificate (.pfx) file.
  - Step 2** Forward the mobileconfig file to the user.
  - Step 3** Use the Cisco ISE native supplicant provisioning process to distribute user certificates.
  - Step 4** Use the Enterprise MDM software to provision and publish certificates to registered devices.
- 

## 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

Cisco recommends 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*.

---

## Group Policies and Profiles

You should use the ASA Device Manager (ASDM) to create group policies, client profiles, and connection profiles. Create your group policies first and then apply those policies to the profiles. Using the ASDM to create profiles ensures that Cisco AnyConnect Secure Mobility Client downloads the profiles after it establishes a connection to ASA for the first time. The ASDM also lets you manage and maintain your policies and profiles in a central location.

See the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for instructions on creating policies and profiles with the ASDM.

## Trusted Network Detection

Trusted Network Detection is a feature that automates secure connections based on user location. When users leave the corporate network, Cisco AnyConnect Secure Mobility Client automatically detects that it is outside the trusted network and then initiates secure access.

You configure Trusted Network Detection on ASA as part of the client profile. For more information, see the *Trusted Network Detection* topic in the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

## Tunnel Policies

Tunnel policies configure how Cisco AnyConnect Secure Mobility Client directs traffic over a secure connection and include the following:

### Full Tunnel Policy

Lets you send all traffic over the secure connection to the ASA gateway.

### Split Include Policy with Network ACL

Enables you to restrict secure connections based on destination IP addresses. For example, in an on-premises deployment, you can specify the IP addresses for Cisco Unified Communications Manager, Cisco Unified Presence, your TFTP server, and other servers to restrict the secure connection only to your client's traffic.

### Split Exclude Policy

Allows you to exclude certain traffic from the secure connection. You can allow client traffic over the secure connection and then exclude traffic from specific destination subnets.

# Survivable Remote Site Telephony

When the Cisco Unified Communication Manager application is unreachable or the WAN is down, use Cisco Unified Survivable Remote Site Telephony (SRST) to retain basic telephony services for your remote Cisco Jabber users. When connectivity is lost, Cisco Jabber fails over to the local router at the remote site.



---

**Note**

SRST versions 8.5 and 8.6 are supported.

---

SRST provides basic call control, when a system is in failover only start, end, hold, resume, mute, unmute, and dual-tone multi-frequency signaling [DTMF]) are enabled.

The following services are not available during failover:

- Video
- Mid-call features (transfer, iDivert, call park, conferencing, send to mobile)
- Dial via Office (DvO)
- Ad hoc conferencing
- Binary Floor Control Protocol (BFCP) sharing

For detailed instructions about configuring SRST, see the relevant release of the *Cisco Unified Communication Manager Administration Guide*.



## Cisco Jabber Features and Options

- [Cisco Jabber Features](#), page 235
- [Cisco Jabber Features for Windows, Mac, iOS and Android](#), page 237
- [Cisco Jabber Features for Windows](#) , page 249
- [Cisco Jabber Features for Mac](#), page 269
- [Cisco Jabber for Android and iOS](#), page 269
- [Cisco Jabber for iOS, Android and Windows](#), page 283

### Cisco Jabber Features

Cisco Jabber includes a broad range of features. As indicated in the following table, some features are client-specific.

| Feature              | Cisco Jabber for Windows | Cisco Jabber for Mac | Cisco Jabber for Android, Cisco Jabber for iPhone and iPad |
|----------------------|--------------------------|----------------------|------------------------------------------------------------|
| Alert When Available | X                        |                      |                                                            |
| Automatic Upgrades   | X                        | X                    | X                                                          |
| Auto-Save Chat       | X                        |                      |                                                            |
| Call Pickup          | X                        |                      |                                                            |
| Call Park            |                          |                      | X                                                          |
| Call Preservation    | X                        | X                    | X                                                          |
| Chat Search          | X                        |                      |                                                            |
| Chat Security Labels | X                        |                      |                                                            |

| Feature                             | Cisco Jabber for Windows | Cisco Jabber for Mac | Cisco Jabber for Android, Cisco Jabber for iPhone and iPad |
|-------------------------------------|--------------------------|----------------------|------------------------------------------------------------|
| Cisco WebEx Meetings integration    | X                        | X                    | X                                                          |
| Custom Contact                      | X                        | X                    |                                                            |
| Dial via Office - Reverse           |                          |                      | X                                                          |
| Expressway Mobile and Remote Access | X                        | X                    | X                                                          |
| File Transfer                       | X                        | X                    | Some of the file transfer features are supported           |
| FIPS Compliance                     | X                        |                      |                                                            |
| Flexible Jabber ID                  | X                        | X                    | X                                                          |
| Group Chat                          | X                        | X                    |                                                            |
| Hunt Group                          | X                        |                      | X                                                          |
| Instant Messaging                   | X                        | X                    | X                                                          |
| Instant Messaging Encryption        | X                        | X                    | X                                                          |
| Locations                           | X                        |                      |                                                            |
| Mandatory Upgrade Support           | X                        | X                    |                                                            |
| Multiple Resource Login             | X                        | X                    | X                                                          |
| Persistent Chat Rooms               | X                        |                      |                                                            |
| Predictive Contact Search           | X                        | X                    | X                                                          |
| Presence                            | X                        | X                    | X                                                          |
| Save Chat History to Outlook Folder | X                        |                      |                                                            |
| Print Chat                          | X                        |                      |                                                            |
| Send to Mobile                      |                          |                      | X                                                          |
| Service Discovery                   | X                        | X                    | X                                                          |
| Single Sign-On                      | X                        | X                    | X                                                          |

| Feature                    | Cisco Jabber for Windows   | Cisco Jabber for Mac | Cisco Jabber for Android, Cisco Jabber for iPhone and iPad |
|----------------------------|----------------------------|----------------------|------------------------------------------------------------|
| Spell Check                | X (Client Options feature) | X (OS feature)       |                                                            |
| Telemetry                  | X                          | X                    | X                                                          |
| URI Dialing                | X                          | X                    | X                                                          |
| Video Desktop Share (BFCP) | X                          | X                    | X (Mobile clients only support BFCP receiving.)            |
| Voice and Video Calling    | X                          | X                    | X                                                          |
| Voice and Video Encryption | X                          | X                    | X                                                          |
| Voicemail                  | X                          | X                    | X                                                          |

## Cisco Jabber Features for Windows, Mac, iOS and Android

### Telemetry

#### Cisco Jabber Analytics

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.

You must install the following root certificate to use the telemetry feature: GoDaddy Class 2 Certification Authority Root Certificate.

For more information, see how to *Set Up Certificate Validation*.

By default, the telemetry data is on. You can configure the following telemetry parameters:

- `Telemetry_Enabled` — Specifies whether analytics data is gathered. The default value is true.
- `TelemetryEnabledOverCellularData` — Specifies whether analytics data is sent over cellular data and WiFi (true), or WiFi only (false). The default value is true.
- `TelemetryCustomerID` — This optional parameter specifies the source of analytic information. This ID can be a string that explicitly identifies an individual customer, or a string that identifies a common source without identifying the customer. We recommend using a tool that generates a *Global Unique Identifier* (GUID) to create a 36 character unique identifier, or to use a reverse domain name.

For more information on these parameters, see *Policies Parameters*.

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 [http://www.cisco.com/web/siteassets/legal/privacy\\_02Jun10.html](http://www.cisco.com/web/siteassets/legal/privacy_02Jun10.html).

### Related Topics

- [Cisco Jabber Features](#)
- [About Certificate Validation](#)
- [Policies Parameters, on page 113](#)

## Call Preservation

The Cisco Unified Communication Manager call preservation feature ensures that an active call is not interrupted when a Cisco Unified Communication Manager node fails or when communication fails between the device and the Cisco Unified Communication Manager node that set up the call.

## Configure Prompts for Presence Subscription Requests

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

### Inside Your Organization

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

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



### Note

---

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

---

### Outside Your Organization

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

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

### Before You Begin

This feature is supported for on-premises deployment and is only available on Cisco Unified Communications Manager Release 8.x, 9.x or later.

### Procedure

---

- Step 1** Open the **Cisco Unified CM IM and Presence Administration** interface.
- Step 2** Select **Presence > Settings**.  
The **Presence Settings** window opens.
- Step 3** Select **Allow users to view the availability of other users without being prompted for approval** to disable prompts and automatically accept all presence subscription requests within your organization.  
This option has the following values:
- Selected**
- The client does not prompt users for presence subscription requests. The client automatically accepts all presence subscription requests without prompting the users.
- Cleared**
- The client prompts users to allow presence subscription requests. This setting requires users to allow other users in your organization to view their availability status.
- Step 4** Select **Save**.
- 

## Disable Temporary Presence in Cisco Unified Communications Manager IM and Presence

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

### Before You Begin

This feature is supported for on-premises deployment and requires Cisco Unified Communications Manager Release 9.x or later.

### Procedure

---

- Step 1** Open the **Cisco Unified CM IM and Presence Administration** interface.
- Step 2** Select **Presence > Settings**.
- Step 3** Uncheck **Enable ad-hoc presence subscriptions** and then select **Save**.  
Cisco Jabber does not display temporary presence. Users can see availability status only for contacts in their contact list.
- 

## Disable Temporary Presence in Cisco Unified Presence

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

### Before You Begin

This feature is supported for on-premises deployment and requires Cisco Unified Communications Manager Release 8.x, 9.x or later.

### Procedure

---

- Step 1** Open the **Cisco Unified Presence Administration** interface.
- Step 2** Select **Presence > Settings**.
- Step 3** Uncheck **Enable ad-hoc presence subscriptions** and then select **Save**.  
Cisco Jabber does not display temporary presence. Users can see availability status only for contacts in their contact list.
- 

## Enable URI Dialing

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

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

### Before You Begin

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



## Associate URIs to Directory Numbers

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

### Automatically Populate Directory Numbers with URIs

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

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

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

#### Procedure

---

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

#### What to Do Next

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

#### *Configure Directory Numbers with URIs*

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

To configure directory numbers with URIs, do the following:

#### Procedure

---

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Select **Call Routing > Directory Number**.  
The **Find and List Directory Numbers** window opens.
- Step 3** Find and select the appropriate directory number.  
The **Directory Number Configuration** window opens.
- Step 4** Locate the **Directory URIs** section.
- Step 5** Specify a valid SIP URI in the **URI** column.
- Step 6** Select the appropriate partition from the **Partition** column.

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

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

**Step 8** Select **Save**.

---

### Associate the Directory URI Partition

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



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

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

---

#### Procedure

---

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

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

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

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

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

---

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

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

### Enable FQDN in SIP Requests for Contact Resolution

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

#### Procedure

---

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

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

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

**Step 3** Find and select the appropriate SIP profile.

**Remember** You cannot edit the default SIP profile. If required, you should create a copy of the default SIP profile that you can modify.

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

---

### What to Do Next

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

## Set Up Voicemail Avoidance

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

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

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

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

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

### Set Up Timer-Controlled Voicemail Avoidance

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

#### Before You Begin

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

### Set Up User-Controlled Voicemail Avoidance



#### Important

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

---

Set up User-Controlled Voicemail Avoidance as follows:

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




---

**Important**

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

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

---

### Set Up Cisco Unified Communications Manager to Support Voicemail Avoidance

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

#### Procedure

---

- Step 1** Open the **Cisco Unified CM Administration** interface.
  - Step 2** Select **System > Service Parameters**.
  - Step 3** In the **Server** drop-down list, select the active Cisco Unified Communications Manager.
  - Step 4** In the **Service** drop-down list, select the **Cisco Call Manager (Active)** service.
  - Step 5** Configure the settings in the **Clusterwide Parameters (System - Mobility Single Number Reach Voicemail)** section.
 

**Note** The settings in this section are not specific to Cisco Jabber. For information about how to configure these settings, see the *Confirmed Answer and DVO VM detection* section in the *Cisco Unified Communications Manager Administrator Guide* for your release.
  - Step 6** Click **Save**.
- 

### Enable Voicemail Avoidance on Mobility Identity

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

#### Before You Begin

- Set up the annunciator on the Cisco Unified Communications Manager. For more information, see the *Annunciator setup* section in the *Cisco Unified Communications Manager Administrator Guide* for your release.

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

## Procedure

---

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Navigate to the device that you want to configure as follows:
- a) Select **Device > Phone**.
  - b) Search for the device that you want to configure.
  - c) Select the device name to open the **Phone Configuration** window.
- Step 3** In the **Associated Mobility Identity** section, click the link for the Mobility Identity.
- Note** To ensure that the Voicemail Avoidance feature works correctly, the DVO Callback Number that the end user enters in the Cisco Jabber client must match the Destination Number that you enter on the Mobility Identity Configuration screen.
- Step 4** Set the policies as follows:
- Cisco Unified Communications Manager Version 9**
- In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.
- Cisco Unified Communications Manager Version 10 without Dial via Office**
- In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.
- Cisco Unified Communications Manager Version 10 with Dial via Office**
- In the **Single Number Reach Voicemail Policy** drop-down list, select **Timer Control**.
  - In the **Dial-via-Office Reverse Voicemail Policy** drop-down list, select **User Control**.
- Step 5** Click **Save**.
- 

## Enable Voicemail Avoidance on Remote Destination

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

### Before You Begin

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

## Procedure

---

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Navigate to the device that you want to configure as follows:
- Select **Device > Phone**.
  - Search for the device that you want to configure.
  - Select the device name to open the **Phone Configuration** window.
- Step 3** In the **Associated Remote Destinations** section, click the link for the associated remote destination.
- Step 4** Set the policies as follows:

### Cisco Unified Communications Manager Version 9

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

### Cisco Unified Communications Manager Version 10 without Dial via Office

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

### Cisco Unified Communications Manager Version 10 with Dial via Office

- In the **Single Number Reach Voicemail Policy** drop-down list, select **Timer Control**.
- In the **Dial-via-Office Reverse Voicemail Policy** drop-down list, select **User Control**.

- Step 5** If using Cisco Unified Communications Manager Version 10 with the Dial via Office feature,
- Step 6** Click **Save**.
- 

## Enable File Transfers and Screen Captures

File transfers and screen captures are enabled in Cisco Unified Communications Manager IM and Presence Service. There are additional parameters that are specified in the Cisco Jabber client configuration file. For more information on these parameters, see the [Policies Parameters, on page 113](#)

To configure file transfers and screen captures in Cisco Unified Communications Manager IM and Presence Service 9.x or later complete the [Enable File Transfers and Screen Captures, on page 247](#)

Cisco Unified Communications Manager IM and Presence Service 10.5.2 or later provides additional file transfer options:

- For peer to peer chats complete the [Enable File Transfer and Screen Captures for Peer to Peer Chats Only, on page 248](#)
- For group chats and chat rooms complete the [Enable File Transfer and Screen Captures for Group Chats and Chat Rooms, on page 247](#)
- To configure maximum file transfer size complete the [Configuring Maximum File Transfer Size, on page 248](#)

If your deployment includes earlier versions of the Cisco Jabber client that do not support these additional file transfer methods, there is an option to select Managed and Peer-to-Peer File Transfer. For more detailed information, see the Cisco Unified Communications Manager IM and Presence Service 10.5.2 guide.

## Enable File Transfers and Screen Captures



---

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

---

### Before You Begin

You can enable or disable file transfers and screen captures on *Cisco Unified Communication Manager IM and Presence Service 9.x and later*, through the Cisco XCP Router service on Cisco Unified Communications Manager IM and Presence Service. File transfers and screen captures parameter is enabled by default. However, you should verify the setting when you set up your deployment.

### Procedure

---

- Step 1** Open the **Cisco Unified CM IM and Presence Administration** interface.
  - Step 2** Select **System > Service Parameters**.
  - Step 3** Select the appropriate server from the **Server** drop-down list.
  - Step 4** Select **Cisco XCP Router** from the **Service** drop-down list.  
The **Service Parameter Configuration** window opens.
  - Step 5** Locate the **Enable file transfer** parameter.
  - Step 6** Select the appropriate value from the **Parameter Value** drop-down list.  
**Remember** If you disable the setting on Cisco Unified Communications Manager IM and Presence Service, you must also disable file transfers and screen captures in the client configuration.
  - Step 7** Select **Save**.
- 

## Enable File Transfer and Screen Captures for Group Chats and Chat Rooms

Files and screen captures transferred are stored on a file server and the metadata is logged to a database server. For Cisco Jabber clients that do not support chat rooms, this option enables file transfer in group chats.

When you enable this option, file transfers and screen captures are also available in peer to peer chats and the files and screen captures transferred are stored on a file server and the metadata is logged to a database server.

### Before You Begin

File transfer and screen captures for group chats and chat rooms is only available on Cisco Unified Communications Manager IM and Presence Service 10.5(2) or later.

Configure an external database to log metadata associated with the file transfer, see *Database Setup for IM and Presence Service on Cisco Unified Communications Manager, Release 10.5(2)* for further information.

Configure a network file server to save the file being transferred, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager, Release 10.5(2)* for further information.

### Procedure

---

- Step 1** Open the **Cisco Unified CM IM and Presence Administration** interface.
  - Step 2** Select **Messaging > File Transfer**.
  - Step 3** In the **File Transfer Configuration** section select **Managed File Transfer**.
  - Step 4** In the **Managed File Transfer Assignment** section, assign the external database and the external file server for each node in the cluster.
  - Step 5** Select **Save**.
- 

### What to Do Next

For each node:

- Copy the node's public key to the external file server's `authorized_keys` file, including the node's IP address, hostname, or FQDN.
- Ensure the **Cisco XCP File Transfer Manager** service is active.
- Restart the **Cisco XCP Router** service.

## Enable File Transfer and Screen Captures for Peer to Peer Chats Only

Enable file transfer for peer to peer chats on Cisco Unified Communications Manager IM and Presence Service 10.5(2) or later. Files and screen captures are only transferred in a peer to peer chat. The file or screen capture information is not logged or archived.

### Procedure

---

- Step 1** Open the **Cisco Unified CM IM and Presence Administration** interface.
  - Step 2** Select **Messaging > File Transfer**.
  - Step 3** In the **File Transfer Configuration** section, select **Peer-to-Peer**.
  - Step 4** Select **Save**.
- 

### What to Do Next

Restart the **Cisco XCP Router** service.

## Configuring Maximum File Transfer Size

The maximum file size is only available on Cisco Unified Communications Manager IM and Presence Service 10.5(2) or later.



### Before You Begin

The file transfer type selected is **Managed File Transfer**.

### Procedure

---

- Step 1** Open the **Cisco Unified CM IM and Presence Administration** interface.
  - Step 2** Select **Messaging > File Transfer**.
  - Step 3** In the **Managed File Transfer Configuration** section enter the amount for the **Maximum File Size**.
  - Step 4** Select **Save**.
- 

### What to Do Next

Restart the **Cisco XCP Router** service.

## Cisco Jabber Features for Windows

### Call Pickup

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

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

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

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

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

#### Call pickup notifications

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

#### Deskphone mode

In desk phone mode the following limitations apply:

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

- The Cisco Unified Communications Manager settings for audio and visual settings are not supported. The visual alerts are always displayed.

### Shared line behavior

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

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

### User not a member of an associated group

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

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

### Expected behavior using group call pickup and directed call pickup

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

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

- Softphone mode—Tone in headset, conversation window appears, and after 15 seconds annunciator followed by the fast busy tone.
- Deskphone mode—Conversation window appears, after 15 seconds annunciator, fast busy tone, and *Pickup failed* error message.

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

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

### Original recipient information not available

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

## Configure Call Pickup Group

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

### Procedure

---

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

For further information on call pickup group notification settings see the call pickup topics in the relevant Cisco Unified Communications Manager documentation.
  - Step 6** Select **Save**.
- 

### What to Do Next

Assign a call pickup group to directory numbers.

## Assign Directory Number

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

### Before You Begin

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

### Procedure

---

- Step 1** Open the **Cisco Unified Communications Manager Administration** interface.
- Step 2** Assign a call pickup group to a directory number using one of the following methods:
- Select **Call Routing > Directory Number**, find and select your directory number and in the Call Forward and Call Pickup Settings area select the call pickup group from the call pickup group drop down list.
  - Select **Device > Phone**, find and select your phone and in the **Association Information** list choose the directory number to which the call pickup group will be assigned.
- Step 3** To save the changes in the database, select **Save**.
- 

## Configure Other Call Pickup

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

### Before You Begin

Before you begin, configure call pickup groups.

### Procedure

---

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

## Configure Directed Call Pickup

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

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

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

### Procedure

---

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

## Auto Call Pickup

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

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

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

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

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

Auto directed call pickup connects the user to an incoming call in a group that is associated with the group of the user. The user enters the directory number of the ringing phone and selects **Pickup** on the client. Upon receiving the directory number, Cisco Unified Communications Manager completes the call connection. If auto directed call pickup is not enabled, the user must dial the directory number of the ringing phone, select **Pickup**, and answer the call that will now ring on the user phone to make the connection.

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

## Configure Auto Call Pickup

### Procedure

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

## Configure Silent Monitoring and Call Recording

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



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

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

### Notes:

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

- 1 Open the **Phone Configuration** window for the device on which you plan to enable silent monitoring and call recording.
- 2 Locate the **Built In Bridge** field.  
If the **Built In Bridge** field is not available on the **Phone Configuration** window, you should download and apply the most recent device packages.

### Before You Begin

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

## Configure Persistent Chat

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

### Before You Begin

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

Persistent chat is only available for Cisco Jabber for Windows.

Refer to *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* for your release for information on the database configuration necessary to support the persistent chat feature. It is available here: [http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_installation_and_configuration_guides_list.html). Database configuration must be performed before continuing with this task.

Local chat message archiving must be enabled for persistent chat. Local chat message archiving is enabled on Cisco Unified Communications Manager IM and Presence Service using the **Allow clients to log instant message history** setting. Refer to [Enable Message Settings](#), on page 30 for information on this setting.

### Procedure

- Step 1** Open the **Cisco Unified CM IM and Presence Administration** interface.
- Step 2** Select **Messaging > Group Chat and Persistent Chat**.
- Step 3** Select **Enable Persistent Chat**.
- Step 4** Ensure the settings **How many users can be in a room at one time** and **How many hidden users can be in a room at one time** under the **Occupancy Settings** section contain the same, non-zero value.
- Step 5** Configure the remaining settings as appropriate for your persistent chat deployment. We recommend the persistent chat settings in following table.

| Persistent Chat Setting                                        | Recommended Value     | Notes                                                    |
|----------------------------------------------------------------|-----------------------|----------------------------------------------------------|
| System automatically manages primary group chat server aliases | Disabled              |                                                          |
| Enable persistent chat                                         | Enabled               |                                                          |
| Archive all room joins and exits                               | Administrator Defined | This value is not currently used by for persistent chat. |

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



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

| Persistent Chat Setting                                                 | Recommended Value     | Notes                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Number of messages in chat history displayed by default                 | Administrator Defined | Cisco recommends a value between 15 and 50. The <b>Number of messages in chat history displayed by default</b> setting does not apply retroactively to persistent chat rooms. Rooms created before the setting is changed will continue to use their originally configured value. |
| Room owners can change the number of messages displayed in chat history | Default Value         | This value is not currently used by Cisco Jabber for persistent chat.                                                                                                                                                                                                             |

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

### What to Do Next

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

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

### Related Topics

[Client Parameters](#)

## Administer and Moderate Persistent Chat Rooms



### Note

- Persistent Chat Rooms and their administration is for on-premises deployments only.
- Persistent Chat Rooms are not available for mobile clients.

You administer persistent chat rooms from the Jabber client by creating rooms, delegating their moderators, and specifying members. The node on which the room is created is created automatically, although you can override it and specify a specific node. Administrators and moderators are privileged users in Persistent Chat rooms. You can administer Persistent Chat rooms on any service node that you are an administrator for on Cisco Unified Presence servers.

### Administrator Capabilities

Administrators can perform the following tasks from the **All Rooms** tab of Persistent Chat in the client hub window:

- Create rooms. When you create a room, you automatically become the room administrator.

- Define and change up to 30 moderators for a chat room (who become *room owners*).
- Specify and change the room name.
- Define the maximum number of participants in a room. This number cannot be less than the number of participants already in a room.
- Add and remove room members.
- Block, remove, and revoke participants.
- Destroy rooms (which removes it from the server, but the history is not deleted).

### Moderator Capabilities

Up to 30 moderators can be defined by an administrator for one Persistent Chat room. Moderators can perform the following tasks:

- Change the subject of a room.
- Edit members (which includes adding, removing, and banning them).

### Room Creation

When creating a room, you can provide the following types of information:

- Room name (required, maximum 200 characters)
- Description
- Room type (public or restricted)  
After the room type has been defined, it cannot be changed by anyone.
- Specify whether to add the room to your **My Rooms** tab (off by default)
- Add up to 30 moderators (who must have a valid Jabber ID to moderate a room).
- Room password

After you create the room, you have the option to add members to the room immediately or at a later time.

## Enable Persistent Chat Room Passwords

Persistent chat rooms that are password protected means that when users enter a room within a Jabber session, they must enter the password. Password protected rooms comply with the XEP-0045 specification from the XMPP Standards Foundation.

### Procedure

- 
- Step 1** To set a password for a room, from the **Chat Rooms** tab on the hub window, select **All rooms > New room > Password**.
  - Step 2** To change the password for a room, open the chat room, click on **Edit Room**, select **Password**, then edit and save the password.
-

## Integrate with Microsoft Products

Cisco Jabber for Windows supports a range of Microsoft products that integrate with the application. This section describes the support and integrations for these products.

### Internet Explorer

Microsoft Internet Explorer 8 or later is required. Cisco Jabber for Windows uses the Internet Explorer rendering engine to display HTML content.

Cisco Jabber for Windows requires Internet Explorer active scripting to render IMs. See <http://windows.microsoft.com/en-US/windows/help/genuine/ie-active-script> for instructions on enabling active scripting.



#### Note

---

Internet Explorer 9 users in Cloud-based deployments that use Single Sign On (SSO) get security alerts when they sign in to Cisco Jabber for Windows. Add **webexconnect.com** to the list of websites in the **Compatibility View Settings** window of Internet Explorer 9 to stop these alerts.

---

### Office

Integration with the following versions of Office is supported:

- Microsoft Office 2010, 32 and 64 bit
- Microsoft Office 2013, 32 and 64 bit

### Office 365

Microsoft Office 365 supports different configuration types based on the plan or subscription type. Cisco Jabber for Windows has been tested with small business plan P1 of Microsoft Office 365. This plan requires an on-premises Active Directory server.

Client-side integration with Microsoft Office 365 is supported with the following applications:

- Microsoft Office 2013 32 bit and 64 bit
- Microsoft Office 2010 32 bit and 64 bit
- Microsoft SharePoint 2010

### SharePoint

Integration with the following versions of SharePoint is supported:

- Microsoft SharePoint 2010
- Microsoft SharePoint 2013

Availability status in Microsoft SharePoint sites is supported only if users access those sites with Microsoft Internet Explorer. You should add the Microsoft SharePoint site to the list of trusted sites in Microsoft Internet Explorer.

## Product Integration

See the following topics for information on product integration:

- [Add Local Contacts from Microsoft Outlook](#), on page 263
- [Enable Calendar Events from Microsoft Outlook](#), on page 261
- [Enable Presence Integration with Microsoft Outlook](#), on page 262

## Calendar Integration

You can use the following client applications for calendar integration:

- Microsoft Outlook 2013 32 bit
- Microsoft Outlook 2013 64 bit
- Microsoft Outlook 2010 32 bit
- Microsoft Outlook 2010 64 bit
- Microsoft Outlook 2007 32 bit
- IBM Lotus Notes 9 32 bit
- IBM Lotus Notes 8.5.3 32 bit
- IBM Lotus Notes 8.5.2 32 bit
- IBM Lotus Notes 8.5.1 32 bit
- Google Calendar

## Enable Calendar Events from Microsoft Outlook

You must apply a setting in Microsoft Outlook so that calendar events display in Cisco Jabber for Windows.

### Procedure

---

- Step 1** Open the email account settings in Microsoft Outlook, as in the following example:
    - a) Select **File > Account Settings**.
    - b) Select the **Email** tab on the **Account Settings** window.
  - Step 2** Double-click the server name.  
In most cases, the server name is **Microsoft Exchange**.
  - Step 3** Select the **Use Cached Exchange Mode** checkbox.
  - Step 4** Apply the setting and then restart Microsoft Outlook.
- 

When users create calendar events in Microsoft Outlook, those events display in the **Meetings** tab.

## Enable Presence Integration with Microsoft Outlook

To enable integration with Microsoft Outlook, you specify `SIP:user@cupdomain` as the value of the `proxyAddresses` attribute in Microsoft Active Directory. Users can then share availability in Microsoft Outlook.

To modify the `proxyAddresses` attribute, you can:

### Use an Active Directory administrative tool such as Active Directory User and Computers

The Active Directory User and Computers administrative tool allows you to edit attributes on Microsoft Windows Server 2008 or later.

### Use the ADSchemaWizard.exe utility

The ADSchemaWizard.exe utility is available in the Cisco Jabber administration package. This utility generates an LDIF file that modifies your directory to add the `proxyAddresses` attribute to each user with the following value: `SIP:user@cupdomain`.

You should use the ADSchemaWizard.exe utility on servers that do not support the edit attribute feature in the Active Directory User and Computers administrative tool. You can use a tool such as ADSI Edit to verify the changes that you apply with the ADSchemaWizard.exe utility.

The ADSchemaWizard.exe utility requires Microsoft .NET Framework version 3.5 or later.

### Create a script with Microsoft Windows PowerShell

Refer to the appropriate Microsoft documentation for creating a script to enable presence in Microsoft Outlook.

## Enable Presence with the Active Directory User and Computers Tool

Complete the following steps to enable presence in Microsoft Outlook for individual users with the Active Directory User and Computers administrative tool:

### Procedure

- 
- Step 1** Start the Active Directory User and Computers administrative tool.  
You must have administrator permissions to run the Active Directory User and Computers administrative tool.
  - Step 2** Select **View** in the menu bar and then select the **Advanced Features** option from the drop-down list.
  - Step 3** Navigate to the appropriate user in the Active Directory User and Computers administrative tool.
  - Step 4** Double click the user to open the **Properties** dialog box.
  - Step 5** Select the **Attribute Editor** tab.
  - Step 6** Locate and select the `proxyAddresses` attribute in the **Attributes** list box.
  - Step 7** Select **Edit** to open the **Multi-valued String Editor** dialog box.
  - Step 8** In the **Value to add** text box, specify the following value: `SIP:user@cupdomain`.  
For example, `SIP:msmith@cisco.com`.

Where the `user@cupdomain` value is the user's instant messaging address. `cupdomain` corresponds to the domain for Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.

## Add Local Contacts from Microsoft Outlook

Cisco Jabber for Windows lets users search for and add local contacts in Microsoft Outlook. To enable this integration with Microsoft Outlook, you must enable Cached Exchange Mode on the Microsoft Exchange server.

To search for local contacts in Microsoft Outlook with the client, users must have profiles set in Microsoft Outlook. In addition, users must do the following:

- 1 Select **File > Options**.
- 2 Select the **Integration** tab.
- 3 Select either **None** or **Microsoft Outlook**.

To add local Microsoft Outlook contacts to contact lists in the client, local contacts must have instant message addresses in Microsoft Outlook.

To show contact photos in the client interface, local contacts in Microsoft Outlook must have instant message addresses.

To communicate with local contacts in Microsoft Outlook using the client, local contacts must have the relevant details. To send instant messages to contacts, local contacts must have an instant message address. To call contacts in Microsoft Outlook, local contacts must have phone numbers.

## Save Chat History to an Outlook Folder

This feature is available to Cisco Jabber for Windows clients.

You can enable the client to automatically save chat histories to a Cisco Jabber Chats folder in users' Microsoft Outlook application. Users can store their conversations in the folder. The folder stores the IM conversation history from the client. The IM conversation is saved by the client to the Exchange server when the chat window is closed. When you enable the feature, a new **Outlook** tab is displayed in the **Options** menu in the client.

In the `jabber-config.xml` file, set the `EnableSaveChatHistoryToExchange` parameter to true.

### Limitations for Saving Chat History to an Outlook Folder

This feature is only valid for Exchange 2013 and Exchange 2010 servers.

### Authentication Modes

You must set up a method of authentication for the client to authenticate with the Exchange server. When authentication is complete, the client has access to the Exchange server which allows saving chat histories to a folder in Outlook.

If you do not specify an authentication method, then users must manually input their Exchange credentials into the client, in the **Outlook** tab of the **Options** menu.

### *Authenticate Using Single Sign On for the Operating System*

The client uses the account details of the logged in user to authenticate with the Exchange server. This authentication method uses the Windows NT Lan Manager (NTLM) security protocol.

**Note**

Do not use this authentication method if some users share the same Windows account. The client authenticates with the account on the Operating System, and not with the user who is logged in to Cisco Jabber. For example, User A logs onto a Windows machine and then logs into Cisco Jabber for a morning shift. When the shift is done, Jabber is reset and User B logs into the client for the afternoon shift. Because User A is logged into the Windows account, then the chat messages from User B are saved in the Outlook account for User A.

**Before You Begin**

Users and their computers must use domains. Authentication using single sign on does not work if users are local Windows users.

**Procedure**

In the Jabber-config.xml file, set the ExchangeAuthenticateWithSystemAccount parameter to true.

### *Authenticate by Syncing Credentials*

You can sync the Exchange credentials with another set of credentials for users, such as the Cisco Unified Presence credentials. Using this method, the client uses the credentials to authenticate to the Exchange server.

**Before You Begin****Procedure**

- 
- Step 1** In the jabber-config.xml file, configure the Exchange\_UseCredentialsFrom parameter.
  - Step 2** Define the value of the parameter as the service that you want used to sync credentials. For example, Exchange\_UseCredentialsFrom=CUCM.  
In this example, Cisco Unified Communications Manager is defined as the service which provides the Exchange server with credentials for authentication.
- 

**Specify Server Addresses**

After you enable an authentication method for the client to access the Exchange server, you must enable a method for the client to specify the Exchange server address.

If you do not specify server addresses, then users must manually enter the internal and external Exchange servers in the client, in the **Outlook > Advanced** tab of the **Options** menu.

### *Detect Server Addresses Automatically*

You can configure the client to automatically discover the Exchange servers based on users' domain. This domain is defined when you set up the authentication method by using the domain that was specified for the user's credentials.



### Procedure

---

- Step 1** In the `jabber-config.xml` file, configure the `ExchangeAutodiscoverDomain` parameter.
- Step 2** Define the value of the parameter as the domain to discover the Exchange server.  
The client uses the domain to search for the Exchange server at one of the following Web addresses:  
`https://<domain>/autodiscover/autodiscover.svc`  
`https://autodiscover.<domain>/autodiscover/autodiscover.svc`
- 

#### Define Server Addresses

You can define the internal and external Exchange server addresses in the configuration file.

### Procedure

---

- Step 1** In the `jabber-config.xml` file, configure the `InternalExchangeServer` and `ExternalExchangeServer` parameters.
- Step 2** Define the value of the parameters using the Exchange server addresses.
- 

## Add Custom Emoticons

You can add custom emoticons to Cisco Jabber for Windows by creating emoticon definitions in an XML file and saving it to the file system.



- Note** To achieve optimal results, your custom emoticons should conform to the following guidelines:
- Dimensions: 17 x 17 pixels
  - Transparent background
  - PNG file format
  - RGB colors
- 

### Procedure

---

- Step 1** Create a file named `emoticonDefs.xml` with any text editor.
- Step 2** Specify the emoticon definitions as appropriate in `emoticonDefs.xml`.  
See *Emoticon Definitions* for more information on the structure and available parameters for `emoticonDefs.xml`.

**Step 3** Save and close `emoticonDefs.xml`.

**Step 4** Save `emoticonDefs.xml` in the appropriate directory on the file system.

Cisco Jabber for Windows loads emoticon definitions from the following directories on the file system:

***Program Files\Cisco Systems\Cisco Jabber\Emoticons***

This folder contains the default emoticons for Cisco Jabber for Windows and the default `emoticonDefs.xml`.

***Program Files\Cisco Systems\Cisco Jabber\CustomEmoticons***

This folder does not exist by default. Administrators can create this folder to contain custom emoticon definitions to include in organizational deployments.

Emoticons that you define in the `CustomEmoticons` folder take precedence over emoticon definitions in the default `Emoticons` folder.

***%USERPROFILE%\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\CustomEmoticons***

This folder contains custom emoticon definitions for individual instances of Cisco Jabber for Windows.

Emoticons that you define in this directory take precedence over emoticon definitions in the `CustomEmoticons` folder in the installation directory.

**Step 5** Restart Cisco Jabber for Windows.

---

Cisco Jabber for Windows loads the custom emoticon definitions in `emoticonDefs.xml`.




---

**Remember** Custom emoticon definitions are available to users only if they are defined locally in `emoticonDefs.xml`. If you send custom emoticons to users who do not have the same emoticon definitions, those users receive the default keys, not the icons; for example:

- 1 User A defines a custom emoticon in `emoticonDefs.xml`.  
The custom emoticon definition exists only on User A's local file system.
  - 2 User A sends that custom emoticon to User B.
  - 3 User B receives only the default key for the custom emoticon. User B does not receive the icon.
- 

## Emoticon Definitions

Cisco Jabber for Windows loads emoticon definitions from `emoticonDefs.xml`.

The following XML snippet shows the basic structure for the emoticon definitions file:

```
<emoticons>
 <emoticon defaultKey="" image="" text="" order="" hidden="">
 <alt></alt>
 </emoticon>
</emoticons>
```

The following table describes the elements and attributes for defining custom emoticons:

Element or attribute	Description
emoticons	This element contains all emoticon definitions.
emoticon	This element contains the definition of an emoticon.
defaultKey	<p>This attribute defines the default key combination that renders the emoticon.</p> <p>Specify any key combination as the value.</p> <p>This attribute is required.</p> <p>defaultKey is an attribute of the emoticon element.</p>
image	<p>This attribute specifies the filename of the emoticon image.</p> <p>Specify the filename of the emoticon as the value. The emoticon image must exist in the same directory as <code>emoticonDefs.xml</code>.</p> <p>This attribute is required.</p> <p>Cisco Jabber for Windows supports any icon that Internet Explorer can render, including <code>.jpeg</code>, <code>.png</code>, and <code>.gif</code>.</p> <p>image is an attribute of the emoticon element.</p>
text	<p>This attribute defines the descriptive text that displays in the <b>Insert emoticon</b> dialog box.</p> <p>Specify any string of unicode characters.</p> <p>This attribute is optional.</p> <p>text is an attribute of the emoticon element.</p>
order	<p>This attribute defines the order in which emoticons display in the <b>Insert emoticon</b> dialog box.</p> <p>Specify an ordinal number beginning from 1 as the value.</p> <p>order is an attribute of the emoticon element.</p> <p>This attribute is required. However, if the value of hidden is true this parameter does not take effect.</p>

Element or attribute	Description
hidden	<p>This attribute specifies whether the emoticon displays in the <b>Insert emoticon</b> dialog box.</p> <p>Specify one of the following as the value:</p> <p><b>true</b></p> <p>Specifies the emoticon does not display in the <b>Insert emoticon</b> dialog box. Users must enter the key combination to render the emoticon.</p> <p><b>false</b></p> <p>Specifies the emoticon displays in the <b>Insert emoticon</b> dialog box. Users can select the emoticon from the <b>Insert emoticon</b> dialog box or enter the key combination to render the emoticon. This is the default value.</p> <p>This attribute is optional.</p> <p>hidden is an attribute of the emoticon element.</p>
alt	<p>This element enables you to map key combinations to emoticons.</p> <p>Specify any key combination as the value.</p> <p>For example, if the value of defaultKey is :), you can specify :-) as the value of alt so that both key combinations render the same emoticon.</p> <p>This element is optional.</p>



**Remember** The default emoticons definitions file contains the following key combinations that enable users to request calls from other users:

- :callme
- :telephone

These key combinations send the callme emoticon, or communicon. Users who receive this emoticon can click the icon to initiate an audio call. You should include these key combinations in any custom emoticons definition file to enable the callme emoticon.

### Emoticon Definition Example

```
<emoticons>
 <emoticon defaultKey=":)" image="Emoticons_Smiling.png" text="Smile" order="1">
 <alt>:-)</alt>
 <alt>^_</alt>
 </emoticon>
 <emoticon defaultKey=":(" image="Emoticons_Frowning.png" text="Frown" order="2">
 <alt>:-(</alt>
 </emoticon>
</emoticons>
```

# Cisco Jabber Features for Mac

## Local Contacts in Mac Address Book

Cisco Jabber allows users search for and add local contacts in the Mac Address book.

To search for local contacts in Mac Address book with the client, users must install the Address Book plug-in:

- 1 Select **Jabber > Install Mac Address Book Plug-In**.

To enable the Address Book plug-in:

- 1 Select **Jabber > Preferences > General > Enable "Mac Address Plug-in"**.
- 2 Restart the client for this to take effect.

To communicate with local contacts in Mac Address book using the client, local contacts must have the relevant details. To send instant messages to contacts, local contacts must have an instant message address. To call contacts in Mac Address book, local contacts must have phone numbers.

# Cisco Jabber for Android and iOS

## Configure Call Park

You can use call park to place a call on hold and pick it up from another phone in a Cisco Unified Communication Manager system. Call park must be enabled and extension numbers must be defined on each Cisco Unified Communication Manager node in a cluster. You can define either a single directory number or a range of directory numbers for use as call park extension numbers.

Complete the following tasks to enable call park. For detailed instructions, see the *Features and Services Guide for Cisco Unified Communication Manager*.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	Configure cluster wide call park	[Optional] Configure call park for the entire cluster, or use the procedure in Step 3 to configure call park on individual nodes within the cluster.
<b>Step 2</b>	Configure a partition	Create a partition to add a call park number.
<b>Step 3</b>	Configure a call park number	Configure a call park number to use call park across nodes in a cluster.  You can define either a single directory number or a range of directory numbers for use as call park extension numbers. You can park only one call at each call park extension number.

	Command or Action	Purpose
--	-------------------	---------

## Set Up Cisco Unified Communications Manager to Support Dial via Office

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

- 1 Complete one or both of the following procedures.
  - *Set Up Enterprise Feature Access Number*
  - *Set Up Mobility Profile*
- 2 Complete the *Verify Device COP File Version* procedure.
- 3 If necessary, create application dial rules to allow the system to route calls to the Mobile Identity phone number to the outbound gateway. Ensure that the format of the Mobile Identity phone number matches the application dial rules.

### Set Up Enterprise Feature Access Number

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

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

#### Before You Begin

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

#### Procedure

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

To support dialing internationally, you can prepend this number with \+.

- Step 5** From the **Route Partition** drop-down list, choose the partition of the DID that is required for enterprise feature access.  
This partition is set under **System > Service Parameters**, in the **Clusterwide Parameters (System - Mobility)** section, in the **Inbound Calling Search Space for Remote Destination** setting. This setting points either to the Inbound Calling Search Space of the Gateway or Trunk, or to the Calling Search Space assigned on the Phone Configuration screen for the device.  
If the user sets up the DvO Callback Number with an alternate number, ensure that you set up the trunk Calling Search Space (CSS) to route to destination of the alternate phone number.
- Step 6** In the **Description** field, enter a description of the Mobility Enterprise Feature Access number.
- Step 7** (Optional) Check the **Default Enterprise Feature Access Number** check box if you want to make this Enterprise Feature Access number the default for this system.
- Step 8** Select **Save**.
- 

## Set Up Mobility Profile

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

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

### Procedure

---

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

## Verify Device COP File Version

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

## Procedure

---

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

## Prerequisite for All Clients

- On-premise Deployment
- Cisco Unified Communications Manager 9.x and higher

## Set Up Dial via Office



### Important

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

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

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

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




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



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

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

**Table 2: Calling Methods used with Calling Options over Different Network Connections**

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

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

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

## Set Up Dial via Office for Each Device

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

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

- 1 Add a Mobility Identity for each user.

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

## Add Mobility Identity

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

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

### Procedure

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

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

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

Setting	Suggested Initial Value
Delay Before Ringing Timer	0 <b>Note</b> This setting does not apply to DvO-R calls.

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

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

**Step 6** Do one of the following:

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

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

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

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

**Step 9** Select **Save**.

### Enable Dial via Office on Each Device

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

## Procedure

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

## What to Do Next

Test this feature.

## Set Up Mobile Connect

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

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

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<a href="#">Enable Mobile Connect, on page 277</a>	
<b>Step 2</b>	<a href="#">Add Mobility Identity, on page 274</a>	To configure the mobile device phone number.
<b>Step 3</b>	<a href="#">Add Remote Destination (Optional), on page 278</a>	To configure an alternate phone number.
<b>Step 4</b>	Test your settings.	<ul style="list-style-type: none"> <li>• Exit Cisco Jabber on the mobile device.</li> <li>• Call the Cisco Jabber extension from another phone.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>Verify that the native mobile network phone number rings and that the call connects when you answer it.</li> </ul>

## Enable Mobile Connect

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

### Procedure

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

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

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

e) Select **Save**.

## Add Remote Destination (Optional)

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

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

### Procedure

- Step 1** Open the **Cisco Unified CM Administration** interface.
- Step 2** Navigate to the device that you want to configure as follows:
  - a) Select **Device > Phone**.
  - b) Search for the device that you want to configure.
  - c) Select the device name to open the **Phone Configuration** window.
- Step 3** In the **Associated Remote Destinations** section, select **Add a New Remote Destination**.
- Step 4** Enter the desired phone number as the Destination Number.  
This number must be routable to an outbound gateway. Generally, the number is the full E.164 number.
- Step 5** Enter the initial values for the following call timers:
  - a) **Answer Too Soon Timer**—Enter 3000

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

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

**Step 6** Do one of the following:

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

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

**Step 8** Select **Save**.

## Transfer Active VoIP Call to the Mobile Network

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

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

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

Implementation Method	Description	Instructions
Mobility Softkey	Cisco Unified Communications Manager calls the phone number of the PSTN mobile service provider for the mobile device.	See the <i>Enable Transfer from VoIP to Mobile Network</i> topic.
None of the above	Disable this feature if you do not want to make it available to users.	Select <b>Disabled</b> for the <b>Transfer to Mobile Network</b> option in the <b>Product Specific Configuration Layout</b> section of the TCT device page.  Select <b>Disabled</b> for the <b>Transfer to Mobile Network</b> option in the <b>Product Specific Configuration Layout</b> section of the BOT device page.

## Enable Handoff from VoIP to Mobile Network

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

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

### Set Up Handoff DN

#### Before You Begin

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

#### Procedure

- 
- Step 1** Open the **Cisco Unified CM Administration** interface.
  - Step 2** Select **Call Routing > Mobility > Handoff Configuration**.
  - Step 3** Enter the Handoff Number for the Direct Inward Dial (DID) number that the device uses to hand off a VoIP call to the mobile network.  
The service provider must deliver the DID digits exactly as configured. Alternately, for Cisco IOS gateways with H.323 or SIP communication to Cisco Unified Communications Manager, you can use Cisco IOS to manipulate the inbound called-party number at the gateway, presenting the digits to Cisco Unified Communications Manager exactly as configured on the handoff number.



**Note** You cannot use translation patterns or other similar manipulations within Cisco Unified Communications Manager to match the inbound DID digits to the configured Handoff DN.

- Step 4** Select the **Route Partition** for the handoff DID.  
This partition should be present in the Remote Destination inbound Calling Search Space (CSS), which points to either the Inbound CSS of the Gateway or Trunk, or the Remote Destination CSS.  
This feature does not use the remaining options on this page.
- Step 5** Select **Save**.
- 

### Match Caller ID with Mobility Identity

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

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

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

#### Before You Begin

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

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

#### Procedure

---

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

## Set Up User and Device Settings for Handoff

### Before You Begin

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

### Procedure

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

## Enable Transfer from VoIP to Mobile Network

### Procedure

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

c) Select the device name to open the **Phone Configuration** window.

**Step 4** For the per-user and per-device settings in Cisco Unified Communications Manager, set the specific device to use the Mobility softkey when the device transfers calls to the mobile voice network. Ensure that you have set up both Mobility Identity and Mobile Connect for the mobile device. After the transfer feature is working, users can enable and disable Mobile Connect at their convenience without affecting the feature.

If the device is an iPod Touch, you can configure a Mobility Identity using an alternate phone number such as the mobile phone of the user.

a) Select the **Owner User ID** on the device page.

b) Select the **Mobility User ID**. The value usually matches that of the Owner User ID.

c) In the Product Specific Configuration Layout section, for the Transfer to Mobile Network option, select **Use Mobility Softkey** or **Use HandoffDN Feature**.

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

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

**Step 7** Select **Apply Config**.

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

---

### What to Do Next

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

## Cisco Jabber for iOS, Android and Windows

### Hunt Group

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

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

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

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

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

#### Logout notification

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

## Line Group

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

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

### Configure Line Group

#### Before You Begin

Configure directory numbers.

#### Procedure

---

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

### What to Do Next

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

## Hunt List

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

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

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

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

### Configure Hunt List

#### Procedure

---

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

### What to Do Next

Add line groups to the hunt list.

## Add Line Group to Hunt List

### Before You Begin

You must configure line groups and configure a hunt list.

### Procedure

---

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

## Hunt Pilot

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

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

## Configure Hunt Pilot

### Procedure

---

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

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







## Cisco Jabber Reference Information

---

- [Client Availability](#), page 289
- [Multiple Resource Login](#), page 290
- [Protocol Handlers](#), page 291
- [Audio and Video Performance Reference](#), page 293
- [Define a Port Range on the SIP Profile](#), page 298
- [Set DSCP Values](#), page 299

### 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**

---

In Cisco Jabber for Android and Cisco Jabber for iPod or iPad, we do not support this meeting integration. But we do support **In a meeting** status in Cisco Jabber for Mac and Cisco Jabber for Windows.

---

- Microsoft Exchange and Cisco Unified 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 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 Presence and Microsoft Exchange integration for the client to set the **In a meeting** availability. The client checks if integration between Cisco Unified 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:

<b>Deployment Scenario</b>	<b>You select In a meeting (according to my calendar)</b>	<b>You do not select In a meeting (according to my calendar)</b>
You enable integration between Cisco Unified Presence and Microsoft Exchange.	Cisco Unified Presence sets availability status	Availability status does not change
You do not enable integration between Cisco Unified 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:

<b>Availability Enabled in the Client</b>	<b>Availability Enabled by Integrating Cisco Unified Presence with Microsoft Exchange</b>
<b>Offline in a meeting</b> availability is not supported.	<b>Offline in a meeting</b> availability is supported.
<b>In a meeting</b> availability is supported for non-calendar events.	<b>In a meeting</b> availability is not supported for non-calendar events.
<p><b>Note</b> 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.</p> <p>Non-calendar events refer to events that do not appear in the user's calendar, such as instant meetings, <b>Offline</b>, or <b>On a call</b>.</p>	

### Related Topics

[Calendar Integration, on page 261](#)

## Multiple Resource Login

All Cisco Jabber clients register with a central IM and Presence Service node when a user logs into the system. This is Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service node in on-premise deployments or Cisco WebEx in cloud-based deployments. This node tracks availability, contact lists, and other aspects of the IM and Presence Service environment.

This IM and Presence Service node tracks all of the registered clients associated with each unique network user. When a new IM session is initiated between two users, the first incoming message is broadcast to all of the registered clients of the receiving user. The IM and Presence Service node then waits for the first response from one of the registered clients. The first client to respond subsequently receives the remainder of the incoming messages until the user starts responded using another registered client. The node then reroutes subsequent messages to this new client.

Adam wishes to initiate an IM conversation with Anita. Anita has previously logged into Cisco Jabber for Windows and Cisco Jabber for Android. Anita has registered two clients with the central IM and Presence Service node. Adam initiates the conversation by sending the message, "Hi Anita. Are you free?"

The node identifies that Anita has two registered clients and broadcasts Adam's message to both.

Anita is sitting at her desk and observes Adam's message appearing on both her laptop and phone. She chooses to respond using her laptop and responds with the message, "I have a meeting in a few moments but I can chat briefly right now."

The IM and Presence Service node identifies that Anita has responded using Cisco Jabber for Windows and marks this as the client to route all subsequent messages to in the conversation. When Adam responds with "This will only take a minute," it is routed directly to Cisco Jabber for Windows. If Anita starts responding to Adam using her phone at some point in the conversation, the IM and Presence Service node then routes subsequent messages there instead of to Cisco Jabber for Windows.

## 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:  
Starts an instant message and opens a chat window in Cisco Jabber.
- IM:  
Starts an instant message and opens a chat window in Cisco Jabber.
- 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:  
Starts an audio or video call with Cisco Jabber.
- SIP:  
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>
 Call 1234

 Send an instant message to Mary Smith
 </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>
 Call 1234

 Call Mary

 Weekly conference call
 </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>
 Create a group chat with Mary Smith and Adam McKenzie
 </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
```

## Audio and Video Performance Reference



### Attention

The following data is based on testing in a lab environment. This data is intended to provide an idea of what you can expect in terms of bandwidth usage. The content in this topic is not intended to be exhaustive or to reflect all media scenarios that might affect bandwidth usage.

### Audio Bit Rates for Cisco Jabber Desktop Clients

The following audio bit rates apply to Cisco Jabber for Windows and Cisco Jabber for Mac.

Codec	RTP (kbits/second)	Actual bitrate (kbits/second)	Notes
g.722.1	24/32	54/62	High quality compressed
g.711	64	80	Standard uncompressed
g.729a	8	38	Low quality compressed

### Audio Bit Rates for Cisco Jabber Mobile Clients

The following audio bit rates apply to Cisco Jabber for iPad and iPhone and Cisco Jabber for Android.

Codec	Codec bit rate (kbits/second)	Network Bandwidth Utilized (kbits/second)
g.711	64	80

Codec	Codec bit rate (kbits/second)	Network Bandwidth Utilized (kbits/second)
g722.1	32	48
g722.1	24	40
g.729a	8	24

## Video Bit Rates for Cisco Jabber Desktop Clients

The following video bit rates (with g.711 audio) apply to Cisco Jabber for Windows and Cisco Jabber for Mac. This table does not list all possible resolutions.

Resolution	Pixels	Measured bit rate (kbits per second) with g.711 audio
w144p	256 x 144	156
w288p This is the default size of the video rendering window for Cisco Jabber.	512 x 288	320
w448p	768 x 448	570
w576p	1024 x 576	890
720p	1280 x 720	1300



**Note**

The measured bit rate is the actual bandwidth used (RTP payload + IP packet overhead).

## Video Bit Rates for Cisco Jabber for Android

The client captures and transmits video at 15 fps.

Resolution	Pixels	Bit Rate (kbits per second) with g.711 audio
w144p	256 x 144	235
w288p	512 x 288	275
w360p	640 x 360	330
w720p	1080 x 720	768

Resolution	Pixels	Bit Rate (kbits per second) with g.711 audio
w1080p	1920 x 1080	768

## Video Bit Rates for Cisco Jabber for iPhone and iPad

The client captures and transmits at 20 fps.

Resolution	Pixels	Bit rate (kbits/second) with g.711 audio
w144p	256 x 144	290
w288p	512 x 288	340
w360p	640 x 360	415

## Presentation Video Bit Rates

Cisco Jabber captures at 8 fps and transmits at 2 to 8 fps.

The values in this table do not include audio.

Pixels	Estimated wire bit rate at 2 fps (kbits per second)	Estimated wire bit rate at 8 fps (kbits per second)
720 x 480	41	164
704 x 576	47	188
1024 x 768	80	320
1280 x 720	91	364
1280 x 800	100	400

## Maximum Negotiated Bit Rate

You specify the maximum payload bit rate in Cisco Unified Communications Manager in the **Region Configuration** window. This maximum payload bit rate does not include packet overhead, so the actual bit rate used is higher than the maximum payload bit rate you specify.

The following table describes how Cisco Jabber allocates the maximum payload bit rate:

Audio	Interactive video (Main video)
Cisco Jabber uses the maximum audio bit rate	Cisco Jabber allocates the remaining bit rate as follows: The maximum video call bit rate minus the audio bit rate.

## Bandwidth Performance Expectations for Cisco Jabber for Windows and Cisco Jabber for Mac

Cisco Jabber for Mac separates the bit rate for audio and then divides the remaining bandwidth equally between interactive video and presentation video. The following table provides information to help you understand what performance you should be able to achieve per bandwidth:

Upload speed	Audio	Audio + Interactive video (Main video)
125 kbps under VPN	At bandwidth threshold for g.711. Sufficient bandwidth for g.729a and g.722.1.	Insufficient bandwidth for video.
384 kbps under VPN	Sufficient bandwidth for any audio codec.	w288p (512 x 288) at 30 fps
384 kbps in an enterprise network	Sufficient bandwidth for any audio codec.	w288p (512 x 288) at 30 fps
1000 kbps	Sufficient bandwidth for any audio codec.	w576p (1024 x 576) at 30 fps
2000 kbps	Sufficient bandwidth for any audio codec.	w720p30 (1280 x 720) at 30 fps

Cisco Jabber for Windows separates the bit rate for audio and then divides the remaining bandwidth equally between interactive video and presentation video. The following table provides information to help you understand what performance you should be able to achieve per bandwidth:

Upload speed	Audio	Audio + Interactive video (Main video)	Audio + Presentation video (Desktop sharing video)	Audio + Interactive video + Presentation video
125 kbps under VPN	At bandwidth threshold for g.711. Sufficient bandwidth for g.729a and g.722.1.	Insufficient bandwidth for video.	Insufficient bandwidth for video.	Insufficient bandwidth for video.
384 kbps under VPN	Sufficient bandwidth for any audio codec.	w288p (512 x 288) at 30 fps	1280 x 800 at 2+ fps	w144p (256 x 144) at 30 fps + 1280 x 720 at 2+ fps
384 kbps in an enterprise network	Sufficient bandwidth for any audio codec.	w288p (512 x 288) at 30 fps	1280 x 800 at 2+ fps	w144p (256 x 144) at 30 fps + 1280 x 800 at 2+ fps
1000 kbps	Sufficient bandwidth for any audio codec.	w576p (1024 x 576) at 30 fps	1280 x 800 at 8 fps	w288p (512 x 288) at 30 fps + 1280 x 800 at 8 fps



Upload speed	Audio	Audio + Interactive video (Main video)	Audio + Presentation video (Desktop sharing video)	Audio + Interactive video + Presentation video
2000 kbps	Sufficient bandwidth for any audio codec.	w720p30 (1280 x 720) at 30 fps	1280 x 800 at 8 fps	w288p (1024 x 576) at 30 fps + 1280 x 800 at 8 fps

Note that VPN increases the size of the payload, which increases the bandwidth consumption.

## Bandwidth Performance Expectations for Cisco Jabber for Android

Note that VPN increases the size of the payload, which increases the bandwidth consumption.

Upload speed	Audio	Audio + Interactive Video (Main Video)
125 kbps under VPN	At bandwidth threshold for g.711. Insufficient bandwidth for video. Sufficient bandwidth for g.729a and g.722.1.	Insufficient bandwidth for video.
256 kbps	Sufficient bandwidth for any audio codec.	<b>Transmission rate (Tx)</b> —256 x 144 at 15 fps <b>Reception rate (Rx)</b> —256 x 144 at 30 fps
384 kbps under VPN	Sufficient bandwidth for any audio codec.	<b>Tx</b> —640 x 360 at 15 fps <b>Rx</b> —640 x 360 at 30 fps
384 kbps in an enterprise network	Sufficient bandwidth for any audio codec.	<b>Tx</b> —640 x 360 at 15 fps <b>Rx</b> —640 x 360 at 30 fps



### Note

Due to device limitations, the Samsung Galaxy SII and Samsung Galaxy SIII devices cannot achieve the maximum resolution listed in this table.

## Bandwidth Performance Expectations for Cisco Jabber for iPhone and iPad

The client separates the bit rate for audio and then divides the remaining bandwidth equally between interactive video and presentation video. The following table provides information to help you understand what performance you should be able to achieve per bandwidth.

Note that VPN increases the size of the payload, which increases the bandwidth consumption.

Upload speed	Audio	Audio + Interactive Video (Main Video)
125 kbps under VPN	At bandwidth threshold for g.711. Insufficient bandwidth for video.  Sufficient bandwidth for g.729a and g.722.1.	Insufficient bandwidth for video.
290 kbps	Sufficient bandwidth for any audio codec.	256 x144 at 20 fps
415 kbps	Sufficient bandwidth for any audio codec.	640 x 360 at 20 fps

## Video Rate Adaptation

Cisco Jabber uses video rate adaptation to negotiate optimum video quality. Video rate adaptation dynamically increases or decreases video bit rate throughput to handle real-time variations on available IP path bandwidth.

Cisco Jabber users should expect video calls to begin at lower resolution and scale upwards to higher resolution over a short period of time. Cisco Jabber saves history so that subsequent video calls should begin at the optimal resolution.

## 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 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**.
- 

### Related Topics

[8.6.x: SIP Profile Configuration](#)

9.0.x: SIP profile setup

## 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.

#### 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

Attributes	Audio Policy	Video Policy	Signaling Policy
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.



### 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 voice and video quality.

### Procedure

**Step 1** Select **Jabber > Preferences > Calls > Advanced**

**Step 2** 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.

