Feature Configuration for Cisco Jabber 14.1

First Published: 2022-02-24

Last Modified: 2023-10-09

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

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

Change history

New and changed information

Date	Description	Location
October 2023	Removed a limitation about recording tone.	*Silent Monitoring and Call Recording*
February 2022	Initial publication	
	Added load balancing for persistent chat rooms.	Persistent chat rooms
	Added information on replacement of Apple WebView with WKWebView.	Custom embedded tabs

CHAPTER 1

Getting started with feature configuration

About Cisco Jabber

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

The applications in the Cisco Jabber family of products are:

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

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

Purpose of this Guide

This document describes some of the features of Cisco Jabber. Configuration information and the list of supported clients is given for each feature.

Feature Configuration Overview

The following table provides an alphabetical list of the features described in this document, and lists which clients are supported for each feature.

Table 1: Feature Quick Reference

Feature Name	Description	Supported Clients
ActiveControl	Hold conferences in Jabber using the Cisco Meetings Server (CMS) 2.3 or later.	All clients
Blocked Domain Support for Webex Messenger Users	Webex Messenger users can add a specific domain or a contact from a specific domain to the blocked list. Contacts from the specified domain cannot view your availability or send you instant messages.	Cisco Jabber for Mac
Bots	A chat bot is an automated service that appears and behaves like a user in Jabber. A Jabber user can add a chat bot to their Contacts list and start a chat conversation with the bot.	All clients
Bridge Escalations	Bridge escalations allow users to quickly escalate a group chat to a conference call.	All clients
Browser Click to Call	Users can start a call from a browser by right-clicking on any number, URI, or alphanumerical string.	Cisco Jabber for Windows Cisco Jabber Softphone for VDI
Calendar Integration and Contact Resolution	Lets users view their events from the Meetings tab. Also, let users search for their local contacts.	All clients
Call Park	You can use call park to place a call on hold and pick it up from another phone in a Cisco UnifiedCommunication Manager system.	All clients
Call Pickup	Call pickup allows users to pick up incoming calls from a group.	Cisco Jabber for Windows Cisco Jabber for Mac Cisco Jabber Softphone for VDI Cisco Jabber for Android Cisco Jabber for iPhone and iPad
Chat History in Microsoft Outlook	Allow users to automatically save chat histories to a Cisco Jabber Chats folder in the user's Microsoft Outlook application.	Cisco Jabber for Windows Cisco Jabber for Mac Cisco Jabber Softphone for VDI

Feature Name	Description	Supported Clients
Chromebook	Allow users to download Cisco Jabber for Android into their Chrombook from Google Play Store. Cisco Jabber on Chromebook works as an Android tablet. Users can access all Cisco Jabber services on Chromebook when connecetd over MRA.	Cisco Jabber for Android.
Cisco Jabber Mobile App Promotion	Allow users to enable a notificaton to promote the use of the Cisco Jabber for Mobile App (Android and iOS).	Cisco Jabber for Windows Cisco Jabber Softphone for VDI
Collaboration Meetings Rooms	Cisco Collaboration Meeting Rooms (CMR) Cloud provides easy access for users to join or start Webex Meetings.	All clients
Custom Embedded Tabs	Custom embedded tabs display HTML content in the client interface.	All clients
Custom Emoticons	Add custom emoticons to Cisco Jabber for Windows by creating emoticon definitions in an XML file and saving it to the file system.	Cisco Jabber for Windows Cisco Jabber Softphone for VDI
Dial via Office	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 for mobile clients
DND Status Cascading	When a user manually sets the IM Presence status as Do Not Disturb from the Cisco Jabber client, then the status is cascaded down to all the phone devices that are owned by the user.	All clients
Enterprise Groups for Cisco Unified Communications Manager IM and Presence Service	Cisco Jabber users can search for groups in Microsoft Active Directory and add them to their contact lists.	All clients
Far End Camera Control	Allow users to adjust the far-end camera to give a better view during video calls.	All clients

Feature Name	Description	Supported Clients
File Transfers and Screen Captures	Allow users to transfer files and screen captures to other users, ad hoc group chat rooms, and persistent chat rooms.	All clients
Flexible DSCP Values	Flexible Differentiated Services Code Point (DSCP) allows you to specify different DSCP values to separate the audio and video streams on the network.	Cisco Jabber for Mac Cisco Jabber for mobile clients
Hunt Group	A Hunt Group is a group of lines that are organized hierarchically, so that if the first number in the hunt group list is busy, the system dials the second number. If the second number is busy, the system dials the next number, and so on.	All clients
IBM Notes Contact Search and Calendar Integration	Cisco Jabber for Windows supports IBM Notes calendar integration in the Meetings tab of the client. Cisco Jabber also lets users search for and add local contacts from IBM Notes.	Cisco Jabber for Windows Cisco Jabber Softphone for VDI
Integration with Microsoft Products	Cisco Jabber supports a range of Microsoft products that integrate with the application: • Internet Explorer • Microsoft Office • Microsoft Office 365 • Microsoft SharePoint	Cisco Jabber for Windows Cisco Jabber for Mac Cisco Jabber Softphone for VDI
Jabber to Jabber Call	Jabber to Jabber voice and video calling provides basic calling capabilities between two Cisco Jabber clients without using Cisco Unified Communications Manager.	All clients
Let Users Without Voicemail Ignore Calls	Choose a No Voicemail profile for users who don't have voicemail configured.	All clients
Location Sharing	Allow users to share their location with their contacts.	Cisco Jabber for Windows Cisco Jabber for Mac

Feature Name	Description	Supported Clients
Logout Inactivity Timer	The sign out inactivity timer allows you to automatically sign users out of the client after a specified amount of time of inactivity.	All clients
Mac Calender Integration for Meetings	Allow users to connect their calendars to their Cisco Jabber client.	Cisco Jabber for Mac
Microsoft Outlook Calendar Events	Display Microsoft Outlook calendar events in the Meetings tab of Cisco Jabber.	Cisco Jabber for Windows Cisco Jabber Softphone for VDI
Microsoft Outlook Presence Integration	Display presence status in Microsoft Outlook	Cisco Jabber for Windows Cisco Jabber for Mac Cisco Jabber Softphone for VDI
Move to Mobile	Users can transfer an active VoIP call from Cisco Jabber to their mobile phone number on the mobile network.	Cisco Jabber for mobile clients
Multiline	You can configure multiple phone lines for your users to perform daily Cisco Jabber tasks. You can add up to eight phone lines per user.	Cisco Jabber for Windows Cisco Jabber for Mac Cisco Jabber Softphone for VDI
Multiple Device Messaging for Cloud Deployments	Users who are signed into multiple devices can see all sent and received IMs on each device regardless of which device is active.	All clients
My Jabber Chats and My Jabber Files Directory Location	Specify a directory location for saved instant messages and file transfers, or let users specify their own location.	Cisco Jabber for Windows Cisco Jabber Softphone for VDI
Persistent Chat Rooms	Persistent chat is a permanent chat room that offers ongoing access to a discussion thread. It is available even if no one is currently in the chat room and remains available until explicitly removed from the system.	All clients

Feature Name	Description	Supported Clients
Personal Rooms	A personal room is a virtual conference room that is always available and can be used to meet with people. Cisco Jabber uses the personal room feature of Cisco Webex Meetings to allow users to easily meet with their contacts using the Meet Now option in the client.	All clients
Problem Reporting	Problem reporting enables users to send a summary of issues that they encounter with the client.	All clients
Prompts for Presence Subscription Requests	You can enable or disable prompts for presence subscription requests from contacts within your organization.	All clients
Push Notification Services for Instant Messaging	The Push Notification service for IM forwards the new IM notification to Cisco Jabber, even if Cisco Jabber is inactive. **Note** When Push Notifications are enabled and Cisco Jabber for Android is inactive, the Android title bar does not display a Jabber icon.	Cisco Jabber for iPhone and iPad, and Android in Jabber team messaging mode.
Push Notification Services for Video and Voice Calls	Receive notification about the incoming voice and video calls, even if Cisco Jabber is inactive. **Note** When Push Notifications are enabled and Cisco Jabber for Android is inactive, the Android title bar does not display a Jabber icon.	Cisco Jabber for iPhone and iPad, and Android.
Restore Chats on Login	Allows users to specify if open 1:1 chat sessions are restored on next sign in.	All clients

Feature Name	Description	Supported Clients
Set Device PIN	You can configure if Jabber checks that the device is secured with a PIN.	Cisco Jabber for mobile clients
Sign into Cisco Jabber Using Face or Fingerprint Recognition	Cisco Jabber supports Touch ID, Face ID, or fingerprint authentication for users to securely sign in.	Cisco Jabber for mobile clients.
Silent Monitoring and Call Recording	Silent call monitoring allows a supervisor to hear both call participants, but neither of the call participants can hear the supervisor. Call recording enables a recording server to archive agent conversations.	All clients
Single Number Reach	You can answer incoming Cisco Jabber calls from any other phone or device such as your mobile or home phone using single number reach.	All clients
Telemetry	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.	All clients
Temporary Presence	You can configure when users can see availability status for contacts in their contact list.	All clients
URI Dialing	URI dialing allows users to make calls and resolve contacts with Uniform Resource Identifiers (URI).	All clients
Voicemail Avoidance	Voicemail avoidance is a feature that prevents calls from being answered by the mobile service provider voicemail.	All clients

Feature Name	Description	Supported Clients
Wireless Location Monitoring Service	Wireless location monitoring service allows you to determine the physical location from where your Cisco Jabber users connect to the corporate network.	All clients except Cisco Jabber Softphone for VDI

CHAPTER 2

Chat and presence

Blocked Domain Support for Webex Messenger Users

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
—	Yes	—	—

Webex Messenger users can now add a specific domain or a contact from a specific domain to the blocked list. Contacts from the specified domain cannot view your availability or send you instant messages.

This feature can be used to prevent spam messages from the non-approved domains. Enterprise compliance is maintained by allowing communications only between organization approved domains.

Step 1 Select **Jabber** > **Preferences** > **Privacy**.

Step 2 Choose the **Policies** section and select **Managed Blocked People**.

Step 3 Add the contact ID or domain in the **Blocked list**.

Chat Bots

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

Jabber clients can be used to interact with XMPP chat bots. A chat bot is an automated service that appears and behaves like a user in Jabber. A Jabber user can add a chat bot to their Contacts list and start a chat conversation with the bot.

You can develop chat bots to help with a business process, answer questions, or have fun. A bot can be as simple as issuing an alert message, like whenever a stock price changes, or a machine sensor that reports a temperature change. More advanced bots can interact with users using artificial intelligence to try and understand the intent of questions it may be asked, like *“Book me a meeting room for next Tuesday in the Dallas office please”*.

Cisco provides an SDK for developers to build bots. The SDK provides a Node.js framework for quickly developing bots based on the public domain Botkit project. Visit the Cisco Devnet for Cisco Jabber Bot SDK Introduction.

If you develop a chat bot developed using the SDK, you must create a Jabber user account in Cisco Webex Messenger or Cisco Unified Communications Manager. You only need to provision the bot for IM.

After you've created a bot, Cisco Jabber users can manually add the bot to their contacts list or you can automatically add it to the users' contacts lists using the `AdminConfiguredBot` parameter. The `AdminConfiguredBot` parameter is not supported in Cisco Jabber for Android. You also have to configure `WhitelistBot` parameter that allows the bot to start a call or a group chat, search for Jabber users to start a conference call, and set up meetings in Cisco Jabber. Cisco Jabber supports both plain text and rich text messaging with Bots.

For more information on configuring `AdminConfiguredBot` and `WhitelistBot` parameters, see the *Parameters Reference Guide for Cisco Jabber*.

Browser Click to Call

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	—	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

With Browser Click to Call, users can start a call from any of the following browsers:

- Internet Explorer, from version 9
- Mozilla Firefox, from version 38.0a1
- Google Chrome, from version 45

Users can highlight and right-click on any number, URI, or alphanumerical string and choose one of the following options:

- Call—Spaces and punctuation are stripped and the call is started.
- Call with Edit—Spaces and punctuation are stripped and the number is displayed in the Search box of the hub window. Users can edit the number before starting the call.

Browser Click to Call is enabled with the CLICK2X installation parameter. If this parameter is set to ENABLED (default value), the feature is enabled. To disable this feature, you must set the CLICK2X installation parameter to DISABLE. For more information about the CLICK2X parameter, see the Deployment Guide for your release.

Click to Call from Google Chrome

Click to Call from the Google Chrome browser requires user input before it can be enabled. After users install and sign into Cisco Jabber, they must restart the Google Chrome browser. When the browser opens, a popup displays requesting users to allow installation of the "Jabber Call" extension. Users must allow the installation by clicking **Enable Extension**. The extension is installed and users can now make calls by highlighting and right-clicking on any phone number that is displayed in the browser.

If users do not have administrator privileges for their machine, they do not receive the popup requesting them to allow installation of the "Jabber Call" extension. In this case, users must contact their system administrator to install the extension.

Click to Call from Mozilla Firefox

Click to Call from the Mozilla Firefox browser requires user input before it can be enabled. After users install Cisco Jabber, they must restart the Firefox browser. When the browser opens, a popup displays requesting users to allow installation of the “JabberCallAddOn” add-on. Users must allow the installation by clicking **Allow this installation** and **Continue**. The add-on is installed and users can now make calls by highlighting and right-clicking on any phone number that is displayed in the browser.

Click to Call from Internet Explorer

Click to Call from the Internet Explorer browser does not require any user permissions or installations.

Custom Emoticons

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	—	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

You can customize Jabber’s emoticon library by either replacing existing emoticons or creating your own. To do this, you’ll need to add your image files to Jabber’s emoticon directory and write new file definitions.

Custom emoticons are visible only to users whose local Jabber installation shares the same custom images and definitions.

Step 1 In your program files, go to the `Cisco Systems\Cisco Jabber` directory and create a folder named `CustomEmoticons`.

Step 2 Create your custom emoticon image as a PNG file in three resolutions: 20 × 20 pixels, 40 × 40 pixels, and 60 × 60 pixels. For best results, use RGB color values and a transparent background. Save these files in the `CustomEmoticons` folder and name them in this format: `example.png` (20 × 20 pixels), `example@2.png` (40 × 40 pixels), and `example@3.png` (60 × 60 pixels).

Step 3 Define your emoticons in the `emoticonDefs.xml` file and the `emoticonRetinaDefs.xml` file, both of which can be found in the `Cisco Systems\Cisco Jabber\Emoticons` directory. The `emoticonDefs.xml` file defines standard-definition emoticons (20 × 20 pixels), while the `emoticonRetinaDefs.xml` file defines the images for high-DPI displays (40 × 40 pixels). Both sets of definitions are required for normal functioning in most systems. See *Emoticon Definitions* for information on the structure and available parameters for these files. New definitions load when you restart Jabber.

Emoticons that you define in the `CustomEmoticons` folder take precedence over emoticon definitions in the default `Emoticons` folder.

Emoticons that you define in the directory `%`*USERPROFILE*`%\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\CustomEmoticons`, which contains custom emoticon definitions for individual instances of Cisco Jabber for Windows, take precedence over emoticon definitions in the `CustomEmoticons` folder in the installation directory.

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	This attribute defines the default key combination that renders the emoticon. Specify any key combination as the value. This attribute is required. defaultKey is an attribute of the emoticon element.
image	This attribute specifies the filename of the emoticon image. Specify the filename of the emoticon as the value. The emoticon image must exist in the same directory as `emoticonDefs.xml`. This attribute is required. Cisco Jabber for Windows supports any icon that the Chromium Embedded Framework can render, including `.jpeg`, `.png`, and `.gif`. image is an attribute of the emoticon element.
text	This attribute defines the descriptive text that displays in the **Insert emoticon** dialog box. Specify any string of unicode characters. This attribute is optional. text is an attribute of the emoticon element.
order	This attribute defines the order in which emoticons display in the **Insert emoticon** dialog box. Specify an ordinal number beginning from 1 as the value. order is an attribute of the emoticon element. This attribute is required. However, if the value of hidden is **`true`** this parameter does not take effect.

Element or attribute	Description
hidden	This attribute specifies whether the emoticon displays in the **Insert emoticon** dialog box. Specify one of the following as the value: **true** Specifies the emoticon does not display in the **Insert emoticon** dialog box. Users must enter the key combination to render the emoticon. **false** Specifies the emoticon displays in the **Insert emoticon** dialog box. Users can select the emoticon from the **Insert emoticon** dialog box or enter the key combination to render the emoticon. This is the default value. This attribute is optional. hidden is an attribute of the emoticon element.
alt	This element enables you to map key combinations to emoticons. Specify any key combination as the value. 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. This element is optional.

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>
```

DND Status Cascading

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

The following scenario occurs when the IM Presence service is supported only by Cisco Unified Communications Manager IM and Presence Service.

When a user manually sets the IM Presence status as **Do Not Disturb** from the Cisco Jabber client, then the status cascades down to all the phone devices that the particular user owns.

However, if the user manually sets the status as **Do Not Disturb** from any of the phone devices, then the status does not cascade to other phone devices that the particular user owns.

Enterprise Groups for Unified CM IM and Presence Service

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	—	—	—

Users can add groups to their contact lists in Cisco Jabber. The groups are created in the enterprise's Microsoft Active Directory and then are imported into Cisco Unified Communications Manager IM and Presence Service. When enterprise groups are set up and enabled on Unified CM IM and Presence Service, Cisco Jabber users can add enterprise groups to their contact list from the client.

Using enterprise groups is supported when on the Expressway for Mobile and Remote Access.

Prerequisites for Enabling Enterprise Groups in Cisco Jabber

- Cisco Unified Communications Manager Release 11.0(1) or later
- Cisco Unified Communications Manager IM and Presence Service Release 11.0 or later

Before you can set up enabling adding enterprise groups to contact lists for your users, you must configure the feature on the server, see *Enable Enterprise Groups* section. For more information about enterprise groups, see the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Limitations

- This feature is available to on-premises deployments only. Cloud deployments already support Enterprise Groups.
- Security Group is supported from Cisco Unified Communications Manager IM and Presence Service 11.5 or later.
- Presence is unsupported for contacts in enterprise groups of over 100 people who are IM-enabled, unless the user has other presence subscriptions for a contact. For example, if users have someone added to their personal contact list who is also listed in an enterprise group of over 100 people, then presence is still displayed for that person. Users who are not IM-enabled do not affect the 100 person presence limit.
- Nested groups cannot be imported as part of an enterprise group. For example, in an AD group, only group members are imported, not any embedded groups within it.
- If your users and AD Group are in different organizational units (OUs), then before you add the contacts to the AD Group, you must sync both OUs with Cisco Unified Communications Manager, and not just the OU that the AD Group is in.
- If you have the minimum character query set to the default value of 3 characters, then user searches for enterprise groups will exclude any two letter group names (for example: HR). To change the minimum character query for CDI or UDS connections, change the value of the MinimumCharacterQuery parameter.
- Enterprise groups with special characters cannot be located during searches if the special characters are among the first 3 characters (or whatever value you have defined as the minimum character query) of the name.
- We recommend that you only change the distinguished name of enterprise groups outside of core business hours, as it would cause unreliable behavior from the Cisco Jabber client for users.
- If you make changes to enterprise groups, you must synch the Active Directory with Cisco Unified Communications Manager afterwards in order for the changes to be applied.
- When a directory group is added to Cisco Jabber, the profile photos are not displayed immediately because of the sudden load that the contact resolution places on the directory server. However, if you right-click on each group member to view their profile, the contact resolution is resolved and the photo is downloaded.
- Intercluster peering with a 10.x cluster: If the synced group includes group members from a 10.x intercluster peer, users on the higher cluster cannot view the presence of synced members from the 10.x cluster. This is due to database updates that were introduced in Cisco Unified Communications Manager Release 11.0(1) for the Enterprise Groups sync. These updates are not a part of the Cisco Unified Communications Manager Releases 10.x. To guarantee that users homed on higher cluster can view the presence of group members homed on the 10.x cluster, users on the higher cluster should manually add the 10.x users to their contact lists. There are no presence issues for manually added user.

UDS Limitations (Applies to Users on the Expressway for Mobile and Remote Access or with UDS on-premises)

There is no search capability for enterprise groups when connecting using UDS, so users must know the exact enterprise group name that they want to add to their contact lists.

Enterprise group names are case-sensitive.

If two enterprise groups within an AD Forest have the same name, then users get an error when trying to add the group. This issue does not apply to clients using CDI.

File Transfers and Screen Captures

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

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.

To configure file transfers and screen captures in Cisco Unified Communications Manager IM and Presence Service 9.x or later, see *Enable File Transfers and Screen Captures.*

Cisco Unified Communications Manager IM and Presence Service, release 10.5(2) or later provides additional file transfer options:

- For peer to peer chats, see *Enable File Transfer and Screen Captures for Peer to Peer Chats only*.
- For group chats and chat rooms, see *Enable File Transfer and Screen Captures for Group Chat Rooms*.
- To configure maximum file transfer size, see *Configuring Maximum File Transfer Size*.

What to do next

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 *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager* guide.

Enable File Transfers and Screen Captures

This applies to Cisco Unified Communication Manager IM and Presence Service 9.x, 10.0.x, and 10.5.1. You can enable or disable file transfers and screen captures using the Cisco XCP Router service on Cisco Unified Communications Manager IM and Presence Service. File transfers and screen captures parameter is enabled by default.

File transfers and screen captures are supported for both desktop and mobile clients.

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

Jabber stores transferred files and screen captures on a file server and logs the metadata to a database server. This feature adds the following functionality:

- File transfers in group chats using Cisco Jabber clients that don't support chat rooms
- File transfers and screen captures in peer-to-peer chats

Before you begin

This feature is available only on Cisco Unified Communications Manager IM and Presence Service, release 10.5(2) or later.

Configure an external database to log metadata associated with the file transfer. For more information, see *Database Setup for IM and Presence Service on Cisco Unified Communications Manager*.

Configure a network file server to save the transferred files. For more information, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

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 public key for the node to the `authorized_keys` file on the external file server. Include the IP address, hostname, or FQDN for the node.
- Ensure that the **Cisco XCP File Transfer Manager** service is active.

- Restart the **Cisco XCP Router** service.

On the DNS server, configure automatic login for Jabber using the _cisco-uds and _collab-edge service (SRV) records. For more information about SRV records, see Service (SRV) Records.

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, release 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.

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.

ECM File Attachment Configuration

The Enterprise Content Manager (ECM) file attachment feature extends Cisco Jabber file attachment to allow users to upload files from OneDrive or SharePoint Online. Users can then view the file and send them through chat to other Jabber users who are authorized to view them.

When users send attachments, they can choose to upload files from their computer or ECM account. Users can choose to send the files to other people in their organization, or to specific people who have access to the file. When the recipient gets the message with the ECM attachment, they must be signed in to that ECM service before they can view or open the file.

Configure ECM File Attachment

Step 1 To enable ECM file attachment for users, go to the **Control Hub**, and select **Settings**.

Step 2 Under **Content Management**, select **Edit Settings** and choose **Microsoft** to enable ECM with OneDrive and SharePoint Online.

Configuring Maximum File Transfer Size

The maximum file size is only available on Cisco Unified Communications Manager IM and Presence Service, release 10.5(2) or later.

Before you begin

The file transfer type selected is **Managed File Transfer**.

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.

Location Sharing

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

Location sharing allows users to share their location with their contacts. When the client detects a new network connection, it prompts the user to name the location: for example, "Home Office" or "San Jose." That name appears next to the user's presence status when they're connected to that network. Location sharing is enabled by default.

You can use the following parameters to configure location sharing. See the *Parameters Reference Guide* for more information.

- Location_Mode: Determines whether the feature is enabled.
- LOCATION_MATCHING_MODE: Determines how Jabber detects the current network location
- Location_Enabled: Determines whether the location tab appears on the client interface.

If the ShowIconWhenMobile parameter is enabled, when a user is signed in to both a desktop and mobile client, only the desktop location is visible.

Location of Saved Chats and Files on Windows

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	—	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	—	Yes

You can automatically save instant messages and transferred files each time a user closes a conversation using the EnableAutosave parameter. That parameter applies for both Windows and Mac. (See the *Parameters Reference Guide* for the Mac behavior.)

In Windows, the default locations for the saved chats and files are `..\documents\MyJabberChats` and `..\documents\MyJabberFiles`. However, you can specify a different location with the AutosaveChatsLocation parameter or let users choose their own location with the AllowUserSelectChatsFileDirectory parameter. If you allow users to set their own directory location, then the user preference takes priority over the system-defined setting. For more information about these Windows-only parameters, see the *Parameters Reference Guide* for your release.

Multiple Device Messaging for Cloud and On-Premises Deployments

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

Multiple Device Messaging for on-premises deployments requires Cisco Unified Communications Manager IM and Presence 11.5.

Users who are signed into multiple devices can see all sent and received IMs on each device regardless of which device is active. Notifications are synchronized; if an IM is read on one device, it shows as read on other signed-in devices. This feature is enabled by default, but can be disabled with the Disable_MultiDevice_Message parameter. The following limitations apply:

- Clients must be signed-in. Signed-out clients do not display sent or received IMs or notifications.

- File transfer is not supported. Files are available only on the active devices that sent or received the file.
- Group chat is not supported.
- Multiple device messaging cannot be enabled if AES encryption is required.

Feature Functionality	Description
Active Jabber clients enabled for Multiple Device Messaging	Sent and received messages are displayed for the entire conversation.
Inactive Jabber clients enabled for Multiple Device Messaging but signed in	Sent and received messages are displayed for the entire conversation.
Non-Multiple Device Messaging enabled Jabber clients and AES Encryption enabled Jabber clients	Sent messages are only seen on sending device. Received messages are displayed on active devices only.

For more information on parameters, see the latest *Parameters Reference Guide for Cisco Jabber*.

Enable Multiple Device Messaging

This configuration procedure is applicable for on-premises deployment.

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the IM and Presence Service Publisher node.

Step 3 From the **Service** drop-down list, choose **Cisco XCP Router (Active)**.

Step 4 Choose Enabled or Disabled, from the **Enable Multi-Device Messaging** drop-down list.

Step 5 Click **Save**.

People Insights

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
—	—	Yes	—

People Insights provides users with expanded profiles of their contacts. Anywhere a contact card appears, user can access People Insights: contact lists, in conversations, from the call history, and voicemail history. The feature displays publicly available information in each user's profile.

For contacts in the same organization, users can also see the internal company directory information for those contacts. This information is not visible to users outside the company. People Insights stores the company directory information in a separate data source from the publicly available information.

Each user can choose to add more data by editing their People Insights profile. A user can also choose to hide parts or all of their People Insights profile.

People Insights encrypts the profile data both in transit and at rest. The feature is compliant with the General Data Protection Regulation (GDPR). For more information, see What Is People Insights.

Enable People Insights

Before you begin

You can enable People Insights if your deployment meets these conditions:

- You use Common Identity (either CI-enabled or CI-linked).
- You enable Directory Synchronization.

People Insights is currently English-only.

To enable People Insights, go to the **Control Hub**, and select **Settings** > **Directory Synchronization and People Insights** and turn on the **Show People Insights** toggle.

Persistent Chat Rooms

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	—	—	—

Note In cloud deployments, you use WebEx Messenger group chats or Jabber team messaging mode instead of persistent chat rooms.

Persistent chat rooms offer you ongoing access to a discussion thread. The room persists even if no one is currently active in the chat. The room remains available until you explicitly remove it from the system. These rooms allow users to participate with team members, customers, and partners in other locations, countries, and time zones. New users can quickly gain the context for an ongoing conversation, making collaboration easier in real time.

Configure Persistent Chat

You enable and configure persistent chat on Cisco Unified Communications Manager IM and Presence Service before users can access persistent chat rooms on the client. Persistent chat rooms are not available in Webex Messenger mode or Jabber team messaging mode.

Before you begin

For Cisco Jabber desktop clients, persistent chat is available on Cisco Unified Communications Manager IM and Presence Service 10.0 and later. For Cisco Jabber mobile clients, Persistent chat is available on Cisco Unified Communications Manager IM and Presence Service 11.5 su5.

See *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* for information on the database configuration to support persistent chats. Perform that database configuration before continuing with this task.

Enable local chat message archiving for persistent chat. You enable local chat message archiving on Cisco Unified Communications Manager IM and Presence Service using the **Allow clients to log instant message history** setting. For more information, see the *Enable Message Settings* topic in the *On-Premises Deployment Guide*.

If you sign into Cisco Jabber on multiple clients, reading a message once marks it read on all clients.

If you enable the Push Notification service, Cisco Jabber chat rooms receive push notifications. This behavior continues even if the user manually terminates Cisco Jabber from the device. For more information on Push Notification, see Push Notification Service for IM, on page 31.

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 the following table.

Note Persistent chat rooms inherit their settings when you create the room. Later changes do not apply to existing rooms. Those changes only apply to rooms created after the changes take effect.

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	Persistent chat does not currently use this value.
Archive all room messages	Enabled	

Persistent Chat Setting	Recommended Value	Notes
Allow only group chat system administrators to create persistent chat rooms	Administrator Defined	
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	Cisco Jabber does not use this value for persistent chat.
Room owners can change whether users can add themselves to rooms as members	Disabled	Cisco Jabber does not use this value for persistent chat.
Members and administrators who are not in a room are still visible in the room	Enabled	Cisco Jabber requires you to enable this setting.
Room owners can change whether members and administrators who are not in a room are still visible in the room	Enabled	Cisco Jabber does not use this value for persistent chat.
Rooms are backwards-compatible with older clients	Disabled	Cisco Jabber does not use this value for persistent chat.
Room owners can change whether rooms are backwards-compatible with older clients	Disabled	Cisco Jabber does not use this value for persistent chat.
Rooms are anonymous by default	Disabled	Cisco Jabber does not support this value for persistent chat. Cisco Jabber cannot join anonymous rooms.
Room owners can change whether or not rooms are anonymous	Disabled	Cisco Jabber does not support this value for persistent chat. Cisco Jabber cannot join anonymous rooms.
Lowest participation level a user can have to invite others to the room	Default Value	Cisco Jabber does not use this value for persistent chat.

Persistent Chat Setting	Recommended Value	Notes
Room owners can change the lowest participation level a user can have to invite others to the room	Disabled	Cisco Jabber does not use this value 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	
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	Cisco Jabber does not use this value for persistent chat.
Room owners can change XHTML formatting setting	Disabled	Cisco Jabber does not use this value for persistent chat.
Rooms are moderated by default	Disabled	Cisco Jabber does not use this value for persistent chat.
Room owners can change whether rooms are moderated by default	Default Value	Cisco Jabber does not use this value for persistent chat.
Maximum number of messages that can be retrieved from the archive	Default Value	
Number of messages in chat history displayed by default	Administrator Defined	Cisco recommends a value from 15 through 50. The **Number of messages in chat history displayed by default** setting does not apply retroactively to persistent chat rooms.
Room owners can change the number of messages displayed in chat history	Default Value	Cisco Jabber does not use this value for persistent chat.

What to do next

Ensure that you configure any client-specific parameters for persistent chat:

- **Desktop clients**—Set Persistent_Chat_Enabled to **`true`**.
- **Mobile clients**—Set Persistent_Chat_Mobile_Enabled to **`true`**.

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

Administer and moderate persistent chat rooms

In the Jabber client, you can administer persistent chat rooms by creating rooms, delegating their moderators, and specifying members. Jabber automatically chooses the node on which to create the room, but you can override and specify a 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 the IM and 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 does not delete the history).

Note An administrator cannot create rooms, add or remove moderators, block or revoke participants in Cisco Jabber for mobile clients.

Moderator Capabilities

An administrator can define up to 30 moderators for one persistent chat room. Moderators can perform these tasks:

- Change the subject of a room.
- Edit members (which includes adding, removing, and banning them).

Room Creation

When creating a room, you can set these properties:

- Room name (required, maximum 200 characters)
- Description
- Room type (public or restricted)

  After you define the room type, no one can change it.
- Location

  Decide on which node to create the room. For details, see Load-balancing for persistent chat rooms , on page 28.
- Specify whether to add the room to your **My Rooms** tab.
- Add up to 30 moderators (who must have a valid Jabber ID to moderate a room).
- Room password

After you create the room, you can add members to the room immediately or later. Refresh the **All Rooms** list to display your new room in the available rooms.

Load-balancing for persistent chat rooms

When you create a new persistent chat room, Jabber assigns the room to a random node by default. You can also assign the room to a specific node through the **Location** drop-down.

If the participants are in the same region, you get better performance by creating the room in your home cluster. You can force Jabber to assign persistent chat rooms to your home cluster. In the **New Room** dialog, choose **Automatically select** in the **Location** drop-down.

Note This feature requires IM and Presence Service Release 14 SU 1.

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.

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.

Limitations

If you disable Disable_IM_History parameter, then it affects the @mention feature in persistent chat rooms.

Presence Sync with Cisco Headsets

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

In releases earlier than Jabber 12.9, the desktop client can toggle the presence LED on some Cisco headsets to show when you're on a call. Starting in Jabber 12.9, when you manually toggle the presence LED of your headset, Jabber can reflect that change by setting your presence to DND.

Prompts for Presence Subscription Requests

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

You can enable or disable prompts for presence subscription requests from contacts within your organization. The client always prompts users for 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 deployments and is only available on Cisco Unified Communications Manager, release 8.x or later.

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**.

Push Notification Service for IM

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
—	—	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	—

The Push Notification service for IM forwards the new IM notification to Cisco Jabber, even if Cisco Jabber is inactive, terminated, or is closed by the user. Cisco Jabber supports Push Notification service for cloud and on-premises deployment modes. Cisco Jabber supports:

- Apple Push Notification (APN) for iPhone and iPad
- Firebase Cloud Messaging (FCM) for Android

To deploy Push Notification service for on-premises and cloud deployments, see *Push Notifications Deployment Guide* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

To receive Apple Push Notification (APN) Push Notification service, you must have ports 5223 and 443 open. To receive Firebase Cloud Messaging (FCM) Push Notification service, you must have ports 5228, 5229, 5230, and 443 open. For more details on ports, see the *Ports and Protocols* section of the *Planning Guide for Cisco Jabber*.

To enable Push Notification service, you have to configure the parameter Push_Notification_Enabled for iOS and FCM_Push_Notification_Enabled for Android. For more information about configuring the parameter, see the latest *Parameter Reference Guide for Cisco Jabber*.

From Cisco Jabber for iPhone and iPad Release 12.1 onwards, this feature supports Advance Encryption Standard (AES) for end-to-end encrypted instant messages and also for Jabber-to-Jabber calls.

Note Before Release 14.0(3), Jabber MAM clients on iOS didn't support push notifications for IMs, only for voice calls.

Restore Chats on Login

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

This feature allows users to specify if open chat sessions are restored on next sign in. This only applies to 1:1 chats.

For desktop clients, this feature is configured using the RestoreChatOnLogin parameter. When the parameter is true, the **Remember my open conversations** check box is selected on the **General** tab of the clients. The check box is not checked by default when users sign into Cisco Jabber for the first time.

For mobile clients, this feature is configured using the RememberChatList parameter. When the parameter is set to `on`, then the user's chat list is saved and restored after relaunching Jabber. Also, **Save chat list** option is available in the client.

For more information on parameters, see the *Parameter Reference Guide* for your release.

Temporary Presence

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

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.

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

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

Step 3 Uncheck **Enable ad-hoc presence subscriptions** and then select **Save**.

Cisco Jabber does not display temporary presence. Users can see availability status only for contacts in their contact list.

CHAPTER 3

Voice and video

Meeting Controls for CMS Meetings

Clients			
Windows	Mac	iPhone and iPad	Android
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

Jabber provides meeting control functions through the Cisco Meeting Server (CMS) ActiveControl feature. The meeting control functions include participant lists, muting participants, dropping participants, and changing the video layout.

To use ActiveControl requires the following in your deployment:

- The call path between the endpoint and Meeting Server supports iX media end to end.
- Appropriate permissions enabled in Meeting Server.

For more information on using CMS, see the Cisco Meeting Server, Deployments with Expressway Planning and Preparation Guide.

As of Release 12.5, Jabber can access Cisco Meeting Server conferences as a SIP device through ActiveControl. You can enter an ActiveControl conference by either:

- Dialing into a room that is configured on CMS
- Merging two calls when a CMS room is configured as the conference bridge

Before you begin

To set up ActiveControl, you need:

- Cisco Meeting Server Release 2.3 or later
- Cisco Unified Communications Manager 12.5.1.11900 or later

Note These are the releases with full support for ActiveControl. Earlier releases of Unified CM and Expressway did not support the control functions over Expressway.

Step 1 Configure a SIP trunk in Cisco Unified Communications Manager with CMS to enable communication using SIP signals. For more information, see System Configuration Guide for Cisco Unified Communications Manager.

Step 2 Configure a route pattern in Cisco Unified Communications Manager to route inbound and outbound SIP calls. For more information, see the *Configure Call Routing* chapter in System Configuration Guide for Cisco Unified Communications Manager.

Step 3 Set up rules in CMS for outbound SIP call routing to the Cisco Unified Communications Manager server. For more information, see the Cisco Meeting Server with Cisco Unified Communications Manager Deployment Guide.

Step 4 Configure your CMS space to manage your conference resources. For more information, see Cisco Meeting Server Release API Reference Guide.

Meeting Controls for Webex Meetings

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

Set up Cisco Jabber so users can join Webex meetings from Jabber without having to launch Webex.

Step 1 Configure your outgoing firewall to allow the following domains: *.ciscospark.com, *.wbx2.com, *.webex.com, *.clouddrive.com.

Step 2 Configure a SIP trunk in Cisco Unified Communications Manager with Expressway for MRA and then Webex to enable communication using SIP signals. For more information, see System Configuration Guide for Cisco Unified Communications Manager.

Step 3 Configure a route pattern in Cisco Unified Communications Manager to route inbound and outbound SIP calls. For more information, see the *Configure Call Routing* chapter in System Configuration Guide for Cisco Unified Communications Manager.

Step 4 Set up rules in Webex for outbound SIP call routing to the Cisco Unified Communications Manager server. For more information, see the Cisco Meeting Server 2.3 with Cisco Unified Communications Manager Deployment Guide.

Meeting Control for CMR Meetings

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
—	Yes	Yes	Yes

Cisco Collaboration Meeting Rooms (CMR) Cloud provides easy access for users to join or start a Cisco Webex meeting. Cisco Jabber provides users with the ability to access the meeting either using Cisco Webex interface or join using video.

There's a limitation on CMR Cloud join experience for attendees of scheduled CMR Cloud meetings. This limitation a Mac users and Windows users who haven't enabled Outlook calendar integration. Because of a server limitation, attendees for these deployment scenarios can join the meeting only by using Cisco Webex. Hosts enjoy the full experience, as does anyone invited to join ad hoc CMR Cloud meetings.

User in CTI control mode can join in directly, rather than by using Webex.

This table lists Jabber support for Cisco Meeting Server methods of joining meetings:

Join in Meeting	Jabber Support
Join in meeting from cross launch in Page	N
Join in meeting from Calendar	N
Join in meeting as SIP URL	Y
Join in meeting as HTTP link	Y
Join in meeting by meeting number	Y
Join in meeting using PIN (host and Guest)	Use Room Number instead
Rejoin in meetings	Y

Note As of Release 12.7, Jabber desktop users can choose to join meetings with Jabber or Webex. Administrators can configure a default for the client to use; in this case, the choice doesn't appear in the client.

This table lists the CMR controls that Cisco Jabber supports by client:

Control	Jabber for Windows	Jabber for Mac	Jabber for Android	Jabber for iPhone and iPad	Jabber Softphone for VDI
Device Indicator (Video and Audio)	Y	Y	N	N	Y
Active Speaker	Y	Y	Y	Y	Y
Participant List (Host and Guest)	Y	Y	Y	Y	Y
Assign Host	Y	Y	Y	Y	Y
Mute / Unmute	Y	Y	Y	Y	Y
Mute All / Unmute All	Y	Y	Y	Y	Y
Self-Mute / Unmute	Y	Y	Y	Y	Y
Drop Participant	Y	Y	Y	Y	Y
Admit People from Lobby	Y	Y	Y	Y	Y

Control	Jabber for Windows	Jabber for Mac	Jabber for Android	Jabber for iPhone and iPad	Jabber Softphone for VDI
Wait in Lobby	Y	Y	Y	Y	Y
End Meeting	Y	Y	Y	Y	Y
Leave Meeting and Assign Host	Y	Y	Y	Y	Y
Lock and Unlock Meeting	Y	Y	Y	Y	Y
Start and Stop Recording	Y	Y	Y	Y	Y
Copy Meeting Link	Y	Y	N	N	Y
Video Layout	Y	Y	Y	Y	Y
Desktop Sharing Send and Receive	Y	Y	Y	Y	Y
Sharing Layout Change	Y	Y	Y	Y	Y
Meeting Information	Y	Y	N	N	Y
Recording Pause / Resume	Y	Y	N	N	Y
Paired Participant with Teams	Y	Y	N	N	Y
Add Participant	N	N	N	N	N
Mobile Remote Access	Y	Y	Y	Y	Y

Before you begin

WebEx Meeting Center videos (CMR) Cloud is available on Cisco Webex Meetings.

Step 1 Configure the Collaboration Meeting Room options.

For more information, visit https://help.webex.com/:

- Site Administration—https://help.webex.com/en-us/6maub2/Configure-Webex-Meetings-in-Cisco-Webex-Site-Administration
- Control Hub—https://help.webex.com/en-us/n8pgczj/Configure-Teleconferencing-Options-for-a-Webex-Site-in-Cisco-Webex-Control-Hub

Step 2 Enable Collaboration Meeting Rooms for your users, on Cisco Webex Meetings.

Step 3 Enable Common Identity (CI) for your Webex site.

If your Webex site isn't CI-enabled, users who join meetings from Jabber get audio and video controls only. They can also share their screens.

Step 4 Collaboration Meeting Room features uses SIP URI, you must enable URI dialing for your users on Cisco Unified Communications Manager. For more information on URI dialing, see the *URI Dialing* topic.

Bridge Escalations

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

Bridge escalations allow users to quickly escalate a group chat to a conference call. Participants are automatically added without the need to merge them into the conference call.

Step 1 Enable bridge escalations in Cisco Jabber clients by setting the EnableBridgeConferencing parameter to true in the `jabber-config.xml` file.

Step 2 (Optional) Specify a mask for the room URI in the UserBridgeUriAdmin parameter in the `jabber-config.xml` file. If you don't specify a mask the user can enter a DN or a SIP URI in the client.

Step 3 Enable URI dialing to allow your users enter a SIP URI for the conference call number. For more information on URI dialing, see the *URI Dialing* topic.

Call Park

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

You can use call park to place a call on hold and pick it up from another phone in a Cisco Unified Communications Manager system. Call park must be enabled and extension numbers must be defined on each Cisco Unified Communications Manager node in the 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 *Feature Configuration Guide for Cisco Unified Communications Manager*.

Step 1 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.

Step 2 Configure a partition

Create a partition to add a call park number.

Step 3 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.

Call Pickup

The Call Pickup feature allows users to answer calls that come in on a directory number other than their own. Call pickup groups have assigned directory numbers. Cisco Unified Communications Manager (Unified CM) automatically dials the appropriate call pickup group number. Users select **Pickup** to answer the call.

Group call pickup

This setting allows users to pick up incoming calls in another group. Users enter the group pickup number, select **Pickup**, and Unified CM automatically dials the appropriate call pickup group number. The user can then pick up an available call in that group.

Other group pickup

This setting allows users to pick up incoming calls in a group that is associated with their group. When the user selects **Other Pickup**, Unified CM automatically searches for the incoming call in the associated groups and connects the call.

Directed call pickup

This setting allows users to pick up an incoming call on a directory number. Users enter the directory number, select **Pickup** and Unified CM connects the incoming call.

To enable call pickup, you use these parameters in the `jabber-config.xml` file, depending on the types of call pickup that you support:

```
<Policies>
  <EnableCallPickup>true</EnableCallPickup>
  <EnableGroupCallPickup>true</EnableGroupCallPickup>
  <EnableOtherGroupPickup>true</EnableOtherGroupPickup>
  <EnableHuntGroup>true</EnableHuntGroup>
</Policies>
```

For more information about configuring call pickup, see the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Call Pickup Notifications

For multiple incoming calls, a notification, *Call(s) available for pickup*, appears. When the user answers a call, the user gets connected to the longest ringing call.

Desk Phone Mode

In desk phone mode, the following limitations apply:

- The Unified CM notification settings aren't supported for the pickup group. The call pickup notification that displays is *CallerA->CallerB*.
- The Unified CM settings for audio and visual settings aren't supported. The visual alerts always appear.

Shared Line Behavior

For users that have a desk phone and also audio on computer with a shared line, the following limitations apply:

- For an attempt to pick up a call using the client when no call is available, *No call available for PickUp* displays on the desk phone.
- For an attempt to pick up a call using the desk phone when no call is available, *No call available for PickUp* displays on the client.

User Not a Member of an Associated Group

For an incoming call to another pickup group where the user isn't a member of an associated group:

- You can use directed call pickup to pick up the incoming call.
- Group pickup doesn't 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:

- If you enter an invalid number:
    - Audio on computer mode—The conversation window appears and the user hears the annunciator immediately.
    - Desk phone mode—The conversation window, fast busy tone, or the annunciator occurs followed by the fast busy tone, *Pickup failed* error message.
- If you enter a valid number with no active call available to pick up:

    - Audio on computer mode—Tone in the headset, no conversation window appears, and *No call available for pickup* error message.
    - Desk phone mode—No conversation window and *No call available for pickup* error message

- If you enter a directory number of a phone in an associated group with no active call available to pick up:
    - Audio on computer mode—Tone in the headset, no conversation window appears, and *No call available for pickup* error message.
    - Desk phone mode—No conversation window and *No call available for pickup* error message

- If you enter a directory number of a phone not in an associated group, but on the same Unified CM node:
    - Audio on computer mode—The conversation window appears and fast busy tone.
    - Desk phone mode—The conversation window appears, fast busy tone, and *Pickup failed* error message.

- If you enter the first digits of a valid group:
    - Audio on computer mode—Tone in the headset, conversation window appears, and, after 15 seconds, the annunciator followed by the fast busy tone.
    - Desk phone mode—The conversation window appears, after 15 seconds, the annunciator, fast busy tone, and *Pickup failed* error message.

Call Pickup Using a Desk Phone That Isn't in a Call Pickup Group

If a user attempts a call pickup from a desk phone that isn't in a call pickup group, the conversation window appears for a moment. Don't configure users to use the call pickup feature if they aren't members of a call pickup group.

Original Recipient Information Not Available

When the Unified CM *Auto Call Pickup Enabled* setting is true, the recipient information isn't available in the client when the call is picked up in audio-on-computer 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.

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.

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.

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 a incoming call directly. The user enters the directory number in the 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.

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 about **Call Pickup**, see the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Configure Auto Call Pickup

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**.

Dial via Office

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
—	—	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	—

Important The following features are not supported if the Dial via Office-Reverse (DvO-R) feature is enabled:

- URI dialing
- Secure Phone

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.

You can make DvO-R calls over Expressway for Mobile and Remote Access when you are outside corporate network. DvO-R is supported on Cisco Expressway X8.7 and Cisco Unified Communications Manager 11.0(1a)SU1.

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.

Note The users do not receive incoming calls on Cisco Jabber in the following situations:

- If users select the **Mobile Voice Network** calling option on any network and the Single Number Reach (SNR) is not configured for their device, they will not receive incoming calls on Cisco Jabber.
- If users select the **Mobile Voice Network** calling option on any network and the Single Number Reach (SNR) is configured with the **Ring Schedule**, they will not receive incoming calls on Cisco Jabber beyond the time set in the **Ring Schedule**.

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	Outgoing: DvO-R	Incoming: Mobile Connect	Outgoing: VoIP	Incoming: VoIP
Noncorporate Wi-Fi						
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 or Android device. See the *Set Up Dial via Office for Each Device* topic for more information.

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.

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** window 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.

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.

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** or **Cisco Dual Mode for Android**.

Step 5 Click **Next**.

Step 6 Scroll down to the Product Specific Configuration Layout section, and verify that you can see the **Video Capabilities** drop-down list.

If you can see the **Video Capabilities** drop-down list, the COP file is already installed on your system.

If you cannot see the **Video Capabilities** drop-down list, locate and download the correct COP file.

Set Up Dial via Office for Each Device

Use the following procedures to set up Dial via Office - Reverse for each TCT or BOT device.

Procedure

	Command or Action	Purpose
Step 1	Add a Mobility Identity for each user.	

	Command or Action	Purpose
Step 2	Enable Dial via Office on each device.	
Step 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.

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.

You must be able to rout this number 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

Setting	Suggested Initial Value
Answer Too Late Timer	20000
Delay Before Ringing Timer	0 **Note** 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 release 9 or earlier — Check the **Enable Mobile Connect** check box.
- Cisco Unified Communications Manager release 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.

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

Step 2 Navigate to the device that you want to configure as follows:

a) Select **Device** > **Phone**.

b) Search for the device that you want to configure.

c) Select the device name to open the **Phone Configuration** window.

Step 3 In the **Device Information** section, check the Enable Cisco Unified Mobile Communicator check box.

Step 4 In the **Protocol Specific Information** section, in the **Rerouting Calling Search Space** drop-down list, select a Calling Search Space (CSS) that can route the call to the DvO callback number.

Step 5 In the **Product Specific Configuration Layout** section, set the **Dial via Office** drop-down list to **Enabled**.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.

Step 8 Instruct the user to sign out of the client and then to sign back in again to access the feature.

Note DVO enabled devices may encounter issues registering with Cisco Unified Communications Manager. Resetting the device from the Cisco Unified Communications Manager administrative interface fixes this issue.

What to do next

Test this feature.

Far End Camera Control (FECC)

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	—

In calls that support far-end camera control (FECC), you can adjust the far-end camera to give you a better view during video calls. FECC is available to users if the endpoint that they are calling supports it.

You can configure whether users can access FECC-enabled endpoints. Disabling the configuration parameter means that users are not provided with the ability to control far-end camera endpoints, even if the endpoint is capable. From a user experience, with FECC disabled, it works the same as dialing in to an endpoint that is not FECC enabled.

To disable FECC, set the EnableFecc parameter to false. For more information about this parameter, see the *Parameters Reference Guide*.

Limitations

FECC is only supported in point-to-point calls, but not in group calls or conferences where multiple video connections are connecting to the same bridge.

FECC is only supported in Softphone mode.

Flexible DSCP Values

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
—	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

Flexible Differentiated Services Code Point (DSCP) allows you to specify different DSCP values to separate the audio and video streams on the network.

The EnableDSCPPacketMarking parameter is used to enable or disable DSCP packet marking in the client.

You can configure the DSCP values for audio calls, video calls, audio portion for video calls, and audio portion for telepresence calls separately. For better bandwidth management and to protect audio stream degradation, separate the audio stream from the higher-bandwidth video stream. This can help when the network is congested or the call quality is impacted.

DSCP values are configured on Cisco Unified Communications Manager. For more information, see the *Configure Flexible DSCP Marking and Video Promotion Policy* section of the *System Configuration Guide for Cisco Unified Communications Manager*.

Hunt Group

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

Applies to all clients

A Hunt Group is a group of lines that are organized hierarchically, so that if the first number in the hunt group list is busy, the system dials the second number. If the second number is busy, the system dials the next number, and so on. Every hunt group has a pilot number that is also called as hunt pilot. A hunt pilot contains a hunt pilot number and an associated hunt list. Hunt pilots provide flexibility in network design. They work with route filters and hunt lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns.

A hunt pilot number is the number that a user dials. A hunt list contains a set of line groups in a specific order. 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. A single-line group can appear in multiple hunt lists.

Unified Communications Manager (Unified CM) identifies a call that is to be routed through a defined hunt list, Unified CM finds the first available device on the basis of the order of the line groups that a hunt list defines.

You can let a user sign in and out of hunt groups by configuring EnableHuntGroup parameter. You can control whether users can decline calls from hunt groups with the PreventDeclineOnHuntCall parameter. For more information, see the *Parameters Reference Guide for Cisco Jabber*.

Unified CM 9.x and later allows configuring of automatic sign out of a hunt member when there is no answer. Once the user is signed out, the system displays a sign out notification whether the user is auto-signed out, manually signed out, or signed out by the Unified CM administrator.

Limitation

Desktop clients must use audio on computer mode before users can sign in to or out of hunt groups.

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.

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:

a. Specify a unique name in the **Line Group Name** field.

b. Specify number of seconds for **RNA Reversion Timeout**.

c. 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.

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.

Note The group call pickup feature and directed call pickup feature do not work with hunt lists.

Configure Hunt List

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:

a. Specify a unique name in the **Name** field.

b. Enter a description for the Hunt List.

c. Select a **Cisco Unified Communications Manager Group** from the drop-down list.

d. The system selects **Enable this Hunt List** by default for a new hunt list when the hunt list is saved.

e. 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.

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 information about hunt pilots, see the *System Configuration Guide for Cisco Unified Communications Manager*.

For more detailed information on the configuration options for hunt pilots, see the relevant *Cisco Unified Communications Manager documentation*.

Configure Hunt Pilot

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**.

Jabber to Jabber Call

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	—

Jabber to Jabber voice and video calling provides basic calling capabilities between two Cisco Jabber clients without using Cisco Unified Communications Manager. If Cisco Jabber users are not registered with Cisco Unified Communications Manager, they can still make Jabber to Jabber calls from Cisco Jabber.

Note

- Jabber to Jabber calling is only supported for users who authenticate to the Cisco Webex Messenger service.
- For Cisco Jabber for Windows clients, we recommend running Internet Explorer 10 or greater while using the Jabber to Jabber calling feature. Using the feature with previous versions of Internet Explorer or with Internet Explorer in Compatibility Mode can cause issues. These issues are with Cisco Jabber client login (non-SSO setup) or Jabber to Jabber calling capability (SSO setup).

Jabber to Jabber Call Experience

A Jabber to Jabber call does not support all the features of a Cisco Unified Communication Manager call. Users can make a Jabber to Jabber call with only one contact at a time. In a Jabber to Jabber call, users can experience any of the following scenarios:

- Cisco Jabber for mobile clients does not support HD video in portrait mode. To achieve HD video, you need to rotate the phone from portrait to landscape mode during the call.
- If two users start a Jabber to Jabber call to each other at the same time, the call is automatically connected. In such case, users do not receive any incoming call notification.
- When users are on a Jabber to Jabber call and start another call, the ongoing call ends immediately, even if the person they called does not answer.
- When on a Jabber to Jabber call and they receive an incoming Jabber to Jabber call, the **End Call And Answer** option is displayed. When they select this button, the ongoing Jabber to Jabber call ends and the incoming call is answered.
- For Jabber to Jabber calls on Cisco Jabber for mobile clients:
  - Cisco Jabber for mobile clients does not support HD video in portrait mode. To achieve HD video, you need to rotate the phone from portrait to landscape mode during the call.
  - When users are on a Jabber to Jabber call and they make a phone call, the ongoing Jabber to Jabber call ends immediately, even if the remote party does not answer.
  - When users are on a mobile call, they cannot answer any Jabber to Jabber call. The incoming Jabber to Jabber call is listed as a missed call.
  - When users are on a Jabber to Jabber call and they receive an incoming mobile call:
    - On an iPhone, the Jabber to Jabber call ends immediately, even if they do not answer the call.
    - On an Android phone, the Jabber to Jabber call ends immediately when they answer the incoming mobile call.

Supported In-Call Features

The following features are supported during a Jabber to Jabber call:

- End a Jabber to Jabber call
- Mute or unmute the audio
- Start or stop the video
- Volume control
- Open or close or move the self-video
- Switch to front or back camera. This feature is only supported on the Cisco Jabber mobile clients.

Jabber to Jabber Call Cloud Deployment

Cloud deployment for Jabber to Jabber call uses the SDP/HTTPS setup. For cloud deployment, ensure the following:

- Install the following root certificate to use the Jabber to Jabber call feature: `GoDaddy Class 2 Certification Authority Root Certificate`. To resolve any warnings about this certificate name, install the required GoDaddy certificate.
- Include the following servers in the proxy server bypass list:
  - https://locus-a.wbx2.com/locus/api/v1
  - https://conv-a.wbx2.com/conversation/api/v1

  For information on proxy server lists, see the *Configure Proxy Settings* in the Cisco Jabber Deployment Guides.
- Enable the range of media ports and protocols for RTP/SRTP over UDP: 33434-33598 and 8000-8100. For Jabber to Jabber call setup over HTTPS, enable port 443.
- Before you enable the Jabber to Jabber calling feature, complete the following tasks:
  - Contact the Cisco Customer Support team or your Cisco Customer Success Manager to request that your organization is added to the Cisco Common Identity server. This process to add users to the Common Identity server takes some time to complete and is necessary to access Jabber to Jabber calling capabilities.
  - For Single Sign On (SSO) users, you must set up SSO for Common Identity. For more information about configuring SSO, see the Cisco Webex Messenger documentation at this link: https://www.cisco.com/c/en/us/support/unified-communications/webex-messenger/products-installation-guides-list.html.

For cloud deployments, Jabber to Jabber calling is configured on the Cisco Webex Messenger Administration tool with one of the following methods:

- Using the *P2P settings* in the *Configuration Tab* section. For more information, see the *Cisco Webex Messenger Administrator's Guide*.
- Using the **Internal VoIP** and **External VoIP** settings in the policy editor for Cisco Webex Messenger Administration tool. You can control the video services for Jabber to Jabber calls using the **Internal Video** and **External Video** policy actions. For more information, see the *Policy Editor* section of the *Cisco Webex Messenger Administration Guide*. Jabber to Jabber calling can be enabled for groups of users or all users.

Jabber to Jabber Hybrid Mode

Jabber to Jabber Call Experience in Hybrid Mode

In addition to the limitations for Jabber to Jabber, the following are the scenarios that occur when using Jabber to Jabber calls and Cisco Unified Communications Manager calls:

- When users are on a Jabber to Jabber call and make a Cisco Unified Communications Manager call, the ongoing Jabber to Jabber call ends immediately, even if the remote party does not answer.
- When users are on a Jabber to Jabber call and resume a Cisco Unified Communications Manager call from on hold, the Jabber to Jabber call ends immediately.

- When users are on a Jabber to Jabber call and receive an incoming Cisco Unified Communications Manager call, a notification with an **End Call And Answer** button displays. If your user selects this button the ongoing Jabber to Jabber call ends and the incoming call is answered.
- When users receive a Cisco Unified Communications Manager call, they can place the ongoing Cisco Unified Communications Manager call on hold to answer the new call.
- When users are on a Cisco Unified Communications Manager call and they choose to make a Jabber to Jabber call, the Cisco Unified Communications Manager call is put on hold immediately, even if the participant in the Jabber to Jabber call does not answer the call.
- When users are on a Cisco Unified Communications Manager call and they answer an incoming Jabber to Jabber call, the Cisco Unified Communications Manager call is put on hold immediately.
- If your user's line is configured on Cisco Unified Communications Manager to auto-answer calls and they receive an incoming Cisco Unified Communications Manager call when they are on a Jabber to Jabber call, the Jabber to Jabber call ends immediately without notification and the Cisco Unified Communications Manager call is answered.

Jabber to Jabber Bandwidth

Specifies the maximum bandwidth (in kilobits per second) to be used for Jabber to Jabber calls. The video quality (resolution) of the call is lowered so that it meets the bandwidth limit. This feature is configured using the J2JMaxBandwidthKbps parameter.

For more information on parameters, see the *Parameter Reference Guide* for your release.

Let Users Without Voicemail Ignore Calls

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

You can choose a NoVoicemail profile for users who don't have voicemail configured. Jabber displays an **Ignore call** option for these users.

Configure a Device with No Voicemail

You can configure a device with no voicemail and users can ignore an incoming call in the Jabber client.

Step 1 From **Cisco Unified CM IM and Presence Administration**, go to **Device** > **Phone**.

Step 2 Find and select the device.

Step 3 In the **Association Information**, choose the directory number.

Step 4 In the **Directory Number Settings**, choose **NoVoicemail** for **Voice Mail Profile**.

Step 5 Click **Save** and then select **Apply Config**.

Move to Mobile

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
—	—	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	—

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.

Note The Move to Mobile feature requires a mobile telephone network connection with a phone number. Users must have a TCT or BOT device.

There are two ways to enable this feature. You can also disable it.

Implementation Method	Description	Instructions
Handoff DN	The mobile device calls Cisco Unified Communications Manager using the mobile network. This method requires a Direct Inward Dial (DID) number. 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. This method does not work for iPodTouch devices.	See the *Enable Handoff from VoIP to Mobile Network* topic.
Mobility Softkey	Cisco Unified Communications Manager calls the phone number of the PSTN mobile service provider for the mobile device.	See the *Enable Transfer from VoIP to Mobile Network* topic.
None of the above	Disable this feature if you do not want to make it available to users.	Select **Disabled** for the **Transfer to Mobile Network** option in the **Product Specific Configuration Layout** section of the TCT device page. Select **Disabled** for the **Transfer to Mobile Network** option in the **Product Specific Configuration Layout** 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).

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.

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.

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

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 callstates.

a) Select **Device** > **Device Settings** > **Softkey Template**.

b) Select the same softkey template that you selected when you configured the device for Mobile Connect.

c) In the **Related Links** drop-down list at the upper right, select **Configure Softkey Layout** and select **Go**.
d) In the call state drop-down list, select the On Hook state and verify that the Mobility key is in the list of selected softkeys.
e) In the call state drop-down list, select the Connected state and verify that the Mobility key is in the list of selected softkeys.

Step 3 Navigate to the device that you want to configure as follows:

a) Select **Device** > **Phone**.
b) Search for the device that you want to configure.
c) Select the device name to open the **Phone Configuration** window.

Step 4 For the per-user and per-device settings in Cisco Unified Communications Manager, set the specific device to use the Mobility softkey when the device transfers calls to the mobile voice network. Ensure that you have set up both Mobility Identity and Mobile Connect for the mobile device. After the transfer feature is working, users can enable and disable Mobile Connect at their convenience without affecting the feature.

If the device is an iPod Touch, you can configure a Mobility Identity using an alternate phone number such as the mobile phone of the user.

a) Select the **Owner User ID** on the device page.
b) Select the **Mobility User ID**. The value usually matches that of the Owner User ID.
c) In the Product Specific Configuration Layout section, for the Transfer to Mobile Network option, select **Use Mobility Softkey** or **Use HandoffDN Feature**.

Step 5 In the User Locale field, choose **English, United States**.

Step 6 Select **Save**.

Step 7 Select **Apply Config**.

Step 8 Instruct the user to sign out of the client and then to sign back in again to access the feature.

What to do next

Test your settings by transferring an active call from VoIP to the mobile network.

Multiline

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

You can configure multiple phone lines for your users to perform daily Cisco Jabber tasks. You can add up to 8 phone lines for each user. You can configure multiline for your users on Cisco Services Framework (CSF) device.

Multiline is supported on Cisco Unified Communications Manager release 11.5 SU3 and later. However, if you are using Cisco Unified Communications Manager release 11.5 SU3 and Cisco Unified Communications Manager release 12.0, you must manually install the Cisco Options Package (COP) file on all cluster nodes and restart Cisco Unified Communications Manager to enable multiline.

After you have installed and configured Multiline, your users can:

- Select a preferred line for making calls.
- View missed calls and voicemails.
- Use call forwarding, transfers, and conference calls on all lines.
- Assign custom ringtones to each line.

Multiline supports the following features on all lines:

- CTI control for the desk phone
- Far End Camera Control (FECC) and Binary Floor Control Protocol (BFCP)
- Hunt groups
- Call recording and silent monitoring
- Shared line, dial rules, and directory lookup
- Accessory manager

If Multiline is enabled, these features are only available on the primary line:

- Call pickup
- Extend & Connect

Configure Multiline

Before you begin

Create and add user profiles in Cisco Unified Communications Manager.

Important For Cisco Jabber Softphone for VDI, merge call functionality requires the following configuration:

- Set **Join And Direct Transfer Policy** to **Same line, across line enable**.
- Check the **Override Enterprise Settings** check box.

Step 1 From **Cisco Unified CM Administration**, go to **Device** > **Phone**, and find and select the device.

Step 2 For each line you want to configure:

a. Click **Add a new DN**, enter a **Directory Number**.

b. Add any additional configurations and click **Save**.

Enable Multiline MRA Access

Multiline is supported when using Cisco Jabber for Desktop in Mobile and Remote Access (MRA) mode. This function can be enabled in the Cisco TelePresence Video Communication Server (VCS-C).

Step 1 Go to VCS-C.

Step 2 Select **VSC-C configuration** > **Unified Communication** > **Configuration** > **SIP Path headers** and set it to **On**.

Personal Rooms

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

A personal room is a virtual conference room that is always available and can be used to meet with people. Cisco Jabber uses the personal room feature of Cisco Webex Meetings to allow users to easily meet with their contacts using the **Start meeting** option in the client.

Step 1 Personal Rooms are enabled by default for users on Cisco Webex Meetings. For more information see the Cisco Webex Meetings documentation available here: https://www.cisco.com/c/en/us/support/conferencing/webex-meeting-center/products-installation-and-configuration-guides-list.html

Step 2 Users can configure their personal rooms for all instant meetings by selecting **Use Personal Room for all my instant meetings** in Cisco Webex Meetings.

Push Notification Service for Cisco Jabber Video and Voice Calls

Clients			
Windows	Mac	iPhone and iPad	Android
—	—	Yes	Yes

Deployments			
On-Premises	Webex Messenger	Team Messaging Mode	Softphone for VDI
Yes	Yes	Yes	—

Cisco Jabber users can receive push notification for Jabber voice and video calls. This feature works when the device is locked, whether Jabber runs in the background or foreground, and whether the Jabber IM service is connected.

For information on push notifications for IMs, see Push Notification Service for IM, on page 31.

Jabber for iPhone and iPad

From Release 12.1 onwards, the Apple Push Notification (APN) implementation supports push notification for users. Use APNs to ensure you receive chat messages and calls while Jabber is in the background.

Note Jabber MAM clients on iOS only support push notifications for voice calls, not for IMs.

Jabber for Android

From Release 12.9.1 onwards, the Firebase Cloud Messaging (FCM) implementation supports push notification for users. Use FCM to ensure you receive chat messages and calls while Jabber is in the background.

Prerequisites

- Jabber for iPhone and iPad
  - Cisco Unified Communications Manager 11.5.1 SU3 version or later

    But, you must upgrade to either version 11.5.1 SU8 or version 12.5.1 SU3 before April 2021.
  - Cisco Expressway X8.10

    But, you must upgrade to version X12.6 before April 2021.
- Jabber for Android
  - Cisco Unified Communications Manager 12.5.1 SU3 version or later
  - Cisco IM and Presence 12.5.1.1 SU3 (Jabber only)
  - Cisco Expressway X12.6

How Push Notifications Are Delivered to Jabber

Jabber registers to APN services during the sign-in process. Users must sign in to Jabber to receive the push notifications service.

The Unified CM server pushes the notification to the Cisco cloud server, and the Cisco cloud server pushes this notification to the APN service. The APN service then delivers this notification to Jabber on the Cisco Jabber devices such as the iPhone and iPad. These devices relaunches Jabber to retrieve the call from the Unified CM server, thus making it possible to receive the incoming calls at any time.

Note If the user manually terminates Jabber with the push notification service enabled, then the **ForceLogoutTimerMobile** parameter doesn’t function. We recommend that you disable the push notification service if you want to use the **ForceLogoutTimerMobile** parameter.

Supported Services

- Phone-only and Full UC modes
- Shared line (You can pick the call from one device and transfer it to Jabber using Hold and Resume functions)
- CallKit (You can switch between Jabber calls, Jabber to native calls, and native to Jabber calls)

Limitations

- If an incoming call disconnects before Jabber retrieves the call from the Unified CM server, then the missed call or call history isn’t recorded.
- If you have both Cisco Jabber and Cisco Webex Teams installed, the application that first receives the incoming call displays the callkit.
- As of Release 12.9, peer-to-peer calls (locus calls) aren't supported.
- If you kill or suspend Jabber and you answer an incoming call, Jabber starts a connection to Unified CM. In this case, you might see a "call connecting" phase.
- The Jabber client disables push notifications as follows:
  - If your device doesn't have Google service(such as Huawei Mate 30and later), the client disables push notification, even if you enable them on the server.
  - If your device has Google service and its region is "China Mainland", the client disables push notification, even if you enable them on the server.
  - For other devices in China, the client uses the server settings for push notifications.

Enable Push Notification Service on Cisco Unified Communications Manager

Step 1 Go to **Cisco Unified CM Administration** > **Advanced Features** > **Cisco Cloud Onboarding**.

Step 2 From the **Notification Settings,** check **Enable Push Notification**.

Step 3 Click **Save**.

(Optional) Use Push Notification with Single Number Reach

The processing time for push notifications can interfere with Single Number Ring (SNR). When you use push notifications with SNR, we recommend extending the wait before ringing to at least 13 seconds. This duration gives you time to answer the call.

Step 1 In Cisco Unified CM Administration, select **Device** > **Phone**.

Step 2 Select your associated mobility identity and find the **Timer Information**.

Step 3 Set **Wait * X seconds before ringing this phone when my business line is dialed.** to at least `13`.

(Optional) Use Push Notification with Voicemail

The default setting for **No Answer Ring Duration (seconds)** for sending the call to voicemail is 12 seconds. Push notification processing can use most of this time. When you use push notifications with voicemail, we recommend extending the duration to at least 25 seconds. This duration gives you time to answer the call.

Step 1 In Cisco Unified CM Administration, select **Call Routing** > **Directory Number**.

Step 2 Select your directory number and find the **Call Forward and Call Pickup Settings**.

Step 3 Set **No Answer Ring Duration (seconds)** to at least `25`.

Single Number Reach

Clients			
Windows	Mac	iPhone and iPad	Android
Yes	Yes	Yes	Yes

Deployments			
On-Premises	Webex Messenger	Team Messaging Mode	Softphone for VDI
Yes	Yes	Yes	Yes

With Single Number Reach (SNR), a user can automatically forward calls from their work number to their mobile phone if:

- Cisco Jabber isn't available.

After Jabber becomes available again and connects to the corporate network, Unified CM sends calls to the Jabber client, rather than using SNR.

- Jabber mobile users select **Mobile Voice Network** or **Autoselect** and they're outside their Wi-Fi network.

A user can select or clear their SNR destination number from Cisco Jabber.

Enable Single Number Reach

Use the following procedure to enable single number reach for your users.

Before you begin

Make sure that the user has a device already assigned to them.

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

Step 2 Configure the end user for single number reach as follows:

a) Go to **User Management** > **End User**, search for the user and click their name.
b) In the **Mobility Information** section, check the **Enable Mobility** check box.
c) On Cisco Unified Communications Manager Release 9.0 and earlier, specify the Primary User Device.
d) Click **Save**.

Step 3 Create their remote destination profile.

a) Go to **Device** > **Device Settings** > **Remote Destination Profile** > **Add New**.
b) Enter the required values and click **Save**.
c) Click **Add a New Directory Number** and enter the directory number of the desk phone to associate with the remote destination profile.
d) Click **Save**.
e) Click **Add a New Remote Destination**, enter the number for your remote destination in **Destination number** and choose the **User ID**.
f) Click **Enable Unified Mobility** features, and click the following options:
   - **Enable Single Number Reach**
   - **Enable Move to Mobile**
g) Click **Save**.

Limitations

For Cisco TelePresence Video Communication Server Control (VCS) versions earlier than 8.10.X, you need to configure the following to enable the single number reach for your users who are using Cisco Jabber over Mobile and Remote Access.

Step 1 From Cisco TelePresence Video Communication Server Control (VCS), choose **Configuration** > **Unified Communications** > **HTTP allow list** > **Editable inbound rules**

Step 2 Click **New** to create a new entry

Step 3 Enter the following details:

- Description—Enter the required description.
- URL—Enter the URL details. For example, `https://[CUCM domain name]: port number`.
- Allowed Methods—Check the default value. For example, `GET, POST, PUT`
- Match Type—Choose **Prefix match** from the drop-down list.

Step 4 Click **Save**.

URI Dialing

You can use the URI dialing feature for on-premises deployments. URI dialing requires Cisco Unified Communications Manager, Release 9.1(2) or later.

Important The mobile clients don't support URI dialing when you enable the Dial via Office-Reverse feature.

You enable this feature in the `jabber-config.xml` file with the EnableSIPURIDialling parameter.

Example: `<EnableSIPURIDialling>True</EnableSIPURIDialling>`

For more information on the values of the parameter, see the *Common Policies* section.

URI dialing allows users to make calls and resolve contacts with Uniform Resource Identifiers (URI). For example, a user whose name is 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 and advanced configuration including ILS setup, see the *URI Dialing* section of the *System Configuration Guide for Cisco Unified Communications Manager* .

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:

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:

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.

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 Click **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.

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.

Voicemail Avoidance

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

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 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.

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.

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 release 9 — In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.
- Cisco Unified Communications Manager release 10 without Dial via Office — In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.
- Cisco Unified Communications Manager release 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.

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

Step 2 Navigate to the device that you want to configure as follows:

a) Select **Device** > **Phone**.
b) Search for the device that you want to configure.
c) Select the device name to open the **Phone Configuration** window.

Step 3 In the **Associated Remote Destinations** section, click the link for the associated remote destination.

Step 4 Set the policies as follows:

- Cisco Unified Communications Manager release 9 — In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.
- Cisco Unified Communications Manager release 10 without Dial via Office — In the **Single Number Reach Voicemail Policy** drop-down list, select **User Control**.
- Cisco Unified Communications Manager release 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**.

Voice Messages

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	—

The voicemail screen includes these extra options:

- Users can record voice messages without making a call and then send the message. Users can select recipients from the voicemail server's catalog.
- Users can directly reply to the sender of a voicemail or to all recipients of that message.
- Users can forward voicemails to new recipients.

The voicemail server's administrator can also create distribution lists to which users can send messages.

Show Sent Voice Messages

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	—	—	—

If you set a retention period for sent messages in Cisco Unity Connection, users can access their sent voice messages in Jabber.

Step 1 In **Unity Connection Administration**, go to **Messaging Configuration**.

Step 2 Set **Sent Messages: Retention Period (in Days)** to a positive number to enable this feature.

Auto Answer Calls

You can configure a CSF device to auto answer incoming Jabber calls. In Unified CM, you can set the device to either auto answer with a headset or with a speakerphone.

Do not configure auto answer on a shared line unless all the connected devices support auto answer.

Note If you also enable zip tones, the zip tone only plays with Jabber when the CSF device auto answers with a headset. Zip tones do not play when a speakerphone auto answers the call.

Jabber with Cisco Unified Contact Center

You can use Cisco Jabber as an agent phone in a contact center environment. We support the following Cisco Unified Contact Center features with Jabber:

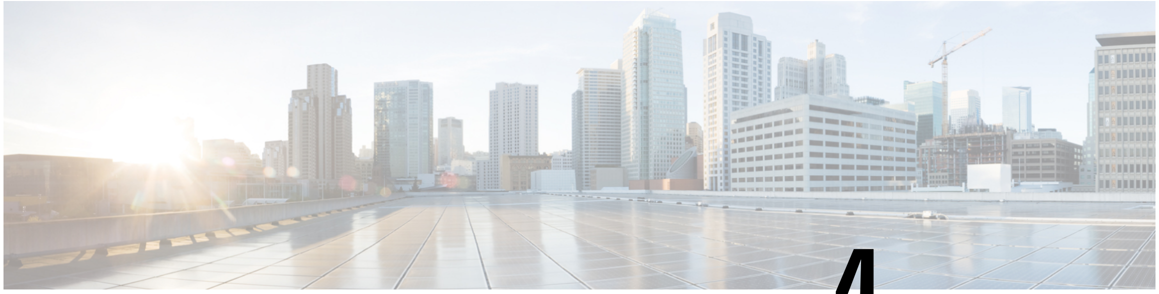
- **CTI Servitude**—Unified Contact Center deployments can control a Jabber softphone through CTI.
- **Auto Answer**—You can configure auto answer for a Jabber CSF device in Unified CM. But, all devices on a shared line must support auto answer.
- **Zip Tone**—You can use zip tones with auto answer with a headset. Auto answer with a speakerphone doesn't support zip tones.
- **Whisper Announcement**—You can use whisper announcement to play an introductory message to the agent.
- **Agent Greeting**—You can use agent greeting to play pre-recorded messages to the customer.
- **Silent Monitoring**—A supervisor can monitor an incoming call.
- **Supervisor Barge-In**—Using cBarge, a supervisor can inject themselves into an active call. You must configure network-based media resources and have them available to Jabber to support this feature. This feature works in cBarge mode even when you enable the Built-in-Bridge (BiB) on Jabber.
- **Call Recording**—You can send a recording stream to a recording server that Cisco Unified Contact Center supports.

Note Jabber doesn't support Extension Mobility in contact center deployments.

Reduce Server Load from Phone Number Resolution Requests

When you launch Jabber, Jabber attempts to look up each caller in the call history from the contact source. In deployments like contact centers where most calls are from external numbers, these requests are unnecessary overhead for external phone numbers. With a high volume of external calls, these requests can place a significant load on your LDAP or UDS server.

If you need to reduce this load, you can use the DisableCallHistoryResolution parameter.



CHAPTER 4

Security and monitoring

Logout Inactivity Timer

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

The sign-out inactivity timer allows you to automatically sign users out of the client after a specified amount of time of inactivity.

Inactivity on the mobile clients includes:

- The client goes into the background.
- No user interaction on voice calls.

You configure this feature on the mobile clients using the ForceLogoutTimerMobile parameter.

Inactivity on the desktop clients includes:

- No keyboard or mouse activity.

- No user interaction on connected accessories for making and answering calls.

You configure this feature on the desktop clients using the ForceLogoutTimerDesktop parameter.

If you do not set the parameter, the client does not automatically sign out.

Problem Reporting

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	—	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

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>
```

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.

Decrypt the Problem Report

The command line tool `CiscoJabberPrtDecrypter.exe` for decrypting the problem reports is only available on Windows machines and is included in the installer. The tool has the following arguments:

- `--help`—Show the help message.
- `--privatekey`—Specify the private key file, this is a privacy enhanced mail (.pem) or a personal information exchange PKCS#12 (.pfx) format.
- `--password`—Optional, if the input private key file is password protected.
- `--encryptionkey`—Specify the encryption secret key file, for example `file.zip.esk`.
- `--encryptedfile`—Specify the encrypted file, for example `file.zip.enc`.
- `--outputfile`—Specify the output file, for example `decryptedfile.zip`.

Before you begin

To decrypt problem reports you need the following:

- Two files from the zip file created when you generated a problem report using encryption:
  - *file.zip.esk*—The encrypted symmetric key.
  - *file.zip.enc*—The original data encrypted using AES256.
- Private Key for the certificate used for encrypting the data.

Step 1 Open a command prompt in Windows.

Step 2 Navigate to the `C:\Program Files(x86)\Cisco Systems\CUCILync\` directory.

Step 3 Enter the command and your parameters.

Example for desktop clients:
```
CiscoJabberPrtDecrypter.exe --privatekey C:\PRT\PrivateKey.pfx --password
12345 --encryptedfile C:\PRT\file.zip.enc --encryptionkey C:\PRT\file.zip.esk --outputfile
C:\PRT\decryptedfile.zip
```

If the decryption is successful the output file is created. If there is an invalid parameter the decryption fails and an error is shown on the command line.

Collect PRT Logs Remotely

Instead of waiting for a user to upload the PRT logs, you can generate the logs remotely in **Unified CM Administration**.

Before you begin

To use this feature, your deployment requires Unified CM Release 12.5.1 SU 1 or later. The RemotePRTServer parameter specifies the script to upload the PRT logs to your server.

Step 1 Select **Device** > **Phone**.

Step 2 Choose the devices for which you need logs.

Step 3 Click **Generate PRT for selected**.

The script uploads the PRT logs to your server.

Note To collect logs from Cisco Sunkist headsets, you require firmware version 1.3 or later.

Set Up for Remote PRT Log Collection

Before you can remotely collect PRT logs, you must specify a script to upload the logs in **Unified CM Administration**.

Step 1 Select **User Management** > **User Setting** > **UC Service**.

Step 2 Add a new UC service with a **UC Service Type** of **Jabber Client Configuration (jabber-config.xml)**.

Step 3 Add a **Jabber Configuration Parameter** with these values:

- **Section**—`Policies`
- **Parameter**—`RemotePRTServer`
- **Value**—The URL for your upload script.

Set Device PIN

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
—	—	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	—

We recommend that you use Jabber only on secured devices. To check if the device is secure, configure the ForceDevicePin parameter with the value `true`.

Example:

```
<ForceDevicePin>true</ForceDevicePin>
```

If the device is not secured:

- Then Jabber displays a notification to set PIN. This is a time bound notification, if the user doesn't tap on **SET PIN** within 13 seconds, then the user is signed out of Jabber.

  After the user taps **SET PIN** option, the users must go the device settings and secure the device with a PIN or fingerprint authentication.

- If the user signs into Jabber, and then puts it in the background immediately, Jabber checks if the user has secured the device or not. If the device is not secured, then the user is signed out of Jabber.

Biometric Authentication on Mobile Clients

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
—	—	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	—

Cisco Jabber supports authentication by fingerprint or facial recognition for users to securely sign in. You can use these authentication methods to ensure that your users can quickly and securely sign in to Cisco Jabber on their mobile devices.

The authentication by fingerprint or facial recognition is used in the following scenarios:

- When a Cisco Jabber for Android user signs in to Jabber after signing out manually or an automatic sign out, they can use authentication by fingerprint or facial recognition.
- When Cisco Jabber for iPhone and iPad users sign in to Cisco Jabber after they sign out manually and after an auto logout they have to sign into Cisco Jabber only using Touch ID or Face ID authentication.

You can enable Cisco Jabber users to sign in using this authentication by configuring the parameter, LocalAuthenticationWithBiometrics.

You can configure this parameter using any of these values:

- AdminEnabled—Cisco Jabber prompts your users to authenticate using fingerprint or facial recognition. Users must use biometric authentication to sign into Cisco Jabber. However, if the user's device does not support biometric capability, then user have to sign in using their password.
- UserDecision (default)—Cisco Jabber prompts your users to authenticate using fingerprint or facial recognition. The users can decide if they want to use biometric authentication to sign into Cisco Jabber.

- AdminDisabled—Cisco Jabber doesn't use authentication by fingerprint or facial recognition. There is no prompt displayed to the user.

If authentication fails, Cisco Jabber prompts your users to enter their credentials each time they sign in.

Example: `<LocalAuthenticationWithBiometrics>AdminDisabled</LocalAuthenticationWithBiometrics>`

Device Requirements for Biometric Authentication

This feature is available only on devices whose operating systems support biometric authentication.

Silent Monitoring and Call Recording

Clients			
Windows	Mac	iPhone and iPad	Android
Yes	Yes	Yes	Yes

Deployments			
On-Premises	Webex Messenger	Team Messaging Mode	Softphone for VDI
Yes	Yes	Yes	Yes

Silent call monitoring is a Cisco Unified Communications Manager feature. It allows a supervisor to hear both call participants, but neither of the call participants can hear the supervisor.

Call recording is a Unified CM feature that enables a recording server to archive agent conversations.

- Jabber doesn’t provide any interface to begin silent monitoring or call recording. Use the appropriate software to silently monitor or record calls.
- Jabber doesn’t currently support monitoring notification tone.
- You can use silent monitoring and call recording functionality only. Jabber doesn’t support other functionality such as barging or whisper coaching.

Server Requirements:

- We support silent monitoring and call recording for on-premises deployments only.
- Cisco Jabber for Windows and Cisco Jabber for Mac require Cisco Unified Communications Manager 9.x or later.
- Cisco Jabber for iPhone and iPad and Cisco Jabber for Android require Cisco Unified Communications Manager 11.0 or later.

Some releases of Unified CM require a device package to enable monitoring and recording capabilities. Verify that the **Built In Bridge** field is available in the **Phone Configuration** window for the device. If the field isn’t available, download and apply the most recent device packages.

For detailed information about how to configure silent monitoring or call recording, see the *Feature Configuration Guide for Cisco Unified Communications Manager*.

On-Demand Recording

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

Rather than record every call, you can offer your users the flexibility to choose when they want to record.

In deployments with Unified Communications Manager Release 12.5(1) and later, Jabber can support Unified CM's on-demand recording using Jabber's Built-In Bridge (BiB). In Cisco Unified CM Administration, set **Device** > **Phone** > **Recording Option** to **Selective Call Recording Enabled** to enable the feature. Also enable the BiB, either cluster-wide or for individual phones.

When you enable this feature, the call control menu includes a **Record** option for the user to start and stop recording at any time.

Preference Between Available Recorders

By default, if the user joins a conference call that has an external bridge set up to record calls, Jabber uses that external bridge for recording. However, some organizations might prefer all recording to use the Jabber BiB for compliance reasons. In those cases, use the Prefer_BIB_recorder parameter to enforce recording on the Jabber BiB.

Telemetry with Cisco Jabber Analytics

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

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`. The telemetry server certificate name is "metrics-a.wbx2.com". To resolve any warnings about this certificate name, install the required GoDaddy certificate. For more information about certificates, see the Planning Guide.

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 Wi-Fi (true), or Wi-Fi 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.

Note The option to disable telemetry is not available to Jabber team messaging mode users.

For more information about these parameters, see the *Parameters Reference Guide*.

You can find details on how Cisco handles analytics data at https://www.cisco.com/c/en/us/about/legal/privacy-full.html.

Jabber Analytics in Webex Control Hub

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	—	—

You can now access Jabber analytics through Webex Control Hub. Your data is available on the **Jabber** tab of the **Analytics** page. Jabber analytics provides key performance indicators with trending, such as:

- Active users
- Messages sent
- Calls made or received from Jabber
- Screen share from Jabber

To access Jabber analytics, you must have Webex Control Hub set up. Set these parameters in `jabber-config.xml`:

- TelemetryEnabled to true
- TelemetryEnabledOverCellularData to true

- TelemetryCustomerID to your OrgID from Control Hub

This feature is available for these deployment modes:

- On-premises with full UC
- On-premises IM-Only
- On-premises Phone-Only
- Jabber with Webex Messenger

Note This is a new feature in Webex Control Hub that impacts Jabber deployments. You can access this feature for any release of Jabber.

Wireless Location Monitoring Service

Applies to: All clients

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

Wireless location monitoring service allows you to determine the physical location from where your Cisco Jabber users connect to the corporate network. This information is stored in Cisco Unified Communications Manager.

You can configure wireless location monitoring service in Cisco Unified Communications Manager 11.5 or later, for more information see the System Configuration Guide for Cisco Unified Communications Manager.

Cisco Jabber monitors your users' locations, gathers Service Set ID (SSID) and Basic Service Set ID (BSSID) information, and sends this information to Unified CM at least every 24 hours, or whenever:

- Their current access point changes.
- They sign in to Cisco Jabber.
- They switch between on-premises and Expressway for Mobile and Remote Access network.
- Cisco Jabber resumes from sleep or is made active.

For on-premises deployments, configure wireless location monitoring using EnableE911OnPremLocationPolicy parameter with the value *true*.

For Expressway for Mobile and Remote Access deployments, you can configure wireless location monitoring using the EnableE911EdgeLocationPolicy with the value *true* and E911EdgeLocationWhiteList with a list of up to 30 SSIDs, separated by a semicolon.

For more details on these parameters, see the latest *Parameter Reference Guide for Cisco Jabber*.

Security Labels for Instant Messages

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	—	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	—	—	Yes

Customers often have data handling rules that restrict who can see which data. Your deployment can use a compliance server to filter instant messages. From Release 12.7, Jabber includes support for the *XEP-0258: Security Labels in XMPP* standard to enable such filtering.

You can define a catalog of security labels with the InstantMessageLabels parameter. The catalog populates a selection list above the chat input field.

When you implement security labels, the general work flow for sending IMs is as follows:

1. The user must choose a security label before they can send their IM.
2. Jabber appends the XMPP security label to the IM.
3. The IM goes to a compliance server.
4. The compliance server checks if its routing rules allow the recipient to see IMs with that classification:
    - If yes, the compliance server allows the IM.
    - If no, the compliance server rejects the IM.
5. When Jabber displays the IM in the chat window, the security label appears above the text.

For more information about using the InstantMessageLabels parameter, see the *Parameter Reference Guide for Cisco Jabber*. You can configure this setting in the Unified CM Administration or in the `jabber-config.xml` configuration file.

The following example shows how you could use the <label> element in the security labels tag:

```
<InstantMessageLabels>
  <item selector="Classified|SECRET">
    <securitylabel xmlns='urn:xmpp: sec-label:0'>
     <displaymarking fgcolor='black' bgcolor='red'>SECRET </displaymarking>
      <label>
       <edhAttrs xmlns="https://www.surevine.com/protocol/xmpp/edh">
       <specification>2.0.2</specification>
       <version>XXXX:1.0.0</version>
       <policyRef></policyRef>
       <originator>Acme</originator>
       <custodian>Acme</custodian>
       <classification>A</classification>
       <nationalities>Acme</nationalities>
       <organisations>Acme</organisations>
       </edhAttrs>
     </label>
    </securitylabel>
  </item>
<item…> … </item>
</InstantMessageLabels>
```

After you set this parameter, Jabber detects the configuration change and asks users to sign back into Jabber. For devices running on Jabber versions that don't support security labels, the IMs display the content of the message without the security label.

CHAPTER 5

Platform

Custom Embedded Tabs

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	Yes	Yes	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

Custom embedded tabs display HTML content in the client interface. You can create custom embedded tab definitions for Cisco Jabber. You can also programmatically adjust your custom tabs to work with the current client theme.

Note

- The Jabber embedded browser doesn’t support cookie sharing with pop-ups from SSO-enabled web pages. The content on the pop-up window may fail to load.
- Configure the HTTP server allow list (whitelist) for any web services inside the enterprise that remote Jabber clients need to access. See the *Mobile and Remote Access Through Cisco Expressway Deployment Guide* for more information.

Custom Embedded Tab Definitions

You can configure a custom embedded tab using the `jabber-config.xml` file. The following XML snippet shows the structure for custom tab definitions:

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

Cisco Jabber for Windows uses the Chromium Embedded Framework to display the content on the custom embedded tabs.

Cisco Jabber for Mac uses the Safari WebKit rendering engine to display the content of the embedded tab.

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

Parameter	Description
browser-plugin	Contains all definitions for custom embedded tabs. The value includes all custom tab definitions.
page	Contains one custom embedded tab definition.
refresh	Controls when the content refreshes. • true—Content refreshes each time users select the tab. • false (default)—Content refreshes when users restart the client or sign in. This parameter is optional and is an attribute of the page element.
preload	Controls when the content loads. • true—Content loads when the client starts. • false (default)—Content loads when users select the tab. This parameter is optional and is an attribute of the page element.
tooltip	Defines hover text for the custom embedded tab. The value is string of unicode characters.

Parameter	Description
icon	Specifies an icon for the tab. You can specify a local or hosted icon as follows: - Local icon—Specify the URL as follows: `file://`*`file_path`*`/`*`icon_name`* - Hosted icon—Specify the URL as follows: `http://`*`path`*`/`*`icon_name`* You can also change local and hosted icons to match the current Jabber theme using the *%JabberTheme%* variable, as follows: `http://`*`path`*`/icon_name_%JabberTheme%.jpg` The Jabber client interprets *%JabberTheme%* when requesting the icon. The possible values are: - default—The default Jabber theme - dark—The Jabber "Dark" theme - distinct—The Jabber "High Contrast" theme - highcontrast—A Windows high-contrast theme If you don't include *%JabberTheme%* in the URL, the icon doesn't change with the theme. Include the theme name in the filename for each icon. If the download of the custom icon fails or you don't have an icon for the selected theme, the Jabber client uses the default image. You can use any icon that the client browser can render, including .JPG, .PNG, and .GIF formats. This parameter is optional. If you don’t specify an icon, the client loads the favicon from the HTML page. If no favicon is available, the client loads the default icon.
url	Specifies the URL where the content for the embedded tab resides. The client uses the browser rendering engine to display the content of the embedded tab. For this reason, you can specify any content that the browser supports. For Cisco Jabber for Mac, the URL element must contain HTTP or HTTPS. This parameter is required. **Note** If the target web page requires Windows integrated authentication, Jabber prompts the user for sign-in credentials by default. To avoid the prompt, you can configure the authentication server whitelist in Windows Registry. Add the whitelisted URLs to these locations: - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\AuthServerWhitelist` - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\AuthNegotiateDelegateWhitelist` For example, suppose you set the `AuthServerWhitelist` and `AuthNegotiateDelegateWhitelist` policies to `*example.com,*foobar.com,*baz`. Any URLs ending in either 'example.com', 'foobar.com', or 'baz' are in the permitted list. Without the '*' prefix, the URL has to match exactly.

Parameter	Description
internal	Specifies if your web page is an internal or an external page to your network. • true (default)—Your web page is an internal page to your network. • false—Your web page is an external page to your network.

User Custom Tabs

You can allow users to specify a tab name and URL for a custom embedded tab through the client user interface. Users cannot set the other parameters for a custom embedded tab.

Set AllowUserCustomTabs to **true** before users can customize their tabs:

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

Note The default value for AllowUserCustomTabs is **true**.

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

You can include different versions of icons to match specific themes. See the description of the icon parameter for details.

Chats and Calls from Custom Tabs

You can use protocol handlers to start chats and calls from custom embedded tabs. Make sure the custom embedded tab is an HTML page.

Use the `XMPP:` or `IM:` protocol handler to start chats.
Use the `TEL:` protocol handler to start audio and video calls.

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 use JavaScript notifications in custom embedded tabs. Jabber provides methods for JavaScript notifications. It’s beyond this guide's scope to describe how to use JavaScript notifications for asynchronous server calls and other custom implementations. See your JavaScript documentation for more information.

Important Apple replaced their WebView object. You must use different methods on Windows and Mac now. See the example JavaScript sections for details.

Notification methods

The client includes an interface that exposes these 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 1–999
  - 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.

Note Not applicable for Jabber for iPhone and iPad

- 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 window activates.
- onHubDeActivated()—The client invokes this method when the client hub window deactivates.

Subscribe to presence in custom tabs

You can use these JavaScript methods to subscribe to a contact's presence 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

- Subscriptions for people not on your contact list expire after 68 minutes. After the subscription expires, you must resubscribe to see their presence data.
- Jabber for iPad and iPhone only supports OnPresenceStateChanged.

Get locale information in custom tabs

You can use these JavaScript methods 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 the client. You can use a string value that contains the client locale information.

Note Jabber for iPad and iPhone only supports OnLocaleInfoAvailable.

Adjust custom tabs to match the client theme

You can use these JavaScript methods to return the current client theme:

- QueryCurrentTheme()—This method enables you to get the current Jabber theme.
- OnThemeChanged(*theme*)—This method passively receives the new theme when the theme changes in Jabber.

The possible values for the theme are:

- default—The default Jabber theme
- dark—The Jabber "Dark" theme
- distinct—The Jabber "High Contrast" theme
- highcontrast—A Windows high-contrast theme

Example JavaScript for Jabber for Windows

This example shows an HTML page that uses JavaScript to display a form for inputting a number 1–999:

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

Example JavaScript for Jabber for Mac

Apple deprecated the NSWebView that previous Jabber releases used. The replacement, WKWebView, doesn't support `window.external`. For your custom embedded tabs on Mac, replace `window.external` with `window.webkit.messageHandlers`.

Here is an example of the new method.

```
<html>
<h3>
    Jabber MAC
</h3>
<div style="padding: 10px;">
 <label title="" id="themestring"></label>
 <button onclick="QueryCurrentThemeAction()">QueryCurrentTheme Action</button>
 <button onclick="SetNotificationBadgeAction()">SetNotificationBadge Action</button>
 <button onclick="GetUserLocaleAction()">GetUserLocale Action</button>
 <label title="" id="UserLocal"></label>
 <button onclick="SubscribePresenceAction()">SubscribePresence Action</button>
 <label title="" id="Presence"></label>
</div>

<script>

function OnThemeChanged(themeString) {
 var themeLabel = document.getElementById('themestring')
 themeLabel.innerHTML = themeString
}

function OnLocaleInfoAvailable(userLocal) {
 var localUserLabel = document.getElementById('UserLocal');
 localUserLabel.innerHTML = userLocal;
}

function QueryCurrentThemeAction() {
 var themeDiv = document.getElementById('MyTheme');
 themeDiv.style.backgroundColor = 'green';
 window.webkit.messageHandlers.QueryCurrentTheme.postMessage(null);
}

function SetNotificationBadgeAction() {
 window.webkit.messageHandlers.SetNotificationBadge.postMessage(40);
}

function GetUserLocaleAction() {
 window.webkit.messageHandlers.GetUserLocale.postMessage(null);
}

function SubscribePresenceAction() {
 window.webkit.messageHandlers.SubscribePresence.postMessage('quxie@hz.jabberqa.cisco.com');
}

function OnPresenceStateChanged(contactUri, presenceState, localizedPresenceString) {
 var Label = document.getElementById('Presence');
 Label.innerHTML =  contactUri + presenceState +  localizedPresenceString;
}

</script>
</html>
```

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>https://www.cisco.com/web/fw/i/logo.gif</icon>
     <url>https://www.cisco.com</url>
    </page>
   </browser-plugin>
  </jabber-plugin-config>
 </Client>
</config>
```

Configure Cisco Jabber for Android on Chromebook

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
—	—	—	Yes

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	—

Checklist to Configure Cisco Jabber for Android on Chromebook

Task	Details
See the device models and OS supported	See *Android OS Requirement and Chromebook Models Supported*
Add MRA configuration in corporate network	see *Add MRA Configuration in Corporate Network*
Configure the Chromebook user as a TAB device type	see *Configure Chromebook Users as TAB Device Type*
Keep the required ports open so that your users access all Cisco Jabber services on Chromebook	see *Configure Ports*

Android OS Requirement and Chromebook Models Supported

Chromebook must have Chrome OS version 53 or later. Users can download Cisco Jabber for Android from Google Play Store.

The chromebook models supported:

- HP Chromebook 13 G1 Notebook PC
- Google Chromebook Pixel
- Samsung Chromebook Pro

Add MRA Configuration in Corporate Network

Use Cisco Jabber on Chromebook while connected from your corporate and Mobile and Remote Access (MRA) network. To use call services, Cisco Jabber must be signed in using MRA Network.

To connect to MRA network when your users are operating within the corporate network, configure your internal Domain Name Server (DNS) with the `"_collab-edge._tls.<domain>.com"` SRV record. For complete details on DNS, see the section *Service Discovery* from the *Cisco Jabber Planning Guide 12.1*.

Configure Chromebook Users as TAB Device Type

You can configure Chromebook users as TAB device type. For complete details on how to configure softphone service for a user, see the section *Configure Softphone* from the *Cisco Jabber On-premises Guide 12.1*.

Configure Ports

Make sure these ports are open to access Cisco Jabber services on Chromebook:

Purpose	Protocol	On-premises Network (Source)	Expressway-E (Destination)
XMPP(IM&P)	TCP	>=1024	5222
HTTP proxy(UDS)	TCP	>=1024	8443
Media	UDP	>=1024	36002 to 59999
SIP signaling	TLS	>=1024	5061

Limitations

During a video call, the video stops if the users switch to another app.

Cisco Jabber Mobile App Promotion

Clients			
Windows	Mac	iPhone and iPad	Android
Yes	—	—	—

Deployments			
On-Premises	Webex Messenger	Team Messaging Mode	Softphone for VDI
Yes	Yes	Yes	Yes

You can enable a notification for Cisco Jabber for Windows users to promote the use of the Cisco Jabber for Mobile App (Android and iOS). Clicking the notification takes the user to the **Settings** page where they can choose to download the app from Google Play or the iTunes Store. A new parameter EnablePromoteMobile is added to control these notifications. This feature is disabled by default.

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

CHAPTER 6

Third-party integrations

Calendar Integration and Contact Resolution

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	—	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

You can use the following client applications for calendar integration and contact resolution:

- Microsoft Outlook 2019, 32 bit and 64 bit
- Microsoft Outlook 2016, 32 bit and 64 bit
- Microsoft Outlook 2013, 32 bit and 64 bit
- Microsoft Outlook 2010, 32 bit and 64 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 (calendar integration only)

Calendar integration and contact resolution are achieved with one or more of the following parameters:

- CalendarIntegrationType—Determines which calendar is integrated with the Meetings tab on the client. Users can overwrite this value with the Calendar integration type field on the Calendar tab of the Options window.
- EnableLocalAddressBookSearch—Specifies if users can search for and add local Microsoft Outlook or IBM Notes contacts to their contact lists.
- EnableLotusNotesContactResolution—Lets users search for and add local IBM Notes contacts to their contact lists.

The following table shows how these parameters interact to achieve calendar integration and contact resolution with third party products.

Table 3: Options for Calendar Integration and Contact Resolution

Parameter Values			**Contact Resolution**	**Calendar Integration**
EnableLocalAddress BookSearch	**EnableLotusNotes ContactResolution**	**CalendarIntegration Type**		
false	false	0 - none	None	None
true	false	0 - none	None	None
false	true	0 - none	None	None
true	true	0 - none	Microsoft Outlook	None
false	false	1 - Microsoft Outlook	None	Microsoft Outlook
true	false	1 - Microsoft Outlook	Microsoft Outlook	Microsoft Outlook
false	true	1 - Microsoft Outlook	None	Microsoft Outlook
true	true	1 - Microsoft Outlook	Microsoft Outlook	Microsoft Outlook
false	false	2 - IBM Notes	None	IBM Notes
true	false	2 - IBM Notes	None	IBM Notes
false	true	2 - IBM Notes	None	IBM Notes
true	true	2 - IBM Notes	IBM Notes	IBM Notes
false	false	3 - Google	None	Google
true	false	3 - Google	None	Google

Parameter Values			Contact Resolution	Calendar Integration
EnableLocalAddress BookSearch	EnableLotusNotes ContactResolution	CalendarIntegration Type		
false	true	3 - Google	None	Google
true	true	3 - Google	None	Google

Chat History in Microsoft Outlook

Clients			
Windows	Mac	iPhone and iPad	Android
Yes	Yes	—	—

Deployments			
On-Premises	Webex Messenger	Team Messaging Mode	Softphone for VDI
Yes	Yes	Yes	Yes

Supported Microsoft Exchange servers: 2010, 2013, 2016, 2019, and Office 365 (Exchange Online)

Jabber can automatically save users' chat histories to a folder in their Microsoft Outlook application. When a user closes the chat window, Jabber saves the conversation to the Exchange server.

To enable this feature, you need to:

Step 1 Set the parameters EnableSaveChatHistoryToExhange and SaveChatHistoryToExhangeOperationMode.

Step 2 Follow the procedure based on your Exchange deployment type:

Option	Description
Office 365 (Exchange Online)	For organizations that use Microsoft's cloud-based Exchange service.
On-Premises Exchange Servers	For organizations that use on-premises Exchange servers.

Set Parameters to Save Chat History

To enable this feature, you must configure the EnableSaveChatHistoryToExchange and SaveChatHistoryToExchangeOperationMode parameters.

Step 1 Set the EnableSaveChatHistoryToExchange parameter a to *true*.

Example:

```
<EnableSaveChatHistoryToExchange>true</EnableSaveChatHistoryToExchange>
```

Step 2 Set the SaveChatHistoryToExchangeOperationMode parameter to one of the following values:

- **EnabledByPolicy**—Chats are saved to Microsoft Outlook. The option **Save chat sessions to "Cisco Jabber Chats" Folder in Microsoft Outlook** is visible on the client, but users cannot access it.

  With this option, you must set up authentication for the client to authenticate with the Exchange server by synching credentials.

- **DisabledByDefault**—Users can save chats to Microsoft Outlook. The option **Save chat sessions to "Cisco Jabber Chats" Folder in Microsoft Outlook** is unchecked in the client, but users can change it.

- **EnabledByDefault**—Users can save chats to Microsoft Outlook. The option **Save chat sessions to "Cisco Jabber Chats" Folder in Microsoft Outlook** is checked in the client, but users can change it.

- **OnPremOnlyByPolicy**—Chats are saved to Microsoft Outlook only when Jabber is on the corporate network. Jabber doesn't save chats to Outlook over MRA. The option **Save chat sessions to "Cisco Jabber Chats" Folder in Microsoft Outlook** is visible on the Outlook tab of the Options menu, but it is greyed out and users cannot change it.

- **OnPremOnlyByDefault**—Users have the option to save chats to Microsoft Outlook only when Jabber is in corporate network. Jabber doesn't save chats to Outlook over MRA. The option **Save chat sessions to "Cisco Jabber Chats" Folder in Microsoft Outlook** is checked on the Outlook tab of the Options menu, but users can change it.

Example:

```
<SaveChatHistoryToExchangeOperationMode>EnabledbyPolicy</SaveChatHistoryToExchangeOperationMode>
```

Office 365 (Exchange Online)

To save chat history to Outlook using Office 365 (Exchange Online), you must enable the ExchangeModernAuthentication parameter. Your users enter their account details in the settings menu in the client.

Step 1 Set the ExchangeModernAuthentication parameter to *true*.

Example:

```
<ExchangeModernAuthentication>true</ExchangeModernAuthentication>
```

When you enable ExchangeModernAuthentication, Jabber ignores these parameters:

- ExchangeAuthenticateWithSystemAccount
- InternalExchangeServer
- ExternalExchangeServer
- ExchangeAutoDiscoverDomain

Step 2 Make sure that the parameter Exchange_UseCredentialFrom does not contain a value.

What to do next

Cisco Jabber requires admin consent to run in Azure AD. The default configuration for Azure AD tenants allows users to provide consent to third-party multi-tenant applications, like Jabber. If your tenant administrator restricts that ability, your users can't sign in to their Azure AD account in Jabber.

Your tenant administrator can give users the permission to grant consent to Jabber by entering these URLs in a browser and following the prompts:

- **Jabber for Windows**—https://login.microsoftonline.com/common/adminconsent?client_id=b7dc2580-cbaf-41a6-94ce-f6b495cc5815&state=12345&redirect_uri=ciscojabber%3A%2F%2Fo365oauth
- **Jabber for Mac**—https://login.microsoftonline.com/common/adminconsent?client_id=fbf6d76d-2021-4972-994c-ebd0957cdf4a&state=12345&redirect_uri=ciscojabber%3A%2F%2Fo365oauth

On-Premises Exchange Servers

To save chat history to Outlook using on-premises Exchange servers, you need to specify the credentials Jabber uses to authenticate and provide the server address for the Exchange servers.

Specify Authentication Credentials

Jabber can automatically authenticate your users with the Exchange server, but you must first specify which credentials to use. When authentication is complete, the client can save chat histories to an Outlook folder on the Exchange server.

If you don’t specify which credentials to use, then your users will have to enter their credentials manually in the client's settings menu.

Authenticate with Windows Domain User Account

For deployments on Windows, Jabber can use domain user account details to authenticate with the Exchange server. This authentication method uses the Windows NT LAN Manager protocol.

We don’t recommend that you use domain user account details for authentication if a Windows account is shared by several users. Even if you reset the client and sign in as another user, Jabber will use the Windows account to authenticate with Exchange. One user’s chat history might be saved to another’s Outlook folder.

Before you begin

Users and their computers must use domain user accounts. This authentication method doesn't work with local Windows accounts.

In the `jabber-config.xml` file, set the ExchangeAuthenticateWithSystemAccount parameter to *true*.

Authenticate with Cisco Credentials

Jabber can authenticate with Exchange using credentials from Cisco’s IM and Presence Service, Unified Communications Manager, or Webex.

Set the Exchange_UseCredentialsFrom parameter to *CUP* (for IM and Presence), *CUCM* (for Unified Communications Manager), or *WEBEX* (for Webex).

Example:

```
<Exchange_UseCredentialsFrom>CUCM</Exchange_UseCredentialsFrom>
```

In this example, Cisco Unified Communications Manager is defined as the service which provides the Exchange server with credentials for authentication.

Specify Exchange Server Addresses

You can either define your Exchange server addresses or set Jabber to discover the Exchange servers automatically in a particular domain.

If you don't specify a way for the client to find the servers, then users will have to enter the server addresses manually in the client's settings 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.

Step 1 In the `jabber-config.xml` file, configure the ExchangeAutodiscoverDomain parameter. For example,

```
<ExchangeAutodiscoverDomain>domain</ExchangeAutodiscoverDomain>
```

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*>

https://autodiscover.<*domain*>

Define Server Addresses

You can define the internal and external Exchange server addresses in the configuration file.

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.

Limitations for Saving Chat History to an Outlook Folder

CUCM Accounts

Users must have a Cisco Unified Communications Manager account.

Cisco Expressway for Mobile and Remote Access

For users connecting via Expressway for Mobile and Remote Access, the following limitations apply:

- If the client detects that the user is connecting via the Expressway, then the client uses the external server option for the Exchange connection. If the external server is not set, then it uses the internal server.
- If the client detects that the user is not connecting via the Expressway, then the client uses the internal server option for the Exchange connection. If the internal server is not set, the client uses the external server.
- However, if either the internal or external server is set, but for some reason Cisco Jabber can't connect to it, the client doesn't revert to using the other server.

IBM Notes Contact Search and Calendar Integration

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	—	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

Prerequisite: IBM Notes contacts must contain a valid value in the Messaging ID field. Without this, users cannot add IBM Notes contacts to their contacts lists.

Cisco Jabber for Windows supports IBM Notes calendar integration in the Meetings tab of the client. Cisco Jabber also lets users search for and add local contacts from IBM Notes. To enable this integration with IBM Notes, you must set the following parameters:

- EnableLocalAddressBookSearch=true
- EnableLotusNotesContactResolution=true
- CalendarIntegrationType=2

The CalendarIntegrationType parameter can be overridden by users. To enable calendar integration and contact resolution with IBM Notes, users must ensure that the **Calendar integration** type on the Calendar tab of the **Options** window is set to **IBM Notes**.

Note Cisco Jabber cannot perform contact search and calendar integration if the backup IBM notes *nsf* files are loaded.

C and C++ Libraries for IBM Notes Integration

If you have Jabber integrated with IBM Notes, it uses the C library by default. You can change the library to C++ using the EnableLotusNotesCLibrarySupport parameter. See the *Parameters Reference Guide* for more information.

Contact Resolution for Incoming Calls

For incoming calls, Cisco Jabber for Windows does not search the address book in IBM Notes, therefore only the phone number for an IBM Notes contact shows in the call history. If Cisco Jabber users subsequently search for the contact associated with the phone number, the call history changes to show the contact's name instead of the phone number.

Integration with Microsoft Products

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	—	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

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.

Office

Integration with the following versions of Office, including the Mac client, is supported:

- Microsoft Office 2019, 32 and 64 bit
- Microsoft Office 2016, 32 and 64 bit
- Microsoft Office 2013, 32 and 64 bit
- Microsoft Office 2010, 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 2019, 32 and 64 bit
- Microsoft Office 2016, 32 bit and 64 bit

- 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 2013
- Microsoft SharePoint 2010

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.

Skype for Business

Jabber for Windows and Skype for Business can compete for the Windows API and other Windows resources. To potentially mitigate this issue, you can install Jabber with the following command:

```
msiexec.exe /i CiscoJabberSetup.msi CLICK2X=DISABLE
```

Mac Calendar Integration For Meetings

Clients			
Windows	Mac	iPhone and iPad	Android
—	Yes	—	—

Deployments			
On-Premises	Webex Messenger	Team Messaging Mode	Softphone for VDI
Yes	Yes	Yes	Yes

You can give users the option to connect their calendars to their Cisco Jabber client.

You can use the following applications for calendar integration:

- Exchange Server 2019, 2016, 2013, and 2010
- Office 365
- Mac Calendar

You configure calendar integration using the following parameters:

- MacCalendarIntegrationType—Defines which calendar options are available to users to select in Cisco Jabber.
  - 0 for None

  - 1 (Default) for Microsoft Outlook
  - 2 for Mac Calendar

- InternalExchangeServer, ExternalExchangeServer, orExchangeAutodiscoverDomain— to define which servers to connect to.
- Exchange_UseCredentialsFrom or ExchangeDomain—to authenticate to those servers.
- CalendarAutoRefreshTime—to define the number of minutes after which calendars refresh. The default value is zero, meaning that the calendars do not automatically refresh.
- EnableReminderForNoneWebexMeeting—to specify whether users receive reminders from Cisco Jabber for non-Webex meetings that are in their calendars.
- DisableNonAcceptMeetingReminder—to specify whether users receive reminders from Cisco Jabber about Cisco Webex Meetings that they haven't accepted.

For more information on how to set up these parameters, see the *Parameters Reference Guide for Cisco Jabber* or later.

Microsoft Outlook Calendar Events

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	—	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

You must apply a setting in Microsoft Outlook so that calendar events display in Cisco Jabber for Windows.

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.

Microsoft Outlook Presence Integration

Clients			
Windows	**Mac**	**iPhone and iPad**	**Android**
Yes	—	—	—

Deployments			
On-Premises	**Webex Messenger**	**Team Messaging Mode**	**Softphone for VDI**
Yes	Yes	Yes	Yes

To enable integration with Microsoft Outlook, specify `SIP:user@cupdomain` as the value of the `proxyAddresses` attribute in Active Directory. Users can then share availability in Microsoft Outlook.

You can use the `OutlookContactResolveMode` parameter to choose how Jabber resolves the presence of a contact in Microsoft Outlook:

- **Auto** (default)—When you configure the `proxyaddress` attribute with `SIP:user@cupdomain`, then Jabber uses `user@cupdomain` as a Jabber ID. If you configure the `proxyaddress` attribute without SIP, Jabber uses an email address to resolve the presence of a contact in Microsoft Outlook.

- **Email**—When you configure the `proxyaddress` attribute with `SIP:user@cupdomain`, then Jabber uses `user@cupdomain` as an email address. If you configure the `proxyaddress` attribute without SIP, Jabber uses an email address to resolve the presence of a contact in Microsoft Outlook.

Use one of the following methods to modify the `proxyAddresses` attribute:

- **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.

- **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:

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.

All local contacts in Microsoft Outlook must have instant message addresses and phone numbers. These details allow client users to do the following:

- add local Microsoft Outlook contact to their contact lists
- see contact photos from the client
- send instant messages to local contacts
- call local contacts from the client

Administrator Tasks

To enable this integration with Microsoft Outlook, you must enable Cached Exchange Mode on the Microsoft Exchange server.

To allow users to search for local contacts in Microsoft Outlook from the client, users must have profiles set in Microsoft Outlook.

User Tasks

Users must set the correct calendar preference on the client.

1. Select **File** > **Options**.
2. Select the **Calendar** tab.

3. Select **Microsoft Outlook**.
4. Restart Cisco Jabber to apply the change.