Chat and Presence

Blocked Domain Support for Cisco 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.

Procedure

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.

Procedure

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.

Element or attribute	Description
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.
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.

Procedure

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

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

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

Step 4 Select **Cisco XCP Router** from the **Service** drop-down list.

The **Service Parameter Configuration** window opens.

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

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

Remember If you disable the setting on Cisco Unified Communications Manager IM and Presence Service, you must also disable file transfers and screen captures in the client configuration.

Step 7 Select **Save**.

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

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*.

Procedure

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

Step 2 Select **Messaging** > **File Transfer**.

Step 3 In the **File Transfer Configuration** section select **Managed File Transfer**.

Step 4 In the **Managed File Transfer Assignment** section, assign the external database and the external file server for each node in the cluster.

Step 5 Select **Save**.

What to do next

For each node:

- Copy the 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.

Procedure

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

Step 2 Select **Messaging** > **File Transfer**.

Step 3 In the **File Transfer Configuration** section, select **Peer-to-Peer**.

Step 4 Select **Save**.

What to do next

Restart the **Cisco XCP Router** service.

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

Procedure

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**.

Procedure

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

Step 2 Select **Messaging** > **File Transfer**.

Step 3 In the **Managed File Transfer Configuration** section enter the amount for the **Maximum File Size**.

Step 4 Select **Save**.

What to do next

Restart the **Cisco XCP Router** service.

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.

Procedure

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.

Procedure

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 23.

Procedure

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

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

Step 3 Select **Enable Persistent Chat**.

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

Step 5 Configure the remaining settings as appropriate for your persistent chat deployment. We recommend the persistent chat settings in 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	
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	

Persistent Chat Setting	Recommended Value	Notes
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	
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.
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	

Persistent Chat Setting	Recommended Value	Notes
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

You administer persistent chat rooms from the Jabber client by creating rooms, delegating their moderators, and specifying members. Jabber automatically creates the node on which the room is created, 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 Cisco Unified Communications Manager 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 the following tasks:

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

Room Creation

When creating a room, you can provide the following types of information:

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

  After you define the room type, no one can change it.
- 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 in order to see your new room in the list of available rooms.

Enable Persistent Chat Room Passwords

Persistent chat rooms that are password protected means that when users enter a room within a Jabber session, they must enter the password. Password protected rooms comply with the XEP-0045 specification from the XMPP Standards Foundation.

Procedure

Step 1 To set a password for a room, from the **Chat Rooms** tab on the hub window, select **All rooms** > **New room** > **Password**.

Step 2 To change the password for a room, open the chat room, click on **Edit Room**, select **Password**, then edit and save the password.

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.

Procedure

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

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

The **Presence Settings** window opens.

Step 3 Select **Allow users to view the availability of other users without being prompted for approval** to disable prompts and automatically accept all presence subscription requests within your organization.

This option has the following values:

- **Selected**—The client does not prompt users for presence subscription requests. The client automatically accepts all presence subscription requests without prompting the users.
- **Cleared**—The client prompts users to allow presence subscription requests. This setting requires users to allow other users in your organization to view their availability status.

Step 4 Select **Save**.

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 Jabber MAM clients on iOS don'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.

Procedure

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.