



Chat and Presence

- [Browser Click to Call](#) , page 1
- [Custom Emoticons](#), page 2
- [Enterprise Groups for Cisco Unified Communications Manager IM and Presence Service](#), page 6
- [File Transfers and Screen Captures](#), page 9
- [My Jabber Chats and My Jabber Files Directory Location](#), page 11
- [Multiple Device Messaging for Cloud Deployments](#), page 12
- [Persistent Chat Rooms](#), page 12
- [Prompts for Presence Subscription Requests](#), page 17
- [Restore Chats on Login](#), page 19
- [Temporary Presence](#), page 19

Browser Click to Call

Applies to: Cisco Jabber for Windows

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

Applies to: Cisco Jabber for Windows

You can add custom emoticons to Cisco Jabber for Windows by creating emoticon definitions in an XML file and saving it to the file system.



Note

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

- Dimensions: 17 x 17 pixels
- Transparent background
- PNG file format
- RGB colors

Procedure

- Step 1** Create a file named `emoticonDefs.xml` with any text editor.
- Step 2** Specify the emoticon definitions as appropriate in `emoticonDefs.xml`.
See *Emoticon Definitions* for more information on the structure and available parameters for `emoticonDefs.xml`.
- Step 3** Save and close `emoticonDefs.xml`.
- Step 4** Save `emoticonDefs.xml` in the appropriate directory on the file system.
Cisco Jabber for Windows loads emoticon definitions from the following directories on the file system.
- The directory can differ depending on your operating system
 - For 32-bit operating systems:
 - `Program Files\Cisco Systems\Cisco Jabber\Emoticons`
 - `Program Files\Cisco Systems\Cisco Jabber\CustomEmoticons`
 - For 64-bit operating systems:
 - `Program Files(x86)\Cisco Systems\Cisco Jabber\Emoticons`
 - `Program Files(x86)\Cisco Systems\Cisco Jabber\CustomEmoticons`
- The `Emoticons` folder contains the default emoticons for Cisco Jabber for Windows and the default `emoticonDefs.xml`.
- The `CustomEmoticons` folder does not exist by default. Administrators can create this folder to contain custom emoticon definitions to include in organizational deployments.
- Emoticons that you define in the `CustomEmoticons` folder take precedence over emoticon definitions in the default `Emoticons` folder.
- `%USERPROFILE%\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\CustomEmoticons`
- This folder contains custom emoticon definitions for individual instances of Cisco Jabber for Windows.
- Emoticons that you define in this directory take precedence over emoticon definitions in the `CustomEmoticons` folder in the installation directory.
- Step 5** Restart Cisco Jabber for Windows.
-

Cisco Jabber for Windows loads the custom emoticon definitions in `emoticonDefs.xml`.

**Remember**

Custom emoticon definitions are available to users only if they are defined locally in `emoticonDefs.xml`. If you send custom emoticons to users who do not have the same emoticon definitions, those users receive the default keys, not the icons; for example:

- 1 User A defines a custom emoticon in `emoticonDefs.xml`.
The custom emoticon definition exists only on User A's local file system.
- 2 User A sends that custom emoticon to User B.
- 3 User B receives only the default key for the custom emoticon. User B does not receive the icon.

Emoticon Definitions

Cisco Jabber for Windows loads emoticon definitions from `emoticonDefs.xml`.

The following XML snippet shows the basic structure for the emoticon definitions file:

```
<emoticons>
  <emoticon defaultKey="" image="" text="" order="" hidden="">
    <alt></alt>
  </emoticon>
</emoticons>
```

The following table describes the elements and attributes for defining custom emoticons:

Element or attribute	Description
emoticons	This element contains all emoticon definitions.
emoticon	This element contains the definition of an emoticon.
defaultKey	<p>This attribute defines the default key combination that renders the emoticon.</p> <p>Specify any key combination as the value.</p> <p>This attribute is required.</p> <p>defaultKey is an attribute of the emoticon element.</p>
image	<p>This attribute specifies the filename of the emoticon image.</p> <p>Specify the filename of the emoticon as the value. The emoticon image must exist in the same directory as <code>emoticonDefs.xml</code>.</p> <p>This attribute is required.</p> <p>Cisco Jabber for Windows supports any icon that Internet Explorer can render, including <code>.jpeg</code>, <code>.png</code>, and <code>.gif</code>.</p> <p>image is an attribute of the emoticon element.</p>

Element or attribute	Description
text	<p>This attribute defines the descriptive text that displays in the Insert emoticon dialog box.</p> <p>Specify any string of unicode characters.</p> <p>This attribute is optional.</p> <p>text is an attribute of the emoticon element.</p>
order	<p>This attribute defines the order in which emoticons display in the Insert emoticon dialog box.</p> <p>Specify an ordinal number beginning from 1 as the value.</p> <p>order is an attribute of the emoticon element.</p> <p>This attribute is required. However, if the value of hidden is true this parameter does not take effect.</p>
hidden	<p>This attribute specifies whether the emoticon displays in the Insert emoticon dialog box.</p> <p>Specify one of the following as the value:</p> <p>true</p> <p>Specifies the emoticon does not display in the Insert emoticon dialog box. Users must enter the key combination to render the emoticon.</p> <p>false</p> <p>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.</p> <p>This attribute is optional.</p> <p>hidden is an attribute of the emoticon element.</p>
alt	<p>This element enables you to map key combinations to emoticons.</p> <p>Specify any key combination as the value.</p> <p>For example, if the value of defaultKey is :), you can specify :-) as the value of alt so that both key combinations render the same emoticon.</p> <p>This element is optional.</p>

**Remember**

The default emoticons definitions file contains the following key combinations that enable users to request calls from other users:

- :callme
- :telephone

These key combinations send the callme emoticon, or communicon. Users who receive this emoticon can click the icon to initiate an audio call. You should include these key combinations in any custom emoticons definition file to enable the callme emoticon.

Emoticon Definition Example

```
<emoticons>
<emoticon defaultKey=":) " image="Emoticons_Smiling.png" text="Smile" order="1">
  <alt>:-)</alt>
  <alt>^ ^</alt>
</emoticon>
<emoticon defaultKey=":( " image="Emoticons_Frowning.png" text="Frown" order="2">
  <alt>:-(</alt>
</emoticon>
</emoticons>
```

Enterprise Groups for Cisco Unified Communications Manager IM and Presence Service

Applies to: All clients

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 Cisco Unified Communications Manager 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, Release 11.0(1)*.

Limitations

- Enterprise Groups for Cisco Unified Communications Manager IM and Presence Service is available to on-premises deployments only. Enterprise Groups are already supported on cloud deployments.
- 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 EDI, BDI, 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. There is a search capability for enterprise groups when connecting using EDI or BDI.

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 EDI or BDI.

Enable Enterprise Groups

The enterprise parameter **Directory Group Operations on Cisco IM and Presence** in the **Enterprise Parameter Configuration** window allows you to enable or disable the Enterprise Groups feature. Follow these steps to enable the Enterprise Groups feature.

Before You Begin

The Cisco DirSync feature service must be running.

Procedure

-
- Step 1** From Cisco Unified CM Administration, choose **System > Enterprise Parameters**. The **Enterprise Parameters Configuration** window appears.
- Step 2** In the **User Management Parameters** section, from the **Directory Group Operations on Cisco IM and Presence** drop-down list, select **Enabled**.
- Step 3** (Optional) From the **Syncing Mode for Enterprise Groups** drop-down list, choose one of the following:
- **None**—If you choose this option, the Cisco Intercluster Sync Agent service does not synchronize the enterprise groups and the group membership records between IM and Presence Service clusters.
 - **Differential Sync**—This is the default option. If you choose this option, after all the enterprise groups and group membership records from remote IM and Presence Service cluster are synchronized, the subsequent syncs synchronize only the records that were updated since the last sync occurred.
 - **Full Sync**—If you choose this option, after all the enterprise groups and group membership records from the remote IM and Presence Service cluster are synchronized, all the records are synchronized during each subsequent sync.
- Note** If the Cisco Intercluster Sync Agent service is not running for more than 24 hours, we recommend that you select the **Full Sync** option to ensure that the enterprise groups and group membership records synchronize completely. After all the records are synchronized, that is, when the Cisco Intercluster Sync Agent has been running for about 30 minutes, choose the **Differential Sync** option for the subsequent syncs. Keeping the value of this parameter set to 'Full Sync' for a longer period could result in extensive CPU usage and therefore we recommend that you use the **Full Sync** option during off-business hours.
- Step 4** (Optional) Set the **LDAP Directory Synchronization Schedule** parameters in the **LDAP Directory Configuration** window to configure the interval at which Microsoft Active Directory groups are synchronized with Cisco Unified Communications Manager. For more information, see the online help.
- Step 5** (Optional) Enter a value for the maximum amount of users each group can contain, in the **Maximum Enterprise Group Size to allow Presence Information** field. The permitted range is from 1 to 200 users. The default value is 100 users.
- Step 6** Click **Save**.
-

File Transfers and Screen Captures

Applies to: All clients

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*.

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, Release 10.5(2)* 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

Files and screen captures transferred are stored on a file server and the metadata is logged to a database server. For Cisco Jabber clients that do not support chat rooms, this option enables file transfer in group chats.

When you enable this option, file transfers and screen captures are also available in peer to peer chats and the files and screen captures transferred are stored on a file server and the metadata is logged to a database server.

Before You Begin

File transfer and screen captures for group chats and chat rooms is only available on Cisco Unified Communications Manager IM and Presence Service, release 10.5(2) or later.

Configure an external database to log metadata associated with the file transfer, see *Database Setup for IM and Presence Service on Cisco Unified Communications Manager, Release 10.5(2)* for further information.

Configure a network file server to save the file being transferred, see *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager, Release 10.5(2)* for further information.

Procedure

-
- Step 1** Open the **Cisco Unified CM IM and Presence Administration** interface.
 - Step 2** Select **Messaging > File Transfer**.
 - Step 3** In the **File Transfer Configuration** section select **Managed File Transfer**.
 - Step 4** In the **Managed File Transfer Assignment** section, assign the external database and the external file server for each node in the cluster.
 - Step 5** Select **Save**.
-

What to Do Next

For each node:

- Copy the node's public key to the external file server's `authorized_keys` file, including the node's IP address, hostname, or FQDN.
- Ensure the **Cisco XCP File Transfer Manager** service is active.
- Restart the **Cisco XCP Router** service.

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

Enable file transfer for peer to peer chats on Cisco Unified Communications Manager IM and Presence Service, 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.

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.

My Jabber Chats and My Jabber Files Directory Location

Applies to: Cisco Jabber for Windows

If instant messages and file transfers are automatically saved each time a user closes a conversation (with the `EnableAutosave` parameter), the default location for these files is the Documents folder. Chats are saved in a folder called `MyJabberChats` and files are saved in a folder called `MyJabberFiles`.

However, you can specify a different location with the `AutosaveChatsLocation` parameter or let users choose their own location with the `AllowUserSelectChatsFileDirectory` parameter. If users are allowed to set their own directory location, then the user setting takes priority over the system-defined setting. For more information about these parameters, see the *Parameters Reference Guide* for your release.

Multiple Device Messaging for Cloud Deployments

Applies to: All clients, 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. 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*.

Persistent Chat Rooms

Applies to: Cisco Jabber for Windows, Cisco Jabber for Mac

Configure Persistent Chat

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

Before You Begin

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

Refer to *Database Setup for IM and Presence Service on Cisco Unified Communications Manager* for your release for information on the database configuration necessary to support the persistent chat feature. Database configuration must be performed before continuing with this task.

Local chat message archiving must be enabled for persistent chat. Local chat message archiving is enabled on Cisco Unified Communications Manager IM and Presence Service using the **Allow clients to log instant message history** setting, for more information, see the *Enable Message Settings* topic.

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.

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

Persistent Chat Setting	Recommended Value	Notes
Only moderators can invite people to members-only rooms	Enabled	Cisco Jabber requires this value to be Enabled.
Room owners can change whether or not only moderators can invite people to members-only rooms	Enabled	
Users can add themselves to rooms as members	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
Room owners can change whether users can add themselves to rooms as members	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
Members and administrators who are not in a room are still visible in the room	Enabled	Cisco Jabber requires this value to be Enabled.
Room owners can change whether members and administrators who are not in a room are still visible in the room	Enabled	
Rooms are backwards-compatible with older clients	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
Room owners can change whether rooms are backwards-compatible with older clients	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
Rooms are anonymous by default	Disabled	This value is not currently supported by Cisco Jabber for persistent chat. Cisco Jabber cannot join anonymous rooms.
Room owners can change whether or not rooms are anonymous	Disabled	This value is not currently supported by Cisco Jabber for persistent chat. Cisco Jabber cannot join anonymous rooms.
Lowest participation level a user can have to invite others to the room	Default Value	This value is not currently used by Cisco Jabber for persistent chat.
Room owners can change the lowest participation level a user can have to invite others to the room	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
How many users can be in a room at one time	Administrator Defined	Cisco recommends using the default value.
How many hidden users can be in a room at one time	Administrator Defined	

Persistent Chat Setting	Recommended Value	Notes
Default maximum occupancy for a room	Default Value	
Room owners can change default maximum occupancy for a room	Default Value	
Lowest participation level a user can have to send a private message from within the room	Default Value	
Room owners can change the lowest participation level a user can have to send a private message from within the room	Default Value	
Lowest participation level a user can have to change a room's subject	Moderator	
Room owners can change the lowest participation level a user can have to change a room's subject	Disabled	
Remove all XHTML formatting from messages	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
Room owners can change XHTML formatting setting	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
Rooms are moderated by default	Disabled	This value is not currently used by Cisco Jabber for persistent chat.
Room owners can change whether rooms are moderated by default	Default Value	This value is not currently used by Cisco Jabber for persistent chat.
Maximum number of messages that can be retrieved from the archive	Default Value	
Number of messages in chat history displayed by default	Administrator Defined	Cisco recommends a value between 15 and 50. The Number of messages in chat history displayed by default setting does not apply retroactively to persistent chat rooms. Rooms created before the setting is changed will continue to use their originally configured value.
Room owners can change the number of messages displayed in chat history	Default Value	This value is not currently used by Cisco Jabber for persistent chat.

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

What to Do Next

Ensure you configure any client-specific parameters for persistent chat. For more information, see the Client parameters section of the latest Parameters Reference Guide for Cisco Jabber.

Enable file transfer in chat rooms. For more information, see [File Transfers and Screen Captures](#).

Administer and Moderate Persistent Chat Rooms



Note

- Persistent Chat Rooms and their administration is for on-premises deployments only.
 - Persistent Chat Rooms are not available for mobile clients.
-

You administer persistent chat rooms from the Jabber client by creating rooms, delegating their moderators, and specifying members. The node on which the room is created is created automatically, although you can override it and specify a specific node. Administrators and moderators are privileged users in Persistent Chat rooms. You can administer Persistent Chat rooms on any service node that you are an administrator for on Cisco Unified 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 the history is not deleted).

Moderator Capabilities

Up to 30 moderators can be defined by an administrator for one Persistent Chat room. Moderators can perform the following tasks:

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

Room Creation

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

- Room name (required, maximum 200 characters)
- Description
- Room type (public or restricted)
After the room type has been defined, it cannot be changed by anyone.
- Specify whether to add the room to your **My Rooms** tab (off by default)
- Add up to 30 moderators (who must have a valid Jabber ID to moderate a room).
- Room password

After you create the room, you have the option to add members to the room immediately or at a later time. 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.
-

Prompts for Presence Subscription Requests

Applies to: All clients

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**.

Restore Chats on Login

Applies to: Cisco Jabber for Windows, Cisco Jabber for Mac.

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

Temporary Presence

Applies to: All clients

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.
