Features for All Clients

Bridge Escalations

Applies to: All clients

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.

Procedure

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.

Collaboration Meeting Rooms

Applies to: All clients

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 is a limitation on CMR Cloud join experience for attendees of scheduled CMR Cloud meetings. This limitation impacts Mac users and Windows users who have not enabled Outlook calendar integration. Due to a server limitation, attendees for these deployment scenarios will only receive the option to join the meeting using Cisco WebEx. Hosts will enjoy the full experience, as will anyone invited to join ad hoc CMR Cloud meetings.

Users who are in CTI control mode will only be able to join using WebEx.

Before You Begin

Cisco Collaboration Meeting Rooms Cloud is available on Cisco WebEx Meeting Center.

Procedure

Step 1 Configure the Collaboration Meeting Room options using the configuration guides available here: https://www.cisco.com/c/en/us/support/conferencing/webex-meeting-center/products-installation-and-configuration-guides-list.html

Step 2 Ensure Collaboration Meeting Rooms are enabled for your users on Cisco WebEx Meeting Center.

Step 3 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.

Personal Rooms

Applies to: All clients

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 Meeting Center to allow users to easily meet with their contacts using the **Meet Now** option in the client.

Procedure

Step 1 Personal Rooms are enabled by default for users on Cisco WebEx Meeting Center. For more information see the Cisco WebEx Meeting Center 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 Meeting Center.

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**.

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`.

- `--mobile`—Specify for the problem reports from mobile clients.

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.

Procedure

Step 1 Open a command prompt in Windows.

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

Example for mobile 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 --mobile
```

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.

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.

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.

URI Dialing

This feature is supported for on-premises deployments. URI dialing is enabled in Cisco Unified Communications Manager, release 9.1(2) or later.

This feature is enabled in the `jabber-config.xml` file using the EnableSIPURIDialling parameter.

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

For more information on the values of the parameter, see the *Parameters Reference* Guide.

Applies to: All clients

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

URI dialing allows users to make calls and resolve contacts with Uniform Resource Identifiers (URI). For example, a user named Adam McKenzie has the following SIP URI associated with his directory number: `amckenzi@example.com`. URI dialing enables users to call Adam with his SIP URI rather than his directory number.

For detailed information on URI dialing requirements, such as valid URI formats, as well as advanced configuration including ILS setup, see the *URI Dialing* section of the *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:

Procedure

Step 1 Add devices.

Step 2 Add directory numbers to the devices.

Step 3 Associate users with the devices.

Step 4 Specify primary extensions for users.

What to Do Next

Verify that the directory URIs are associated with the directory numbers.

Configure Directory Numbers with URIs

You can specify URIs for directory numbers that are not associated with users. You should configure directory numbers with URIs for testing and evaluation purposes only.

To configure directory numbers with URIs, do the following:

Procedure

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

Step 2 Select **Call Routing** > **Directory Number**.
The **Find and List Directory Numbers** window opens.

Step 3 Find and select the appropriate directory number.
The **Directory Number Configuration** window opens.

Step 4 Locate the **Directory URIs** section.

Step 5 Specify a valid SIP URI in the **URI** column.

Step 6 Select the appropriate partition from the **Partition** column.

Note You cannot manually add URIs to the system **Directory URI** partition. You should add the URI to the same route partition as the directory number.

Step 7 Add the partition to the appropriate calling search space so that users can place calls to the directory numbers.

Step 8 Select **Save**.

Associate the Directory URI Partition

You must associate the default partition into which Cisco Unified Communications Manager places URIs with a partition that contains directory numbers.

Important To enable URI dialing, you must associate the default directory URI partition with a partition that contains directory numbers.

If you do not already have a partition for directory numbers within a calling search space, you should create a partition and configure it as appropriate.

Procedure

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

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

The **Enterprise Parameters Configuration** window opens.

Step 3 Locate the **End User Parameters** section.

Step 4 In the **Directory URI Alias Partition** row, select the appropriate partition from the drop-down list.

Step 5 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.

Procedure

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

Step 2 Select **Device** > **Device Settings** > **SIP Profile**.
The **Find and List SIP Profiles** window opens.

Step 3 Find and select the appropriate SIP profile.

Remember You cannot edit the default SIP profile. If required, you should create a copy of the default SIP profile that you can modify.

Step 4 Select **Use Fully Qualified Domain Name in SIP Requests** and then select **Save**.

What to Do Next

Associate the SIP profile with all devices that have primary extensions to which you associate URIs.

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 Click **Save**.

Far End Camera Control (FECC)

Applies to: All clients

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.

Hunt Group

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.

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

You can let a user log in to hunt groups by configuring EnableHuntGroup parameter. For more information, see the latest *Parameters Reference Guide for Cisco Jabber*.

Cisco Unified Communications Manager 9.x and later allows configuring of automatic log out of a hunt member when there is no answer. Once the user is logged out, the system displays a log out notification regardless of whether the user is auto logged out, manually logged out, or logged out by the Cisco Unified Communications Manager administrator.

Hunt group features supported by the Cisco Jabber clients:

Features	Mobile Clients	Desktop Clients
Log in to hunt group and log out of hunt group	Not supported	Supported
Call, answer, and decline	Supported	Supported

Line Group

A line group allows you to designate the order in which directory numbers are chosen. Cisco Unified Communications Manager distributes a call to an idle or available member of a line group based on the call distribution algorithm and on the Ring No Answer (RNA) Reversion timeout setting.

Users cannot pick up calls to a DN that belongs to a line group by using the directed call pickup feature.

Configure Line Group

Before You Begin

Configure directory numbers.

Procedure

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

Step 2 Select **Call Routing** > **Route/Hunt** > **Line Group**.
The **Find and List Line Groups** window opens.

Step 3 Select **Add New**.
The **Line Group Configuration** window opens.

Step 4 Enter settings in the **Line Group Information** section as follows:

1. Specify a unique name in the **Line Group Name** field.
2. Specify number of seconds for **RNA Reversion Timeout**.
3. Select a **Distribution Algorithm** to apply to the line group.

Step 5 Enter settings in the **Hunt Options** section as follows:

- Select a value for **No Answer** from the drop-down list.
- Select **Automatically Logout Hunt Member on No Answer** to configure auto logout of the hunt list.
- Select a value for **Busy** from the drop-down list.
- Select a value for **Not Available** from the drop-down list.

Step 6 In the **Line Group Member Information** section, you can do the following:

- Find directory numbers or route partitions to add to the line group.

- Reorder the directory numbers or route partitions in the line group.
- Remove directory numbers or route partitions from the line group.

Step 7 Select **Save**.

What to Do Next

Configure a hunt list and add the line group to the hunt list.

Hunt List

A hunt list contains a set of line groups in a specific order. A hunt list associates with one or more hunt pilots and determines the order in which those line groups are accessed. The order controls the progress of the search for available directory numbers for incoming calls.

A hunt list comprises a collection of directory numbers as defined by line groups. After Cisco Unified Communications Manager determines a call that is to be routed through a defined hunt list, Cisco Unified Communications Manager finds the first available device on the basis of the order of the line group(s) that a hunt list defines.

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

Procedure

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

Step 2 Select **Call Routing** > **Route/Hunt** > **Hunt List**.
The **Find and Hunt List Groups** window opens.

Step 3 Select **Add New**.
The **Hunt List Configuration** window opens.

Step 4 Enter settings in the **Hunt List Information** section as follows:

1. Specify a unique name in the **Name** field.
2. Enter a description for the Hunt List.
3. Select a **Cisco Unified Communications Manager Group** from the drop-down list.
4. The system selects **Enable this Hunt List** by default for a new hunt list when the hunt list is saved.
5. If this hunt list is to be used for voice mail, select **For Voice Mail Usage**.

Step 5 Select **Save** to add the hunt list.

What to Do Next

Add line groups to the hunt list.

Add Line Group to Hunt List

Before You Begin

You must configure line groups and configure a hunt list.

Procedure

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

Step 2 Select **Call Routing** > **Route/Hunt** > **Hunt List**.
The **Find and Hunt List Groups** window opens.

Step 3 Locate the hunt list to which you want to add a line group.

Step 4 To add a line group, select **Add Line Group**.
The **Hunt List Detail Configuration** window displays.

Step 5 Select a line group from the **Line Group** drop-down list.

Step 6 To add the line group, select **Save**.

Step 7 To add additional line groups, repeat Step 4 to Step 6.

Step 8 Select Save.

Step 9 To reset the hunt list, select **Reset**. When the dialog box appears, select **Reset**.

Hunt Pilot

A hunt pilot comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a hunt list. Hunt pilots provide flexibility in network design. They work in conjunction with route filters and hunt lists to direct calls to specific devices and to include, exclude, or modify specific digit patterns. For more 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

Procedure

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

Step 2 Select **Call Routing** > **Route/Hunt** > **Hunt Pilot**.
The **Find and List Hunt Pilots** window opens.

Step 3 Select **Add New**.
The **Hunt Pilot Configuration** window opens.

Step 4 Enter the hunt pilot, including numbers and wildcards.

Step 5 Select a hunt list from the **Hunt List** drop-down list.

Step 6 Enter any additional configurations in the **Hunt Pilot Configuration** window. For more information on hunt pilot configuration settings, see the relevant Cisco Unified Communications Manager documentation.

Step 7 Select **Save**.

Jabber to Jabber Call

Applies to: All clients

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.

Logout Inactivity Timer

Applies to: All clients

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.

This feature is configured 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.

This feature is configured on the desktop clients using the ForceLogoutTimerDesktop parameter.

If the parameter is not set, the client will not automatically sign out.

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*.

Voicemail Avoidance

Applies to: All clients

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.

Procedure

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

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

Step 3 In the **Server** drop-down list, select the active Cisco Unified Communications Manager.

Step 4 In the **Service** drop-down list, select the **Cisco Call Manager (Active)** service.

Step 5 Configure the settings in the **Clusterwide Parameters (System - Mobility Single Number Reach Voicemail)** section.

Note The settings in this section are not specific to Cisco Jabber. For information about how to configure these settings, see the *Confirmed Answer and DvO VM detection* section in the *Cisco Unified Communications Manager Administrator Guide* for your release.

Step 6 Click **Save**.

Enable Voicemail Avoidance on Mobility Identity

Use this procedure to enable user-controlled voicemail avoidance for the end user's mobility identity.

Before You Begin

- Set up the annunciator on the Cisco Unified Communications Manager. For more information, see the *Annunciator setup* section in the *Cisco Unified Communications Manager Administrator Guide* for your release.
- If you set up a Media Resource Group on the Cisco Unified Communications Manager, set up the annunciator on the Media Resource Group. For more information, see the *Media resource group setup* section in the *Cisco Unified Communications Manager Administrator Guide* for your release.

Procedure

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

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

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

Step 3 In the **Associated Mobility Identity** section, click the link for the Mobility Identity.

Note To ensure that the Voicemail Avoidance feature works correctly, the DvO Callback Number that the end user enters in the Cisco Jabber client must match the Destination Number that you enter on the Mobility Identity Configuration screen.

Step 4 Set the policies as follows:

- Cisco Unified Communications Manager 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.

Procedure

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

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

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

Step 3 In the **Associated Remote Destinations** section, 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**.

Telemetry

Cisco Jabber Analytics

Applies to: All clients

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.

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

Full details on what analytics data Cisco Jabber does and does not collect can be found in the Cisco Jabber Supplement to Cisco's On-Line Privacy Policy at https://www.cisco.com/web/siteassets/legal/privacy_02Jun10.html.