



Configure the Clients

- [Introduction to Client Configuration, on page 1](#)
- [Configure Service Profiles, on page 2](#)
- [Create and Host Client Configuration Files, on page 9](#)
- [Problem Reporting, on page 43](#)
- [Configure Automatic Updates, on page 44](#)
- [Custom Embedded Tabs, on page 46](#)

Introduction to Client Configuration

Cisco Jabber can retrieve configuration settings from the following sources:

- **Service Profiles** — You can configure some client settings in UC service profiles on Cisco Unified Communications Manager release 9 and later. When users launch the client, it discovers the Cisco Unified Communications Manager home cluster using a DNS SRV record and automatically retrieves the configuration from the UC service profile.

Applies to on-premises deployments only.

- **Phone Configuration** — You can set some client settings in the phone configuration on Cisco Unified Communications Manager release 9 and later. The client retrieves the settings from the phone configuration in addition to the configuration in the UC service profile.

Applies to on-premises deployments only.

- **Cisco Unified Communications Manager IM and Presence Service** — You can enable instant messaging and presence capabilities and configure certain settings such as presence subscription requests.

In the **Advanced settings** window, if you select either **Cisco IM & Presence** or **Cisco Communications Manager 8.x**, the client retrieves UC services from Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service. The client does not use service profiles or SSO discovery.

Applies to on-premises deployments only.

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

Applies to on-premises and cloud-based deployments.

- Cisco Webex Administration Tool — You can configure some client settings with the Cisco Webex Administration Tool.

Applies to cloud-based deployments only.

Configure Service Profiles

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



Important

- Cisco Jabber only retrieves configuration from service profiles on Cisco Unified Communications Manager if the client gets the `_cisco-uds` SRV record from a DNS query.

In a hybrid environment, if the CAS URL lookup is successful Cisco Jabber retrieves the configurations from Cisco WebEx Messenger service and the `_cisco-uds` SRV record is ignored.

- In an environment with multiple Cisco Unified Communications Manager clusters, you can configure the Intercluster Lookup Service (ILS). ILS enables the client to find the user's home cluster and discover services.

If you do not configure ILS, then you must manually configure remote cluster information, similar to the EMCC remote cluster set up. For more information on Remote Cluster Configuration, see the *Cisco Unified Communications Manager Features and Services Guide*.

Related Topics

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

Set Parameters on Service Profile

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

Parameters in Service Profiles

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

IM and Presence Service Profile

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

Parameter	Description
Product type	<p>Provides the source of authentication to Cisco Jabber and has the following values:</p> <ul style="list-style-type: none"> Unified CM (IM and Presence Service) — Cisco Unified Communications Manager IM and Presence Service is the authenticator. WebEx (IM and Presence Service) — The Cisco WebEx Messenger service is the authenticator. <p>Note As of this release, the client issues an HTTP query in addition to the query for SRV records. The HTTP query allows the client to determine if it should authenticate to the Cisco WebEx Messenger service.</p> <p>As a result of the HTTP query, the client connects to the Cisco WebEx Messenger service in cloud-based deployments before getting the <code>_cisco-uds</code> SRV record. Setting the value of the Product type field to WebEx may have no practical effect if the WebEx service has already been discovered by a CAS lookup.</p> <ul style="list-style-type: none"> Not set — If the service profile does not contain an IM and presence service configuration, the authenticator is Cisco Unified Communications Manager.
Primary server	<p>Specifies the address of your primary presence server.</p> <ul style="list-style-type: none"> On-Premises Deployments — You should specify the fully qualified domain name (FQDN) of Cisco Unified Communications Manager IM and Presence Service. Cloud-Based Deployments — The client uses the following URL as default when you select WebEx as the value for the Product type parameter: https://loginp.webexconnect.com/cas/auth.do This default URL overrides any value that you set.

Voicemail Profile

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

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

Conferencing Profile

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

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

Directory Profile

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

CTI Profile

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

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

Add Cisco Unified Communications Manager Services

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

Procedure

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

The **Find and List UC Services** window opens.

Step 3 Select **Add New**.

The **UC Service Configuration** window opens.

Step 4 Select the UC service type you want to add and then select **Next**.

Step 5 Configure the UC service as appropriate and then select **Save**.

What to do next

Add your UC services to service profiles.

Create Service Profiles

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

Procedure

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

Step 2 Select **User Management > User Settings > Service Profile**.

The **Find and List UC Services** window opens.

Step 3 Select **Add New**.

The **Service Profile Configuration** window opens.

Step 4 Enter a name for the service profile in the **Name** field.

Step 5 Select **Make this the default service profile for the system** if you want the service profile to be the default for the cluster.

Note On Cisco Unified Communications Manager release 9.x only, users who have only instant messaging capabilities (IM only) must use the default service profile. For this reason, you should set the service profile as the default if you plan to apply the service profile to IM only users.

Step 6 Add your UC services, apply any additional configuration, and then select **Save**.

What to do next

Apply service profiles to end user configuration.

Apply Service Profiles

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

Procedure

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

Step 2 Select **User Management > End User**.

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

Step 3 Enter the appropriate search criteria to find existing users and then select a user from the list.

The **End User Configuration** window opens.

Step 4 Locate the **Service Settings** section.

Step 5 Select a service profile to apply to the user from the **UC Service Profile** drop-down list.

Important Cisco Unified Communications Manager release 9.x only: If the user has only IIM and Presence Service capabilities (IM only), you must select **Use Default**. For IM only users, Cisco Unified Communications Manager release 9.x always applies the default service profile regardless of what you select from the **UC Service Profile** drop-down list.

Step 6 Apply any other configuration as appropriate and then select **Save**.

Associate Users with Devices

On Cisco Unified Communications Manager version 9.x only, when the client attempts to retrieve the service profile for the user, it first gets the device configuration file from Cisco Unified Communications Manager. The client can then use the device configuration to get the service profile that you applied to the user.

For example, you provision Adam McKenzie with a CSF device named CSFAKenzi. The client retrieves CSFAKenzi.cnf.xml from Cisco Unified Communications Manager when Adam signs in. The client then looks for the following in CSFAKenzi.cnf.xml:

```
<userId serviceProfileFile="identifier.cnf.xml">amckenzi</userId>
```

For this reason, if you are using Cisco Unified Communications Manager version 9.x, you should do the following to ensure that the client can successfully retrieve the service profiles that you apply to users:

- Associate users with devices.
- Set the **User Owner ID** field in the device configuration to the appropriate user. The client will retrieve the Default Service Profile if this value is not set.



Note

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

Procedure

Step 1 Associate users with devices.

- Open the **Unified CM Administration** interface.
- Select **User Management > End User**.

- c) Find and select the appropriate user.
The **End User Configuration** window opens.
- d) Select **Device Association** in the **Device Information** section.
- e) Associate the user with devices as appropriate.
- f) Return to the **End User Configuration** window and then select **Save**.

Step 2 Set the **User Owner ID** field in the device configuration.

- a) Select **Device > Phone**.
- b) Find and select the appropriate device.
The **Phone Configuration** window opens.
- c) Locate the **Device Information** section.
- d) Select **User** as the value for the **Owner** field.
- e) Select the appropriate user ID from the **Owner User ID** field.
- f) Select **Save**.

Set Parameters on Phone Configuration for Desktop Clients

The client can retrieve configuration settings in the phone configuration from the following locations on Cisco Unified Communications Manager:

Enterprise Phone Configuration

Applies to the entire cluster.



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

Common Phone Profile Configuration

Applies to groups of devices and takes priority over the cluster configuration.

Cisco Unified Client Services Framework (CSF) Phone Configuration

Applies to individual CSF devices and takes priority over the group configuration.

Parameters in Phone Configuration

The following table lists the configuration parameters you can set in the **Product Specific Configuration Layout** section of the phone configuration and maps corresponding parameters from the client configuration file:

Desktop Client Settings Configuration	Description
Video Calling	<p>Enables or disables video capabilities.</p> <p>Enabled (default) Users can send and receive video calls.</p> <p>Disabled Users cannot send or receive video calls.</p> <p>Restriction This parameter is available only on the CSF device configuration.</p>
File Types to Block in File Transfer	<p>Restricts users from transferring specific file types.</p> <p>Set a file extension as the value, for example, <code>.exe</code>.</p> <p>Use a semicolon to delimit multiple values, for example, <code>.exe;.msi;.rar;.zip</code></p>
Automatically Start in Phone Control	<p>Sets the phone type for users when the client starts for the first time. Users can change their phone type after the initial start. The client then saves the user preference and uses it for subsequent starts.</p> <p>Enabled Use the desk phone device for calls.</p> <p>Disabled (default) Use the software phone (CSF) device for calls.</p>
Jabber For Windows Software Update Server URL	<p>Specifies the URL to the XML file that holds client update information. The client uses this URL to retrieve the XML file from your web server.</p> <p>In hybrid cloud-based deployments, you should use the Cisco WebexAdministration Tool to configure automatic updates.</p>
Problem Report Server URL	<p>Specifies the URL for the custom script that allows users to submit problem reports.</p>

Set Parameters on Phone Configuration for Mobile Clients

The client can retrieve configuration settings in the phone configuration from the following locations on Cisco Unified Communications Manager:

- Cisco Dual Mode for iPhone (TCT) Configuration — Applies to individual TCT devices and takes priority over the group configuration.
- Cisco Jabber for Tablet (TAB) Configuration — Applies to individual TAB devices and takes priority over the group configuration.

Parameters in Phone Configuration

The following table lists the configuration parameters you can set in the **Product Specific Configuration Layout** section of the phone configuration and maps corresponding parameters from the client configuration file:

Parameter	Description
On-Demand VPN URL	URL for initiating on-demand VPN. Note Applicable for iOS only.
Preset Wi-fi Networks	Enter the SSIDs for Wi-Fi networks (SSIDs) approved by your organization. Separate SSIDs with a forward slash (/). Devices do not connect to secure connect if connected to one of the entered Wi-Fi networks.
Default Ringtone	Sets the default ringtone to Normal or Loud .
Video Capabilities	Enables or disables video capabilities. <ul style="list-style-type: none"> • Enabled (default) — Users can send and receive video calls. • Disabled — Users cannot send or receive video calls.
Dial via Office Note TCT and BOT devices only.	Enables or disables Dial via Office. <ul style="list-style-type: none"> • Enabled — Users can dial via office. • Disabled (default) — Users cannot dial via office.

Create and Host Client Configuration Files

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

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

For Cisco Jabber for iPhone and iPad and Cisco Jabber for Android, you must create a global configuration file to set up:

- Directory integration for on-premises deployments.
- Voicemail service credentials for hybrid-cloud deployments.



Note In most environments, Cisco Jabber for Windows and Cisco Jabber for Mac do not require any configuration to connect to services. Create a configuration file only if you require custom content such as automatic updates, problem reporting, or user policies and options.

Before you begin

Note the following configuration file requirements:

- Configuration filenames are case-sensitive. Use lowercase letters in the filename to prevent errors and to ensure the client can retrieve the file from the TFTP server.
- You must use utf-8 encoding for the configuration files.
- The client cannot read configuration files that do not have a valid XML structure. Check the structure of your configuration file for closing elements and confirm that elements are nested correctly.
- Valid XML character entity references only are permitted in your configuration file. For example, use `&` instead of `&`. If your XML contains invalid characters, the client cannot parse the configuration file.

To validate your configuration file, open the file in Microsoft Internet Explorer.

- If Internet Explorer displays the entire XML structure, your configuration file does is valid.
- If Internet Explorer displays only part of the XML structure, it is likely that your configuration file contains invalid characters or entities.

Procedure

	Command or Action	Purpose
Step 1	Specify Your TFTP Server Address, on page 10	Specify your TFTP server address for client to enable access to your configuration file.
Step 2	Create Global Configurations, on page 12	Configure the clients for users in your deployment.
Step 3	Create Group Configurations, on page 13	Apply different configuration to different set of users.
Step 4	Host Configuration Files, on page 14	Host configuration files on any TFTP server.
Step 5	Restart Your TFTP Server, on page 14	Restart the TFTP server before the client can access the configuration files.

Specify Your TFTP Server Address

The client gets configuration files from a TFTP server. The first step in configuring the client is to specify your TFTP server address so the client can access your configuration file.

**Attention**

If Cisco Jabber gets the `_cisco-uds` SRV record from a DNS query, it can automatically locate the user's home cluster. As a result, the client can also locate the Cisco Unified Communications Manager TFTP service. You do not need to specify your TFTP server address if you deploy the `_cisco-uds` SRV record.

Specify Your TFTP Server on Cisco Unified Presence

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

Procedure

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

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

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

The **Cisco Jabber Settings** window opens.

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

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

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

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

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

Step 5 Select **Save**.

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

If you are using Cisco Unified Communications Manager release 9.x, then you do not need to follow the steps below.

Procedure

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

Step 2 Select **Application > Legacy Clients > Settings**.

The **Legacy Client Settings** window opens.

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

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

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

Step 5 Select **Save**.

Specify TFTP Servers in Phone Mode

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

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

Specify TFTP Servers with the Cisco WebEx Administration Tool

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

Procedure

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

Create Global Configurations

The client downloads the global configuration file from your TFTP server during the login sequence. Configure the client for all users in your deployment.

Before you begin

If the structure of your configuration file is not valid, the client cannot read the values you set. Review the XML samples in this chapter for more information.

Procedure

-
- Step 1** Create a file named `jabber-config.xml` with any text editor.
- Use lowercase letters in the filename.
 - Use UTF-8 encoding.
- Step 2** Define the required configuration parameters in `jabber-config.xml`.
- Step 3** Host the group configuration file on your TFTP server.
- If your environment has multiple TFTP servers, ensure that the configuration file is the same on all TFTP servers.
-

Create Group Configurations

Group configuration files apply to subsets of users and are supported on Cisco Jabber for desktop (CSF devices) and on Cisco Jabber for mobile devices. Group configuration files take priority over global configuration files.

If you provision users with CSF devices, specify the group configuration filenames in the **Cisco Support Field** field on the device configuration. If users do not have CSF devices, set a unique configuration filename for each group during installation with the `TFTP_FILE_NAME` argument.

Before you begin

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

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

- If the structure of your configuration file is not valid, the client cannot read the values you set. Review the XML samples in this chapter for more information.

Procedure

-
- Step 1** Create an XML group configuration file with any text editor.
- The group configuration file can have any appropriate name; for example, `jabber-groupa-config.xml`.
- Step 2** Define the required configuration parameters in the group configuration file.

- Step 3** Add the group configuration file to applicable CSF devices.
- Open the **Cisco Unified CM Administration** interface.
 - Select **Device > Phone**.
 - Find and select the appropriate CSF device to which the group configuration applies.
 - In the **Phone Configuration** window, navigate to **Product Specific Configuration Layout > Desktop Client Settings**.
 - In the **Cisco Support Field** field, enter `configurationfile=group_configuration_file_name.xml`. For example, enter `configurationfile=groupa-config.xml`.

Note If you host the group configuration file on your TFTP server in a location other than the default directory, you must specify the path and the filename; for example, `configurationfile=/customFolder/groupa-config.xml`.

Do not add more than one group configuration file. The client uses only the first group configuration in the **Cisco Support Field** field.
 - Select **Save**.

- Step 4** Host the group configuration file on your TFTP server.
-

Host Configuration Files

You can host configuration files on any TFTP server. However, Cisco recommends hosting configuration files on the Cisco Unified Communications Manager TFTP server, which is the same as that where the device configuration file resides.

Procedure

- Step 1** Open the **Cisco Unified OS Administration** interface on Cisco Unified Communications Manager.
 - Step 2** Select **Software Upgrades > TFTP File Management**.
 - Step 3** Select **Upload File**.
 - Step 4** Select **Browse** in the **Upload File** section.
 - Step 5** Select the configuration file on the file system.
 - Step 6** Do not specify a value in the **Directory** text box in the **Upload File** section.
You should leave an empty value in the **Directory** text box so that the configuration file resides in the default directory of the TFTP server.
 - Step 7** Select **Upload File**.
-

Restart Your TFTP Server

You must restart your TFTP server before the client can access the configuration files.

Procedure

-
- Step 1** Open the **Cisco Unified Serviceability** interface on Cisco Unified Communications Manager.
- Step 2** Select **Tools > Control Center - Feature Services**.
- Step 3** Select **Cisco Tftp** from the **CM Services** section.
- Step 4** Select **Restart**.
- A window displays to prompt you to confirm the restart.
- Step 5** Select **OK**.
- The **Cisco Tftp Service Restart Operation was Successful** status displays.
- Step 6** Select **Refresh** to ensure the **Cisco Tftp** service starts successfully.
-

What to do next

To verify that the configuration file is available on your TFTP server, open the configuration file in any browser. Typically, you can access the global configuration file at the following URL:
http://tftp_server_address:6970/jabber-config.xml

Configuration File Structure

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

XML Declaration

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

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

Root Element

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

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

Group Elements

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

XML Structure

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

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

```

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

```

Group Elements and Parameters

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

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

Client Parameters

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

Parameter	Description
CachePasswordMobile	<p>Specifies whether the password is remembered or not on the client side.</p> <p>true (default) — The password is prefilled and Automatic sign-in is shown. Users can allow the client to cache their password. This option allows users to automatically sign in when the client starts.</p> <p>false — After the client successfully registers to the Cisco Unified Communications Manager, the password field is empty and Automatic sign-in is not shown. Users cannot allow the client to cache their password. Users must enter their password each time the client starts.</p> <p>Note The client displays Automatic sign-in on first sign-in, or if the user clears the application data.</p>
PrtLogServerURL	Specifies the custom script for submitting problem reports.
UpdateURL	Specifies the URL to the automatic updates XML definition file on your HTTP server. The client uses this URL to retrieve the update XML file.
jabber-plugin-config	Contains plug-in definitions such as custom embedded tabs that display HTML content.
Forgot_Password_URL	<p>Specifies the URL of your web page for users to reset or retrieve forgotten passwords.</p> <p>In hybrid cloud-based deployments, use the Cisco WebEx Administration Tool to direct users to the web page to reset or retrieve forgotten passwords.</p>
Persistent_Chat_Enabled	<p>Specifies whether the persistent chat feature is available in the client.</p> <ul style="list-style-type: none"> • true — The persistent chat interface is shown in the client. • false (default) — The default value is assumed if the setting is not present in the configuration file.
MaxNumberOfBookmarks	<p>Specifies the maximum number of bookmarks allowed in persistent chat rooms.</p> <ul style="list-style-type: none"> • 30 (default) - sets a maximum of 30 bookmarks.
Mention_P2Pchat	<p>Specifies whether mentions are enabled in person to person chat.</p> <ul style="list-style-type: none"> • true (default) — Enables mentions in person to person chat. • false — Disables mentions in person to person chat.

Parameter	Description
Mention_GroupChat	Specifies whether mentions are enabled in group chat. <ul style="list-style-type: none"> • true (default) — Enables mentions in group chat. • false — Disables mentions in group chat.
Mention_PersistentChat	Specifies whether mentions are enabled in persistent chat. <ul style="list-style-type: none"> • true (default) — Enables mentions in persistent chat. • false — Disables mentions in persistent chat.
spell_check_enabled	Specifies whether spell check is enabled in the client. Spell check supports autocorrect, allows users to select the correct word from a list of suggestions, and add the word to a dictionary. <ul style="list-style-type: none"> • true — Spell check is enabled. • false (default) — Spell check is disabled.
spell_check_language	Specifies the default spell check language for users. By default, the client uses the Jabber language as the default spell check language. You can define the default language dictionary that you want to set the client to use. From the conversation windows, users may select different default languages for each user they IM with. <code><spell_check_language>1031</spell_check_language></code> defines German as the default spell check language.
Disable_IM_History	Specifies whether to retain chat history after participants close the chat window. <p>Note This parameter is not available for IM-only deployments.</p> <ul style="list-style-type: none"> • true—Do not retain chat history after participants close the chat window. • false (default)—Retain chat history: <ul style="list-style-type: none"> • After participants close the chat window. • Until the participants sign out. <p>If the participants re-open the chat window, the last 99 messages show.</p> <p>Message archiving should be disabled on the server.</p>

Parameter	Description
EnableAutosave	<p>Specifies whether users can save instant messages automatically each time they close a conversation. Enables the option in the client under: File > Options > Chats > Autosave each chat when closing the conversation.</p> <ul style="list-style-type: none"> • true — The check box is available. • false (default) — The check box is unavailable.
AutosaveChatsLocation	<p>Defines the path where instant messages are saved automatically each time a user closes a conversation. Use the absolute path on the local file system.</p>
SystemIdleDuringCalls	<p>Cisco Jabber for Windows only.</p> <p>Specifies if the screen saver or computer lock function activates during a Cisco Jabber call if the user is inactive and if the function is enabled on your Windows computer. This parameter does not control any behavior for incoming calls when the screen is already locked or the screen saver is already on.</p> <ul style="list-style-type: none"> • true—Screen saver can activate during calls. • false (default)—Screen saver cannot activate during calls or when users receive a new incoming call alert. When the call ends or the new incoming call alert is accepted or rejected, then the screen saver or screen lock is enabled again.
ShowRecentsTab	<p>Cisco Jabber for Windows only.</p> <p>Specify whether you want to show or hide users' call history from the Recents tab on the Cisco Jabber hub window.</p> <ul style="list-style-type: none"> • true (default)—The Recents tab is shown. • false—The Recents tab is hidden.
SwapDisplayNameOrder	<p>Cisco Jabber for Windows only.</p> <p>Specifies that for certain locales, when the displayname directory field is empty or not available, users' own display names and the display names of their contacts can be changed to <i>Lastname, Firstname</i> format.</p> <ul style="list-style-type: none"> • true (default)—In the following locales: Chinese (Hong Kong), Chinese (People's Republic of China), Chinese (Taiwan), Japanese, Korean; the format for users' own display names and the display names of their contacts is in the <i>Lastname, Firstname</i> format. • false—This feature is not available.

Options Parameters

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

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

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

Parameter	Description
Location_Enabled	Specifies whether the Location tab is available in the client. <ul style="list-style-type: none"> • true (default)—The Location tab is shown in the client. • false—The Location tab is not shown in the client.
LOCATION_MATCHING_MODE	Determines how the client detects the current network locations for the Location feature. <ul style="list-style-type: none"> • MacAddressOnly (default) - The client uses the Mac address of the network default gateway. • MacAddressWithSubnet - The client uses a unique pair of subnet addresses and Mac address of the default gateway.
Location_Mode	Specifies whether the Location feature is enabled and whether users are notified when new locations are detected. Determines the option in the client under: File > Options > Location <ul style="list-style-type: none"> • ENABLED (default)—Location feature is turned on. Users are notified when new locations are detected. • DISABLED—Location feature is turned off. Users are not notified when new locations are detected. • ENABLEDNOPROMPT—Location feature is turned on. Users are not notified when new locations are detected.
DockedWindowVisible	Specifies if the docked window displays when the client starts. <ul style="list-style-type: none"> • true (default) — The docked window displays when the client starts. • false — The docked window does not display when the client starts.
DockedWindowPosition	Sets the position of the docked window on the user's screen. <ul style="list-style-type: none"> • TopCenter (default) — The position of the docked window is at the top center of the screen. • TopLeft — The position of the docked window is at the top left of the screen. • TopRight — The position of the docked window is at the top right of the screen.
Callhistory_Expire_Days	Sets the number of days before the call history is deleted. If the value is 0 or not specified in the configuration file, the call history is not deleted until the count exceeds the maximum number of stored calls.

Parameter	Description
EnableSaveChatHistoryToExchange	<p>Cisco Jabber for Windows only</p> <p>Enables the client to automatically save chat histories to a Cisco Jabber Chats folder in users' Microsoft Outlook application.</p> <ul style="list-style-type: none"> • true — Enables saving chat history to an Outlook folder. • false (default) — Does not save chat history to an Outlook folder.
ExchangeAuthenticateWithSystemAccount	<p>Cisco Jabber for Windows only</p> <p>An authentication method to Exchange server. To save chat history to an Outlook folder, it enables the client to use the Operating System account details of the logged in user to authenticate with the Exchange server. This authentication method uses the Windows NT LAN Manager (NTLM) security protocol.</p> <ul style="list-style-type: none"> • true (default)—The client uses the Operating System account details of the user to authenticate to the Exchange server. • false—The client does not use the users' Operating System account details to authenticate to the Exchange server.
Exchange_UseCredentialsFrom	<p>Cisco Jabber for Windows only</p> <p>An authentication method to Exchange server. To save chat history to an Outlook folder, it synchronizes the Exchange credentials using one of the following Authenticator argument credentials for users: CUP, CUCM, WEBEX.</p> <ul style="list-style-type: none"> • CUP -- Use CUP credentials for Exchange • CUCM -- Use CUCM credentials for Exchange • WEBEX -- Use WebEx credentials for Exchange <p>Define the value of the parameter as the authenticator for the service that you want used to sync credentials. For example, <code><Exchange_UseCredentialsFrom>CUCM</Exchange_UseCredentialsFrom></code>.</p>
ExchangeAutodiscoverDomain	<p>Cisco Jabber for Windows only</p> <p>Method of specifying server address. To save chat history to an Outlook folder, enables the client to automatically discover the Exchange servers based on users' domain from their credentials.</p> <p>Define the value of the parameter as the domain to discover the Exchange server. The client uses the domain to search for the Exchange server at one of the following web addresses:</p> <pre>https://<domain>/autodiscover/autodiscover.svc https://autodiscover.<domain>/ autodiscover/autodiscover.svc</pre>

Parameter	Description
InternalExchangeServer	Cisco Jabber for Windows only Method of specifying server address. To save chat history to an Outlook folder, manually defines the internal Exchange server.
ExternalExchangeServer	Cisco Jabber for Windows only Method of specifying server address. To save chat history to an Outlook folder, manually defines the external Exchange server.
CalendarIntegrationType	<p>This parameter works with the Meetings_Enabled parameter.</p> <ul style="list-style-type: none"> • 0—Disables calendar integration in the Meetings tab of the client user interface. If you disable this parameter, the Meetings tab in the client is empty, but the Meetings tab remains on the hub window. • 1—Enables Microsoft Outlook calendar integration in the Meetings tab of the client user interface. • 2—Enables IBM Lotus Notes calendar integration in the Meetings tab of the client user interface. • 3—Enables Google Calendar integration in the Meetings tab of the client user interface. <p>Restart Cisco Jabber to apply the changes.</p>

Phone Parameters

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

Parameter	Description
CcmcipServer1	<p>Specifies the address of the primary CCMCIP server.</p> <p>This parameter is required:</p> <ul style="list-style-type: none"> Only if the address of your CCMCIP server is not the same as the TFTP server address. <p>If the address of the CCMCIP server is the same as the TFTP server address, the client can use the TFTP server address to connect to the CCMCIP server.</p> <ul style="list-style-type: none"> In deployments with Cisco Unified Communications Manager Release 8. <p>In deployments with Cisco Unified Communications Manager release 9 and later, the client can discover the CCMCIP server if you provision the <code>_cisco-uds</code> SRV record.</p> <p>Cisco Unified Communications Manager release 9.x and earlier—If you enable Cisco Extension Mobility, the <code>Cisco Extension Mobility</code> service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the <i>Feature and Services</i> guide for your Cisco Unified Communications Manager release.</p>
CcmcipServer2	<p>Specifies the address of the secondary CCMCIP server.</p> <p>This parameter is optional.</p>
CtiServer1	<p>Specifies the address of the primary CTI server.</p> <p>You should specify a CTI server address in the client configuration if users have desk phone devices.</p>
CtiServer2	<p>Specifies the address of the secondary CTI server.</p> <p>This parameter is optional.</p>
EnableCallPark	<p>Specifies whether the call park feature is available in the client. To access the call park feature, choose the More option in the call window.</p> <ul style="list-style-type: none"> true (default) — Call park is enabled. false — Call park is disabled. There is no call park option under the More button.
EnableDSCPPacketMarking	<p>Applicable to Jabber for Mac only.</p> <p>Specifies if DSCP marking is applied to the packets:</p> <ul style="list-style-type: none"> true (default) — DSCP marking is enabled and the checkbox in the client is not shown. false — DSCP marking is not made to packets and the checkbox in the client is not shown.

Parameter	Description
Meeting_Server_Address	<p>Specifies the primary Cisco webEx meeting site URL for users.</p> <p>The Jabber for Windows client populates the meeting site in the user's host account on the Options window. The Jabber for Mac client populates the meeting site in the user's host account on the Preferences > Meetings window. Users can enter their credentials to set up the host account and access their Cisco webEx meetings, if the meeting site requires credentials.</p> <p>Important If you specify an invalid meeting site, users cannot add, or edit, any meetings sites in the client user interface.</p> <p>This parameter is optional.</p>
Meeting_Server_Address_Backup	<p>Specifies the secondary Cisco webEx meeting site URL for users.</p> <p>This parameter is optional.</p>
Meeting_Server_Address_Backup2	<p>Specifies the tertiary Cisco webEx meeting site URL for users.</p> <p>This parameter is optional.</p>
TftpServer1	<p>Specifies the address of the primary Cisco Unified Communications Manager TFTP service where device configuration files reside. Set one of the following as the value:</p> <ul style="list-style-type: none"> • Hostname (<i>hostname</i>) • IP address (<i>123.45.254.1</i>) • FQDN (<i>hostname.domain.com</i>) <p>You should set this parameter in the client configuration only if:</p> <ul style="list-style-type: none"> • You deploy the client in phone mode. • The TFTP server address for the device configuration is different to the TFTP server address for the client configuration. <p>During installation, you should set the address of the TFTP server where the client configuration file resides with the following argument: TFTP.</p>
TftpServer2	<p>Specifies the address of the secondary Cisco Unified Communications Manager TFTP service.</p> <p>This parameter is optional.</p>

Parameter	Description
useCUCMGroupForCti	<p>Specifies if the Cisco Unified Communications Manager Group handles load balancing for CTI servers. Set one of the following values:</p> <ul style="list-style-type: none"> • true — The Cisco Unified Communications Manager Group handles CTI load balancing. You should set this value in phone mode deployments only. In full UC mode, the presence server automatically handles CTI load balancing. • false (default) — The Cisco Unified Communications Manager Group does not handle CTI load balancing.

Policies Parameters

Policies parameters let you control specific client functionality.

On-Premises Policies

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

Parameter	Description
Screen_Capture_Enabled	<p>Specifies if users can take screen captures.</p> <ul style="list-style-type: none"> • true (default) — Users can take screen captures. • false — Users cannot take screen captures.
File_Transfer_Enabled	<p>Specifies if users can transfer files to each other.</p> <ul style="list-style-type: none"> • true (default) — Users can transfer files to each other. • false — Users cannot transfer files to each other.
Disallowed_File_Transfer_Types	<p>Restricts users from transferring specific file types.</p> <p>Set file extensions as the value, for example, <code>.exe</code>.</p> <p>Use a semicolon to delimit multiple file extensions, for example, <code>.exe;.msi;.rar;.zip</code>.</p>

Parameter	Description
PreferredFT	<p>When Cisco Unified Communications Manager IM & Presence server provides both Managed File Transfer and Peer-to-Peer File Transfer, this parameter specifies the preferred method of transferring files in the client.</p> <ul style="list-style-type: none"> • MFT — Files are transferred using the managed file transfer option. • P2P — Files are transferred using peer to peer file transfer. <p>If the parameter is not defined, the client checks Cisco Unified Communications Manager IM and Presence node and when managed file transfer is available the client uses this option, otherwise it uses peer to peer file transfer.</p>
DisableMFTForConversationTypes	<p>When the Managed File Transfer option is available, this parameter specifies the conversation types that disable the setting.</p> <ul style="list-style-type: none"> • P2P — Managed file transfer is disabled for peer to peer conversations. • GroupChat — Managed file transfer is disabled for group chats. • PersistentChat — Managed file transfer is disabled for persistent chat rooms. <p>Use a semicolon to delimit multiple conversation types, for example P2P;GroupChat;PersistentChat.</p>
Customize_Phone_Server	<p>Allows users to change their phone server settings in the client in on-premises deployments. Do not set this parameter to true if you are deploying SAML SSO, as changing phone server settings could interfere with SSO working properly.</p> <ul style="list-style-type: none"> • true — Users can change their phone server settings. • false (default) — Users cannot change their phone server settings.
Customize_Voicemail_Server	<p>Allows users to change their voicemail server settings in the client in on-premises deployments. Do not set this parameter to true if you are deploying SAML SSO, as changing voicemail server settings could interfere with SSO working properly.</p> <ul style="list-style-type: none"> • true — Users can change their voicemail server settings. • false (default) — Users cannot change their voicemail server settings.

Related Topics

[Common Policies](#), on page 29

[Cisco WebEx Policies](#), on page 40

Common Policies

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

Parameter	Description
CalendarAutoRefreshTime	<p>Cisco Jabber for Windows only.</p> <p>Specifies the number of minutes after which IBM Lotus Notes or Google calendars refresh.</p> <p>The default value is 0.</p>
Disallow_File_Transfer_On_Mobile	<p>Specifies whether the user can send or receive files on mobile.</p> <ul style="list-style-type: none"> • true — Users cannot send or receive files on mobile. • false (default) — Users can send or receive files on mobile.
EnableVideo	<p>Enables or disables video capabilities.</p> <ul style="list-style-type: none"> • true (default) — Users can make and receive video calls. • false — Users cannot make or receive video calls.
InitialPhoneSelection	<p>Sets the phone type for users when the client starts for the first time. Users can change their phone type after the initial start. The client then saves the user preference and uses it for subsequent starts.</p> <ul style="list-style-type: none"> • deskphone — Use the desk phone device for calls. • softphone (default) — Use the software phone (CSF) device for calls. <p>The client selects devices in the following order:</p> <ol style="list-style-type: none"> 1. Software phone devices 2. Desk phone devices <p>If you do not provision users with software phone devices, the client automatically selects desk phone devices.</p>

Parameter	Description
UserDefinedRemoteDestinations	<p>Lets users add, edit, and delete remote destinations through the client interface. Use this parameter to change the default behavior when you provision Extend and Connect capabilities.</p> <p>By default, if a user's device list contains only a CTI remote device, the client does not let that user add, edit, or delete remote destinations. This occurs to prevent users from modifying dedicated remote devices that you assign. However, if the user's device list contains a software device or a desk phone device, the client lets users add, edit, and delete remote destinations.</p> <ul style="list-style-type: none"> • true — Users can add, edit, and delete remote destinations. • false (default) — Users cannot add, edit, and delete remote destinations.
EnableLocalAddressBookSearch	<p>Lets users search for and add local Microsoft Outlook contacts to their contact lists.</p> <ul style="list-style-type: none"> • true (default) — Users can search for and add local contacts to their contact lists. • false — Users cannot search for or add local contacts to their contact lists.
EnableAccessoriesManager	<p>Enables the accessories API in the client. This API lets accessory vendors create plugins to enable call management functionality for devices such as headsets.</p> <ul style="list-style-type: none"> • true (default) — Enable the accessories API. • false — Disable the accessories API.
BlockAccessoriesManagerPlugins	<p>Disables specific Accessories Manager plugins from third party vendors such as Jabra or Logitech. You should set the name of the plugin DLL file as the value. Use a comma to separate multiple values, for example, on Microsoft Windows:</p> <pre><BlockAccessoriesManagerPlugins> JabraJabberPlugin.dll,lucpcisco.dll </BlockAccessoriesManagerPlugins></pre>
ForceFontSmoothing	<p>Specifies if the client applies anti-aliasing to smooth text.</p> <ul style="list-style-type: none"> • true (default) — The client applies anti-aliasing to text. • false — The operating system applies anti-aliasing to text.

Parameter	Description
EnableBFCPVideoDesktopShare	<p>Enables BFCP video desktop sharing capabilities.</p> <ul style="list-style-type: none"> • true (default) — Enables BFCP video desktop sharing on the client. • false — Disables BFCP video desktop sharing.
Meetings_Enabled	<p>Enables meetings capabilities in the client. Works in conjunction with the CalendarIntegrationType parameter.</p> <ul style="list-style-type: none"> • true (default) — Enables meetings capabilities, allowing you to create meetings and get reminders to join meetings. • false — Disables meetings capabilities.
Telephony_Enabled	<p>Enables audio and video capabilities and user interface in the client.</p> <ul style="list-style-type: none"> • true (default) — Enables audio and video capabilities and user interface. • false — Disables audio and video capabilities and user interface. <p>If your client is enabled for IM-only mode, then you must set this parameter to false. If you do not set this parameter in IM-only mode deployments, then users may see disabled telephony capabilities on their user interface.</p>
Voicemail_Enabled	<p>Enables voicemail capabilities and user interface in the client.</p> <ul style="list-style-type: none"> • true (default) — Enables voicemail capabilities and user interface. • false — Disables voicemail capabilities and user interface.
EnableTelProtocolHandler	<p>Specifies if the client registers as the protocol handler for the <code>tel:</code> URI.</p> <ul style="list-style-type: none"> • true (default) — The client registers as the protocol handler for the <code>tel:</code> URI. • false — The client does not register as the protocol handler for the <code>tel:</code> URI.

Parameter	Description
EnableIMProtocolHandler	<p>Specifies if the client registers as the protocol handler for the <code>IM: URI</code>.</p> <ul style="list-style-type: none"> • true (default) — The client registers as the protocol handler for the <code>IM: URI</code>. • false — The client does not register as the protocol handler for the <code>IM: URI</code>.
EnableSIPProtocolHandler	<p>Specifies if the client registers as the protocol handler for the <code>SIP: URI</code>.</p> <ul style="list-style-type: none"> • true (default) — The client registers as the protocol handler for the <code>SIP: URI</code>. • false — The client does not register as the protocol handler for the <code>SIP: URI</code>.
EnableSaveChatToFile	<p>Allows users to save their chats to the file system as HTML.</p> <ul style="list-style-type: none"> • true (default) — Users can save their chats to file. • false — Users cannot save their chats to file.
printchat_enabled	<p>Cisco Jabber for Windows</p> <p>Specifies whether users have the ability to print conversations from the chat window.</p> <ul style="list-style-type: none"> • true (default)—Users can print conversations from the chat window by right-clicking and selecting Print. • false—Users cannot print conversations from the chat window. If they right-click inside the window, the Print option is not in the menu.

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

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

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

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

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

Parameter	Description
EnableTelProtocolPopupWindow CiscoTelProtocolPermissionEnabled	<p>Specifies whether the dialog box is enabled or disabled which asks users to confirm if they want to make a call after they click on a ciscotel:uri enabled number.</p> <ul style="list-style-type: none"> • true (default) — Dialog box is enabled and users are asked to confirm that they want to place the call. • false — Dialog box is disabled and the call is made without requesting confirmation first. This may cause accidental or unwanted calls. <p>Note The CiscoTelProtocolPermissionEnabled parameter replaces the EnableTelProtocolPopupWindow parameter. Both parameters are supported in the client, however the dialog box is disabled if either parameter is set to false.</p>
CiscoTelProtocolCrossLaunchBackNotificationEnabled	<p>Specifies if a dialog box is shown asking users whether they want to return to another application when a call ends or to stay in Jabber.</p> <ul style="list-style-type: none"> • true (default) — Dialog box is shown. • false — Dialog box is not shown.
CiscoTelProtocolCrossLaunchBackSchema	<p>Specifies a white list of application types that can be cross launched back to when a call is ended.</p> <ul style="list-style-type: none"> • none (default) — No list. • <i>schema_names</i> — Semicolon-delimited list of permitted application types. <p>For example:</p> <pre><CiscoTelProtocolCrossLaunchBackSchema>AppSchema1;AppSchema2</CiscoTelProtocolCrossLaunchBackSchema></pre>
SSO_Enabled	<p>Specifies whether users sign in by using single sign-on (SSO).</p> <ul style="list-style-type: none"> • TRUE (default) — Users sign in by using SSO. • FALSE — Users do not use SSO to sign in.
ServicesDomainSsoEmailPrompt	<p>Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.</p> <ul style="list-style-type: none"> • ON — The prompt is shown. • OFF (default) — The prompt is not shown.

Parameter	Description
EnableP2PDesktopShare	<p>Allows users to share their screen if not on a call.</p> <ul style="list-style-type: none"> • true (default) — Allows users to share their screens. • false — Users cannot do person to person screen sharing.
PreferP2PDesktopShare	<p>Specifies that person to person screen sharing is preferred over video sharing.</p> <ul style="list-style-type: none"> • true — Person to person screen sharing is preferred. • false (default) — Video sharing is preferred.
EnableForensicsContactData	<p>Specifies whether users' Contacts folder is collected by the Problem Reporting Tool (PRT) when reporting a problem that is related to their contacts.</p> <ul style="list-style-type: none"> • true (default) — Contacts folder is collected by the PRT tool. • false — Contacts folder is not collected by the PRT tool.
SharePortRangeStart	<p>This parameter is used with SharePortRangeSize to specify a port range to use when users share their screen from a chat window in Cisco Jabber for Windows.</p> <p>If you do not configure these parameters, the client uses the default port range for IM screen share, 49152 to 65535. For more information on default port ranges, see the topic on <i>Ports and Protocols for Cisco Jabber for Windows and Cisco Jabber for Mac</i> in the <i>Cisco Jabber 10.6 Deployment Guide</i> or the <i>Cisco Jabber 10.6 Planning Guide</i>.</p> <p>The value you enter specifies the start of the port range. For example:</p> <pre><Policies> <SharePortRangeStart>45130</SharePortRangeStart> <SharePortRangeSize>100</SharePortRangeSize> </Policies></pre> <p>The minimum value is 1024. The value cannot exceed 65535 minus the SharePortRangeSize.</p>
SharePortRangeSize	<p>Specifies the size of the port range, when used with the SharePortRangeStart parameter. The minimum value is 40. The value when added to the SharePortRangeStart parameter cannot exceed 65535</p> <p>For more information on port ranges, see the topic on <i>Ports and Protocols for Cisco Jabber for Windows and Cisco Jabber for Mac</i> in the <i>Cisco Jabber 10.6 Deployment and Installation Guide</i> or the <i>Cisco Jabber 10.6 Planning Guide</i>.</p>

Parameter	Description
selfcareURL	<p>Value: The fully qualified domain name (FQDN) of CUCM service.</p> <p>Defines the URL for the Self Care Portal when no default service profile is selected in Cisco Unified Communications Manager.</p>
EnableLoadAddressBook	<p>Specifies whether users can search and view the native contacts stored in their iOS device on the Search or call window in Cisco Jabber for iPhone and iPad.</p> <p>Note This parameter is only applicable in Phone Only mode.</p> <ul style="list-style-type: none"> • true (default) — Native contacts in the iOS device can be searched from the Search or call window in Cisco Jabber for iPhone and iPad. • false — Native contacts in the iOS device cannot be searched from the Search or call window in Cisco Jabber for iPhone and iPad. <p>Note The users can always search the native contacts on the keypad window of the iOS device.</p>

Related Topics

[On-Premises Policies](#), on page 27

[Cisco WebEx Policies](#), on page 40

Cisco WebEx Policies

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

Related Topics

[On-Premises Policies](#), on page 27

[Common Policies](#), on page 29

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

Presence Parameters

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

Parameter	Description
LoginResource	<p>Controls user sign in to multiple client instances.</p> <ul style="list-style-type: none"> • multiResource (default) — Users can sign in to multiple instances of the client at the same time. • wbxconnect — Users can sign in to one instance of the client at a time. <p>The client appends the <code>wbxconnect</code> suffix to the user's JID. Users cannot sign in to any other Cisco Jabber client that uses the <code>wbxconnect</code> suffix.</p>
PresenceServerAddress	<p>Specifies the address of a presence server for on-premises deployments. Set one of the following as the value:</p> <ul style="list-style-type: none"> • Hostname (<i>hostname</i>) • IP address (<i>123.45.254.1</i>) • FQDN (<i>hostname.domain.com</i>)
PresenceServerURL	<p>Specifies the Central Authentication Service (CAS) URL for the Cisco WebEx Messenger service. The following is an example of a URL you can set as the value:</p> <p><code>https://loginp.webexconnect.com/cas/sso/ex_org/orgadmin.app</code></p>
CalendarWebExMeetingPresence	<p>Enables users' presence to change to "In a WebEx meeting" even if they do not join the WebEx session link but the meeting is in their Microsoft Outlook calendar.</p> <ul style="list-style-type: none"> • true - Users' presence changes to "In a WebEx meeting" even if they do not join the WebEx session link. • false (default) - Users must join the WebEx session link for their presence to change to "In a WebEx meeting". Otherwise, their presence remains "Available", even if the meeting is in their Microsoft Outlook calendar.

Voicemail Parameters

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

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

Service Credentials Parameters

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

Voicemail Service Credentials

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

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

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

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

Example Configuration

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

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Client>
    <PrtLogServerUrl>http://server_name:port/path/prt_script.php</PrtLogServerUrl>
    <jabber-plugin-config>
      <browser-plugin>
        <page refresh="true" preload="true">
          <tooltip>Cisco</tooltip>
          <icon>http://www.cisco.com/web/fw/i/logo.gif</icon>
          <url>www.cisco.com</url>
        </page>
      </browser-plugin>
    </jabber-plugin-config>
  </Client>
  <Options>
    <Set_Status_Inactive_Timeout>20</Set_Status_Inactive_Timeout>
    <StartCallWithVideo>false</StartCallWithVideo>
  </Options>
```

```

<Policies>
  <Disallowed_File_Transfer_Types>.exe;.msi</Disallowed_File_Transfer_Types>
</Policies>
<Directory>
  <BDIPresenceDomain>example.com</BDIPresenceDomain>
  <BDIPrimaryServerName>dir.example.com</BDIPrimaryServerName>
  <BDISearchBase1>ou=staff,dc=example,dc=com</BDISearchBase1>
  <BDIConnectionUsername>ad_jabber_access@example.com</BDIConnectionUsername>
  <BDIConnectionPassword>jabber</BDIConnectionPassword>
  <BDIPhotoUriSubstitutionEnabled>True</BDIPhotoUriSubstitutionEnabled>
  <BDIPhotoUriSubstitutionToken>sAMAccountName</BDIPhotoUriSubstitutionToken>
  <BDIPhotoUriWithToken>http://example.com/photo/sAMAccountName.jpg
  </BDIPhotoUriWithToken>
</Directory>
</config>

```

Problem Reporting

Applies to: Cisco Jabber for Windows

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

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

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

Before you begin

Complete the following steps to prepare your environment:

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

The following is an example form that accepts problem reports:

```

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

```

Procedure

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

Configure Automatic Updates

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

To enable automatic updates, you create an XML file that contains the information for the most recent version, including the URL of the installation package on the HTTP server. The client retrieves the XML file when users sign in, resume their computer from sleep mode, or perform a manual update request from the **Help** menu.



Note

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

XML File Structure

XML files for automatic updates have the following structure:

```
<JabberUpdate>
  <App name="JabberWin">
    <LatestBuildNum>12345</LatestBuildNum>
    <LatestVersion>10.5.x</LatestVersion>
    <Mandatory>true</Mandatory>
    <Message>
      <![CDATA[<b>This new version of Cisco Jabber lets you do the
        following:</b><ul><li>Feature 1</li><li>Feature 2</li></ul>For
        more information click <a target="_blank"
        href="http://cisco.com/go/jabber">here</a>.</li></li>]]>
    </Message>
    <DownloadURL>http://http_server_name/CiscoJabberSetup.msi</DownloadURL>
  </App>
</JabberUpdate>
```

Example XML File 1

The following is example XML file for automatic updates:

```
<JabberUpdate>
<App name="JabberWin">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.x</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2</li></ul>For
more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.</li></li>]]></Message>
  <DownloadURL>http://http_server_name/CiscoJabberSetup.msi</DownloadURL>
</App>
</JabberUpdate>
```

Example XML File 2

The following is an example XML file for automatic updates for both Cisco Jabber for Windows and Cisco Jabber for Mac:

```
<JabberUpdate>
  <App name="JabberMac">
    <LatestBuildNum>12345</LatestBuildNum>
    <LatestVersion>9.6.1</LatestVersion>
    <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2</li>
```

```

    </ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.</li>
</Message>

<DownloadURL>http://http_server_name/Cisco-Jabber-Mac-9.6.1-12345-MrbCdd.zip</DownloadURL>

</App>
<App name="JabberWin">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.0</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2
</li></ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.</li>
</Message>
  <DownloadURL>http://http_server_name/CiscoJabberSetup.msi
</DownloadURL>
</App>
</JabberUpdate>

```

Before you begin

- Install and configure an HTTP server to host the XML file and installation package.
- Ensure users have permission to install software updates on their workstations.

Microsoft Windows stops update installations if users do not have administrative rights on their workstations. You must be logged in with administrative rights to complete installation.

Procedure

-
- Step 1** Host the update installation program on your HTTP server.
- Step 2** Create an update XML file with any text editor.
- Step 3** Specify values in the XML as follows:
- name—Specify the following ID as the value of the name attribute for the App element:
 - JabberWin—The update applies to Cisco Jabber for Windows.
 - JabberMac—The update applies to Cisco Jabber for Mac.
 - LatestBuildNum—Build number of the update.
 - LatestVersion—Version number of the update.
 - Mandatory—(Windows clients only) True or False. Determines whether users must upgrade their client version when prompted.
 - Message—HTML in the following format:


```
<![CDATA[your_html]]>
```
 - DownloadURL—URL of the installation package on your HTTP server.
For Cisco Jabber for Mac the URL file must be in the following format:
`Cisco-Jabber-Mac-version-size-dsaSignature.zip`

- Step 4** Save and close your update XML file.
- Step 5** Host your update XML file on your HTTP server.
- Step 6** Specify the URL of your update XML file as the value of the UpdateUrl parameter in your configuration file.

Custom Embedded Tabs

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



Note The Jabber embedded browser does not support cookie sharing with pop-ups from SSO enabled webpages. The content on the pop-up window may fail to load.

Custom Embedded Tab Definitions

The custom embedded tab can only be configured using the `jabber-config.xml` file. The following XML snippet shows the structure for custom tab definitions:

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

Cisco Jabber for Windows supports Internet Explorer version 9 or earlier. The client uses Internet Explorer in version 9 mode if a later version is on the workstation.

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

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

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

User Custom Tabs

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

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

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



Note User custom embedded tabs are set to true by default.

Custom Icons

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

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

Chats and Calls from Custom Tabs

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

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

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

Related Topics

[Protocol Handlers](#)

UserID Tokens

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



Tip

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

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

1. You specify the following in your custom embedded tab:
2. Mary Smith signs in. Her username is msmith.
3. The client replaces the `${UserID}` token with Mary's username as follows:

```
<url>www.cisco.com/${UserID}/profile</url>
```

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

JavaScript Notifications

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

Notification Methods

The client includes an interface that exposes the following methods for JavaScript notifications:

- **SetNotificationBadge** — You call this method from the client in your JavaScript. This method takes a string value that can have any of the following values:
 - Empty — An empty value removes any existing notification badge.
 - A number from 1 to 999
 - Two digit alphanumeric combinations, for example, A1
- **onPageSelected()** — The client invokes this method when users select the custom embedded tab.
- **onPageDeselected()** — The client invokes this method when users select another tab.



Note Not applicable for Jabber for iPhone and iPad

- **onHubResized()** — The client invokes this method when users resize or move the client hub window.
- **onHubActivated()** — The client invokes this method when the client hub windows is activated.
- **onHubDeActivated()** — The client invokes this method when the client hub window is deactivated.

Subscribe to Presence in Custom Tabs

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

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



Note

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

Get Locale Information in Custom Tabs

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

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



Note Jabber for iPad and iPhone only supports `OnLocaleInfoAvailable`.

Example JavaScript

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

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

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

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

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

        cell.innerHTML = currentLocale;
      }

      function onHubActivated()
      {
        var cell = document.getElementById("hubActive");
        cell.innerHTML = "TRUE";
      }

      function onHubDeActivated()
      {
        var cell = document.getElementById("hubActive");
        cell.innerHTML = "FALSE";
      }

      function onHubResized()
      {
        alert("Hub Resized or Moved");
      }

      function OnLoadMethods()
```

```

        {
            SubscribePresence();
            GetUserLocale();
        }
    </script>
</head>

<body onload="OnLoadMethods()">
    <table>
        <tr>
            <td>John Doe</td>
            <td id="johndoe@example.com">unknown</td>
        </tr>
    </table>
    <table>
        <tr>
            <td>Jabber Locale: </td>
            <td id="JabberLocale">Null</td>
        </tr>
        <tr>
            <td>Hub Activated: </td>
            <td id="hubActive">---</td>
        </tr>
    </table>
</body>
</html>

```

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

Show Call Events in Custom Tabs

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

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

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

```

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

```

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

```

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

```

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

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

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

```
function OnTelephonyConversationStateChanged(json) {
    console.log("OnTelephonyConversationStateChanged");
    try {
        var conversation = JSON.parse(json);
        console.log("conversation state=" + conversation.state);
        console.log("conversation acceptanceState=" + conversation.acceptanceState);
        console.log("conversation callType=" + conversation.callType);
        for (var i=0; i<conversation.remoteParticipants.length; i++) {
            console.log("conversation remoteParticipants[" + i + "]=");
            console.log("voiceMediaDisplayName=" +
conversation.remoteParticipants[i].voiceMediaDisplayName);
            console.log("voiceMediaNumber=" +
conversation.remoteParticipants[i].voiceMediaNumber);
            console.log("translatedNumber=" +
conversation.remoteParticipants[i].translatedNumber);
            console.log("voiceMediaPhoneType=" +
conversation.remoteParticipants[i].voiceMediaPhoneType);
            console.log("voiceMediaState=" +
conversation.remoteParticipants[i].voiceMediaState);
        }
        console.log("conversation localParticipant=");
        console.log("  voiceMediaDisplayName=" +
conversation.localParticipant.voiceMediaDisplayName);
        console.log("  voiceMediaNumber=" + conversation.localParticipant.voiceMediaNumber);

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

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

Custom Embedded Tab Example

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

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Client>
    <jabber-plugin-config>
```

```
<browser-plugin>
  <page refresh ="true" preload="true">
    <tooltip>Cisco</tooltip>
    <icon>https://www.cisco.com/web/fw/i/logo.gif</icon>
    <url>https://www.cisco.com</url>
  </page>
</browser-plugin>
</jabber-plugin-config>
</Client>
</config>
```

