# CONTENTS

## PREFACE
- Change History vii
- Change History vii

## CHAPTER 1
**Jabber Overview** 1
- Purpose of this Guide 1
- About Cisco Jabber 1
- Jabber Team Messaging Mode Deployment Options 2
- Prerequisites for Jabber Team Messaging Mode Installation 3

## PART I
**Configure the Cloud** 5

## CHAPTER 2
**Configure Cisco Webex Control Hub** 7
- Bulk Configure Users in Cisco Webex Control Hub 7
- Set Up Calling for Team Messaging Mode Users 8
- Enable Individual Jabber Users with Team Messaging Mode and Jabber Calling 9
- Create Upgrade Profiles in Cisco Webex Control Hub 9
- Deliver Jabber Configuration File Through Cisco Webex Control Hub 10

## PART II
**Configure Cisco Unified Communications Manager** 11

## CHAPTER 3
**Configure the Clients** 13
- Client Configuration Workflow 13
  - Introduction to Client Configuration 13
  - Set Client Configuration Parameters in Unified CM 14
  - Define Jabber Configuration Parameters 14
  - Assign Jabber Client Configuration to Service Profile 14
| Create and Host the Client Configuration Files | 15 |
| Specify Your TFTP Server Address | 16 |
| Create Global Configurations | 17 |
| Create Group Configurations | 17 |
| Host Configuration Files | 18 |
| Restart Your TFTP Server | 18 |
| Configuration File | 19 |
| Set Parameters on Phone Configuration for Desktop Clients | 19 |
| Parameters in Phone Configuration | 19 |
| Set Parameters on Phone Configuration for Mobile Clients | 20 |
| Parameters in Phone Configuration | 20 |
| Optional Configuration of Proxy Settings | 21 |
| Configure Proxy Settings for Cisco Jabber for Windows | 22 |
| Configure Proxy Settings for Cisco Jabber for Mac | 23 |
| Configure Proxy Settings for Cisco Jabber iPhone and iPad | 23 |
| Configure Proxy Settings for Cisco Jabber for Android | 23 |

**CHAPTER 4**

Create Users on Unified Communications Manager | 25 |
---|---
Enable Synchronization | 25 |
Specify an LDAP Attribute for the User ID | 26 |
Specify an LDAP Attribute for the Directory URI | 26 |
Perform Synchronization | 27 |
Assign Roles and Groups | 27 |
Authentication Options | 28 |
Enable SAML SSO in the Client | 28 |
Authenticate with the LDAP Server | 29 |

**CHAPTER 5**

Configure Service Discovery for Remote Access | 31 |
---|---
Service Discovery Requirements | 31 |
DNS Requirements | 31 |
Certificate Requirements | 32 |
Test_collab-edge SRV Record | 32 |

**CHAPTER 6**

Configure Deskphone Control | 33 |
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prerequisites</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Configure Deskphone Control Taskflow</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Enable Device for CTI</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>Configure Desk Phone Video</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>Troubleshooting Desk Phone Video</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Enable Video Rate Adaptation</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Enable RTCP on Common Phone Profiles</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Enable RTCP on Device Configurations</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Configure User Associations</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Reset Devices</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td><strong>Configure Softphone</strong></td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>Create Softphones Workflow</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>Create and Configure Cisco Jabber Devices</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>Provide Users with Authentication Strings</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Add a Directory Number to the Device</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Associate Users with Devices</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Create Mobile SIP Profiles</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>Setting up System SIP Parameters</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Configure the Phone Security Profile</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td><strong>Configure Extend and Connect</strong></td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>Configure Extend and Connect Workflow</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>Enable User Mobility</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>Create CTI Remote Devices</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>Add a Remote Destination</td>
<td>53</td>
</tr>
<tr>
<td><strong>PART III</strong></td>
<td><strong>Deploy Jabber</strong></td>
<td>55</td>
</tr>
<tr>
<td></td>
<td><strong>Deploy Cisco Jabber Applications and Jabber Softphone for VDI</strong></td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>Download the Cisco Jabber Clients</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>Install Cisco Jabber for Windows</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>Use the Command Line</td>
<td>58</td>
</tr>
<tr>
<td></td>
<td>Example Installation Commands</td>
<td>58</td>
</tr>
</tbody>
</table>
Command Line Arguments 59
LCID for Languages 72
Run the MSI Manually 74
Create a Custom Installer 75
   Get the Default Transform File 75
   Create Custom Transform Files 75
   Transform the Installer 76
   Installer Properties 78
Deploy with Group Policy 78
   Set a Language Code 79
   Deploy the Client with Group Policy 80
Uninstall Cisco Jabber for Windows 81
   Use the Installer 81
   Use the Product Code 81
Install Cisco Jabber for Mac 82
   Installer for Cisco Jabber for Mac 82
      Run Installer Manually 83
   URL Configuration for Cisco Jabber for Mac 84
   Configure Automatic Updates for Mac 86
Install Cisco Jabber Mobile Clients 87
   URL Configuration for Cisco Jabber for Android, iPhone, and iPad 88
   Mobile Configuration Using Enterprise Mobility Management 90
      FIPS_MODE Parameter 91
      CC_MODE Parameter 91
      AllowUrlProvisioning Parameter 91
Install Jabber Softphone for VDI 92
## Change History

- Change History, on page vii

### Change History

<table>
<thead>
<tr>
<th>Date</th>
<th>Status</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>September, 2019</td>
<td>Initial Publication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Changed</td>
<td>Your Webex org domain can be different from the voice services domain.</td>
<td>Configure Cisco UC Manager Settings in Cisco Webex Control Hub</td>
<td></td>
</tr>
<tr>
<td>New</td>
<td>Use Control Hub to distribute Jabber configuration files.</td>
<td>Deliver Jabber Configuration File Through Cisco Webex Control Hub</td>
<td></td>
</tr>
<tr>
<td>Changed</td>
<td>Added AllowTeamsUseEmbeddedSafari for installing Jabber mobile clients.</td>
<td>URL Configuration for Cisco Jabber for Android, iPhone, and iPad</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile Configuration Using Enterprise Mobility Management</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 1

Jabber Overview

• Purpose of this Guide, on page 1
• About Cisco Jabber, on page 1
• Jabber Team Messaging Mode Deployment Options, on page 2
• Prerequisites for Jabber Team Messaging Mode Installation, on page 3

Purpose of this Guide

This guide includes the basic tasks required to get Cisco Jabber with Team Messaging Mode up and running. You can deploy team messaging mode on its own or with calling capabilities. The tasks include installing, configuring, and deploying.

• Part 1 of the guide focuses on how to configure Cisco Jabber on the Cisco Webex Control Hub. If you are deploying team messaging mode for IM-only, this is the only configuration you need to do.

• Part 2 of the guide focuses on how to configure telephony for your users. This configuration is done on Cisco Unified Communications Manager to enable softphones, deskphone control, extend and connect, and service discovery. If you want an IM-Only deployment, you can skip this part.

• Part 3 of the guide focuses on how to deploy Jabber for Windows, Mac, iPhone and iPad, Android, and in virtual environments.


About Cisco Jabber

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

The applications in the Cisco Jabber family of products are:

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


Jabber Team Messaging Mode Deployment Options

Cisco Jabber is a modular Unified Communications client that you can deploy in various ways. You have access to a number of collaboration work flows, including these:

• Audio and video calling on your computer
• Deskphone control of audio and video calling
• Messaging and presence
• Contacts integration
• Meetings
• Voicemail

You can enable some or all of these work flows to meet your needs. For example, a phone-only deployment of Jabber doesn't enable the messaging work flow.

This figure shows the architecture of a Jabber hybrid cloud-based deployment with the Cisco Webex Platform service.
Prerequisites for Jabber Team Messaging Mode Installation

Before you install Jabber team messaging mode, complete these tasks:


2. Create user accounts in Unified Communications Manager.

3. Create user accounts in Cisco Webex Control Hub.
   

4. If your deployment uses Unified Communications Manager Release 12.5 or later, we recommend that you use SIP OAuth with Jabber team messaging mode. See the chapter on SIP OAuth mode in the Feature Configuration Guide for Cisco Unified Communications Manager at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.
Configure the Cloud

• Configure Cisco Webex Control Hub, on page 7
CHAPTER 2

Configure Cisco Webex Control Hub

- Bulk Configure Users in Cisco Webex Control Hub, on page 7
- Set Up Calling for Team Messaging Mode Users, on page 8
- Enable Individual Jabber Users with Team Messaging Mode and Jabber Calling, on page 9
- Create Upgrade Profiles in Cisco Webex Control Hub, on page 9
- Deliver Jabber Configuration File Through Cisco Webex Control Hub, on page 10

Bulk Configure Users in Cisco Webex Control Hub

You can configure up to 20,000 Jabber users in the Control Hub using a CSV file. When you add the user information in the CSV file, you can also assign services to the users.

Procedure

Step 1
From the customer view in https://admin.webex.com go to Users, click Manage Users and choose CSV Add or Modify Users.

You might see a message about sending welcome emails to the users. Click Next to proceed or cancel and change your account settings.

Step 2
Click Export to download a CSV file with the current configuration for your users. Click download CSV template to download a template without your current user information instead.

In the CSV file that you download, you can update the existing information or add a new user on an empty row. Enter the following information in the available columns:

- To assign a service, add True in that service's column, and to exclude a service, add False.
- User ID/Email (Required)—Enter the user information.
- For your Jabber deployment enter information for each user in the following columns of the CSV file:
  - Jabber team messaging mode—Add True to assign team messaging mode to your Jabber users.
  - Jabber calling—Add True to assign Jabber calling to your users.
  - UC Manager Profile—Add your Cisco UC Manager profile name from Control Hub.
  - Contact Migration Required—Add True to migrate users' contacts from Webex Messenger or the Cisco Unified Communications Manager IM & Presence service to their Jabber contacts.
ContactMigrationCompleted remains **False** by default, allowing an administrator to later perform contact migration for specific users.

**Note**

- **Upgrade Profile**—Add the profile name if you created one. This setting does not apply for mobile clients.
- If you have an active license template, leave all the service columns blank. The Control Hub automatically assigns the template for the new user in that row.

**Step 3** Click **Import**, select your file, and click **Open**.

**Step 4** Choose either **Add services only** or **Add and remove services**.
If you have an active license template, choose **Add services only**.

**Step 5** Click **Submit**.

Submitting the CSV file uploads it and creates your task. You can close the browser or this window and your task continues to run. You can review the progress of tasks. For more information, see Manage Tasks in Cisco Webex Control Hub.

---

### Set Up Calling for Team Messaging Mode Users

You can set up calling for your Jabber users on team messaging mode in Control Hub. You can either create a profile for your Cisco UC Manager server settings in Control Hub, or choose from your existing deployment options. The Jabber client uses these settings to connect to the Cisco UC Manager server for calling capabilities.

**Procedure**

**Step 1** From the customer view in https://admin.webex.com go to **Services** and then click **Settings** on the **Message** card, then toggle on **Enable Jabber team messaging mode**.

**Step 2** Select **Add Profile** under **UC Manager Profiles**.

**Step 3** Enter a profile name, then select one of the following options:

- **Voice Services Domain**—Enter the domain for your voice services.
- **UDS Server**—Enter the IP address or hostname for your UDS Server and your backup UDS server.
- (Optional)—Click **Allow users to edit server address** to allow your users to change the server settings in their Jabber client.

**Step 4** Save the profile.
Enable Individual Jabber Users with Team Messaging Mode and Jabber Calling

Rather than using the bulk import method, you can set up individual Jabber users for team messaging mode in Control Hub.

Procedure

**Step 1**
From the customer view in [https://admin.webex.com](https://admin.webex.com) go to **Users**.

**Step 2**
Select a user and under the **Services** section, select **Cisco Webex Teams**.

**Step 3**
Choose from the following options:

- **Enable Jabber team messaging mode**—The Jabber user is assigned team messaging mode.
- **Contact Migration Required**—The user is asked to migrate their contacts from Webex Messenger or the Cisco Unified Communications Manager IM & Presence service to Jabber. The user must first reset Jabber before logging back in.
- **Enable Jabber calling**—The Jabber user is assigned Jabber calling.

(Optional) You can choose a Cisco UC Manager profile for the user. Or, if you don't choose a profile, then Jabber uses the services_domain, the voice services domain, the domain of the user name, or the UPN domain to query the DNS SRV records to connect to your Cisco UC Manager.

Create Upgrade Profiles in Cisco Webex Control Hub

For Jabber deployments with team messaging mode, you can control the upgrade path for your Jabber users. You can apply organization-wide settings, or you create an upgrade profile to assign to individual users.

Upgrade profiles allow you to control how desktop users upgrade to new versions. You can set users to automatically upgrade to the latest version of team messaging mode or to only upgrade to a specific version. The profiles do not apply to mobile clients.

When you specify a version in the upgrade profile, users do not upgrade to versions after the specified version. However, upgrade profiles that specify an unsupported Jabber version are invalid. In that case, your users upgrade to the latest Jabber version. Typically, Jabber supports a release for Jabber team messaging mode for 1 year. Periodically update the profile to specify a valid version to which your users upgrade.

Procedure

**Step 1**
From the customer view in [https://admin.webex.com](https://admin.webex.com), go to **Services** and then click **Settings** on the **Message** card.

**Step 2**
Under **Jabber team messaging mode**, select **Add Upgrade Profile**.

**Step 3**
Name the profile, and specify the upgrade paths for Jabber for Windows and Jabber for Mac users.
• Automatically upgrade users to the latest version.
• Upgrade their clients to a specific version.

Step 4  Save the upgrade profile.
Step 5  Associate the upgrade profile to appropriate users.

Deliver Jabber Configuration File Through Cisco Webex Control Hub

You can run Jabber Team Messaging Mode in IM-Only Mode. This mode doesn't need Cisco Unified Communications Manager and its calling capabilities.

To replace Unified CM as the deployment site for the Jabber configuration file, you can upload your Jabber configuration file to the Control Hub. You can upload one configuration file for each organization. The file must be in .xml format. You can delete the configuration file in the Control Hub if necessary.

If your deployment includes a Unified CM server and a configuration file is detected there, the Unified CM configuration file takes precedence.

Procedure

Step 1  In Cisco Webex Control Hub, select Services.
Step 2  Select the Message card and choose Settings.
Step 3  Select Upload Configuration File and choose your Jabber configuration file.
PART II

Configure Cisco Unified Communications Manager

• Configure the Clients, on page 13
• Create Users on Unified Communications Manager, on page 25
• Configure Service Discovery for Remote Access, on page 31
• Configure Deskphone Control, on page 33
• Configure Softphone, on page 41
• Configure Extend and Connect, on page 51
CHAPTER 3

Configure the Clients

- Client Configuration Workflow, on page 13

Client Configuration Workflow

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Introduction to Client Configuration</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Set Client Configuration Parameters in Unified CM (highest priority) or Create and Host the Client Configuration Files</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Set Parameters on Phone Configuration for Desktop Clients</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Set Parameters on Phone Configuration for Mobile Clients</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure Proxy Setting—Optional</td>
<td></td>
</tr>
</tbody>
</table>

Introduction to Client Configuration

Cisco Jabber can retrieve configuration settings from the following sources:

- Client Configuration—You can set client configuration parameters that are applied when users sign in, by either:
  - Set the client configuration parameters with Unified CM.
  - Create XML files using an XML editor that contain configuration parameters. You then host the XML files on a TFTP server.
Set Client Configuration Parameters in Unified CM

Set client configuration parameters and assign to service profiles in Unified CM.

For Cisco Jabber for iPhone and iPad and Cisco Jabber for Android, you must set the parameters for:

• 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. Set client configuration parameters only if you require custom content such as automatic updates, problem reporting, or user policies and options.

Procedure

Step 1 Define Jabber Configuration Parameters, on page 14
Step 2 Assign Jabber Client Configuration to Service Profile, on page 14

Define Jabber Configuration Parameters

Unified CM allows you to add, search, display, and maintain information about UC Services including Jabber client configuration.

Procedure

Step 1 Open the Cisco Unified CM Administration interface.
Step 2 Select User Management > User Settings > UC Service.
Step 3 Select Add New.
Step 4 Select Jabber Client Configuration (jabber-config.xml) as the UC Service Type.
Step 5 Select Next.
Step 6 Enter a name in the UC Service Information section, refer to Unified CM Help for more requirements.
Step 7 Enter the parameters in the Jabber Configuration Parameters section, for information regarding the parameters see the latest version of the Parameters Reference Guide for Cisco Jabber.
Step 8 Select Save.

Assign Jabber Client Configuration to Service Profile

Unified CM allows you to assign Jabber client configuration to users through service profiles.
Procedure

Step 1 Open the Cisco Unified CM Administration interface.
Step 2 Select User Management > User Settings > Service Profile.
Step 3 Select Add New or select the existing service profile you want to assign the Jabber client configuration to.
Step 4 Select the name of the configuration you want to apply to the profile in the section Jabber Client Configuration (jabber-config.xml) Profile.
Step 5 Select Save.

Create and Host the Client Configuration Files

Create client configuration files and host them on the Cisco Unified Communications Manager TFTP service.

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.

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 that the client can retrieve the file from the TFTP server.
- 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 correct nesting of elements.
- Use only valid XML character entity references in your configuration file. For example, use &amp; 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 is valid.
- If Internet Explorer displays only part of the XML structure, your configuration file likely contains invalid characters or entities.
### Specify Your TFTP Server Address

The client gets configuration files from a TFTP server.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Specify Your TFTP Server Address, on page 16</td>
<td>Specify your TFTP server address so the client can access your configuration file.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Create Global Configurations, on page 17</td>
<td>Configure the clients for users in your deployment.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Create Group Configurations, on page 17</td>
<td>Apply different configuration to different set of users.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Host Configuration Files, on page 18</td>
<td>Host configuration files on any TFTP server.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Restart Your TFTP Server, on page 18</td>
<td>Restart the TFTP server before the client can access the configuration files.</td>
</tr>
</tbody>
</table>

#### 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.

#### 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.
Create Global Configurations

The client downloads the global configuration file from your TFTP server during the sign in 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 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.
   a) Open the Cisco Unified CM Administration interface.
   b) Select Device > Phone.
c) Find and select the appropriate CSF device to which the group configuration applies.

d) In the **Phone Configuration** window, navigate to **Product Specific Configuration Layout > Desktop Client Settings**.

e) 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.

f) 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, we recommend hosting configuration files on the Cisco Unified Communications Manager TFTP server, which is where the device configuration file resides.

**Procedure**

1. **Step 1** Open the **Cisco Unified OS Administration** interface on Cisco Unified Communications Manager.
2. **Step 2** Select **Software Upgrades > TFTP File Management**.
3. **Step 3** Select **Upload File**.
4. **Step 4** Select **Browse** in the **Upload File** section.
5. **Step 5** Select the configuration file on the file system.
6. **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.

7. **Step 7** Select **Upload File**.

---

### Restart Your TFTP Server

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

**Procedure**

1. **Step 1** Open the **Cisco Unified Serviceability** interface on Cisco Unified Communications Manager.
2. **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
For detailed information on the jabber-config.xml configuration file structure, group elements, parameters, and examples, see the Parameters Reference Guide for Cisco Jabber.

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 desktop 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**

<table>
<thead>
<tr>
<th>Video Calling</th>
<th>Enables or disables video capabilities.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabled (default)</strong></td>
<td>Users can send and receive video calls.</td>
</tr>
<tr>
<td><strong>Disabled</strong></td>
<td>Users cannot send or receive video calls.</td>
</tr>
<tr>
<td><strong>Restriction</strong></td>
<td>This parameter is available only on the CSF device configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>File Types to Block in File Transfer</th>
<th>Restricts users from transferring specific file types.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set a file extension as the value, for example, .exe.</td>
</tr>
<tr>
<td></td>
<td>Use a semicolon to delimit multiple values, for example,</td>
</tr>
<tr>
<td></td>
<td>.exe;.msi;.rar;.zip</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Automatically Start in Phone Control</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabled</strong></td>
<td>Use the desk phone device for calls.</td>
</tr>
<tr>
<td><strong>Disabled (default)</strong></td>
<td>Use the software phone (CSF) device for calls.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Jabber For Windows Software Update Server URL</th>
<th>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.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Problem Report Server URL</th>
<th>Specifies the URL for the custom script that allows users to submit problem reports.</th>
</tr>
</thead>
</table>

---

**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:
### Optional Configuration of Proxy Settings

Your client might use proxy settings to connect to services.

The following limitations apply when using a proxy for these HTTP requests:

- The bypass list supports wildcards.
- Cisco Jabber supports proxy for HTTP request using HTTP CONNECT, but does not support proxy when using HTTPS CONNECT.
- Jabber doesn't support Web Proxy Auto Discovery (WPAD). You must disable WPAD.

If necessary, configure the proxy settings by following the steps for your client type.

### Proxy Authentication Support

As of Release 12.7, Jabber team messaging mode supports proxy authentication. Depending on your platform, you can use the following proxy authentication types:

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Authenticates By…</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>In Domain</td>
</tr>
<tr>
<td>No Auth¹</td>
<td>Autocompletion</td>
</tr>
<tr>
<td>Basic</td>
<td>User dialog</td>
</tr>
<tr>
<td>NTLM</td>
<td>Autocompletion</td>
</tr>
</tbody>
</table>

---

## Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Demand VPN URL</td>
<td>URL for initiating on-demand VPN.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Applicable for iOS only.</td>
</tr>
<tr>
<td>Preset Wi-fi Networks</td>
<td>Enter the SSIDs for Wi-Fi networks (SSIDs) approved by your organization.</td>
</tr>
<tr>
<td></td>
<td>Separate SSIDs with a forward slash (/). Devices do not connect to secure</td>
</tr>
<tr>
<td></td>
<td>connect if connected to one of the entered Wi-Fi networks.</td>
</tr>
<tr>
<td>Default Ringtone</td>
<td>Sets the default ringtone to <strong>Normal</strong> or <strong>Loud</strong>.</td>
</tr>
<tr>
<td>Video Capabilities</td>
<td>Enables or disables video capabilities.</td>
</tr>
<tr>
<td></td>
<td>• Enabled (default) — Users can send and receive video calls.</td>
</tr>
<tr>
<td></td>
<td>• Disabled — Users cannot send or receive video calls.</td>
</tr>
<tr>
<td>Dial via Office</td>
<td>Enables or disables Dial via Office.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>TCT and BOT devices only.</td>
</tr>
<tr>
<td></td>
<td>• Enabled — Users can dial via office.</td>
</tr>
<tr>
<td></td>
<td>• Disabled (default) — Users cannot dial via office.</td>
</tr>
</tbody>
</table>
The available authentication types vary by client, as outlined in this table:

<table>
<thead>
<tr>
<th>Client</th>
<th>Authentication Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No Auth</td>
</tr>
<tr>
<td>Cisco Jabber for Windows</td>
<td>Y</td>
</tr>
<tr>
<td>Cisco Jabber Softphone for VDI</td>
<td>Y</td>
</tr>
<tr>
<td>Cisco Jabber for Mac</td>
<td>Y</td>
</tr>
<tr>
<td>Cisco Jabber for iPhone and iPad</td>
<td>Y</td>
</tr>
<tr>
<td>Cisco Jabber for Android</td>
<td>Y</td>
</tr>
</tbody>
</table>


**Proxy Authentication and Certificates**

If you deploy a TLS-inspecting proxy, install a CA certificate into the OS of the device with a trust chain that allows a successful certificate validation.

Jabber validates the certificates of the systems with which it communicates. Jabber validates the certificates for a TLS session against the list of trusted root certificate authorities in the other system's OS. Jabber also checks the certificates against known malicious or compromised certificate authorities.

**Configure Proxy Settings for Cisco Jabber for Windows**

Configure proxy settings for Windows in the Local Area Network (LAN) settings for Internet properties.

**Procedure**

**Step 1** In the **Connections** tab select **LAN Settings**.

**Step 2** Configure a proxy using one of the following options:
Configure Proxy Settings for Cisco Jabber for Mac
Configure proxy settings for Mac in System Preferences.

Procedure

Step 1 Select System Preferences > Network
Step 2 Choose your network service from the list and select Advanced > Proxies.
Step 3 Configure a proxy using one of the following options:
   • For automatic configuration, specify a .pac file URL.
   • For Proxy Server, specify an explicit proxy address.

Configure Proxy Settings for Cisco Jabber iPhone and iPad
Configure proxy settings in the Wi-Fi settings of an iOS device using one of the following methods:

Procedure

Step 1 Select Wi-Fi > HTTP PROXY > Auto and specify a .pac file URL as the automatic configuration script.
Step 2 Select Wi-Fi > HTTP PROXY > Manual and specify an explicit proxy address.

Configure Proxy Settings for Cisco Jabber for Android
Configure proxy settings in the Wi-Fi settings of an Android device using one of the following methods:

Procedure

   • Specify a .pac file URL as the automatic configuration script in the Wi-Fi > Modify Network > Show Advanced Options > Proxy Settings > Auto tab.
   
   Note This method is only supported on devices with Android OS 5.0 and later, and Cisco DX series devices.

   • Specify an explicit proxy address in the Wi-Fi Networks > Modify Network > Show Advanced Options > Proxy Settings > Auto tab.
CHAPTER 4

Create Users on Unified Communications Manager

- Enable Synchronization, on page 25
- Specify an LDAP Attribute for the User ID, on page 26
- Specify an LDAP Attribute for the Directory URI, on page 26
- Perform Synchronization, on page 27
- Assign Roles and Groups, on page 27
- Authentication Options, on page 28

Enable Synchronization

To ensure that contact data in your directory server is replicated to Cisco Unified Communications Manager, you must synchronize with the directory server. Before you can synchronize with the directory server, you must enable synchronization.

Procedure

Step 1 Open the Cisco Unified CM Administration interface.
Step 2 Select System > LDAP > LDAP System.
   The LDAP System Configuration window opens.
Step 3 Locate the LDAP System Information section.
Step 4 Select Enable Synchronizing from LDAP Server.
Step 5 Select the type of directory server from which you are synchronizing data from the LDAP Server Type drop-down list.

What to do next

Specify an LDAP attribute for the user ID.
Specify an LDAP Attribute for the User ID

When you synchronize from your directory source to Cisco Unified Communications Manager, you can populate the user ID from an attribute in the directory. The default attribute that holds the user ID is sAMAccountName.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Locate the <strong>LDAP Attribute for User ID</strong> drop-down list on the <strong>LDAP System Configuration</strong> window.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Specify an attribute for the user ID as appropriate and then select <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

**Important** If the attribute for the user ID is other than **sAMAccountName** and you are using the default IM address scheme in Cisco Unified Communications Manager IM and Presence Service, you must specify the attribute as the value for the parameter in your client configuration file as follows:

- The **CDI parameter** is **UserAccountName**.

  `<UserAccountName>attribute-name</UserAccountName>`

If you do not specify the attribute in your configuration, and the attribute is other than **sAMAccountName**, the client cannot resolve contacts in your directory. As a result, users do not get presence and cannot send or receive instant messages.

Specify an LDAP Attribute for the Directory URI

On Cisco Unified Communications Manager release 9.0(1) and later, you can populate the directory URI from an attribute in the directory.

**Before you begin**

Enable Synchronization.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select <strong>System &gt; LDAP &gt; LDAP Directory</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the appropriate LDAP directory or select <strong>Add New</strong> to add an LDAP directory.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Locate the <strong>Standard User Fields To Be Synchronized</strong> section.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select one of the following LDAP attributes from the <strong>Directory URI</strong> drop-down list:</td>
</tr>
</tbody>
</table>

- **msRTCSIP-primaryuseraddress**—This attribute is populated in the AD when Microsoft Lync or Microsoft OCS are used. This is the default attribute.
- **mail**
Perform Synchronization

After you add a directory server and specify the required parameters, you can synchronize Cisco Unified Communications Manager with the directory server.

Procedure

2. Select Add New.
   The LDAP Directory window opens.
   See the Cisco Unified Communications Manager Administration Guide for more information about the values and formats you can specify.
4. Create an LDAP Directory Synchronization Schedule to ensure that your information is synchronized regularly.
5. Select Save.
6. Select Perform Full Sync Now.

Note: The amount of time it takes for the synchronization process to complete depends on the number of users that exist in your directory. If you synchronize a large directory with thousands of users, you should expect the process to take some time.

User data from your directory server is synchronized to the Cisco Unified Communications Manager database. Cisco Unified Communications Manager then synchronizes the user data to the presence server database.

Assign Roles and Groups

For all deployment types assign users to the Standard CCM End Users group.

Procedure

1. Open the Cisco Unified CM Administration interface.
2. Select User Management > End User
   The Find and List Users window opens.
3. Find and select the user from the list.
   The End User Configuration window opens.
4. Locate the Permission Information section.
5. Select Add to Access Control Group.
The **Find and List Access Control Groups** dialog box opens.

**Step 6**
Select the access control groups for the user.

At a minimum you should assign the user to the following access control groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**—This option is used for desk phone control.

If you provision users with secure phone capabilities, do not assign the users to the **Standard CTI Secure Connection** group.

Certain phone models require additional control groups, as follows:

- Cisco Unified IP Phone 9900, 8900, or 8800 series or DX series, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**.
- Cisco Unified IP Phone 6900 series, select **Standard CTI Allow Control of Phones supporting Rollover Mode**.

**Step 7**
Select **Add Selected**.

The **Find and List Access Control Groups** window closes.

**Step 8**
Select **Save** on the **End User Configuration** window.

---

### Authentication Options

**Enable SAML SSO in the Client**

**Before you begin**

- Enable SSO on Cisco Unified Communications Applications 10.5.1 Service Update 1—For information about enabling SAML SSO on this service, read the *SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 10.5*.

- Enable SSO on Cisco Unity Connection version 10.5—For more information about enabling SAML SSO on this service, read *Managing SAML SSO in Cisco Unity Connection*.

**Procedure**

**Step 1**
Deploy certificates on all servers so that the certificate can be validated by a web browser, otherwise users receive warning messages about invalid certificates. For more information about certificate validation, see *Certificate Validation*.

**Step 2**
Ensure Service Discovery of SAML SSO in the client. The client uses standard service discovery to enable SAML SSO in the client. Enable service discovery by using the following configuration parameters: ServicesDomain, VoiceServicesDomain, and ServiceDiscoveryExcludedServices. For more information about how to enable service discovery, see *Configure Service Discovery for Remote Access*.

**Step 3**
Define how long a session lasts.
A session is comprised of cookie and token values. A cookie usually lasts longer than a token. The life of the cookie is defined in the Identity Provider, and the duration of the token is defined in the service.

Step 4
When SSO is enabled, all Cisco Jabber users sign in using SSO by default. Administrators can change this on a user-by-user basis so that certain users do not use SSO and instead sign in with their Cisco Jabber username and password. To disable SSO for a Cisco Jabber user, set the value of the SSO Enabled parameter to FALSE.

If you have configured Cisco Jabber not to ask users for their email address, their first sign in to Cisco Jabber may be non-SSO. In some deployments, the parameter ServicesDomainSsoEmailPrompt needs to be set to ON. This ensures that Cisco Jabber has the information required to perform a first-time SSO sign in. If users signed in to Cisco Jabber previously, this prompt is not needed because the required information is available.

For Webex Control Hub configuration, see *Single Sign-On Integration With Webex Control Hub*.

### Authenticate with the LDAP Server

Perform this procedure if you want to enable LDAP authentication so that end user passwords are authenticated against the password that is assigned in the company LDAP directory. LDAP authentication gives system administrators the ability to assign an end user a single password for all company applications. This configuration applies to end user passwords only and does not apply to end user PINs or application user passwords. When users sign in to the client, the presence service routes that authentication to Cisco Unified Communications Manager. Cisco Unified Communications Manager then sends that authentication to the directory server.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Open the Cisco Unified CM Administration interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select System &gt; LDAP &gt; LDAP Authentication.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Use LDAP Authentication for End Users.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Specify LDAP credentials and a user search base as appropriate.</td>
</tr>
</tbody>
</table>

See the *Cisco Unified Communications Manager Administration Guide* for information about the fields on the LDAP Authentication window.

| Step 5 | Select Save.                                      |

---
Authenticate with the LDAP Server
Configure Service Discovery for Remote Access

- Service Discovery Requirements, on page 31

Service Discovery Requirements

Service discovery enables clients to automatically detect and locate services on your enterprise network. Expressway for Mobile and Remote Access allows you to access the services on your enterprise network. You should meet the following requirements to enable the clients to connect through Expressway for Mobile and Remote Access and discover services:

- DNS requirements
- Certificate requirements
- Test external SRV _collab-edge.

DNS Requirements

The DNS requirements for service discovery through remote access are:

- Configure a _collab-edge DNS SRV record on an external DNS server.
- Configure a _cisco-uds DNS SRV record on the internal name server.
- Optionally, for a hybrid cloud-based deployment with different domains for the IM and Presence server and the voice server, configure the Voice Services Domain to locate the DNS server with the _collab-edge record.

Note

Jabber attempts connections to a maximum of three SSO-enabled servers, which are chosen randomly from all SSO-enabled servers that the DNS SRV records (_collab-edge and _cisco-uds) identify. If Jabber fails to connect three times, it considers Edge SSO unsupported.
Certificate Requirements

Before you configure remote access, download the Cisco VCS Expressway and Cisco Expressway-E Server certificate. The Server certificate is used for both HTTP and XMPP.

For more information on configuring Cisco VCS Expressway certificate, see Configuring Certificates on Cisco VCS Expressway.

Test _collab-edge SRV Record

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Open a command prompt.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter <code>nslookup</code>. The default DNS server and address is displayed. Confirm that this is the expected DNS server.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter <code>set type=SRV</code>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the name for each of your SRV records.</td>
</tr>
</tbody>
</table>

For example `_collab-edge.exampledomain`

- Displays server and address—SRV record is accessible.
- Displays `_collab-edge.exampledomain`: Non-existent domain—There is an issue with your SRV record.
# Configure Deskphone Control

- Prerequisites, on page 33
- Configure Deskphone Control Taskflow, on page 33
- Enable Device for CTI, on page 34
- Configure Desk Phone Video, on page 34
- Enable Video Rate Adaptation, on page 35
- Configure User Associations, on page 37
- Reset Devices, on page 38

## Prerequisites

The Cisco CTI Manager service must be running in the Cisco Unified Communications Manager cluster.

## Configure Deskphone Control Taskflow

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enable Device for CTI, on page 34</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Configure Desk Phone Video, on page 34.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enable Video Rate Adaptation, on page 35</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configure User Associations, on page 37</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Reset Devices, on page 38</td>
</tr>
</tbody>
</table>
Enable Device for CTI

If you want Cisco Jabber desktop clients to be able to control the desk phone of the user, you must select the Allow Control of Device from CTI option when you create the device for the user.

**Procedure**

**Step 1**
In Cisco Unified CM Administration, click Device > Phone and search for the phone.

**Step 2**
In the Device Information section, check Allow Control of Device from CTI.

**Step 3**
Click Save.

Configure Desk Phone Video

Desk phone video capabilities let you receive the video signal on your laptop and the audio signal on your desk phone. Physically connect your computer to the desk phone through the computer port for the client to establish a connection to the Jabber client. You cannot use this feature with a wireless connection to your desk phone.

**Note**
If you have both wireless and wired connections available, configure Microsoft Windows to not prioritize wireless connections over wired connections. See Microsoft's *An explanation of the Automatic Metric feature for Internet Protocol routes* for more information.

First, download and install Jabber Desk Phone Video Services Interface from Cisco.com. Jabber Desk Phone Video Services Interface provides the Cisco Discover Protocol (CDP) driver. CDP enables the client to:

- Discover the desk phone.
- Establish and maintain a connection to the desk phone using the Cisco Audio Session Tunnel (CAST) protocol.

**Desk Phone Video Considerations**

Review the following considerations and limitations before you set up the desk phone video feature:

- You cannot have more than one video device connected with CAST. You cannot use a desk phone with a built-in camera with this feature. If your desk phone has a local USB camera, remove it before using this feature.
- You cannot use this feature with devices that do not support CTI.
- You cannot use both video screen sharing, using the BFCP protocol, and desk phone video.
- It is not possible for endpoints that use SCCP to receive video only. SCCP endpoints must send and receive video. Instances where SCCP endpoints do not send a video signal result in audio only calls.
• 7900 series phones must use SCCP for desk phone video capabilities. 7900 series phones cannot use SIP for desk phone video capabilities.

• If you start a call from a desk phone's keypad, the call starts as an audio call on the desk phone. Jabber then escalates the call to video. For this reason, you cannot make video calls to devices that do not support the escalation, such as H.323 endpoints. To use this feature with devices that do not support escalation, begin calls from the Jabber client.

• A compatibility issue exists with Cisco Unified IP Phones that use firmware version SCCP45.9-2-1S. Upgrade your firmware to version SCCP45.9-3-1 to use this feature.

• Some antivirus or firewall applications, such as Symantec EndPoint Protection, block inbound CDP packets. This blockage disables desk phone video. Configure your antivirus or firewall application to allow inbound CDP packets.

See the following Symantec technical document for more details about this issue: *Cisco IP Phone version 7970 and Cisco Unified Video Advantage is Blocked by Network Threat Protection.*

• Do not select the **Media Termination Point Required** check box on the SIP trunk configuration for Cisco Unified Communications Manager (Unified CM). That setting disables desk phone video.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Physically connect your computer to the computer port on your desk phone.</td>
</tr>
<tr>
<td>2</td>
<td>Enable the desk phone for video in Unified CM.</td>
</tr>
<tr>
<td>3</td>
<td>Install Jabber Desk Phone Video Services Interface on your computer.</td>
</tr>
</tbody>
</table>

### Troubleshooting Desk Phone Video

If you encounter an error that indicates desk phone video capabilities are unavailable or the desk phone device is unknown, do the following:

1. Ensure you enable the desk phone device for video in Cisco Unified Communications Manager.
2. Reset the physical desk phone.
3. Exit the client.
4. Run services.msc on the computer where you installed the client.
5. Restart Jabber Desk Phone Video Services Interface from the Services tab of the Windows Task Manager.
6. Restart the client.

### Enable Video Rate Adaptation

The client uses video rate adaptation to negotiate optimum video quality. Video rate adaptation dynamically increases or decreases video quality based on network conditions.
To use video rate adaptation, you must enable Real-Time Transport Control Protocol (RTCP) on Cisco Unified Communications Manager.

**Note**
RTCP is enabled on software phone devices by default. However, you must enable RTCP on desk phone devices.

### Enable RTCP on Common Phone Profiles

You can enable RTCP on a common phone profile to enable video rate adaptation on all devices that use the profile.

**Note**
RTCP is an integral component of Jabber Telephony services. Jabber will continue to send RTCP packets even when disabled.

**Procedure**

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

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

**Step 3**
Specify the appropriate filters in the **Find Common Phone Profile where** field and then select **Find** to retrieve a list of profiles.

**Step 4**
Select the appropriate profile from the list.

The **Common Phone Profile Configuration** window opens.

**Step 5**
Locate the **Product Specific Configuration Layout** section.

**Step 6**
Select **Enabled** from the RTCP drop-down list.

**Step 7**
Select **Save**.

### Enable RTCP on Device Configurations

You can enable RTCP on specific device configurations instead of a common phone profile. The specific device configuration overrides any settings you specify on the common phone profile.

**Procedure**

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

**Step 2**
Select **Device > Phone**.

The **Find and List Phones** window opens.
Configure User Associations

Configure User Associations

When you associate a user with a device, you provision that device to the user.

Before you begin

Create and configure Cisco Jabber devices.

Procedure

Step 1
Open the Cisco Unified CM Administration interface.

Step 2
Select User Management > End User.

Step 3
Specify the appropriate filters in the Find User where field and then select Find to retrieve a list of users.

Step 4
Select the appropriate user from the list.

Step 5
Locate the Service Settings section.

Step 6
Select the appropriate service profile for the user from the UC Service Profile drop-down list.

Step 7
Locate the Device Information section.

Step 8
Select Device Association.

Step 9
Select the devices to which you want to associate the user. Jabber only supports a single softphone association per device type. For example, only one TCT, BOT, CSF, and TAB device can be associated with a user.

Step 10
Select Save Selected/Changes.

Step 11
Select User Management > End User and return to the Find and List Users window.

Step 12
Find and select the same user from the list.

Step 13
Locate the Permissions Information section.

Step 14
Select Add to Access Control Group.

The Find and List Access Control Groups dialog box opens.
Step 15 Select the access control groups to which you want to assign the user.

At a minimum you should assign the user to the following access control groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**

**Remember** If you are provisioning users with secure phone capabilities, do not assign the users to the **Standard CTI Secure Connection** group.

Certain phone models require additional control groups, as follows:

- Cisco Unified IP Phone 9900, 8900, or 8800 series or DX series, select **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**.
- Cisco Unified IP Phone 6900 series, select **Standard CTI Allow Control of Phones supporting Rollover Mode**.

Step 16 Select **Add Selected**.

The **Find and List Access Control Groups** window closes.

Step 17 Select **Save** on the **End User Configuration** window.

---

**Reset Devices**

After you create and associate users with devices, you should reset those devices.

**Procedure**

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

Step 2 Select **Device > Phone**.

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

Step 3 Specify the appropriate filters in the **Find Phone where** field and then select **Find** to retrieve a list of devices.

Step 4 Select the appropriate device from the list.

The **Phone Configuration** window opens.

Step 5 Locate the **Association Information** section.

Step 6 Select the appropriate directory number configuration.

The **Directory Number Configuration** window opens.

Step 7 Select **Reset**.

The **Device Reset** dialog box opens.

Step 8 Select **Reset**.
Step 9  Select Close to close the Device Reset dialog box.
Configure Cisco Unified Communications Manager

Reset Devices
CHAPTER 7

Configure Softphone

• Create Softphones Workflow, on page 41

Create Softphones Workflow

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Create and Configure Cisco Jabber Devices, on page 41</td>
<td>Create at least one device for every user who accesses Cisco Jabber. Generate an authentication string to provide to users.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Add a Directory Number to the Device, on page 45</td>
<td>For each device you create, add a directory number.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Associate Users with Devices, on page 45</td>
<td>Associate users with devices.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Create Mobile SIP Profiles, on page 46.</td>
<td>Complete this task if you have Cisco Unified Communications Manager release 9 and plan to configure devices for mobile clients.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Configure the Phone Security Profile, on page 47</td>
<td>Complete this task to set up secure phone capabilities for all devices.</td>
</tr>
</tbody>
</table>

Create and Configure Cisco Jabber Devices

Create at least one device for every user that accesses Cisco Jabber. A user can have multiple devices.

Note

Users can only remove participants from a conference call when using the softphone (CSF) device for calls.

Before you begin

• Install COP files.
Create SIP profiles if you have Cisco Unified Communications Manager release 9 or earlier and plan to configure devices for mobile clients.

Create the Phone Security Profile if you plan to set up secure phone capabilities for all devices.

If you are using CAPF enrollment, for Cisco Unified Communications Manager release 10 or later, ensure that the Cisco Certificate Authority Proxy Function (CAPF) service parameters value for **Certificate Issuer to Endpoint** is **Cisco Certificate Authority Proxy Function**. This is the only option supported by Cisco Jabber. For information on configuring the CAPF service parameter see the **Update CAPF Service Parameters** topic in the Cisco Unified Communications Manager Security Guides.

Before you create TCT devices, BOT devices, or TAB devices for Cisco Jabber for mobile users, specify the organization top domain name to support registration between Cisco Jabber and the Cisco Unified Communications Manager. In Unified CM Administration interface, select **System > Enterprise Parameters**. Under the Clusterwide Domain Configuration section, enter the organization top domain name. For example, cisco.com. This top domain name is used by Jabber as the DNS domain of the Cisco Unified Communications Manager servers for phone registration. For example, CUCMServer1@cisco.com.

**Procedure**

**Step 1** Log in to the Cisco Unified CM Administration interface.

**Step 2** Select **Device > Phone**.

**Step 3** Select **Add New**.

**Step 4** From the **Phone Type** drop-down list, select the option that is applicable to the device type you are configuring and then select **Next**.

For Jabber users, you can only create one type of device per user although you can create multiple devices for each user. For example, you can create one tablet device and one CSF device but not two CSF devices.

- **Cisco Unified Client Services Framework**—Select this option to create a CSF device for Cisco Jabber for Mac or Cisco Jabber for Windows.
- **Cisco Dual Mode for iPhone**—Select this option to create a TCT device for an iPhone.
- **Cisco Jabber for Tablet**—Select this option to create a TAB device for an iPad or an Android tablet or for Chromebooks.
- **Cisco Dual Mode for Android**—Select this option to create a BOT device for an Android device.

**Step 5** From the **Owner User ID** drop-down list, select the user for whom you want to create the device.

For the **Cisco Unified Client Services Framework** option in a Phone mode deployment, ensure that **User** is selected.

**Step 6** In the **Device Name** field, use the applicable format to specify a name for the device:

<table>
<thead>
<tr>
<th>If You Select</th>
<th>Required Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Client Services Framework</td>
<td>• Valid characters: a–z, A–Z, 0–9.</td>
</tr>
<tr>
<td></td>
<td>• 15-character limit.</td>
</tr>
</tbody>
</table>
### If You Select | Required Format
---|---
**Cisco Dual Mode for iPhone** | • The device name must begin with *TCT*.
  For example, if you create a TCT device for user, Tanya Adams, whose username is tadams, enter *TCTTADAMS*.
  • Must be uppercase.
  • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-).
  • 15-character limit.

**Cisco Jabber for Tablet** | • The device name must begin with *TAB*.
  For example, if you create a TAB device for user, Tanya Adams, whose username is tadams, enter *TABTADAMS*.
  • Must be uppercase.
  • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-).
  • 15-character limit.

**Cisco Dual Mode for Android** | • The device name must begin with *BOT*.
  For example, if you create a BOT device for user, Tanya Adams, whose username is tadams, enter *BOTTADAMS*.
  • Must be uppercase.
  • Valid characters: A–Z, 0–9, period (.), underscore (_), hyphen (-).
  • 15-character limit.

---

**Step 7**

If you are using CAPF enrollment, complete the following steps to generate an authentication string:

1. Users can use the authentication string that you can provide to access their devices and securely register to Cisco Unified Communications Manager, navigate to the **Certification Authority Proxy Function (CAPF) Information** section.

2. From the **Certificate Operation** drop-down list, select **Install/Upgrade**.

3. From the **Authentication Mode** drop-down list, select **By Authentication String** or **By Null String**. Using the CAPF Authentication mode **By Null String** with JVDI and Jabber for Windows CSF devices is not supported. It causes Jabber registration with Cisco Unified Communications Manager to fail.

4. Click **Generate String**. The Authentication String autopopulates with a string value. This is the string that you will provide to end users.

5. From the **Key Size (Bits)** drop-down list, select the same key size that you set in the phone security profile.
6. In the **Operation Completes By** fields, specify an expiration value for the authentication string or leave as default.

7. If you are using a group configuration file, specify it in the **Cisco Support Field** of the Desktop Client Settings. Cisco Jabber does not use any other settings that are available on the Desktop Client Settings.

**Step 8**  
Select **Save**.

**Step 9**  
Click **Apply Config**.

---

**What to do next**

Add a Directory Number to the device.

---

### Provide Users with Authentication Strings

If you are using CAPF enrollment to configure secure phones, then you must provide users with authentication strings. Users must specify the authentication string in the client interface to access their devices and securely register with Cisco Unified Communications Manager.

When users enter the authentication string in the client interface, the CAPF enrollment process begins.

---

**Note**

The time it takes for the enrollment process to complete can vary depending on the user's computer or mobile device and the current load for Cisco Unified Communications Manager. It can take up to one minute for the client to complete the CAPF enrollment process.

The client displays an error if:

- Users enter an incorrect authentication string.

  Users can attempt to enter authentication strings again to complete the CAPF enrollment. However, if a user continually enters an incorrect authentication string, the client might reject any string the user enters, even if the string is correct. In this case, you must generate a new authentication string on the user's device and then provide it to the user.

- Users do not enter the authentication string before the expiration time you set in the **Operation Completes By** field.

  In this case, you must generate a new authentication string on the user's device. The user must then enter that authentication string before the expiration time.

---

**Important**

When you configure the end users in Cisco Unified Communications Manager, you must add them to the following user groups:

- **Standard CCM End Users**
- **Standard CTI Enabled**

Users must not belong to the Standard CTI Secure Connection user group.
Add a Directory Number to the Device

After you create and configure each device, you must add a directory number to the device. This topic provides instructions on adding directory numbers using the **Device > Phone** menu option.

**Before you begin**
Create a device.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Locate the <strong>Association Information</strong> section on the <strong>Phone Configuration</strong> window.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>Add a new DN</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Directory Number</strong> field, specify a directory number.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the <strong>Users Associated with Line</strong> section, click <strong>Associate End Users</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the <strong>Find User where</strong> field, specify the appropriate filters and then click <strong>Find</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>From the list that appears, select the applicable users and click <strong>Add Selected</strong>.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Specify all other required configuration settings as appropriate.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Select <strong>Apply Config</strong>.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Select <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

**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:

```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.

**Before you begin**

**Note**
Do not associate a CSF to multiple users if you intend to use different service profiles for these users.
Procedure

Step 1  Associate users with devices.
     a) Open the Unified CM Administration interface.
     b) 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.

Create Mobile SIP Profiles

This procedure is required only when you use Cisco Unified Communication Manager release 9 and are configuring devices for mobile clients. Use the default SIP profile provided for desktop clients. Before you create and configure devices for mobile clients, you must create a SIP profile that allows Cisco Jabber to stay connected to Cisco Unified Communication Manager while Cisco Jabber runs in the background.

If you use Cisco Unified Communication Manager Release 10, choose the Standard SIP Profile for Mobile Device default profile when you create and configure devices for mobile clients.

Procedure

Step 1  Open the Cisco Unified CM Administration interface.
Step 2  Select Device > Device Settings > SIP Profile.
         The Find and List SIP Profiles window opens.
Step 3  Do one of the following to create a new SIP profile:
         • Find the default SIP profile and create a copy that you can edit.
         • Select Add New and create a new SIP profile.
Step 4  In the new SIP profile, set the following values:
         • Timer Register Delta = 120
         • Timer Register Expires = 720
**Setting up System SIP Parameters**

If you are connected to a low-bandwidth network and finding it difficult to take an incoming call on your mobile device, you can set the system SIP parameters to improve the condition. Increase the SIP Dual Mode Alert Timer value to ensure that calls to the Cisco Jabber extension are not prematurely routed to the mobile-network phone number.

**Before you begin**

This configuration is only for mobile clients.

Cisco Jabber must be running to receive work calls.

**Procedure**

1. **Step 1** Open the Cisco Unified CM Administration interface.
2. **Step 2** Select System > Service Parameters.
3. **Step 3** Select the node.
4. **Step 4** Select the Cisco CallManager (Active) service.
5. **Step 5** Scroll to the Clusterwide Parameters (System - Mobility) section.
6. **Step 6** Increase the SIP Dual Mode Alert Timer value to 10000 milliseconds.
7. **Step 7** Select Save.

**Note** If, after you increase the SIP Dual Mode Alert Timer value, incoming calls that arrive in Cisco Jabber are still terminated and diverted using Mobile Connect, you can increase the SIP Dual Mode Alert Timer value again in increments of 500 milliseconds.

**Configure the Phone Security Profile**

You can optionally set up secure phone capabilities for all devices. Secure phone capabilities provide secure SIP signaling, secure media streams, and encrypted device configuration files.

If you enable secure phone capabilities for users, device connections to Cisco Unified Communications Manager are secure. However, calls with other devices are secure only if both devices have a secure connection.

**Before you begin**

- Configure the Cisco Unified Communications Manager security mode using the Cisco CTL Client. At minimum, select mixed mode security.
For instructions on how to configure mixed mode with the Cisco CTL Client, see the Cisco Unified Communications Manager Security Guide.

- For conference calls, ensure that the conferencing bridge supports secure phone capabilities. If the conferencing bridge does not support secure phone capabilities, calls to that bridge are not secure. Likewise, all parties must support a common encryption algorithm for the client to encrypt media on conference calls.

- If your deployment uses Unified Communications Manager Release 12.5 or later, we recommend using SIP OAuth with Cisco Jabber. For details, see the chapter on SIP OAuth in the Feature Configuration Guide for Cisco Unified Communications Manager at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

**Procedure**

**Step 1** In Cisco Unified Communications Manager, select System > Security > Phone Security Profile.

**Step 2** Select Add New.

**Step 3** From the Phone Type drop-down list, select the option that is applicable to the device type you are configuring and then select Next.

- **Cisco Unified Client Services Framework**—Select this option to create a CSF device for Cisco Jabber for Mac or Cisco Jabber for Windows.
- **Cisco Dual Mode for iPhone**—Select this option to create a TFTP device for an iPhone.
- **Cisco Jabber for Tablet**—Select this option to create a TAB device for an iPad or an Android tablet or for Chromebooks.
- **Cisco Dual Mode for Android**—Select this option to create a BOT device for an Android device.
- **CTI Remote Device**—Select this option to create a CTI remote device.

CTI remote devices are virtual devices that monitor and have call control over a user's remote destination.

**Step 4** In the Name field of the Phone Security Profile Configuration window, specify a name for the phone security profile.

**Step 5** For Device Security Mode, select one of the following options:

- **Authenticated**—The SIP connection is over TLS using NULL-SHA encryption.
- **Encrypted**—The SIP connection is over TLS using AES 128/SHA encryption. The client uses Secure Real-time Transport Protocol (SRTP) to offer encrypted media streams.

**Step 6** For Transport Type, leave the default value of TLS.

**Step 7** Select the TFTP Encrypted Config check box to encrypt the device configuration file that resides on the TFTP server.

**Note** For a TCT/BOT/Tablet device, do not select the TFTP Encrypted Config check box here. For Authentication Mode, select By Authentication String or Null String.

**Step 8** For Authentication Mode, select **By Authentication String** or **By Null String**.

**Note** Using the CAPF Authentication mode **By Null String** with JVDI and Jabber for Windows CSF devices is not supported. It causes Jabber registration with Cisco Unified Communications Manager to fail.
Step 9 For **Key Size (Bits)**, select the appropriate key size for the certificate. Key size refers to the bit length of the public and private keys that the client generates during the CAPF enrollment process.

The Cisco Jabber clients were tested using authentication strings with 1024-bit length keys. The Cisco Jabber clients require more time to generate 2048-bit length keys than 1024-bit length keys. As a result, if you select 2048, expect it to take longer to complete the CAPF enrollment process.

Step 10 For **SIP Phone Port**, leave the default value.

The port that you specify in this field takes effect only if you select **Non Secure** as the value for **Device Security Mode**.

Step 11 Click **Save**.
Configure Cisco Unified Communications Manager

Configure the Phone Security Profile
Configure Extend and Connect

• Configure Extend and Connect Workflow, on page 51
• Enable User Mobility, on page 51
• Create CTI Remote Devices, on page 52
• Add a Remote Destination, on page 53

Configure Extend and Connect Workflow

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Enable User Mobility, on page 51</td>
<td>Enable users mobility and you can assign users as owners of CTI remote devices.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Create CTI Remote Devices, on page 52</td>
<td>Create CTI remote devices, these virtual devices monitor and have call control over a user's remote destination.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Add a Remote Destination, on page 53</td>
<td>(Optional) If you plan to provision users with dedicated CTI remote devices, add a remote destination in Cisco Unified Communications Manager.</td>
</tr>
</tbody>
</table>

Enable User Mobility

This task is only for desktop clients.

You must enable user mobility to provision CTI remote devices. If you do not enable mobility for users, you cannot assign those users as owners of CTI remote devices.

Before you begin

This task is applicable only if:

• You plan to assign Cisco Jabber for Mac or Cisco Jabber for Windows users to CTI remote devices.
• You have Cisco Unified Communication Manager release 9.x and later.

Procedure

**Step 1** Select User Management > End User.  
The Find and List Users window opens.

**Step 2** Specify the appropriate filters in the Find User where field to and then select Find to retrieve a list of users.

**Step 3** Select the user from the list.  
The End User Configuration window opens.

**Step 4** Locate the Mobility Information section.

**Step 5** Select Enable Mobility.

**Step 6** Select Save.

---

**Create CTI Remote Devices**

CTI remote devices are virtual devices that monitor and have call control over a user's remote destination.

Procedure

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

**Step 2** Select Device > Phone.  
The Find and List Phones window opens.

**Step 3** Select Add New.

**Step 4** Select CTI Remote Device from the Phone Type drop-down list and then select Next.  
The Phone Configuration window opens.

**Step 5** Select the appropriate user ID from the Owner User ID drop-down list.

*Note* Only users for whom you enable mobility are available from the Owner User ID drop-down list.  
For more information, see Enable SAML SSO in the Client.

Cisco Unified Communications Manager populates the Device Name field with the user ID and a CTIRD prefix; for example, CTIRDusername

**Step 6** Edit the default value in the Device Name field, if appropriate.

**Step 7** Ensure you select an appropriate option from the Rerouting Calling Search Space drop-down list in the Protocol Specific Information section.

The Rerouting Calling Search Space drop-down list defines the calling search space for re-routing and ensures that users can send and receive calls from the CTI remote device.
Step 8 Specify all other configuration settings on the Phone Configuration window as appropriate.

See the CTI remote device setup topic in the System Configuration Guide for Cisco Unified Communications Manager documentation for more information.

Step 9 Select Save.

The fields to associate directory numbers and add remote destinations become available on the Phone Configuration window.

Add a Remote Destination

Remote destinations represent the CTI controllable devices that are available to users.

You should add a remote destination through the Cisco Unified CM Administration interface if you plan to provision users with dedicated CTI remote devices. This task ensures that users can automatically control their phones and place calls when they start the client.

If you plan to provision users with CTI remote devices along with software phone devices and desk phone devices, you should not add a remote destination through the Cisco Unified CM Administration interface. Users can enter remote destinations through the client interface.

Note

- You should create only one remote destination per user. Do not add two or more remote destinations for a user.
- Cisco Unified Communications Manager does not verify if it can route remote destinations that you add through the Cisco Unified CM Administration interface. For this reason, you must ensure that Cisco Unified Communications Manager can route the remote destinations you add.
- Cisco Unified Communications Manager automatically applies application dial rules to all remote destination numbers for CTI remote devices.

Procedure

Step 1 Open the Cisco Unified CM Administration interface.
Step 2 Select Device > Phone.

The Find and List Phones window opens.
Step 3 Specify the appropriate filters in the Find Phone where field to and then select Find to retrieve a list of phones.
Step 4 Select the CTI remote device from the list.

The Phone Configuration window opens.
Step 5 Locate the Associated Remote Destinations section.
Step 6 Select Add a New Remote Destination.
The **Remote Destination Information** window opens.

**Step 7**
Specify JabberRD in the **Name** field.

**Restriction** You must specify JabberRD in the **Name** field. The client uses only the JabberRD remote destination. If you specify a name other than JabberRD, users cannot access that remote destination.

The client automatically sets the JabberRD name when users add remote destinations through the client interface.

**Step 8**
Enter the destination number in the **Destination Number** field.

**Step 9**
Specify all other values as appropriate.

**Step 10**
Select **Save**.

---

**What to do next**
Complete the following steps to verify the remote destination and apply the configuration to the CTI remote device:

1. Repeat the steps to open the **Phone Configuration** window for the CTI remote device.
2. Locate the **Associated Remote Destinations** section.
3. Verify the remote destination is available.
4. Select **Apply Config**.

---

**Note**
The **Device Information** section on the **Phone Configuration** window contains a **Active Remote Destination** field.

When users select a remote destination in the client, it displays as the value of **Active Remote Destination**. **none** displays as the value of **Active Remote Destination** if:

- Users do not select a remote destination in the client.
- Users exit or are not signed in to the client.
PART III

Deploy Jabber

• Deploy Cisco Jabber Applications and Jabber Softphone for VDI, on page 57
Deploy Cisco Jabber Applications and Jabber Softphone for VDI

- Download the Cisco Jabber Clients, on page 57
- Install Cisco Jabber for Windows, on page 57
- Install Cisco Jabber for Mac, on page 82
- Install Cisco Jabber Mobile Clients, on page 87
- Install Jabber Softphone for VDI, on page 92

Download the Cisco Jabber Clients

If required, you can add your own Customer signature to the Jabber Installer or Cisco Dynamic Libraries by using the signing tools from the Operating System for that client.

Note

For Cisco Jabber for Mac, the installer includes the product installer file. Use the Terminal tool to extract the pkg file from the installer and sign the pkg file before adding to the installer.

Procedure

Download the client from the applicable source.

- Visit the Cisco Software Center to download the Cisco Jabber for Mac and Cisco Jabber for Windows clients.
- For Cisco Jabber for Android, download the app from Google Play.
- For Cisco Jabber for iPhone and iPad, download the app from the App store.

Install Cisco Jabber for Windows

Cisco Jabber for Windows provides an MSI installation package that you can use in the following ways:
Use the Command Line

Specify installation arguments in a command line window.

Procedure

**Step 1**
Open a command line window.

**Step 2**
Enter the following command:

```
msiexec.exe /i CiscoJabberSetup.msi
```

**Step 3**
Specify command line arguments as parameter=value pairs.

```
msiexec.exe /i CiscoJabberSetup.msi argument=value
```

**Step 4**
Run the command to install Cisco Jabber for Windows.

Example Installation Commands

Review examples of commands to install Cisco Jabber for Windows.
Cisco Unified Communications Manager, Release 9.x

msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1

Where:

CLEAR=1 — Deletes any existing bootstrap file.
/quiet — Specifies a silent installation.

Related Topics

Command Line Arguments, on page 59
LCID for Languages, on page 72

Command Line Arguments

Review the command line arguments you can specify when you install Cisco Jabber for Windows.

Related Topics

Example Installation Commands, on page 58
LCID for Languages, on page 72

Override Argument

The following table describes the parameter you must specify to override any existing bootstrap files from previous installations:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLEAR</td>
<td>1</td>
<td>Specifies if the client overrides any existing bootstrap file from previous installations. The client saves the arguments and values you set during installation to a bootstrap file. The client then loads settings from the bootstrap file at startup.</td>
</tr>
</tbody>
</table>

If you specify CLEAR, the following occurs during installation:

1. The client deletes any existing bootstrap file.
2. The client creates a new bootstrap file.

If you do not specify CLEAR, the client checks for existing bootstrap files during installation.

- If no bootstrap file exists, the client creates a bootstrap file during installation.
- If a bootstrap file exists, the client does not override that bootstrap file and preserves the existing settings.

Note

If you are reinstalling Cisco Jabber for Windows, you should consider the following:

- The client does not preserve settings from existing bootstrap files. If you specify CLEAR, you must also specify all other installation arguments as appropriate.
- The client does not save your installation arguments to an existing bootstrap file. If you want to change the values for installation arguments, or specify additional installation arguments, you must specify CLEAR to override the existing settings.
To override existing bootstrap files, specify CLEAR in the command line as follows:

```
msiexec.exe /i CiscoJabberSetup.msi CLEAR=1
```

### Mode Type Argument

The following table describes the command line argument with which you specify the product mode:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRODUCT_MODE</td>
<td>Phone_Mode</td>
<td>Specifies the product mode for the client. You can set the following value:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Phone_Mode — Cisco Unified Communications Manager is the authenticator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Choose this value to provision users with audio devices as base functionality.</td>
</tr>
</tbody>
</table>

### When to Set the Product Mode

In phone mode deployments Cisco Unified Communications Manager is the authenticator. When the client gets the authenticator, it determines the product mode is phone mode. However, because the client always starts in the default product mode on the initial launch, users must restart the client to enter phone mode after sign in.

---

**Note**

Cisco Unified Communications Manager, Release 9.x and Later — You should not set PRODUCT_MODE during installation. The client gets the authenticator from the service profile. After the user signs in, the client requires a restart to enter phone mode.

### Change Product Modes

To change the product mode, you must change the authenticator for the client. The client can then determine the product mode from the authenticator.

The method for changing from one product mode to another after installation, depends on your deployment.

---

**Note**

In all deployments, the user can manually set the authenticator in the Advanced settings window.

In this case, you must instruct the user to change the authenticator in the Advanced settings window to change the product mode. You cannot override the manual settings, even if you uninstall and then reinstall the client.

### Change Product Modes with Cisco Unified Communications Manager Version 9.x and Later

To change product modes with Cisco Unified Communications Manager version 9.x and later, you change the authenticator in the service profile.

### Procedure

**Step 1**

Change the authenticator in the service profiles for the appropriate users.
Change Default Mode > Phone Mode
Do not provision users with an IM and Presence service.
If the service profile does not contain an IM and presence service configuration, the authenticator is Cisco Unified Communications Manager.

Change Phone Mode > Default Mode
Provision users with an IM and Presence service.
If you set the value of the Product type field in the IM and Presence profile to:

- Unified CM (IM and Presence) the authenticator is Cisco Unified Communications Manager IM and Presence Service.
- Webex (IM and Presence) the authenticator is the Cisco Webex Messenger service.

Step 2
Instruct users to sign out and then sign in again.
When users sign in to the client, it retrieves the changes in the service profile and signs the user in to the authenticator. The client then determines the product mode and prompts the user to restart the client.

After the user restarts the client, the product mode change is complete.

Authentication Arguments
The following table describe the command line arguments you can set to specify the source of authentication:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTHENTICATOR</td>
<td>Webex</td>
<td>Specifies the source of authentication for the client. This value is used if Service Discovery fails. Set the following as the value:</td>
</tr>
<tr>
<td>CUP_ADDRESS</td>
<td>IP address</td>
<td>Specifies the address of Cisco Unified Communications Manager IM and Presence Service. Set one of the following as the value:</td>
</tr>
<tr>
<td></td>
<td>Hostname</td>
<td>- Hostname (hostname)</td>
</tr>
<tr>
<td></td>
<td>FQDN</td>
<td>- IP address (123.45.254.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- FQDN (hostname.domain.com)</td>
</tr>
</tbody>
</table>
## Authentication Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TFTP</strong></td>
<td>IP address</td>
<td>Specifies the address of your TFTP server. Set one of the following as the value:</td>
</tr>
<tr>
<td></td>
<td>Hostname</td>
<td>• Hostname (<em>hostname</em>)</td>
</tr>
<tr>
<td></td>
<td>FQDN</td>
<td>• IP address (<em>123.45.254.1</em>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FQDN (<em>hostname.domain.com</em>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You should specify this argument if you set Cisco Unified Communications Manager as the authenticator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you deploy:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In phone mode—you should specify the address of the TFTP server that hosts the client configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In default mode—you can specify the address of the Cisco Unified Communications Manager TFTP service that hosts the device configuration.</td>
</tr>
<tr>
<td><strong>CTI</strong></td>
<td>IP address</td>
<td>Sets the address of your CTI server.</td>
</tr>
<tr>
<td></td>
<td>Hostname</td>
<td>Specify this argument if:</td>
</tr>
<tr>
<td></td>
<td>FQDN</td>
<td>• You set Cisco Unified Communications Manager as the authenticator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Users have desk phone devices and require a CTI server.</td>
</tr>
<tr>
<td><strong>CCMCIP</strong></td>
<td>IP address</td>
<td>Sets the address of your CCMCIP server.</td>
</tr>
<tr>
<td></td>
<td>Hostname</td>
<td>Specify this argument if:</td>
</tr>
<tr>
<td></td>
<td>FQDN</td>
<td>• You set Cisco Unified Communications Manager as the authenticator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The address of your CCMCIP server is not the same as the TFTP server address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The client can locate the CCMCIP server with the TFTP server address if both addresses are the same.</td>
</tr>
<tr>
<td><strong>SERVICES_DOMAIN</strong></td>
<td>Domain</td>
<td>Sets the value of the domain where the DNS SRV records for Service Discovery reside.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This argument can be set to a domain where no DNS SRV records reside if you want the client to use installer settings or manual configuration for this information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If this argument is not specified and Service Discovery fails, the user will be prompted for services domain information.</td>
</tr>
</tbody>
</table>
In Hybrid deployments, the domain required to discover Webex through CAS lookup can be a different domain than where the DNS records are deployed. If this is the case then set the SERVICES_DOMAIN to be the domain used for Webex discovery (or let the user enter an email address) and set the VOICE_SERVICES_DOMAIN to be the domain where DNS records are deployed. If this setting is specified, the client uses the value of VOICE_SERVICES_DOMAIN to lookup the following DNS records for the purposes of Service Discovery and Edge Detection:

- _cisco-uds
- _cuplogin
- _collab-edge

This setting is optional and if not specified, the DNS records are queried on the Services Domain which is obtained from the SERVICES_DOMAIN, email address input by the user, or cached user configuration.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| VOICE_SERVICES_DOMAIN     | Domain      | In Hybrid deployments, the domain required to discover Webex through CAS lookup can be a different domain than where the DNS records are deployed. If this is the case then set the SERVICES_DOMAIN to be the domain used for Webex discovery (or let the user enter an email address) and set the VOICE_SERVICES_DOMAIN to be the domain where DNS records are deployed. If this setting is specified, the client uses the value of VOICE_SERVICES_DOMAIN to lookup the following DNS records for the purposes of Service Discovery and Edge Detection:
  - _cisco-uds
  - _cuplogin
  - _collab-edge

This setting is optional and if not specified, the DNS records are queried on the Services Domain which is obtained from the SERVICES_DOMAIN, email address input by the user, or cached user configuration. |
| EXCLUDED_SERVICES         | One or more of: Webex, CUCM | Lists the services that you want Jabber to exclude from Service Discovery. For example, suppose that you did a trial with Webex and your company domain is registered on Webex. But, you want Jabber to authenticate with CUCM server, rather than with Webex. In this case set:
  - EXCLUDED_SERVICES=WEBEX
  Possible values are CUCM, Webex

If you exclude all services, you need to use manual configuration or bootstrap configuration to configure the Jabber client. |
**Description**

ValueArgument

**Argument** | **Value** | **Description**
---|---|---
UPN_DISCOVERY_ENABLED | true false | Allows you to define whether the client uses the User Principal Name (UPN) of a Windows session to get the User ID and domain for a user when discovering services.
  - true (default)—The UPN is used to find the User ID and the domain of the user, which is used during service discovery. Only the user discovered from UPN can log in to the client.
  - false—The UPN is not used to find the User ID and domain of the user. The user is prompted to enter credentials to find the domain for service discovery.

**Example installation command:**
`msiexec.exe /i CiscoJabberSetup.msi /quiet
UPN_DISCOVERY_ENABLED=false`

---

**TFTP Server Address**

Cisco Jabber for Windows retrieves two different configuration files from the TFTP server:

- Client configuration files that you create.
- Device configuration files that reside on the Cisco Unified Communications Manager TFTP service when you provision users with devices.

To minimize effort, you should host your client configuration files on the Cisco Unified Communications Manager TFTP service. You then have only one TFTP server address for all configuration files and can specify that address as required.

You can, however, host your client configuration on a different TFTP server to the one that contains the device configuration. In this case, you have two different TFTP server addresses, one address for the TFTP server that hosts device configuration and another address for the TFTP server that hosts client configuration files.

**Default Deployments**

This section describes how you should handle two different TFTP server addresses in deployments that have a presence server.

You should do the following:

1. Specify the address of the TFTP server that hosts the client configuration on the presence server.
2. During installation, specify the address of the Cisco Unified Communications Manager TFTP service with the TFTP argument.

When the client starts for the first time, it:

1. Retrieves the address of the Cisco Unified Communications Manager TFTP service from the bootstrap file.
2. Gets device configuration from the Cisco Unified Communications Manager TFTP service.
3. Connects to the presence server.
4. Retrieves the address of the TFTP service that hosts the client configuration from the presence server.
5. Gets client configuration from the TFTP server.

**Phone Mode Deployments**

This section describes how you should handle two different TFTP server addresses in phone mode deployments. You should do the following:

1. During installation, specify the address of the TFTP server that hosts the client configuration with the TFTP argument.
2. Specify the address of the TFTP server that hosts the device configuration in your client configuration file with the following parameter: TftpServer1.
3. Host the client configuration file on the TFTP server.

When the client starts for the first time, it:

1. Retrieves the address of the TFTP server from the bootstrap file.
2. Gets client configuration from the TFTP server.
3. Retrieves the address of the Cisco Unified Communications Manager TFTP service from the client configuration.
4. Gets device configuration from the Cisco Unified Communications Manager TFTP service.

**Common Installation Arguments**

The following table describes some common command line arguments:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTOMATIC_SIGN_IN</td>
<td>true</td>
<td>Specifies whether the <strong>Sign me in when Cisco Jabber starts</strong> check box is checked when the user installs the client.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• true—The <strong>Sign me in when Cisco Jabber starts</strong> check box is checked when the user installs the client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• false (default)—The <strong>Sign me in when Cisco Jabber starts</strong> check box is not checked when the user installs the client.</td>
</tr>
<tr>
<td>CC_MODE</td>
<td>true</td>
<td>Specifies whether Jabber is running in Common Criteria mode.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>The default value is false.</td>
</tr>
<tr>
<td>Argument</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CLICK2X</td>
<td>DISABLE Click2Call</td>
<td>Disables click-to-x functionality with Cisco Jabber. If you specify this argument during installation, the client does not register as a handler for click-to-x functionality with the operating system. This argument prevents the client from writing to the Microsoft Windows registry during installation. You must re-install the client and omit this argument to enable click-to-x functionality with the client after installation.</td>
</tr>
</tbody>
</table>
| DIAGNOSTICSTOOLENABLED | true/false         | Specifies whether the Cisco Jabber Diagnostics Tool is available to Cisco Jabber for Windows users.  
- true (default)—Users can display the Cisco Jabber Diagnostics Tool by entering Ctrl + Shift + D.  
- false—The Cisco Jabber Diagnostics Tool is not available to users. |
### Common Installation Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENABLE_DPI_AWARE</td>
<td>true/false</td>
<td>Enables DPI awareness. DPI awareness enables Cisco Jabber to automatically adjust the display of text and images to suit different screen sizes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• true (default)— • on Windows 8.1 and Windows 10, Cisco Jabber adjusts to different DPI settings on each monitor.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• on Windows 7 and Windows 8, Cisco Jabber displays according to the system DPI settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• false—DPI awareness is not enabled.</td>
</tr>
</tbody>
</table>

DPI awareness is enabled by default. To disable DPI awareness, use the following command:

```
msiexec.exe /i CiscoJabberSetup.msi CLEAR=1 ENABLE_DPI_AWARE=false
```

**Note** If you are installing Cisco Jabber with the command line, remember to include the CLEAR=1 argument. If you are not installing Cisco Jabber from the command line, you must manually delete the jabber-bootstrap.properties file.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENABLE_PRT</td>
<td>true/false</td>
<td>• true (default)—The <strong>Report a problem</strong> menu item is enabled in the <strong>Help</strong> menu in the client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• false—The Jabber menu item option <strong>Report a problem</strong> is removed from the <strong>Help</strong> menu in the client.</td>
</tr>
</tbody>
</table>

If you set the argument to false, users can still manually use the **Start Menu > Cisco Jabber** directory, or the Program files directory and launch the Problem Report Tool manually. If a user manually creates a PRT, and this parameter value is set to false, then the zip file created from the PRT has no content.
<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENABLE_PRT_ENCRYPTION</td>
<td>true/false</td>
<td>Enables problem report encryption. You must configure this argument with the PRT_CERTIFICATE_NAME argument.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• true—PRT files sent by Jabber clients are encrypted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• false (default)—PRT files sent by Jabber clients are not encrypted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRT encryption requires a public/private key pair to encrypt and decrypt the Cisco Jabber problem report.</td>
</tr>
<tr>
<td>FIPS_MODE</td>
<td>true/false</td>
<td>Specifies whether Cisco Jabber is in FIPS mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco Jabber can be in FIPS mode on an operating system that is not FIPS enabled. Only connections with non-Windows APIs are in FIPS mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you don't include this setting, Cisco Jabber will determine the FIPS mode from the operating system.</td>
</tr>
<tr>
<td>FORWARD_VOICEMAIL</td>
<td>true/false</td>
<td>Enables voicemail forwarding in the Voice Messages tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• true (default)—Users can forward voicemails to contacts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• false—Voicemail forwarding is not enabled.</td>
</tr>
<tr>
<td>INVALID_CERTIFICATE_BEHAVIOR</td>
<td>RejectAndNotify/PromptPerSession</td>
<td>Specifies the client behavior for invalid certificates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RejectAndNotify—A warning dialog displays and the client doesn't load.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For invalid certificates in FIPS mode, this argument is ignored, the client displays a warning message and doesn't load.</td>
</tr>
</tbody>
</table>
### Team Messaging Mode Deployment for Cisco Jabber 12.7

**IP_Mode**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4-Only</td>
<td>Specifies the network IP protocol for the Jabber client.</td>
</tr>
<tr>
<td>IPv6-Only</td>
<td>• IPv4-Only—Jabber will only attempt to make IPv4 connections.</td>
</tr>
<tr>
<td>Two Stacks</td>
<td>• IPv6-Only—Jabber will only attempt to make IPv6 connections.</td>
</tr>
<tr>
<td></td>
<td>• Two Stacks (Default)—Jabber can connect with either IPv4 or IPv6.</td>
</tr>
</tbody>
</table>

**Note** IPv6-only support is available only for desktop devices on-premise deployment. All Jabber mobile devices must be configured as Two Stacks.

For more details about IPv6 deployment, see the IPv6 Deployment Guide for Cisco Collaboration Systems Release.

There are a number of factors used to determine the network IP protocol used by Jabber, for more information see the IPv6 Requirements section in the Planning Guide.
<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| LANGUAGE          | LCID in decimal        | Defines the Locale ID (LCID), in decimal, of the language that Cisco Jabber for Windows uses. The value must be an LCID in decimal that corresponds to a supported language. For example, you can specify one of the following:  
  • 1033 specifies English.  
  • 1036 specifies French.  
  See the LCID for Languages topic for a full list of the languages that you can specify.  
  This argument is optional.  
  If you do not specify a value, Cisco Jabber for Windows checks the value for the UseSystemLanguage parameter. If the UseSystemLanguage parameter is set to true, the same language is used as for the operating system. If the UseSystemLanguage parameter is set to false or not defined, then the client uses the regional language for the current user as the default.  
  The regional language is set at Control Panel > Region and Language > Change the date, time, or number format > Formats tab > Format dropdown. |
| LOCATION_MODE     | ENABLED | Specifies whether the Location feature is enabled and whether users are notified when new locations are detected.  
  • 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. |
<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOG_DIRECTORY</td>
<td>Absolute path on the local filesystem</td>
<td>Defines the directory where the client writes log files. Use quotation marks to escape space characters in the path, as in the following example: &quot;C:\my_directory\Log Directory&quot;. The path you specify must not contain Windows invalid characters. The default value is %USER_PROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs.</td>
</tr>
</tbody>
</table>
| LOGINRESOURCE            | WBX, MUT    | Controls user sign in to multiple client instances. By default, users can sign in to multiple instances of Cisco Jabber at the same time. Set one of the following values to change the default behavior:  

  • WBX—Users can sign in to one instance of Cisco Jabber for Windows at a time. Cisco Jabber for Windows appends the wbxconnect suffix to the user's JID. Users cannot sign in to any other Cisco Jabber client that uses the wbxconnect suffix.  

  • MUT—Users can sign in to one instance of Cisco Jabber for Windows at a time, but can sign in to other Cisco Jabber clients at the same time. Each instance of Cisco Jabber for Windows appends the user's JID with a unique suffix. |
<p>| PRT_CERTIFICATE_NAME     | Certificate name | Specifies the name of a certificate with a public key in the Enterprise Trust or Trusted Root Certificate Authorities certificate store. The certificate public key is used to encrypt Jabber Problem reports. You must configure this argument with the ENABLE_PRT_ENCRYPTION argument. |</p>
<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| RESET_JABBER       | 1     | Resets the user's local and roaming profile data. These folders are deleted:  
• %appdata%\Cisco\Unified Communications\Jabber  
• %localappdata%\Cisco\Unified Communications\Jabber |
| SSO_EMAIL_PROMPT   | ON/OFF| Specifies whether the user is shown the email prompt for determining their home cluster.  
In order for the email prompt to work defined by ServicesDomainSsoEmailPrompt the installer requirements are:  
• SSO_EMAIL_PROMPT=ON  
• UPN_DISCOVERY_ENABLED=False  
• VOICE_SERVICES_DOMAIN=<domain_name>  
• SERVICES_DOMAIN=<domain_name>  
Example: msiexec.exe /i CiscoJabberSetup.msi SSO_EMAIL_PROMPT=ON UPN_DISCOVERY_ENABLED=False VOICE_SERVICES_DOMAIN=example.cisco.com SERVICES_DOMAIN=example.cisco.com CLEAR=1 |
| TFTP_FILE_NAME     | Filename | Specifies the unique name of a group configuration file.  
You can specify either an unqualified or fully qualified filename as the value. The filename you specify as the value for this argument takes priority over any other configuration file on your TFTP server.  
This argument is optional.  
**Remember** You can specify group configuration files in the [Cisco Support Field](https://www.cisco.com/support) on the CSF device configuration on Cisco Unified Communications Manager. |

**LCID for Languages**

The following table lists the Locale Identifier (LCID) or Language Identifier (LangID) for the languages that the Cisco Jabber clients support.
<table>
<thead>
<tr>
<th>Supported Languages</th>
<th>Cisco Jabber for Windows</th>
<th>Cisco Jabber for Mac</th>
<th>Cisco Jabber for Android, Cisco Jabber for iPhone and iPad</th>
<th>LCID/LangID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arabic - Saudi Arabia</td>
<td>X</td>
<td></td>
<td>X</td>
<td>1025</td>
</tr>
<tr>
<td>Bulgarian - Bulgaria</td>
<td>X</td>
<td>X</td>
<td></td>
<td>1026</td>
</tr>
<tr>
<td>Catalan - Spain</td>
<td>X</td>
<td>X</td>
<td></td>
<td>1027</td>
</tr>
<tr>
<td>Chinese (Simplified) - China</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>2052</td>
</tr>
<tr>
<td>Chinese (Traditional) - Taiwan</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1028</td>
</tr>
<tr>
<td>Croatian - Croatia</td>
<td>X</td>
<td>X</td>
<td></td>
<td>1050</td>
</tr>
<tr>
<td>Czech - Czech Republic</td>
<td>X</td>
<td>X</td>
<td></td>
<td>1029</td>
</tr>
<tr>
<td>Danish - Denmark</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1030</td>
</tr>
<tr>
<td>Dutch - Netherlands</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1043</td>
</tr>
<tr>
<td>English - United States</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1033</td>
</tr>
<tr>
<td>Finnish - Finland</td>
<td>X</td>
<td>X</td>
<td></td>
<td>1035</td>
</tr>
<tr>
<td>French - France</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1036</td>
</tr>
<tr>
<td>German - Germany</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1031</td>
</tr>
<tr>
<td>Greek - Greece</td>
<td>X</td>
<td>X</td>
<td></td>
<td>1032</td>
</tr>
<tr>
<td>Hebrew - Israel</td>
<td>X</td>
<td></td>
<td></td>
<td>1037</td>
</tr>
<tr>
<td>Hungarian - Hungary</td>
<td>X</td>
<td>X</td>
<td></td>
<td>1038</td>
</tr>
<tr>
<td>Italian - Italy</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1040</td>
</tr>
<tr>
<td>Japanese - Japan</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1041</td>
</tr>
<tr>
<td>Korean - Korea</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1042</td>
</tr>
<tr>
<td>Norwegian - Norway</td>
<td>X</td>
<td>X</td>
<td></td>
<td>2068</td>
</tr>
<tr>
<td>Polish - Poland</td>
<td>X</td>
<td>X</td>
<td></td>
<td>1045</td>
</tr>
<tr>
<td>Portuguese - Brazil</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1046</td>
</tr>
</tbody>
</table>
### Run the MSI Manually

You can run the installation program manually to install a single instance of the client and specify connection settings in the Advanced settings window.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Launch <code>CiscoJabberSetup.msi</code>. The installation program opens a window to guide you through the installation process.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Follow the steps to complete the installation process.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Start Cisco Jabber for Windows.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Select <em>Manual setup and sign in</em>. The Advanced settings window opens.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Specify values for the connection settings properties.</td>
</tr>
</tbody>
</table>

---

### Related Topics

- [Example Installation Commands](#), on page 58
- [Command Line Arguments](#), on page 59
Create a Custom Installer

You can transform the default installation package to create a custom installer.

**Note**
You use Microsoft Orca to create custom installers. Microsoft Orca is available as part of the Microsoft Windows SDK for Windows 7 and .NET Framework 4.

Download and install Microsoft Windows SDK for Windows 7 and .NET Framework 4 from the Microsoft website.

**Procedure**

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Get the Default Transform File, on page 75</td>
<td>You must have the default transform file to modify the installation package with Microsoft Orca.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Create Custom Transform Files, on page 75</td>
<td>Transform files contain installation properties that you apply to the installer.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Transform the Installer, on page 76</td>
<td>Apply a transform file to customize the installer.</td>
</tr>
</tbody>
</table>

Get the Default Transform File

You must have the default transform file to modify the installation package with Microsoft Orca.

**Procedure**

- **Step 1**: Download the Cisco Jabber administration package from Software Download page.
- **Step 2**: Copy CiscoJabberProperties.msi from the Cisco Jabber administration package to your file system.

**What to do next**
Create Custom Transform Files, on page 75

Create Custom Transform Files

To create a custom installer, you use a transform file. Transform files contain installation properties that you apply to the installer.

The default transform file lets you specify values for properties when you transform the installer. You should use the default transform file if you are creating one custom installer.
You can optionally create custom transform files. You specify values for properties in a custom transform file and then apply it to the installer.

Create custom transform files if you require more than one custom installer with different property values. For example, create one transform file that sets the default language to French and another transform file that sets the default language to Spanish. You can then apply each transform file to the installation package separately. The result is that you create two installers, one for each language.

**Before you begin**

*Get the Default Transform File, on page 75*

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Start Microsoft Orca.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Open <em>CiscoJabberSetup.msi</em> and then apply <em>CiscoJabberProperties.msi</em>.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specify values for the appropriate installer properties.</td>
</tr>
</tbody>
</table>
| **Step 4** | Generate and save the transform file.  
  a) Select *Transform > Generate Transform*.  
  b) Select a location on your file system to save the transform file.  
  c) Specify a name for the transform file and select *Save*. |

The transform file you created is saved as *file_name.mst*. You can apply this transform file to modify the properties of *CiscoJabberSetup.msi*.

**What to do next**

*Transform the Installer, on page 76*

**Transform the Installer**

Apply a transform file to customize the installer.

**Note**

Applying transform files will alter the digital signature of *CiscoJabberSetup.msi*. Attempts to modify or rename *CiscoJabberSetup.msi* will remove the signature entirely.

**Before you begin**

*Create Custom Transform Files, on page 75*

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Start Microsoft Orca.</td>
</tr>
</tbody>
</table>
| **Step 2** | Open *CiscoJabberSetup.msi* in Microsoft Orca.  
  a) Select *File > Open*. |
b) Browse to the location of CiscoJabberSetup.msi on your file system.
c) Select CiscoJabberSetup.msi and then select Open.

The installation package opens in Microsoft Orca. The list of tables for the installer opens in the Tables pane.

**Step 3**
Required: Remove all language codes except for 1033 (English).

**Restriction** You must remove all language codes from the custom installer except for 1033 (English).

Microsoft Orca does not retain any language files in custom installers except for the default, which is 1033. If you do not remove all language codes from the custom installer, you cannot run the installer on any operating system where the language is other than English.

a) Select View > Summary Information.

The Edit Summary Information window displays.

b) Locate the Languages field.
c) Delete all language codes except for 1033.
d) Select OK.

English is set as the language for your custom installer.

**Step 4**
Apply a transform file.
a) Select Transform > Apply Transform.
b) Browse to the location of the transform file on your file system.
c) Select the transform file and then select Open.

**Step 5**
Select Property from the list of tables in the Tables pane.

The list of properties for CiscoJabberSetup.msi opens in the right panel of the application window.

**Step 6**
Specify values for the properties you require.

**Tip** Values are case sensitive. Ensure the value you enter matches the value in this document.

**Tip** Set the value of the CLEAR property to 1 to override any existing bootstrap file from previous installations. If you do not override existing bootstrap files, the values you set in the custom installer do not take effect.

**Step 7**
Remove any properties that you do not require.

It is essential to remove any properties that are not being set, otherwise the properties being set will not take effect. Remove each property that is not needed one at a time.
a) Right-click the property you want to remove.
b) Select Drop Row.
c) Select OK when Microsoft Orca prompts you to continue.

**Step 8**
Required: Enable your custom installer to save embedded streams.
a) Select Tools > Options.
b) Select the Database tab.
c) Select Copy embedded streams during 'Save As'.
d) Select Apply and then OK.

**Step 9**
Save your custom installer.
a) Select File > Save Transformed As.
b) Select a location on your file system to save the installer.
c) Specify a name for the installer and then select **Save**.

---

**Installer Properties**

The following are the properties you can modify in a custom installer:

- CLEAR
- PRODUCT_MODE
- AUTHENTICATOR
- CUP_ADDRESS
- TFTP
- CTI
- CCMCIP
- LANGUAGE
- TFTP_FILE_NAME
- FORGOT_PASSWORD_URL
- SSO_ORG_DOMAIN
- LOGIN_RESOURCE
- LOG_DIRECTORY
- CLICK2X
- SERVICES_DOMAIN

These properties correspond to the installation arguments and have the same values.

**Deploy with Group Policy**

Install Cisco Jabber for Windows with Group Policy using the Microsoft Group Policy Management Console (GPMC) on Microsoft Windows Server.

---

**Note**

To install Cisco Jabber for Windows with Group Policy, all computers or users to which you plan to deploy Cisco Jabber for Windows must be in the same domain.
Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Set a Language Code, on page 79</td>
<td>You must use this procedure and set the Language field to 1033 only if the MSI is to be modified by Orca in any way.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Deploy the Client with Group Policy, on page 80</td>
<td>Deploy Cisco Jabber for Windows with Group Policy.</td>
</tr>
</tbody>
</table>

**Set a Language Code**

Altering the installation language is not necessary in Group Policy deployment scenarios where the exact MSI file provided by Cisco will be used. The installation language will be determined from the Windows User Locale (Format) in these situations. You must use this procedure and set the Language field to 1033 only if the MSI is to be modified by Orca in any way.

For a list of the Locale Identifier (LCID) or Language Identifier (LangID) for languages that Jabber clients support, see LCID for Languages, on page 72.

Procedure

**Step 1** Start Microsoft Orca.

Microsoft Orca is available as part of the Microsoft Windows SDK for Windows 7 and .NET Framework 4 that you can download from the Microsoft website.

**Step 2** Open CiscoJabberSetup.msi.

a) Select File > Open.

b) Browse to the location of CiscoJabberSetup.msi on your file system.

c) Select CiscoJabberSetup.msi and then select Open.

**Step 3** Select View > Summary Information.

**Step 4** Locate the Languages field.

**Step 5** Set the Languages field to 1033.

**Step 6** Select OK.

**Step 7** Required: Enable your custom installer to save embedded streams.

a) Select Tools > Options.

b) Select the Database tab.

c) Select Copy embedded streams during 'Save As'.

d) Select Apply and then OK.

**Step 8** Save your custom installer.

a) Select File > Save Transformed As.

b) Select a location on your file system to save the installer.

c) Specify a name for the installer and then select Save.
What to do next
Deploy the Client with Group Policy, on page 80

Deploy the Client with Group Policy

Complete the steps in this task to deploy Cisco Jabber for Windows with Group Policy.

Before you begin
Set a Language Code, on page 79

Procedure

Step 1
Copy the installation package to a software distribution point for deployment.
All computers or users to which you plan to deploy Cisco Jabber for Windows must be able to access the installation package on the distribution point.

Step 2
Select Start > Run and then enter the following command:
GPMC.msc
The Group Policy Management console opens.

Step 3
Create a new group policy object.
a) Right-click on the appropriate domain in the left pane.
b) Select Create a GPO in this Domain, and Link it here.
The New GPO window opens.
c) Enter a name for the group policy object in the Name field.
d) Leave the default value or select an appropriate option from the Source Starter GPO drop-down list and then select OK.
The new group policy displays in the list of group policies for the domain.

Step 4
Set the scope of your deployment.
a) Select the group policy object under the domain in the left pane.
The group policy object displays in the right pane.
b) Select Add in the Security Filtering section of the Scope tab.
The Select User, Computer, or Group window opens.
c) Specify the computers and users to which you want to deploy Cisco Jabber for Windows.

Step 5
Specify the installation package.
a) Right-click the group policy object in the left pane and then select Edit.
The Group Policy Management Editor opens.
b) Select Computer Configuration and then select Policies > Software Settings.
c) Right-click Software Installation and then select New > Package.
d) Enter the location of the installation package next to **File Name**; for example, \\server\software_distribution.

**Important** You must enter a Uniform Naming Convention (UNC) path as the location of the installation package. If you do not enter a UNC path, Group Policy cannot deploy Cisco Jabber for Windows.

e) Select the installation package and then select **Open**.

f) In the **Deploy Software** dialog box, select **Assigned** and then **OK**.

---

Group Policy installs Cisco Jabber for Windows on each computer the next time each computer starts.

### Uninstall Cisco Jabber for Windows

You can uninstall Cisco Jabber for Windows using either the command line or the Microsoft Windows control panel. This document describes how to uninstall Cisco Jabber for Windows using the command line.

#### Use the Installer

If the installer is available on the file system, use it to remove Cisco Jabber for Windows.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Open a command line window.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter the following command:</td>
</tr>
<tr>
<td></td>
<td>msiexec.exe /x path_to_CiscoJabberSetup.msi</td>
</tr>
<tr>
<td></td>
<td>For example,</td>
</tr>
<tr>
<td></td>
<td>msiexec.exe /x C:\Windows\Installer\CiscoJabberSetup.msi /quiet</td>
</tr>
<tr>
<td></td>
<td>Where /quiet specifies a silent uninstall.</td>
</tr>
</tbody>
</table>

The command removes Cisco Jabber for Windows from the computer.

#### Use the Product Code

If the installer is not available on the file system, use the product code to remove Cisco Jabber for Windows.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Find the product code.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a)</td>
<td>Open the Microsoft Windows registry editor.</td>
</tr>
<tr>
<td>b)</td>
<td>Locate the following registry key: HKEY_CLASSES_ROOT\Installer\Products</td>
</tr>
<tr>
<td>c)</td>
<td>Select <strong>Edit &gt; Find</strong>.</td>
</tr>
<tr>
<td>d)</td>
<td>Enter Cisco Jabber in the <strong>Find what</strong> text box in the <strong>Find</strong> window and select <strong>Find Next</strong>.</td>
</tr>
<tr>
<td>e)</td>
<td>Find the value of the <strong>ProductIcon</strong> key.</td>
</tr>
</tbody>
</table>
The product code is the value of the `ProductIcon` key, for example, `C:\Windows\Installer\{product_code}\ARPPRODUCTICON.exe`.

**Note** The product code changes with each version of Cisco Jabber for Windows.

**Step 2** Open a command line window.

**Step 3** Enter the following command:

```
msiexec.exe /x product_code
```

For example,

```
msiexec.exe /x 45992224-D2DE-49BB-B085-6524845321C7 /quiet
```

Where `/quiet` specifies a silent uninstall.

The command removes Cisco Jabber for Windows from the computer.

---

## Install Cisco Jabber for Mac

### Installer for Cisco Jabber for Mac

#### Installing the Client

You can choose to install the client using one of the following methods:

- Provide the installer for users to manually install the application. The client is installed in the `Applications` folder. Previous versions of the client need to be removed.
- Configure automatic updates for users, the installer silently updates the application.

For automatic updates, the client is always added in the `Applications` folder.

- If the client existed in a different folder, or a sub folder of the `Applications` folder, then a link is created in that folder to run the client in the Applications folder.
- If the user previously renamed the client, then the installer will rename the new client to match.

Users are prompted for system credentials similar to installing other OS X installers.

**Quiet Install**—To install the client quietly, in the Terminal tool use the following Mac OS X command:

```
sudo installer -pkg /path_to/Install_Cisco-Jabber-Mac.pkg -target /
```

For more information on the installer command, refer to the installer manual pages on your Mac.

#### Accessories Manager

Accessories Manager is a component that provides Unified Communication control APIs to accessory device vendors. Third party devices can use these APIs to perform tasks such as mute audio, answer calls, and end calls from the device. Third party vendors write plugins that are loaded by the application. Standard headsets can be connected with speaker and microphone support.
Only specific devices interact with Accessories Manager for call control. Please contact your devices vendor for more information. Desktop phones are not supported.

The client installer includes the third party plug-ins from the vendors. They are installed in the /Library/Cisco/Jabber/Accessories/ folder.

Supported third party vendors:
- Logitech
- Sennheiser
- Jabra
- Plantronics

Accessories manager functionality is enabled by default and configured using the EnableAccessoriesManager parameter. You can disable specific Accessories Manager plugins from third party vendors using the BlockAccessoriesManager parameter.

**Configuration**

Provide configuration information for your users to sign into the client. Choose one of the following:
- Provide your users with a configuration URL with optional server information. For further information, see the **URL Configuration for Cisco Jabber for Mac** section.
- Provide your users with the server information to connect manually. For further information, see the **Manual Connection Settings** section.
- Use service discovery. For more information, see the **Service Discovery** section.

**Run Installer Manually**

You can run the installation program manually to install a single instance of the client and specify connection settings in the **Preferences** settings.

**Before you begin**

Remove any older versions of the client.

**Procedure**

**Step 1**
Launch the **jabber-mac.pkg**.
The installer opens a window to guide you through the installation process.

**Step 2**
Follow the steps to complete the installation process.
The installer prompts the user to enter the system credentials.

**Step 3**
Launch the client, using either a configuration URL or running the client directly.
Enter user credentials.
URL Configuration for Cisco Jabber for Mac

To enable users to launch Cisco Jabber without manually entering service discovery information, create and distribute a configuration URL to users.

You can provide a configuration URL link to users by emailing the link to the user directly, or by posting the link to a website.

You can include and specify the following parameters in the URL:

- **ServicesDomain**—Required. Every configuration URL must include the domain of the IM and presence server that Cisco Jabber needs for service discovery.

- **VoiceServiceDomain**—Required only if you deploy a hybrid cloud-based architecture where the domain of the IM and presence server differs from the domain of the voice server. Set this parameter to ensure that Cisco Jabber can discover voice services.

- **ServiceDiscoveryExcludedServices**—Optional. You can exclude any of the following services from the service discovery process:
  - **Webex**—When you set this value, the client:
    - Does not perform CAS lookup
    - Looks for:
      - _cisco-uds
      - _cuplogin
      - _collab-edge
  - **CUCM**—When you set this value, the client:
    - Does not look for _cisco-uds
    - Looks for:
      - _cuplogin
      - _collab-edge
  - **CUP**—When you set this value, the client:
    - Does not look for _cuplogin
    - Looks for:
      - _cisco-uds
      - _collab-edge

You can specify multiple, comma-separated values to exclude multiple services.

If you exclude all three services, the client does not perform service discovery and prompts the user to manually enter connection settings.
• ServicesDomainSsoEmailPrompt—Optional. Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.
  • ON
  • OFF

• EnablePRTEncryption—Optional. Specifies that the PRT file is encrypted. Applies to Cisco Jabber for Mac.
  • true
  • false

• PRTCertificateName—Optional. Specifies the name of the certificate. Applies to Cisco Jabber for Mac.

• InvalidCertificateBehavior—Optional. Specifies the client behavior for invalid certificates.
  • RejectAndNotify—A warning dialog displays and the client doesn't load.
  • PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate.

• Telephony_Enabled—Specifies whether the user has phone capability or not. The default is true.
  • True
  • False

• DiagnosticsToolEnabled—Specifies whether the diagnostics tool is available in the client. The default is true.
  • True
  • False

Create the configuration URL in the following format:

ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>

Note

The parameters are case sensitive.

Examples

• ciscojabber://provision?ServicesDomain=cisco.com

• ciscojabber://provision?ServicesDomain=cisco.com
  &VoiceServicesDomain=alphauk.cisco.com

• ciscojabber://provision?ServicesDomain=service_domain
  &VoiceServicesDomain=voicesservice_domain&ServiceDiscoveryExcludedServices=WEBEX

• ciscojabber://provision?ServicesDomain=cisco.com
  &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP
Configure Automatic Updates 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.

XML File Structure

The following is an example XML file for automatic updates:

```xml
<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>.]]></Message>
  </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:

```xml
<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>.]]></Message>
  </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>.]]></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.

Configure Web servers to escape special characters to ensure the DSA signature succeeds. For example, on Microsoft IIS the option is: Allow double spacing.

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—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:
     Install_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.

Install Cisco Jabber Mobile Clients

Procedure

Step 1  To install Cisco Jabber for Android, download the app from Google Play from your mobile device.
Step 2  To install Cisco Jabber for iPhone and iPad, download the app from the App Store from your mobile device.
URL Configuration for Cisco Jabber for Android, iPhone, and iPad

To enable users to launch Cisco Jabber without manually entering service discovery information, create and distribute a configuration URL to users.

You can provide a configuration URL link to users by emailing the link to the user directly, or by posting the link to a website.

You can include and specify the following parameters in the URL:

- **ServicesDomain**—Required. Every configuration URL must include the domain of the IM and presence server that Cisco Jabber needs for service discovery.

- **VoiceServiceDomain**—Required only if you deploy a hybrid cloud-based architecture where the domain of the IM and presence server differs from the domain of the voice server. Set this parameter to ensure that Cisco Jabber can discover voice services.

- **ServiceDiscoveryExcludedServices**—Optional. You can exclude any of the following services from the service discovery process:
  - **Webex**—When you set this value, the client:
    - Does not perform CAS lookup
    - Looks for:
      - _cisco-uds
      - _cuplogin
      - _collab-edge
  
  - **CUCM**—When you set this value, the client:
    - Does not look for _cisco-uds
    - Looks for:
      - _cuplogin
      - _collab-edge
  
  - **CUP**—When you set this value, the client:
    - Does not look for _cuplogin
    - Looks for:
      - _cisco-uds
      - _collab-edge

You can specify multiple, comma-separated values to exclude multiple services.

If you exclude all three services, the client does not perform service discovery and prompts the user to manually enter connection settings.
- **ServicesDomainSsoEmailPrompt**—Optional. Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.
  - ON
  - OFF

- **InvalidCertificateBehavior**—Optional. Specifies the client behavior for invalid certificates.
  - **RejectAndNotify**—A warning dialog displays and the client doesn't load.
  - **PromptPerSession**—A warning dialog displays and the user can accept or reject the invalid certificate.

- **PRTCertificateUrl**—Specifies the name of a certificate with a public key in the trusted root certificate store. Applies to Cisco Jabber mobile clients.

- **Telephony_Enabled**—Specifies whether the user has phone capability or not. The default is true.
  - True
  - False

- **ForceLaunchBrowser**—Used to force user to use the external browser. Applies to Cisco Jabber mobile clients.
  - True
  - False

**Note**
ForceLaunchBrowser is used for client certificate deployments and for devices with Android OS below 5.0.

- **AllowTeamsUseEmbeddedSafari**—Enables users to do SSO authentication with the Webex platform through the Safari browser view. Applies only with the MDM solution on Cisco Jabber for iPhone and iPad. The default is false.
  - True
  - False

Create the configuration URL in the following format:

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>&VoiceServicesDomain=<domain_for_voice_services>&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>&ServicesDomainSsoEmailPrompt=<ON/OFF>
```

**Note**
The parameters are case sensitive.

**Examples**

- `ciscojabber://provision?ServicesDomain=cisco.com`
Before using Enterprise Mobility Management (EMM), ensure:

- The EMM vendor supports Android for Work or Apple Managed App Configuration.
- Android devices OS is 5.0 or later.

To allow users to launch Cisco Jabber for Android or Cisco Jabber for iPhone and iPad, you can configure Cisco Jabber using Enterprise Mobility Management (EMM).

For more information on setting up EMM, refer to the instructions for administrators provided by the EMM provider.

If you want Jabber to run only on managed devices, then you can deploy certificate-based authentication, and enroll the client certificate through EMM.

You can configure Cisco Jabber for iPhone and iPad as the default dialer for the local contacts that are imported from Microsoft Exchange Server. Configure the profile with the Exchange ActiveSync and enter the value `com.cisco.jabberIM` in the Default Audio Call App field of the MDM configuration file.

When using EMM, disable URL configuration by setting the AllowUrlProvisioning parameter to `False` in the EMM application. For more information on configuring the parameter, refer to the topic AllowUrlProvisioning Parameter.

EMM vendors may allow different value types to be set in Application Configuration settings, but Cisco Jabber only reads String value types. In EMM, configure the following parameters:

- ServicesDomain
- VoiceServicesDomain
- ServiceDiscoveryExcludedServices
- ServicesDomainSsoEmailPrompt
- EnablePRTEncryption
- PRTCertificateURL
- PRTCertificateName
- InvalidCertificateBehavior
- Telephony_Enabled
- ForceLaunchBrowser

Mobile Configuration Using Enterprise Mobility Management

Mobile Configuration Using Enterprise Mobility Management

Team Messaging Mode Deployment for Cisco Jabber 12.7
• FIPS_MODE
• CC_MODE
• LastLoadedUserProfile
• AllowUrlProvisioning
• IP_Mode
• AllowTeamsUseEmbeddedSafari—Cisco Jabber for iPhone and iPad only

**FIPS_MODE Parameter**

Use this parameter to enable or disable FIPS mode on Cisco Jabber mobile clients using EMM.

- **true**—Runs Cisco Jabber in FIPS mode.
- **false**—Does not run Cisco Jabber in FIPS mode.

Example:

```xml
<FIPS_MODE>false</FIPS_MODE>
```

**CC_MODE Parameter**

Use this parameter to enable or disable Common Criteria mode on Cisco Jabber mobile clients using EMM.

- **true**—Runs Cisco Jabber in Common Criteria mode.
- **false** (default)—Does not run Cisco Jabber in Common Criteria mode.

Example:

```xml
<CC_MODE>true</CC_MODE>
```

**Note**

To enable CC_MODE, the RSA key size must be at least 2048 bits. For more information about how to set up Jabber to run in common criteria mode, read about how to **Deploy Cisco Jabber Applications** in the **On-Premises Deployment Guide for Cisco Jabber 12.5**.

**AllowUrlProvisioning Parameter**

Use this parameter when migrating users from URL configuration to EMM.

The following values apply to this parameter:

- **true** (default)—Bootstrap configuration is performed using URL configuration
- **false**—Bootstrap configuration is not performed using URL configuration

Example:

```xml
-AllowURLProvisioning>false</AllowURLProvisioning>
```
Install Jabber Softphone for VDI

Procedure

**Step 1**  Complete the workflow for deploying Jabber.

**Step 2**  To install Jabber Softphone for VDI, follow the instructions in the *Deployment and Installation Guide for Cisco Jabber Softphone for VDI* for the client you are installing.