THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.
CONTENTS

CHAPTER 1
Cisco Jabber for Windows 1
   Documentation 1
   Community Resources 1

CHAPTER 2
Plan for Installation 3
   Hardware Requirements for Cisco Jabber for Windows 3
   Software Requirements 4
      Operating Systems for Cisco Jabber for Windows 4
      On-Premises Servers for Cisco Jabber for Windows and Cisco Jabber for Mac 4
      High Availability for Instant Messaging and Presence 5
   Cloud-Based Servers 6
   Directory Servers 7
   Microsoft Internet Explorer 7
   Microsoft Office 7
      Add Local Contacts from Microsoft Outlook 8
      Microsoft Outlook Calendar Events 8
      Microsoft Outlook Presence Integration 8
   Microsoft SharePoint 10
   Microsoft Office 365 10
   Calendar Integration 10
      Calendar Integration Issues after Upgrading to Outlook 2013 11
   Computer Telephony Integration 11
   Ports and Protocols for Desktop Clients 11
   Call Control with Accessories API 13
      Compatible Third Party Accessories 13
   Install Vendor Plugins 13
CHAPTER 5

Deployment Options 41

On-Premises Deployments 41

Product Modes 41

Default Mode Diagrams 42

Diagram with Cisco Unified Presence 42

Diagram with Cisco Unified Communications IM and Presence 43

Phone Mode Diagram 44

Cloud-Based Deployments 46

Cloud-Based Diagram 46

Hybrid Cloud-Based Diagram 47

How the Client Connects to Services 48

Recommended Connection Methods 48

Sources of Authentication 50

Initial Launch Sequence 50

How the Client Gets an Authenticator 51

About Service Discovery 52

How the Client Locates Services 53

Client Issues HTTP Query 54

Cisco UDS SRV Record 54

CUP Login SRV Record 56

Manual Connection Settings 57

Manual Connection Settings for On-Premises Deployments 57

Manual Connection Settings for On-Premises Deployments in Phone Mode 58
Install Cisco Jabber 75

Methods of Installation 75
Use the Command Line 76
   Example Installation Commands 76
Run the MSI Manually 77
Create a Custom Installer 78
   Get the Default Transform File 78
   Create Custom Transform Files 79
   Transform the Installer 79
Deploy with Group Policy 81
   Set a Language Code 81
   Deploy the Client with Group Policy 82
Command Line Arguments 83
   Override Argument 83
   Mode Type Argument 84
      When to Set the Product Mode 85
      Change Product Modes 85
   Authentication Arguments 86
      TFTP Server Address 89
Common Installation Arguments 91
SSO Arguments 93
   Cloud-Based SSO Arguments 93
Installer Properties 94
Supported Languages 95
Cisco Media Services Interface 95
  Traffic Marking 95
  Desk Phone Video Capabilities 96
Prepare Your Network 96
Install Cisco Media Services Interface 96
Uninstall Cisco Jabber for Windows 97
  Use the Installer 97
  Use the Product Code 97

CHAPTER 7

Configure Cisco Jabber 99
  Introduction to Client Configuration 99
  Configure Service Profiles 100
    Set Parameters on Service Profile 100
      Parameters in Service Profiles 100
      Add Cisco Unified Communications Manager Services 102
    Create Service Profiles 103
    Apply Service Profiles 104
    Associate Users with Devices 104
  Set Parameters on Phone Configuration for Desktop Clients 105
    Parameters in Phone Configuration 105
  Create and Host Client Configuration Files 106
    Client Configuration Files 107
      Global Configuration Files 107
      Group Configuration Files 107
      Configuration File Requirements 108
    Specify Your TFTP Server Address 108
      Specify Your TFTP Server on Cisco Unified Presence 108
      Specify Your TFTP Server on Cisco Unified Communications Manager IM and Presence Service 109
      Specify TFTP Servers in Phone Mode 109
      Specify TFTP Servers with the Cisco WebEx Administration Tool 110
    Create Global Configurations 110
Specify an LDAP Attribute for the User ID 144
Perform Synchronization 145
Authenticate with the LDAP Server 146
Contact Sources 146
Enhanced Directory Integration 147
Domain Name Retrieval 148
Directory Server Discovery 148
Cisco Unified Communications Manager User Data Service 149
Enable Integration with UDS 149
Set UDS Service Parameters 150
Contact Resolution with Multiple Clusters 151
Client Configuration for Directory Integration 151
When to Configure Directory Integration 152
Configure Directory Integration in a Service Profile 152
Directory Profile Parameters 153
Summary of Directory Integration Configuration Parameters 156
Directory Integration Parameters 158
Attribute Mapping Parameters 158
Directory Connection Parameters 160
Directory Query Parameters 164
Phone Number Masks Parameter 167
Contact Photo Parameters 168
UDS Parameters 172
Contact Photo Retrieval with UDS 173
Contact Photo Formats and Dimensions 174
Directory Server Configuration Examples 176
Domain Controller Connection 176
Manual Server Connection 176
UDS Integration 176
LDAP Integration with Expressway for Mobile and Remote Access 177
Simple Authentication for Cisco Jabber for Windows 178
Simple Authentication with SSL for Cisco Jabber for Windows 178
OpenLDAP Integration 178
AD LDS Integration 180
Federation 182
Interdomain Federation 182
Intradomain Federation 183
Configure Intradomain Federation for BDI or EDI 183
Example of Intradomain Federation 184

CHAPTER 9
Customize Cisco Jabber for Windows 187
Custom Emoticons 187
Emoticon Definitions 188
Create Custom Embedded Tabs 191

CHAPTER 10
Appendix 193
Migrate Your Unified Communications Server Infrastructure 193
Differences in Server Infrastructures 193
Upgrade Servers from Version 8.x to Version 9.x or Higher 195
ADSI Error Codes 196
Cisco Jabber for Windows

Cisco Jabber for Windows is a unified communications client within the Cisco Jabber suite of collaboration software. This document contains the information you need to install and configure the client.

Find out more about Cisco Jabber at www.cisco.com/go/jabber

- Documentation, on page 1
- Community Resources, on page 1

Documentation

Cisco Jabber for Windows provides the following documentation in addition to this guide:


Community Resources

Cisco provides different community resources where you can engage with support representatives or join other community members in product discussions.

Cisco product conversation and sharing site

Join other community members in discussing features, functions, licensing, integration, architecture, challenges, and more. Share useful product resources and best practices.

https://communities.cisco.com/community/technology/collaboration/product

Cisco support community

Visit the Cisco support community for IT installation, implementation, and administrative questions.

https://supportforums.cisco.com/community/netpro/collaboration-voice-video/jabber
Cisco support and downloads

Find a wealth of product support resources, download application software, and find bugs based on product and version.


Cisco expert corner

Engage, collaborate, create, and share with Cisco experts. The Cisco expert corner is a collection of resources that various experts contribute to the community, including videos, blogs, documents, and webcasts.

https://supportforums.cisco.com/community/netpro/expert-corner#view=ask-the-experts
Plan for Installation

Review what the client supports before you begin installation. Learn about hardware and software requirements. Find out what ports the client requires and what protocols it uses.

- Hardware Requirements for Cisco Jabber for Windows, on page 3
- Software Requirements, on page 4
- Ports and Protocols for Desktop Clients, on page 11
- Call Control with Accessories API, on page 13
- CTI Supported Devices, on page 14
- Supported Codecs for Cisco Jabber for Windows and Cisco Jabber for Mac, on page 14
- COP Files for Cisco Jabber for Windows and Cisco Jabber for Mac, on page 14
- Client Availability, on page 15
- Instant Message Encryption, on page 16
- Quality of Service Configuration, on page 21
- Protocol Handlers, on page 25
- Audio and Video Performance Reference, on page 27

Hardware Requirements for Cisco Jabber for Windows

**Installed RAM**

2 GB RAM on Microsoft Windows 7 and Windows 8

**Free Physical Memory**

128 MB

**Free Disk Space**

256 MB

**CPU Speed and Type**

Mobile AMD Sempron Processor 3600+ 2 GHz

Intel Core2 CPU T7400 @ 2.16 GHz
Software Requirements

For successful deployment, ensure that client workstations meet the software requirements.

Operating Systems for Cisco Jabber for Windows

You can install Cisco Jabber for Windows on the following operating systems:

- Microsoft Windows 8.1 32 bit
- Microsoft Windows 8.1 64 bit
- Microsoft Windows 8 32 bit
- Microsoft Windows 8 64 bit
- Microsoft Windows 7 32 bit
- Microsoft Windows 7 64 bit

Note: Cisco Jabber for Windows does not require the Microsoft .NET Framework or any Java modules.

Note: For Microsoft Windows 7 or 8.x, you can download Cisco Media Services Interface (MSI) 4.1.2 for use with deskphone video.

Important: Cisco Jabber for Windows supports Microsoft Windows 8 in desktop mode only.

On-Premises Servers for Cisco Jabber for Windows and Cisco Jabber for Mac

Cisco Jabber uses domain name system (DNS) servers during startup. DNS servers are mandatory for Cisco Jabber.

Cisco Jabber supports the following on-premises servers:

- Cisco Unified Communications Manager, release 8.0(1) or later
- Cisco Unified Presence, release 8.0(3) or later
• Cisco Unity Connection, release 8.5 or later
• Cisco WebEx Meetings Server, version 1.1 or later
• Cisco Expressway Series for Cisco Unified Communications Manager
  • Cisco Expressway-E, version 8.1.1 or later
  • Cisco Expressway-C, version 8.1.1 or later
• Cisco TelePresence Video Communications Server
  • Cisco VCS Expressway, version 8.1.1 or later
  • Cisco VCS Control, version 8.1.1 or later

Cisco Jabber supports the following features with Cisco Unified Survivable Remote Site Telephony, Version 8.5:
• Basic call functionality
• Ability to hold and resume calls


For Cisco Unified Communications Manager Express support details, refer to the Cisco Unified CME documentation: http://www.cisco.com/en/us/products/sw/voicesw/ps4625/products_device_support_tables_list.html

**High Availability for Instant Messaging and Presence**

High availability refers to an environment in which multiple nodes exist in a subcluster to provide failover capabilities for instant messaging and presence services. If one node in a subcluster becomes unavailable, the instant messaging and presence services from that node failover to another node in the subcluster. In this way, high availability ensures reliable continuity of instant messaging and presence services for Cisco Jabber.

When using an LDAP or UDS contact source on Cisco Jabber for Mac and Cisco Jabber for mobile clients, high availability is not supported. High availability is only supported for LDAP (EDI) on Cisco Jabber for Windows.

Cisco Jabber supports high availability with the following servers:

**Cisco Unified Presence releases 8.5 and 8.6**

Use the following Cisco Unified Presence documentation for more information about high availability.

**Configuration and Administration of Cisco Unified Presence Release 8.6**

Multi-node Deployment Administration

Troubleshooting High Availability

**Deployment Guide for Cisco Unified Presence Release 8.0 and 8.5**

Planning a Cisco Unified Presence Multi-NODE Deployment
Cisco Unified Communications Manager IM and Presence Service release 9.0 and higher

Use the following Cisco Unified Communications Manager IM and Presence Service documentation for more information about high availability.

Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager

- High Availability Client Login Profiles
- Troubleshooting High Availability

Active Calls on Hold During Failover

You cannot place an active call on hold if failover occurs from the primary instance of Cisco Unified Communications Manager to the secondary instance.

High Availability in the Client

Client Behavior During Failover

If high availability is configured on the server, then after the primary server fails over to the secondary server, the client temporarily loses presence states for up to one minute. Configure the re-login parameters to define how long the client waits before attempting to re-login to the server.

Configure Login Parameters

In Cisco Unified Communications Manager IM and Presence Service, you can configure the maximum and minimum number of seconds that Cisco Jabber waits before attempting to re-login to the server. On the server, you specify the re-login parameters in the following fields:

- Client Re-Login Lower Limit
- Client Re-Login Upper Limit

Related Topics

- Cisco Unified Communications Manager Configuration Guides
- Cisco Unified Presence Configuration Guides
- Supported Services, on page 67

Cloud-Based Servers

Cisco Jabber supports integration with the following hosted servers:

- Cisco WebEx Messenger service
- Cisco WebEx Administration Tool, minimum supported version is 7.5
- Cisco WebEx Meeting Center, minimum supported versions are as follows:
  - Version T26L with Service Pack EP 20
  - Version T27L with Service Pack 9
Directory Servers

You can use the following directory servers with Cisco Jabber:

- Active Directory Domain Services for Windows Server 2012 R2
- Active Directory Domain Services for Windows Server 2008 R2
- Active Directory for Windows Server 2003 R2
- Cisco Unified Communications Manager User Data Server (UDS)

Cisco Jabber supports UDS using the following Cisco Unified Communications Manager versions:

- Cisco Unified Communications Manager, version 9.1(2), with the following Cisco Options Package (COP) file: cmterm-cucm-uds-912-5.cop.sgn.
- Cisco Unified Communications Manager, version 10.0(1). No COP file is required.

- OpenLDAP
- Active Directory Lightweight Directory Service (AD LDS) or Active Directory Application Mode (ADAM)

Restriction

Directory integration with OpenLDAP, AD LDS, or ADAM requires that you define specific parameters in a Cisco Jabber configuration file.

Microsoft Internet Explorer

Cisco Jabber for Windows requires Microsoft Internet Explorer 7 or later. Cisco Jabber for Windows uses the Internet Explorer rendering engine to display HTML content.

Attention

Cisco Jabber for Windows requires Internet Explorer active scripting to render instant messages. See the following Microsoft documentation for instructions to enable active scripting: http://windows.microsoft.com/en-US/windows/help/genuine/ie-active-script

Known Issues with Internet Explorer

- In cloud-based deployments that use single sign-on (SSO), an issue exists with Internet Explorer 9. Users with Internet Explorer 9 get security alerts when they sign in to Cisco Jabber for Windows. To resolve this issue, add webexconnect.com to the list of websites in the Compatibility View Settings window.

Microsoft Office

Cisco Jabber for Windows supports integration with the following software:

- Microsoft Office 2007 32 bit
- Microsoft Office 2010, 32 and 64 bit
Add Local Contacts from Microsoft Outlook

Cisco Jabber for Windows lets users search for and add local contacts in Microsoft Outlook. To enable this integration with Microsoft Outlook, you must enable Cached Exchange Mode on the Microsoft Exchange server.

To search for local contacts in Microsoft Outlook with the client, users must have profiles set in Microsoft Outlook. In addition, users must do the following:

1. Select File > Options.
2. Select the Integration tab (Calendar tab from release 11.0).
3. Select either None or Microsoft Outlook.

To add local Microsoft Outlook contacts to contact lists in the client, local contacts must have instant message addresses in Microsoft Outlook.

To show contact photos in the client interface, local contacts in Microsoft Outlook must have instant message addresses.

To communicate with local contacts in Microsoft Outlook using the client, local contacts must have the relevant details. To send instant messages to contacts, local contacts must have an instant message address. To call contacts in Microsoft Outlook, local contacts must have phone numbers.

Microsoft Outlook Calendar Events

Applies to: Cisco Jabber for Windows

You must apply a setting in Microsoft Outlook so that calendar events display in Cisco Jabber for Windows.

Procedure

**Step 1**
Open the email account settings in Microsoft Outlook, as in the following example:

a) Select File > Account Settings.
b) Select the Email tab on the Account Settings window.

**Step 2**
Double-click the server name.

In most cases, the server name is Microsoft Exchange.

**Step 3**
Select the Use Cached Exchange Mode checkbox.

**Step 4**
Apply the setting and then restart Microsoft Outlook.

When users create calendar events in Microsoft Outlook, those events display in the Meetings tab.

Microsoft Outlook Presence Integration

Applies to: Cisco Jabber for Windows
To enable integration with Microsoft Outlook, you must specify SIP:user@cupdomain as the value of the proxyAddresses attribute in Microsoft Active Directory. Users can then share availability in Microsoft Outlook.

Use one of the following methods to modify the proxyAddresses attribute:

- **An Active Directory administrative tool such as Active Directory User and Computers**
  The Active Directory User and Computers administrative tool allows you to edit attributes on Microsoft Windows Server 2008 or later.

- **ADSchemaWizard.exe utility**
  The ADSchemaWizard.exe utility is available in the Cisco Jabber administration package. This utility generates an LDIF file that modifies your directory to add the proxyAddresses attribute to each user with the following value: SIP:user@cupdomain.

  You should use the ADSchemaWizard.exe utility on servers that do not support the edit attribute feature in the Active Directory User and Computers administrative tool. You can use a tool such as ADSI Edit to verify the changes that you apply with the ADSchemaWizard.exe utility.

  The ADSchemaWizard.exe utility requires Microsoft .NET Framework version 3.5 or later.

- **Create a script with Microsoft Windows PowerShell**
  Refer to the appropriate Microsoft documentation for creating a script to enable presence in Microsoft Outlook.

### Enable Presence with the Active Directory User and Computers Tool

Complete the following steps to enable presence in Microsoft Outlook for individual users with the Active Directory User and Computers administrative tool:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Start the Active Directory User and Computers administrative tool. You must have administrator permissions to run the Active Directory User and Computers administrative tool.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Select View in the menu bar and then select the <strong>Advanced Features</strong> option from the drop-down list.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Navigate to the appropriate user in the Active Directory User and Computers administrative tool.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Double click the user to open the <strong>Properties</strong> dialog box.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Select the <strong>Attribute Editor</strong> tab.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Locate and select the proxyAddresses attribute in the <strong>Attributes</strong> list box.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Select <strong>Edit</strong> to open the <strong>Multi-valued String Editor</strong> dialog box.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>In the <strong>Value to add</strong> text box, specify the following value: SIP:user@cupdomain. For example, SIP:<a href="mailto:msmith@cisco.com">msmith@cisco.com</a>.</td>
</tr>
</tbody>
</table>

Where the user@cupdomain value is the user’s instant messaging address. cupdomain corresponds to the domain for Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.
Microsoft SharePoint

Cisco Jabber for Windows supports the following versions of Microsoft SharePoint:

- Microsoft SharePoint 2007
- Microsoft SharePoint 2010
- Microsoft SharePoint 2013

Important
Cisco Jabber for Windows supports availability status in Microsoft SharePoint sites only if users access those sites with Microsoft Internet Explorer. You should add the Microsoft SharePoint site to the list of trusted sites in Microsoft Internet Explorer.

Microsoft Office 365

Microsoft Office 365 supports different configuration types based on the plan, or subscription, type. Cisco Jabber for Windows has been tested with small business plan P1 of Microsoft Office 365, which requires an on-premise Active Directory server.

Cisco Jabber for Windows supports client-side integration with Microsoft Office 365 with the following applications:

- Microsoft Office 2013 32 bit and 64 bit
- Microsoft Office 2010 32 bit and 64 bit
- Microsoft Office 2007 32 bit
- Microsoft SharePoint 2010

Calendar Integration

You can use the following client applications for calendar integration:

- Microsoft Outlook 2013, 32 bit and 64 bit
- Microsoft Outlook 2010, 32 bit and 64 bit
- IBM Lotus Notes 9, 32 bit
- IBM Lotus Notes 8.5.3, 32 bit
- IBM Lotus Notes 8.5.2, 32 bit
- IBM Lotus Notes 8.5.1, 32 bit
- Google Calendar

Related Topics
Deployment in a Virtual Environment, on page 72
Calendar Integration Issues after Upgrading to Outlook 2013

There is a known issue when upgrading to a version of Outlook 2013 that is not part of Microsoft Office Professional Plus 2013. If users find that their calendar integration does not work, do the following:

**Procedure**

**Step 1**
In the Microsoft Windows registry editor locate the following key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Messaging Subsystem.

**Step 2**
Add a new string value with the name: MAPIX.

**Step 3**
Open the new string value and enter 1 for the value data.

**Step 4**
Restart the Cisco Jabber client.

Computer Telephony Integration

Cisco Jabber for Windows and Cisco Jabber for Mac for Mac support CTI of Cisco Jabber from a third party application.

Computer Telephony Integration (CTI) enables you to use computer-processing functions while making, receiving, and managing telephone calls. A CTI application can allow you to retrieve customer information from a database on the basis of information that caller ID provides and can enable you to use information that an interactive voice response (IVR) system captures.

For more information on CTI, see the CTI sections in the appropriate release of the *Cisco Unified Communications Manager System Guide*. Or you can see the following sites on the Cisco Developer Network for information about creating applications for CTI control through Cisco Unified Communications Manager APIs:

- Cisco TAPI: [https://developer.cisco.com/site/jtapi/overview/](https://developer.cisco.com/site/jtapi/overview/)
- Cisco JTAPI: [https://developer.cisco.com/site/jtapi/overview/](https://developer.cisco.com/site/jtapi/overview/)

Ports and Protocols for Desktop Clients

The following table lists outbound ports and protocols that Cisco Jabber uses.
<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
</table>
| 443   | TCP      | XMPP traffic to the WebEx Messenger service. The client sends XMPP through this port in cloud-based deployments only. If port 443 is blocked, the client falls back to port 5222. **Note** Cisco Jabber can also use this port for:  
  • HTTPS traffic to Cisco Unity Connection and Cisco WebEx Meetings Server.  
  • Saving chats to the Microsoft Exchange server. |
| 30000 to 39999 | UDP | The client uses this port for far end camera control. |
| 636   | LDAPS    | LDAP directory server (secure). |
| 2748  | TCP      | Computer Telephony Interface (CTI) used for desk phone control. |
| 3268  | TCP      | Global Catalog server. |
| 3269  | LDAPS    | Global Catalog server (secure). |
| 5070 to 6070 | UDP | Binary Floor Control Protocol (BFCP) for video desktop sharing capabilities. |
| 5222  | TCP (XMPP) | XMPP traffic to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service. |
| 8443  | TCP (HTTPS) | Traffic to Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service. |
| 7080  | TCP (HTTPS) | Cisco Unity Connection for notifications of voice messages (new message, message update, and message deletion). |
| 53    | UDP/TCP  | Domain Name System (DNS) traffic. |
| 80    | HTTP     | Saving chats to Microsoft Exchange server. Depending on your server configuration on Microsoft Exchange, use either port 80 or 443, but not both. |
| 37200 | SOCKS5 Bytestreams | Peer-to-peer file transfers. In on-premises deployments, the client also uses this port to send screen captures. |
### Ports for Additional Services and Protocols

In addition to the ports listed in this section, you should review the required ports for all protocols and services in your deployment. See to the appropriate documentation for your server version. You can find the port and protocol requirements for different servers in the following documents:

- For Cisco Unified Communications Manager, Cisco Unified Communications Manager IM and Presence Service, and Cisco Unified Presence, see the *TCP and UDP Port Usage Guide*.
- For Cisco Unity Connection, see the *System Administration Guide*.
- For Cisco WebEx Meetings Server, see the *Administration Guide*.
- For Cisco WebEx services, see the *Administrator's Guide*.
- Expressway for Mobile and Remote Access, refer to *Cisco Expressway IP Port Usage for Firewall Traversal*.

### Call Control with Accessories API

Cisco Jabber for Windows includes an API that exposes call control functions to third party accessories. This API lets our vendor partners create software plugins that enable their accessories to use the API call control functions in Cisco Jabber.

#### Compatible Third Party Accessories

You can use certain Cisco compatible accessories such as headsets, speakers, keyboards, and audio devices to perform call control actions with Cisco Jabber from the device. For example, with some headsets you can use controls to answer incoming calls, end active calls, mute audio, and place calls on hold.


---

You can use certain third party accessories that are not Cisco compatible. However, Cisco cannot guarantee an optimal user experience with such third party accessories. For the best user experience, you should use only Cisco compatible devices with Cisco Jabber.

---

#### Install Vendor Plugins

To use compatible accessories with Cisco Jabber, you must do the following:
Procedure

| Step 1 | Download a compatible plugin from the third party vendor site. |
| Step 2 | Install the plugin separately to Cisco Jabber. |

Plugin Versions

The following are the minimum plugin versions required for integration with Cisco Jabber:

- Jabra PC Suite Version 2.12.3655
- Logitech UC Plugin 1.1.27

CTI Supported Devices

To view the list of Computer Telephony Integration (CTI) supported devices: From Cisco Unified Reporting, select Unified CM Phone Feature List. From the Feature drop-down list, select CTI controlled.

Supported Codecs for Cisco Jabber for Windows and Cisco Jabber for Mac

**Supported Audio Codecs**

- G.722.1—32k and 24k. G.722.1 is supported on Cisco Unified Communications Manager 8.6.1 or later.
- G.711—a-law and u-law
- G.729a

**Supported Video Codec**

- H.264/AVC

COP Files for Cisco Jabber for Windows and Cisco Jabber for Mac

In certain cases, you might need to apply COP files to Cisco Unified Communications Manager.

You can download the following COP files from the Cisco Jabber administration package on Cisco.com:
### COP File

<table>
<thead>
<tr>
<th>COP File</th>
<th>Description</th>
<th>Cisco Unified Communications Manager Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ciscocm.installcsfdevicetype.cop.sgn</td>
<td>Adds the CSF device type to Cisco Unified Communications Manager. For more information, see <em>Software Requirements</em>.</td>
<td>7.1.3</td>
</tr>
<tr>
<td>cmterm-bfcp-e.8-6-2.cop.sgn</td>
<td>Enables CSF devices to support BFCP video desktop sharing. For more information, see <em>Apply COP File for BFCP Capabilities</em>.</td>
<td>8.6.2 only</td>
</tr>
<tr>
<td>ciscocm.addcsfsupportfield.cop.sgn</td>
<td>Adds the <strong>CSF Support Field</strong> field for group configuration files. For more information, see <em>Create Group Configurations</em>.</td>
<td>8.6.1 and earlier</td>
</tr>
<tr>
<td>cmterm-cupc-dialrule-wizard-0.1.cop.sgn</td>
<td>Publishes application dial rules and directory lookup rules to Cisco Jabber. For more information, see <em>Publish Dial Rules</em>.</td>
<td>8.6.1 and earlier</td>
</tr>
</tbody>
</table>

### Related Topics

- **Download software**

## Client Availability

Users can define whether their availability reflects their calendar events by setting an option to let others know they are in a meeting from the **Status** tab of the **Options** window from the client. This option synchronizes events in your calendar with your availability. The client only displays **In a meeting** availability for supported integrated calendars.

The client supports using two sources for the **In a meeting** availability:

- **Microsoft Exchange and Cisco Unified Communication Manager IM and Presence Integration** — Applies to on-premises deployments. The **Include Calendar information in my Presence Status** field in Cisco Unified Presence is the same as the **In a meeting** option in the client. Both fields update the same value in the Cisco Unified Communication Manager IM and Presence database.

  If users set both fields to different values, then the last field that the user sets takes priority. If users change the value of the **Include Calendar information in my Presence Status** field while the client is running, the users must restart the client for those changes to apply.

- **Cisco Jabber Client** — Applies to on-premises and cloud-based deployments. You must disable Cisco Unified Communication Manager IM and Presence and Microsoft Exchange integration for the client to support this feature.

---

*Note: Cisco Jabber for mobile clients don't support this meeting integration.*
set the **In a meeting** availability. The client checks if integration between Cisco Unified Communication Manager IM and Presence and Microsoft Exchange is on or off. The client can only set availability if integration is off.

The following deployment scenarios describe how availability is created:

<table>
<thead>
<tr>
<th>Deployment Scenario</th>
<th>You select In a meeting (according to my calendar)</th>
<th>You do not select In a meeting (according to my calendar)</th>
</tr>
</thead>
<tbody>
<tr>
<td>You enable integration</td>
<td>Cisco Unified Communication Manager IM and Presence sets availability status</td>
<td>Availability status does not change</td>
</tr>
<tr>
<td>between Cisco Unified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication Manager IM and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence and Microsoft Exchange.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>You do not enable integration</td>
<td>Client sets availability status</td>
<td>Availability status does not change</td>
</tr>
<tr>
<td>between Cisco Unified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication Manager IM and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence and Microsoft Exchange.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud-based deployments</td>
<td>Client sets availability status</td>
<td>Availability status does not change</td>
</tr>
</tbody>
</table>

Additionally, the following table describes availability that is supported differently by each deployment scenarios:

<table>
<thead>
<tr>
<th>Availability Enabled in the Client</th>
<th>Availability Enabled by Integrating Cisco Unified Communication Manager IM and Presence with Microsoft Exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline in a meeting availability is not supported.</td>
<td>Offline in a meeting availability is supported.</td>
</tr>
<tr>
<td><strong>In a meeting</strong> availability is supported for non-calendar events.</td>
<td><strong>In a meeting</strong> availability is not supported for non-calendar events.</td>
</tr>
</tbody>
</table>

**Note**

Offline in a meeting availability refers to when the user is not logged in to the client but an event exists in the user’s calendar.

Non-calendar events refer to events that do not appear in the user’s calendar, such as instant meetings, **Offline**, or **On a call**.

**Related Topics**

[Calendar Integration](#), on page 10

---

**Instant Message Encryption**

Cisco Jabber uses Transport Layer Security (TLS) to secure Extensible Messaging and Presence Protocol (XMPP) traffic over the network between the client and server. Cisco Jabber encrypts point to point instant messages.
On-Premises Encryption

The following table summarizes the details for instant message encryption in on-premises deployments.

<table>
<thead>
<tr>
<th>Connection</th>
<th>Protocol</th>
<th>Negotiation Certificate</th>
<th>Expected Encryption Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client to server</td>
<td>XMPP over TLS v1.2</td>
<td>X.509 public key infrastructure certificate</td>
<td>AES 256 bit</td>
</tr>
</tbody>
</table>

Server and Client Negotiation

The following servers negotiate TLS encryption with Cisco Jabber using X.509 public key infrastructure (PKI) certificates with the following:

- Cisco Unified Communications Manager IM and Presence
- Cisco Unified Communications Manager

After the server and client negotiate TLS encryption, both the client and server generate and exchange session keys to encrypt instant messaging traffic.

The following table lists the PKI certificate key lengths for Cisco Unified Communications Manager IM and Presence Service.

<table>
<thead>
<tr>
<th>Version</th>
<th>Key Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager IM and Presence Service versions 9.0.1 and higher</td>
<td>2048 bit</td>
</tr>
<tr>
<td>Cisco Unified Presence version 8.6.4</td>
<td>2048 bit</td>
</tr>
<tr>
<td>Cisco Unified Presence versions lower than 8.6.4</td>
<td>1024 bit</td>
</tr>
</tbody>
</table>

XMPP Encryption

Cisco Unified Communications Manager IM and Presence Service uses 256-bit length session keys that are encrypted with the AES algorithm to secure instant message traffic between Cisco Jabber and the presence server.

If you require additional security for traffic between server nodes, you can configure XMPP security settings on Cisco Unified Communications Manager IM and Presence Service. See the following for more information about security settings:

- Cisco Unified Presence—Configuring Security on Cisco Unified Presence
- Cisco Unified Communications Manager IM and Presence Service—Security configuration on IM and Presence

Instant Message Logging

You can log and archive instant messages for compliance with regulatory guidelines. To log instant messages, you either configure an external database or integrate with a third-party compliance server. Cisco Unified Communications Manager IM and Presence Service does not encrypt instant messages that you log in external...
databases or in third party compliance servers. You must configure your external database or third party compliance server as appropriate to protect the instant messages that you log.

See the following for more information about compliance:

- Cisco Unified Presence—*Instant Messaging Compliance Guide*
- Cisco Unified Communications Manager IM and Presence Service—*Instant Messaging Compliance for IM and Presence Service*

For more information about encryption levels and cryptographic algorithms, including symmetric key algorithms such as AES or public key algorithms such as RSA, see *Next Generation Encryption* at this link [https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html](https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html).

For more information about X.509 public key infrastructure certificates, see the *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* document at this link [https://www.ietf.org/rfc/rfc2459.txt](https://www.ietf.org/rfc/rfc2459.txt).

**Related Topics**

- Instant Messaging Compliance Guide
- Configuring Security on Cisco Unified Presence
- Instant Messaging Compliance for IM and Presence Service
- Security configuration on IM and Presence
- Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- Next Generation Encryption

### Cloud-Based Encryption

The following table summarizes the details for instant message encryption in cloud-based deployments:

<table>
<thead>
<tr>
<th>Connection</th>
<th>Protocol</th>
<th>Negotiation Certificate</th>
<th>Expected Encryption Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client to server</td>
<td>XMPP within TLS</td>
<td>X.509 public key infrastructure certificate</td>
<td>AES 128 bit</td>
</tr>
<tr>
<td>Client to client</td>
<td>XMPP within TLS</td>
<td>X.509 public key infrastructure certificate</td>
<td>AES 256 bit</td>
</tr>
</tbody>
</table>

**Server and Client Negotiation**

The following servers negotiate TLS encryption with Cisco Jabber using X.509 public key infrastructure (PKI) certificates with the Cisco Webex Messenger service.

After the server and client negotiate TLS encryption, both the client and server generate and exchange session keys to encrypt instant messaging traffic.

**XMPP Encryption**

The Cisco Webex Messenger service uses 128-bit session keys that are encrypted with the AES algorithm to secure instant message traffic between Cisco Jabber and the Cisco Webex Messenger service.

You can optionally enable 256-bit client-to-client AES encryption to secure the traffic between clients.
Instant Message Logging

The Cisco Webex Messenger service can log instant messages, but it does not archive those instant messages in an encrypted format. However, the Cisco Webex Messenger service uses stringent data center security, including SAE-16 and ISO-27001 audits, to protect the instant messages that it logs.

The Cisco Webex Messenger service cannot log instant messages if you enable AES 256 bit client-to-client encryption.

For more information about encryption levels and cryptographic algorithms, including symmetric key algorithms such as AES or public key algorithms such as RSA, see Next Generation Encryption at this link https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html.

For more information about X.509 public key infrastructure certificates, see the Internet X.509 Public Key Infrastructure Certificate and CRL Profile document at this link https://www.ietf.org/rfc/rfc2459.txt.

Related Topics

- Client to Client Encryption
- Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- Next Generation Encryption

Client-to-Client Encryption

By default, instant messaging traffic between the client and the Cisco WebEx Messenger service is secure. You can optionally specify policies in the Cisco WebEx Administration Tool to secure instant messaging traffic between clients.

The following policies specify client-to-client encryption of instant messages:

- **Support AES Encoding For IM**—Sending clients encrypt instant messages with the AES 256-bit algorithm. Receiving clients decrypt instant messages.

- **Support No Encoding For IM**—Clients can send and receive instant messages to and from other clients that do not support encryption.

The following table describes the different combinations that you can set with these policies.

<table>
<thead>
<tr>
<th>Policy Combination</th>
<th>Client-to-Client Encryption</th>
<th>When the Remote Client Supports AES Encryption</th>
<th>When the Remote Client Does not Support AES Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support AES Encoding For IM = false</td>
<td>No</td>
<td>Cisco Jabber sends unencrypted instant messages.</td>
<td>Cisco Jabber sends and receives unencrypted instant messages.</td>
</tr>
<tr>
<td>Support No Encoding For IM = true</td>
<td></td>
<td>Cisco Jabber does not negotiate a key exchange. As a result, other clients do not send Cisco Jabber encrypted instant messages.</td>
<td></td>
</tr>
<tr>
<td>Policy Combination</td>
<td>Client-to-Client Encryption</td>
<td>When the Remote Client Supports AES Encryption</td>
<td>When the Remote Client Does not Support AES Encryption</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Support AES Encoding For IM = true</td>
<td>Yes</td>
<td>Cisco Jabber sends and receives encrypted instant messages.</td>
<td>Cisco Jabber sends encrypted instant messages.</td>
</tr>
<tr>
<td>Support No Encoding For IM = true</td>
<td></td>
<td>Cisco Jabber displays an icon to indicate instant messages are encrypted.</td>
<td>Cisco Jabber receives unencrypted instant messages.</td>
</tr>
<tr>
<td>Support AES Encoding For IM = true</td>
<td>Yes</td>
<td>Cisco Jabber sends and receives encrypted instant messages.</td>
<td>Cisco Jabber does not send or receive instant messages to the remote client.</td>
</tr>
<tr>
<td>Support No Encoding For IM = false</td>
<td></td>
<td>Cisco Jabber displays an icon to indicate instant messages are encrypted.</td>
<td>Cisco Jabber displays an error message when users attempt to send instant messages to the remote client.</td>
</tr>
</tbody>
</table>

*Note*
Cisco Jabber does not support client-to-client encryption with group chats. Cisco Jabber uses client-to-client encryption for point-to-point chats only.

For more information about encryption and Cisco WebEx policies, see *About Encryption Levels* in the Cisco WebEx documentation.

**Related Topics**
*About Encryption Levels*

## Encryption Icons
Review the icons that the client displays to indicate encryption levels.

### Lock Icon for Client to Server Encryption
In both on-premises and cloud-based deployments, Cisco Jabber displays the following icon to indicate client to server encryption:

![Lock Icon](image)

### Padlock Icon for Client to Client Encryption
In cloud-based deployments, Cisco Jabber displays the following icon to indicate client to client encryption:
Local Chat History

Chat history is retained after participants close the chat window and until participants sign out. If you do not want to retain chat history after participants close the chat window, set the Disable_IM_History parameter to true. This parameter is available to all clients except IM-only users.

For on-premises deployment of Cisco Jabber for Mac, if you select the Save chat archives to: option in the Chat Preferences window of Cisco Jabber for Mac, chat history is stored locally in the Mac file system and can be searched using Spotlight.

Cisco Jabber does not encrypt archived instant messages when local chat history is enabled.

For mobile clients, you can disable local chat history if you do not want unencrypted instant messages to be stored locally.

For desktop clients, you can restrict access to chat history by savings archives to the following directories:

- Windows, %USERPROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\History\uri.db
- Mac: ~/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/History/uri.db.

Quality of Service Configuration

Cisco Jabber supports the following methods for prioritizing and classifying Real-time Transport Protocol (RTP) traffic as it traverses the network:

- Deploy with Cisco Media Services Interface
- Set DSCP values in IP headers of RTP media packets

Tip

Cisco recommends deploying with Cisco Media Services Interface (MSI). This method effectively improves the quality of experience and reduces cost of deployment and operations. MSI also enables the client to become network aware so it can dynamically adapt to network conditions and integrate more tightly with the network.

Cisco Media Services Interface

Cisco Media Services Interface provides a service that works with Cisco Prime Collaboration Manager and Cisco Medianet-enabled routers to ensure that Cisco Jabber can send audio media and video media on your network with minimum latency or packet loss.

Before Cisco Jabber sends audio media or video media, it checks for Cisco Media Services Interface.

- If the service exists on the computer, Cisco Jabber provides flow information to Cisco Media Services Interface.
The service then signals the network so that routers classify the flow and provide priority to the Cisco Jabber traffic.

- If the service does not exist, Cisco Jabber does not use it and sends audio media and video media as normal.

Note
Cisco Jabber checks for Cisco Media Services Interface for each audio call or video call.

You must install Cisco Media Services Interface separately and ensure your network is enabled for Cisco Medianet. You must also install Cisco Prime Collaboration Manager and routers enabled for Cisco Medianet.

Related Topics
Install Cisco Media Services Interface, on page 96

Set DSCP Values

Set Differentiated Services Code Point (DSCP) values in RTP media packet headers to prioritize Cisco Jabber traffic as it traverses the network.

Port Ranges on Cisco Unified Communications Manager

You define the port range that the client uses on the SIP profile in Cisco Unified Communications Manager. The client then uses this port range to send RTP traffic across the network.

Define a Port Range on the SIP Profile

The client uses the port range to send RTP traffic across the network. The client divides the port range equally and uses the lower half for audio calls and the upper half for video calls. As a result of splitting the port range for audio media and video media, the client creates identifiable media streams. You can then classify and prioritize those media streams by setting DSCP values in the IP packet headers.

Procedure

Step 1
Open the Cisco Unified CM Administration interface.

Step 2
Select Device > Device Settings > SIP Profile.

Step 3
Find the appropriate SIP profile or create a new SIP profile.

The SIP Profile Configuration window opens.

Step 4
Specify the port range in the following fields:

- **Start Media Port** — Defines the start port for media streams. This field sets the lowest port in the range.
- **Stop Media Port** — Defines the stop port for media streams. This field sets the highest port in the range.

Step 5
Select Apply Config and then OK.

Related Topics

8.6.x: SIP Profile Configuration
How the Client Uses Port Ranges

Cisco Jabber equally divides the port range that you set in the SIP profile. The client then uses the port range as follows:

- Lower half of the port range for audio streams
- Upper half of the port range for video streams

For example, if you use a start media port of 3000 and an end media port of 4000, the client sends media through ports as follows:

- Ports 3000 to 3501 for audio streams
- Ports 3502 to 4000 for video streams

As a result of splitting the port range for audio media and video media, the client creates identifiable media streams. You can then classify and prioritize those media streams by setting DSCP values in the IP packet headers.

Options for Setting DSCP Values

The following table describes the options for setting DSCP values:

<table>
<thead>
<tr>
<th>Method for Setting DSCP Values</th>
<th>Microsoft Windows 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set DSCP values with Microsoft Group Policy</td>
<td>Yes</td>
</tr>
<tr>
<td>Set DSCP values on network switches and routers</td>
<td>Yes</td>
</tr>
<tr>
<td>Set DSCP values on Cisco Unified Communications Manager</td>
<td>No</td>
</tr>
</tbody>
</table>

Set DSCP Values on Cisco Unified Communications Manager

You can set DSCP values for audio media and video media on Cisco Unified Communications Manager. Cisco Jabber can then retrieve the DSCP values from the device configuration and apply them directly to the IP headers of RTP media packets.

Restriction

For later operating systems such as Microsoft Windows 7, Microsoft implements a security feature that prevents applications from setting DSCP values on IP packet headers. For this reason, you should use an alternate method for marking DSCP values, such as Microsoft Group Policy.

Procedure

Step 1: Open the Cisco Unified CM Administration interface.

Step 2: Select System > Service Parameters.
The **Service Parameter Configuration** window opens.

**Step 3** Select the appropriate server and then select the **Cisco CallManager** service.

**Step 4** Locate the **Clusterwide Parameters (System - QOS)** section.

**Step 5** Specify DSCP values as appropriate and then select **Save**.

---

### Set DSCP Values with Group Policy

If you deploy Cisco Jabber for Windows on a later operating system such as Microsoft Windows 7, you can use Microsoft Group Policy to apply DSCP values.

Complete the steps in the following Microsoft support article to create a group policy:


You should create separate policies for audio media and video media with the following attributes:

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Audio Policy</th>
<th>Video Policy</th>
<th>Signaling Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application name</td>
<td>CiscoJabber.exe</td>
<td>CiscoJabber.exe</td>
<td>CiscoJabber.exe</td>
</tr>
<tr>
<td>Protocol</td>
<td>UDP</td>
<td>UDP</td>
<td>TCP</td>
</tr>
<tr>
<td>Port number or range</td>
<td>Corresponding port number or range from the SIP profile on Cisco Unified Communications Manager.</td>
<td>Corresponding port number or range from the SIP profile on Cisco Unified Communications Manager.</td>
<td>5060 for SIP 5061 for secure SIP</td>
</tr>
<tr>
<td>DSCP value</td>
<td>46</td>
<td>34</td>
<td>24</td>
</tr>
</tbody>
</table>

### Set DSCP Values on the Network

You can configure switches and routers to mark DSCP values in the IP headers of RTP media.

To set DSCP values on the network, you must identify the different streams from the client application.

- **Media Streams** — Because the client uses different port ranges for audio streams and video streams, you can differentiate audio media and video media based on those port range. Using the default port ranges in the SIP profile, you should mark media packets as follows:
  - Audio media streams in ports from 16384 to 24574 as EF
  - Video media streams in ports from 24575 to 32766 as AF41

- **Signaling Streams** — You can identify signaling between the client and servers based on the various ports required for SIP, CTI QBE, and XMPP. For example, SIP signaling between Cisco Jabber and Cisco Unified Communications Manager occurs through port 5060.

  You should mark signaling packets as AF31.
Protocol Handlers

Cisco Jabber registers the following protocol handlers with the operating system to enable click-to-call or click-to-IM functionality from web browsers or other applications:

- XMPP: or XMPP://
  Starts an instant message and opens a chat window in Cisco Jabber.

- IM: or IM://
  Starts an instant message and opens a chat window in Cisco Jabber.

- TEL: or TEL://
  Starts an audio or video call with Cisco Jabber.

Note
TEL is registered by Apple native phone. It cannot be used to cross launch Cisco Jabber for iPhone and iPad.

- CISCOTEL: or CISCOTEL://
  Starts an audio or video call with Cisco Jabber.

- SIP: or SIP://
  Starts an audio or video call with Cisco Jabber.

- CISCOTELCONF:
  Starts a conference call with Cisco Jabber.

Registry Entries for Protocol Handlers

To register as a protocol handler, the client writes to the following locations in the Microsoft Windows registry:

- HKEY_CLASSES_ROOT\tel\shell\open\command
- HKEY_CLASSES_ROOT\xmpp\shell\open\command
- HKEY_CLASSES_ROOT\im\shell\open\command

In the case where two or more applications register as handlers for the same protocol, the last application to write to the registry takes precedence. For example, if Cisco Jabber registers as a protocol handler for XMPP: and then a different application registers as a protocol handler for XMPP:, the other application takes precedence over Cisco Jabber.

Related Topics
Protocol Handlers on HTML Pages, on page 26
Protocol Handlers on HTML Pages

You can add protocol handlers on HTML pages as part of the href attribute. When users click the hyperlinks that your HTML pages expose, the client performs the appropriate action for the protocol.

**TEL and IM Protocol Handlers**

Example of the TEL: and IM: protocol handlers on an HTML page:

```html
<html>
  <body>
    <a href="TEL:1234">Call 1234</a><br/>
    <a href="IM:msmith@domain">Send an instant message to Mary Smith</a>
  </body>
</html>
```

In the preceding example, when users click the hyperlink to call 1234, the client starts an audio call to that phone number. When users click the hyperlink to send an instant message to Mary Smith, the client opens a chat window with Mary.

**CISCOTEL and SIP Protocol Handlers**

Example of the CISCOTEL and SIP protocol handlers on an HTML page:

```html
<html>
  <body>
    <a href="CISCOTEL:1234">Call 1234</a><br/>
    <a href="SIP:msmith@domain">Call Mary</a><br/>
    <a href="CISCOTELCONF:msmith@domain;amckenzi@domain">Weekly conference call</a>
  </body>
</html>
```

In the preceding example, when users click the Call 1234 or Call Mary hyperlinks, the client starts an audio call to that phone number.

**CISOTELCONF Protocol Handler**

Example of the CISOTELCONF protocol handler on an HTML page:

```html
<html>
  <body>
    <a href="CISCOTELCONF:msmith@domain;amckenzi@domain">Weekly conference call</a>
  </body>
</html>
```

In the preceding example, when users click the Weekly conference call hyperlink, a conference call is set up between Mary, Adam, and the user who clicked the link.

**Tip**

Add lists of contacts for the CISOTELCONF: handler to create conference calls. Use a semi-colon to delimit contacts, as in the following example:

```
CISCOTELCONF:user_a@domain.com;user_b@domain.com;user_c@domain.com;user_d@domain.com
```

**XMPP Protocol Handlers**

Example of a group chat using the XMPP: protocol handler on an HTML page:
In the preceding example, when users click the hyperlink to create a group chat with Mary Smith and Adam McKenzie, the client opens a group chat window with Mary and Adam.

**Tip**

Add lists of contacts for the XMPP: and IM: handlers to create group chats. Use a semi-colon to delimit contacts, as in the following example:

/XMPP:user_a@domain.com;user_b@domain.com;user_c@domain.com;user_d@domain.com

**Audio and Video Performance Reference**

The following data is based on testing in a lab environment. This data is intended to provide an idea of what you can expect in terms of bandwidth usage. The content in this topic is not intended to be exhaustive or to reflect all media scenarios that might affect bandwidth usage.

### Audio Bit Rates for Cisco Jabber Desktop Clients

The following audio bit rates apply to Cisco Jabber for Windows and Cisco Jabber for Mac.

<table>
<thead>
<tr>
<th>Codec</th>
<th>RTP (kbits/second)</th>
<th>Actual bit rate (kbits/second)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.722.1</td>
<td>24/32</td>
<td>54/62</td>
<td>High quality compressed</td>
</tr>
<tr>
<td>G.711</td>
<td>64</td>
<td>80</td>
<td>Standard uncompressed</td>
</tr>
<tr>
<td>G.729a</td>
<td>8</td>
<td>38</td>
<td>Low quality compressed</td>
</tr>
</tbody>
</table>

### Video Bit Rates for Cisco Jabber Desktop Clients

The following video bit rates (with g.711 audio) apply to Cisco Jabber for Windows and Cisco Jabber for Mac. This table does not list all possible resolutions.

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Pixels</th>
<th>Measured bit rate (kbits per second) with g.711 audio</th>
</tr>
</thead>
<tbody>
<tr>
<td>w144p</td>
<td>256 x 144</td>
<td>156</td>
</tr>
</tbody>
</table>
Presentation Video Bit Rates

Cisco Jabber captures at 8 fps and transmits at 2 to 8 fps. The values in this table do not include audio.

### Estimated wire bit rate at 2 fps (kbits per second)

<table>
<thead>
<tr>
<th>Pixels</th>
<th>Estimated wire bit rate at 2 fps (kbits per second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>720 x 480</td>
<td>41</td>
</tr>
<tr>
<td>704 x 576</td>
<td>47</td>
</tr>
<tr>
<td>1024 x 768</td>
<td>80</td>
</tr>
<tr>
<td>1280 x 720</td>
<td>91</td>
</tr>
<tr>
<td>1280 x 800</td>
<td>100</td>
</tr>
</tbody>
</table>

### Estimated wire bit rate at 8 fps (kbits per second)

<table>
<thead>
<tr>
<th>Pixels</th>
<th>Estimated wire bit rate at 8 fps (kbits per second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>720 x 480</td>
<td>164</td>
</tr>
<tr>
<td>704 x 576</td>
<td>188</td>
</tr>
<tr>
<td>1024 x 768</td>
<td>320</td>
</tr>
<tr>
<td>1280 x 720</td>
<td>364</td>
</tr>
<tr>
<td>1280 x 800</td>
<td>400</td>
</tr>
</tbody>
</table>

Maximum Negotiated Bit Rate

You specify the maximum payload bit rate in Cisco Unified Communications Manager in the **Region Configuration** window. This maximum payload bit rate does not include packet overhead, so the actual bit rate used is higher than the maximum payload bit rate you specify.

The following table describes how Cisco Jabber allocates the maximum payload bit rate:

<table>
<thead>
<tr>
<th>Desktop sharing session</th>
<th>Audio</th>
<th>Interactive video (Main video)</th>
<th>Presentation video (Desktop sharing video)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Cisco Jabber uses the maximum audio bit rate.</td>
<td>Cisco Jabber allocates the remaining bit rate as follows: The maximum video call bit rate minus the audio bit rate.</td>
<td>—</td>
</tr>
</tbody>
</table>
Cisco Jabber allocates half of the remaining bandwidth after subtracting the audio bit rate.

Cisco Jabber uses the maximum audio bit rate.

Cisco Jabber for Windows separates the bit rate for audio and then divides the remaining bandwidth equally between interactive video and presentation video. The following table provides information to help you understand what performance you should be able to achieve per bandwidth:

### Bandwidth Performance Expectations for Cisco Jabber Desktop Clients

<table>
<thead>
<tr>
<th>Upload speed</th>
<th>Audio</th>
<th>Interactive video (Main video)</th>
<th>Presentation video (Desktop sharing video)</th>
</tr>
</thead>
<tbody>
<tr>
<td>125 kbps under VPN</td>
<td>At bandwidth threshold for g.711, sufficient bandwidth for g.729a and g.722.1</td>
<td>Insufficient bandwidth for video.</td>
<td>Insufficient bandwidth for video.</td>
</tr>
<tr>
<td></td>
<td>Sufficient bandwidth for any audio codec.</td>
<td>w288p (512 x 288) at 30 fps</td>
<td>w144p (256 x 144) at 30 fps + 1280 x 720 at 2+ fps</td>
</tr>
<tr>
<td>384 kbps under VPN</td>
<td>Sufficient bandwidth for any audio codec.</td>
<td>w288p (512 x 288) at 30 fps</td>
<td>w144p (256 x 144) at 30 fps + 1280 x 800 at 2+ fps</td>
</tr>
<tr>
<td>384 kbps in an enterprise network</td>
<td>Sufficient bandwidth for any audio codec.</td>
<td>w576p (1024 x 576) at 30 fps</td>
<td>w288p (512 x 288) at 30 fps + 1280 x 800 at 8 fps</td>
</tr>
<tr>
<td>1000 kbps</td>
<td>Sufficient bandwidth for any audio codec.</td>
<td>w576p (1024 x 576) at 30 fps</td>
<td>w288p (1024 x 576) at 30 fps + 1280 x 800 at 8 fps</td>
</tr>
<tr>
<td>2000 kbps</td>
<td>Sufficient bandwidth for any audio codec.</td>
<td>w720p30 (1280 x 720) at 30 fps</td>
<td>w288p (1024 x 576) at 30 fps + 1280 x 800 at 8 fps</td>
</tr>
</tbody>
</table>

Note that VPN increases the size of the payload, which increases the bandwidth consumption.

### Video Rate Adaptation

Cisco Jabber uses video rate adaptation to negotiate optimum video quality. Video rate adaptation dynamically increases or decreases video bit rate throughput to handle real-time variations on available IP path bandwidth.
Cisco Jabber users should expect video calls to begin at lower resolution and scale upwards to higher resolution over a short period of time. Cisco Jabber saves history so that subsequent video calls should begin at the optimal resolution.
Set Up Servers

Set up the servers before you install the client. Add users to your environment and provision them with services.

- Server Setup Guide, on page 31

Server Setup Guide

The Cisco Jabber Server Setup Guide describes the tasks you need to complete to set up and configure services for Cisco Jabber.
CHAPTER 4

About Certificate Validation

Cisco Jabber uses certificate validation to establish secure connections with servers. When attempting to establish secure connections, servers present Cisco Jabber with certificates. Cisco Jabber for Windows validates those certificates against certificates in the Microsoft Windows certificate store. If the client cannot validate a certificate, it prompts the user to confirm if they want to accept the certificate.

In Expressway for Mobile and Remote Access deployment, when using an online certificate status protocol (OCSP) or online certificate revocation lists (CRL) to obtain the revocation status of the certificates, the Cisco Jabber client expects a response time of less than 5 seconds. Connections will fail if the response time is greater than the expected 5 seconds.

- On-Premises Servers, on page 33
- Certificate Requirements for Cloud-Based Servers, on page 39

On-Premises Servers

Review which certificates on-premises servers present to the client and the tasks involved in getting those certificates signed.

Required Certificates for On-Premises Servers

On-premises servers present the following certificates to establish a secure connection with Cisco Jabber:

<table>
<thead>
<tr>
<th>Server</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Communications Manager IM and Presence Service</td>
<td>HTTP (Tomcat)</td>
</tr>
<tr>
<td></td>
<td>XMPP</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>HTTP (Tomcat) and CallManager certificate (secure SIP call signaling for secure phone)</td>
</tr>
<tr>
<td>Cisco Unity Connection</td>
<td>HTTP (Tomcat)</td>
</tr>
<tr>
<td>Cisco Webex Meetings Server</td>
<td>HTTP (Tomcat)</td>
</tr>
</tbody>
</table>
Certificate Server

Server certificate (used for HTTP, XMPP, and SIP call signaling)

Cisco VCS Expressway
Cisco Expressway-E

Important Notes

• Security Assertion Markup Language (SAML) single sign-on (SSO) and the Identity Provider (IdP) require an X.509 certificate.

• You should apply the most recent Service Update (SU) for Cisco Unified Communications Manager IM and Presence Service before you begin the certificate signing process.

• The required certificates apply to all server versions.

• Each cluster node, subscriber, and publisher, runs a Tomcat service and can present the client with an HTTP certificate.

You should plan to sign the certificates for each node in the cluster.

• To secure SIP signaling between the client and Cisco Unified Communications Manager, you should use Certification Authority Proxy Function (CAPF) enrollment.

Get Certificates Signed by Certificate Authority

Cisco recommends using server certificates that are signed by one of the following types of Certificate Authority (CA):

• Public CA — A third-party company verifies the server identity and issues a trusted certificate.

• Private CA — You create and manage a local CA and issue trusted certificates.

The signing process varies for each server and can vary between server versions. It is beyond the scope of this document to provide detailed steps for every version of each server. You should consult the appropriate server documentation for detailed instructions on how to get certificates signed by a CA. However, the following steps provide a high-level overview of the procedure:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Generate a Certificate Signing Request (CSR) on each server that can present a certificate to the client.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Submit each CSR to the CA. If the process your company uses means you must wait for the CSRs to be sent back to you before you can apply them, then you may wish to configure your services now while you wait for the CSRs. Then you can apply the certificates after the service configuration is complete, prior to deployment.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Upload the certificates that the CA issues to each server.</td>
</tr>
</tbody>
</table>
Certificate Signing Request Formats and Requirements

A public certificate authority (CA) typically requires a certificate signing request (CSR) to conform to specific formats. For example, a public CA might only accept CSRs that have the following requirements:

- Are Base64-encoded.
- Do not contain certain characters, such as @ & !, in the Organization, OU, or other fields.
- Use specific bit lengths in the server's public key.

If you submit CSRs from multiple nodes, public CAs might require that the information is consistent in all CSRs.

To prevent issues with your CSRs, you should review the format requirements from the public CA to which you plan to submit the CSRs. You should then ensure that the information you enter when configuring your server conforms to the format that the public CA requires.

One Certificate Per FQDN—Some public CAs sign only one certificate per fully qualified domain name (FQDN).

For example, to sign the HTTP and XMPP certificates for a single Cisco Unified Communications Manager IM and Presence Service node, you might need to submit each CSR to different public CAs.

Revocation Servers

Cisco Jabber cannot connect to the Cisco Unified Communications Manager servers if the revocation server is not reachable. Also, if a certificate authority (CA) revokes a certificate, Cisco Jabber does not allow users to connect to that server.

Users are not notified of the following outcomes:

- The certificates do not contain revocation information.
- The revocation server cannot be reached.

To validate certificates, the certificate must contain an HTTP URL in the CDP or AIA fields for a reachable server that can provide revocation information.

To ensure that your certificates are validated when you get a certificate issued by a CA, you must meet one of the following requirements:

- Ensure that the CRL Distribution Point (CDP) field contains an HTTP URL to a certificate revocation list (CRL) on a revocation server.
- Ensure that the Authority Information Access (AIA) field contains an HTTP URL for an Online Certificate Status Protocol (OCSP) server.

Server Identity in Certificates

As part of the signing process, the CA specifies the server identity in the certificate. When the client validates that certificate, it checks that:

- A trusted authority has issued the certificate.
Public CAs generally require a fully qualified domain name (FQDN) as the server identity, not an IP address.

**Identifier Fields**

The client checks the following identifier fields in server certificates for an identity match:

- **XMPP certificates**
  - SubjectAltName\OtherName\xmppAddr
  - SubjectAltName\OtherName\srvName
  - SubjectAltName\dnsNames
  - Subject CN

- **HTTP certificates**
  - SubjectAltName\dnsNames
  - Subject CN

**Tip**

The **Subject CN** field can contain a wildcard (*) as the leftmost character, for example, *.cisco.com.

**Prevent Identity Mismatch**

If users attempt to connect to a server with an IP address or hostname, and the server certificate identifies the server with an FQDN, the client cannot identify the server as trusted and prompts the user.

If your server certificates identify the servers with FQDNs, you should plan to specify each server name as FQDN in many places on your servers. For more information, see *Prevent Identity Mismatch* section in Troubleshooting TechNotes.

**Provide XMPP Domain to Clients**

This task is not required if you are using Cisco Unified Communications Manager IM and Presence Service version 10.0 or later.

The client identifies XMPP certificates using the XMPP domain, rather than the FQDN. The XMPP certificates must contain the XMPP domain in an identifier field.

When the client attempts to connect to the presence server, the presence server provides the XMPP domain to the client. The client can then validate the identity of the presence server against the XMPP certificate.

Complete the following steps to ensure the presence server provides the XMPP domain to the client:

**Procedure**

**Step 1**

Open the administration interface for your presence server, as follows:
• Cisco Unified Communications Manager IM and Presence Service — Open the Cisco Unified CM IM and Presence Administration interface.
• Cisco Unified Presence — Open the Cisco Unified Presence Administration interface.

Step 2
Select System > Security > Settings.

Step 3
Locate the XMPP Certificate Settings section.

Step 4
Specify the presence server domain in the following field: Domain name for XMPP Server-to-Server Certificate Subject Alternative Name.

Step 5
Select the following checkbox: Use Domain Name for XMPP Certificate Subject Alternative Name.

Step 6
Click Save.

Import Root Certificates on Client Computers

Every server certificate should have an associated root certificate present in the trust store on client computers. Cisco Jabber validates the certificates that servers present against the root certificates in the trust store.

If you get server certificates signed by a public CA, the public CA should already have a root certificate present in the trust store on the client computer. In this case, you do not need to import root certificates on the client computers.

You should import root certificates into the Microsoft Windows certificate store if:
• The certificates are signed by a CA that does not already exist in the trust store, such as a private CA.
  Import the private CA certificate to the Trusted Root Certification Authorities store.
• The certificates are self-signed.
  Import self-signed certificates to the Enterprise Trust store.

Important
If root certificates are not present in the trust store, Cisco Jabber prompts users to accept certificates from each server in your environment.

When the client prompts users to accept a certificate, users can:
• Accept the certificate — The client saves the certificate to the Enterprise Trust store.
• Decline the certificate — The client:
  • Does not save the certificate.
  • Does not connect to the server.
  • Displays an error notification.

When users restart the client, it prompts them to accept the certificate again.

You can use any appropriate method to import certificates into the Microsoft Windows certificate store, including the following. For detailed instructions on importing certificates, refer to the appropriate Microsoft documentation.
**Procedure**

- Use the **Certificate Import Wizard** to import certificates individually.
- Deploy certificates to users with the **CertMgr.exe** command line tool on Microsoft Windows Server.

---

**Note**

This option requires you to use the Certificate Manager tool, **CertMgr.exe**, not the Certificates Microsoft Management Console, **CertMgr.msc**.

- Deploy certificates to users with a Group Policy object (GPO) on Microsoft Windows Server.

---

**Deploy Certificates on Client Computers**

Every server certificate should have an associated certificate in the Keychain on the client computers. Cisco Jabber validates the certificates that the servers present against the certificates in the Keychain.

---

**Important**

If root certificates are not present in the Keychain, Cisco Jabber prompts users to accept certificates from each server in your environment.

When the client prompts users to verify a certificate, users can:

- **Always trust server name** — The client saves the certificate to the Keychain.
- **Continue** — The client will connect, but when the user restarts the client they are prompted to accept the certificate again.
- **Cancel** — The client:
  - Does not save the certificate.
  - Does not connect to the server.

Prevent the warning dialogs by downloading the certificates from the **Cisco Unified OS Administration** interface. Complete the following steps to deploy self-signed certificates to the user.

---

**Procedure**

**Step 1**
For each Cisco node, download the corresponding “tomcat-trust” certificate from the **Cisco Unified OS Administration** interface. Select **Security > Certificate Management**.

**Step 2**
Concatenate the certificates into a single file with the extension **.pem** (for example, “companyABCcertificates.pem”).

**Step 3**
Send the file to your Cisco Jabber users and ask them to double-click it. Doing so launches the Keychain Access application and imports the certificates.

**Note**
The operating system requires that the user enter the Mac OS X administration password for each certificate that is being imported.
Certificate Requirements for Cloud-Based Servers

Cisco WebEx Messenger and Cisco WebEx Meeting Center present the following certificates to the client:

• Central Authentication Service (CAS)
• WLAN Authentication and Privacy Infrastructure (WAPI)

Cisco WebEx certificates are signed by a public certificate authority (CA). Cisco Jabber validates these certificates to establish secure connections with cloud-based services.

As of Cisco Jabber for Windows 9.7.2 and Cisco Jabber for Mac 9.6.1, Cisco Jabber validates the XMPP certificate received from Cisco WebEx Messenger. If your operating system does not contain the following certificates for Cisco WebEx Messenger, you must provide them:

• VeriSign Class 3 Public Primary Certification Authority—G5 (stored in the Trusted Root Certificate Authority)
• VeriSign Class 3 Secure Server CA—G3 (stored in the Intermediate Certificate Authority)

The same set of certificates are applicable for Cisco Jabber for Android, iPhone and iPad.

The certificate that is stored in the Intermediate Certificate Authority validates the Cisco WebEx Messenger server identity.

For Cisco Jabber for Windows 9.7.2 or later, you can find more information and installation instructions for the root certificate at http://www.identrust.co.uk/certificates/trustid/install-nes36.html.

For Cisco Jabber for Mac 9.6.1 or later and iOS, you can find more information for the root certificate on the Apple support website at https://support.apple.com.

Update Profile Photo URLs

In cloud-based deployments, Cisco Webex assigns unique URLs to profile photos when you add or import users. When Cisco Jabber resolves contact information, it retrieves the profile photo from Cisco Webex at the URL where the photo is hosted.

Profile photo URLs use HTTP Secure (https://server_name/) and present certificates to the client. If the server name in the URL is:

• A fully qualified domain name (FQDN) that contains the Cisco Webex domain — The client can validate the web server that is hosting the profile photo against the Cisco Webex certificate.

• An IP address — The client cannot validate the web server that is hosting the profile photo against the Cisco Webex certificate. In this case, the client prompts users to accept certificates whenever they look up contacts with an IP address in their profile photo URLs.
We recommend that you update all profile photo URLs that contain an IP address as the server name. Replace the IP address with the FQDN that contains the Cisco Webex domain to ensure that the client does not prompt users to accept certificates.

When you update a photo, the photo can take up to 24 hours to refresh in the client.

The following steps describe how to update profile photo URLs. Refer to the appropriate Cisco Webex documentation for detailed instructions.

Procedure

| Step 1 | Export user contact data in CSV file format with the Cisco Webex Administration Tool. |
| Step 2 | In the `userProfilePhotoURL` field, replace IP addresses with the Cisco Webex domain. |
| Step 3 | Save the CSV file. |
| Step 4 | Import the CSV file with the Cisco Webex Administration Tool. |
Deployment Options

Learn about options for deploying Cisco Jabber.

• On-Premises Deployments, on page 41
• Cloud-Based Deployments, on page 46
• How the Client Connects to Services, on page 48
• Cloud-Based SSO, on page 64
• Expressway for Mobile and Remote Access Deployments, on page 65
• Deployment in a Virtual Environment, on page 72

On-Premises Deployments

An on-premises deployment is one in which you set up, manage, and maintain all services on your corporate network.

Product Modes

You can deploy the client in the following modes:

Full UC and Cisco Jabber for Everyone (IM Only)

The default product mode is one in which the user's primary authentication is to a presence server. At a minimum, users have instant messaging and presence capabilities.

Both full UC and Cisco Jabber for Everyone deployments use the default product mode.

To deploy full UC, you enable instant messaging and presence capabilities. You then provision users with devices for audio and video in addition to voicemail and conferencing capabilities.

To deploy Cisco Jabber for Everyone, you enable instant messaging and presence capabilities. You can optionally provision users with desk phone devices that they can control with the client.

Phone Mode

In phone mode, the user's primary authentication is to Cisco Unified Communications Manager.

To deploy phone mode, you provision users with devices for audio and video capabilities. You can also provision users with additional services such as voicemail.
Default Mode Diagrams

Review architecture diagrams for on-premises deployments in the default product mode.

Diagram with Cisco Unified Presence

The following diagram illustrates the architecture of an on-premises deployment that includes Cisco Unified Presence:

*Figure 1: On-Premises Architecture*

The following are the services available in an on-premises deployment:

**Presence**

Users can publish their availability and subscribe to other users' availability through Cisco Unified Presence.

**Instant Messaging**

Users send and receive instant messages through Cisco Unified Presence.

**Audio Calls**

Users place audio calls through desk phone devices or on their computers through Cisco Unified Communications Manager.
Video
Users share their screens and place video calls through Cisco Unified Communications Manager.

Voicemail
Users send and receive voice messages through Cisco Unity Connection.

Conferencing
Integrate with one of the following:
Cisco WebEx Meeting Center
Provides hosted meeting capabilities.
Cisco WebEx Meeting Server
Provides on-premises meeting capabilities.

Related Topics
Integrate with Directory Sources, on page 143

Diagram with Cisco Unified Communications IM and Presence
The following diagram illustrates the architecture of an on-premise deployment that includes Cisco Unified Communications IM and Presence:

Figure 2: On-Premise architecture
The following are the services available in an on-premise deployment:

**Presence**

Users can publish their availability and subscribe to other users' availability through Cisco Unified Communications IM and Presence.

**Instant Messaging**

Users send and receive instant messages through Cisco Unified Communications IM and Presence.

**Audio Calls**

Users place audio calls through desk phone devices or on their computers through Cisco Unified Communications Manager.

**Video**

Users share their screens and place video calls through Cisco Unified Communications Manager.

**Voicemail**

Users send and receive voice messages through Cisco Unity Connection.

**Conferencing**

Integrate with one of the following:

- **Cisco WebEx Meeting Center**
  
  Provides hosted meeting capabilities.

- **Cisco WebEx Meetings Server**
  
  Provides on-premise meeting capabilities.

**Related Topics**

[Integrate with Directory Sources], on page 143

---

**Phone Mode Diagram**

The following diagram illustrates the architecture of an on-premise deployment for phone mode:
The following are the services available in a phone mode deployment:

**Audio Calls**

Users place audio calls through desk phone devices or on their computers through Cisco Unified Communications Manager.

**Video**

Users share their screens and place video calls through Cisco Unified Communications Manager.

**Voicemail**

Users send and receive voice messages through Cisco Unity Connection.

**Conferencing**

Integrate with one of the following:

- **Cisco WebEx Meeting Center**
  
  Provides hosted meeting capabilities.

- **Cisco WebEx Meetings Server**
  
  Provides on-premise meeting capabilities.
Cloud-Based Deployments

In cloud-based deployments, the user's primary authentication is to the Cisco WebEx Messenger service. Cisco WebEx hosts all services. You manage and monitor cloud-based deployments with the Cisco WebEx Administration Tool.

Related Topics
WebEx Single Sign-On Documentation

Cloud-Based Diagram

The following diagram illustrates the architecture of a cloud-based deployment:

*Figure 4: Cloud-Based Architecture*

The following are the services available in a cloud-based deployment:

- Contact Source — The Cisco WebEx Messenger service provides contact resolution.
- Presence — The Cisco WebEx Messenger service lets users publish their availability and subscribe to other users’ availability.
• Instant Messaging — The Cisco WebEx Messenger service lets users send and receive instant messages.
• Conferencing — Cisco WebEx Meeting Center provides hosted meeting capabilities.

Hybrid Cloud-Based Diagram

The following diagram illustrates the architecture of a hybrid cloud-based deployment:

*Figure 5: Hybrid Cloud-Based Architecture*

The following are the services available in a hybrid cloud-based deployment:

- **Contact Source** — The Cisco WebEx Messenger service provides contact resolution.
- **Presence** — The Cisco WebEx Messenger service lets users can publish their availability and subscribe to other users' availability.
- **Instant Messaging** — The Cisco WebEx Messenger service lets users send and receive instant messages.
- **Conferencing** — Cisco WebEx Meeting Center provides hosted meeting capabilities.
- **Audio Calls** — Users place audio calls through desk phone devices or on their computers through Cisco Unified Communications Manager.
- **Video** — Users share their screens and place video calls through Cisco Unified Communications Manager.
• Voicemail — Users send and receive voice messages through Cisco Unity Connection.

How the Client Connects to Services

To connect to services, Cisco Jabber requires the following information:

• Source of authentication that enables users to sign in to the client.

• Location of services.

You can provide that information to the client with the following methods:

Service Discovery

The client automatically locates and connects to services.

Manual Connection Settings

Users manually enter connection settings in the client user interface.

Bootstrap File

You manually enter connection settings during installation.

Recommended Connection Methods

The method that you should use to provide the client with the information it needs to connect to services depends on your deployment type, server versions, and product modes. The following tables highlight various deployment methods and how to provide the client with the necessary information.

Table 1: On-Premises Deployments for Cisco Jabber for Windows

<table>
<thead>
<tr>
<th>Product Mode</th>
<th>Server Versions</th>
<th>Discovery Method</th>
<th>Non DNS SRV Record Method</th>
</tr>
</thead>
</table>
| Full UC (default mode) | Release 9.1.2 and later:  
• Cisco Unified Communications Manager  
• Cisco Unified Communications Manager IM and Presence Service | A DNS SRV request against _cisco-uds.<domain> | Use the following installer switches and values:  
  • AUTHENTICATOR=CUP  
  • CUP_ADDRESS=  
  <presence_server_address> |
| Full UC (default mode) | Release 8.x:  
• Cisco Unified Communications Manager  
• Cisco Unified Presence | A DNS SRV request against _cuplogin.<domain> | Use the following installer switches and values:  
  • AUTHENTICATOR=CUP  
  • CUP_ADDRESS=  
  <presence_server_address> |
## Recommended Connection Methods

<table>
<thead>
<tr>
<th>Product Mode</th>
<th>Server Versions</th>
<th>Discovery Method</th>
<th>Non DNS SRV Record Method</th>
</tr>
</thead>
</table>
| IM Only (default mode) | Release 9 and later: Cisco Unified Communications Manager IM and Presence Service | A DNS SRV request against _cisco-uds.<domain> | Use the following installer switches and values:  
• AUTHENTICATOR=CUP  
• CUP_ADDRESS= <presence_server_address> |
| IM Only (default mode) | Release 8.x: Cisco Unified Presence | A DNS SRV request against _cuplogin.<domain> | Use the following installer switches and values:  
• AUTHENTICATOR=CUP  
• CUP_ADDRESS= <presence_server_address> |
| Phone Mode | Release 9 and later: Cisco Unified Communications Manager | A DNS SRV request against _cisco-uds.<domain> | Use the following installer switches and values:  
• AUTHENTICATOR=CUCM  
• TFTP=<CUCM_address>  
• CCMCIP=<CUCM_address>  
• PRODUCT_MODE=phone_mode  
High availability is not supported using this method of deployment. |
| Phone Mode | Release 8.x: Cisco Unified Communications Manager | Manual connection settings or bootstrap file | Use the following installer switches and values:  
• AUTHENTICATOR=CUCM  
• TFTP=<CUCM_address>  
• CCMCIP=<CUCM_address>  
• PRODUCT_MODE=phone_mode  
High availability is not supported using this method of deployment. |

Cisco Unified Communications Manager release 9.x and earlier—if you enable Cisco Extension Mobility, the Cisco Extension Mobility service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the Feature and Services guide for your Cisco Unified Communications Manager release.

---

**Note**

Cisco Jabber release 9.6 and later can still discover full Unified Communications and IM-only services using the _cuplogin DNS SRV request but a _cisco-uds request will take precedence if it is present.

Use the SERVICES_DOMAIN installer switch to specify the value of the domain where DNS records reside if you want users to bypass the email screen during the first login of a fresh installation.
The services domain is read from a cached configuration if you are upgrading from Cisco Jabber for Windows 9.2.

### Table 2: Hybrid Cloud-Based Deployments

<table>
<thead>
<tr>
<th>Server Versions</th>
<th>Connection Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Webex Messenger</td>
<td>HTTPS request against <a href="https://loginp.webexconnect.com/cas/FederatedSSO?org=">https://loginp.webexconnect.com/cas/FederatedSSO?org=</a>&lt;domain&gt;</td>
</tr>
</tbody>
</table>

### Table 3: Cloud-Based Deployments

<table>
<thead>
<tr>
<th>Deployment Type</th>
<th>Connection Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled for single sign-on (SSO)</td>
<td>Cisco Webex Administration Tool Bootstrap file to set the SSO_ORG_DOMAIN argument.</td>
</tr>
<tr>
<td>Not enabled for SSO</td>
<td>Cisco Webex Administration Tool</td>
</tr>
</tbody>
</table>

### Sources of Authentication

A source of authentication, or an authenticator, enables users to sign into the client.

Three possible sources of authentication are as follows:

- Cisco Unified Communications Manager IM and Presence—On-premises deployments in either full UC or IM only.
- Cisco Unified Communications Manager—On-premises deployments in phone mode.
- Cisco Webex Messenger Service—Cloud-based or hybrid cloud-based deployments.

### Initial Launch Sequence

On the initial launch after installation, Cisco Jabber starts in the default product mode. The client then gets an authenticator and signs the user in. After sign in, the client determines the product mode.

The following diagram illustrates the initial launch sequence:
How the Client Gets an Authenticator

Cisco Jabber looks for an authenticator as follows:

   
   Users can manually enter authenticator through the client user interface.

2. Client checks cache to discover if the user's domain is a Webex organisation.
   
   The client chooses Webex as the authenticator.

3. Client makes a Webex cloud service HTTP request to discover if the user's organisation domain is a Webex organisation.
   
   The client chooses Webex as the authenticator.

   
   The client loads settings from previous queries for service (SRV) records.

5. Client queries for SRV records.
   
   The client queries the DNS name server for SRV records to locate services.
   
   If the client finds the _cisco-uds SRV record, it can get the authenticator from the service profile.

6. Client reads from the bootstrap file.
   
   You can optionally set the authenticator during installation.

If the client cannot get an authenticator, it prompts the user to manually select the source of authentication in the client user interface.
About Service Discovery

Service discovery enables clients to automatically detect and locate services on your enterprise network. Clients query domain name servers to retrieve service (SRV) records that provide the location of servers.

The primary benefits to using service discovery are as follows:

- Speeds time to deployment.
- Allows you to centrally manage server locations.

If you are migrating from Cisco Unified Presence 8.x to Cisco Unified Communications Manager IM and Presence Service 9.0 or later, you must specify the Cisco Unified Presence server FQDN in the migrated UC service on Cisco Unified Communications Manager. Open Cisco Unified Communications Manager Administration interface. Select User Management > User Settings > UC Service.

For UC services with type IM and Presence, when you migrate from Cisco Unified Presence 8.x to Cisco Unified Communications Manager IM and Presence Service the Host Name/IP Address field is populated with a domain name and you must change this to the Cisco Unified Presence server FQDN.

However, the client can retrieve different SRV records that indicate to the client different servers are present and different services are available. In this way, the client derives specific information about your environment when it retrieves each SRV record.

The following table lists the SRV records that you can deploy and explains the purpose and benefits of each record:

<table>
<thead>
<tr>
<th>SRV Record</th>
<th>Purpose</th>
<th>Why You Deploy</th>
</tr>
</thead>
</table>
| _cisco-uds | Provides the location of Cisco Unified Communications Manager version 9.0 and later. The client can retrieve service profiles from Cisco Unified Communications Manager to determine the authenticator. | • Eliminates the need to specify installation arguments.  
• Lets you centrally manage configuration in UC service profiles.  
• Enables the client to discover the user's home cluster.  
As a result, the client can automatically get the user's device configuration and register the devices. You do not need to provision users with Cisco Unified Communications Manager IP Phone (CCMCIP) profiles or Trivial File Transfer Protocol (TFTP) server addresses.  
• Supports mixed product modes.  
You can easily deploy users with full UC, IM only, or phone mode capabilities.  
• Supports Expressway for Mobile and Remote Access. |
### SRV Record | Purpose | Why You Deploy
---|---|---
`_cuplogin` | Provides the location of Cisco Unified Presence. Sets Cisco Unified Presence as the authenticator. | - Supports deployments with Cisco Unified Communications Manager and Cisco Unified Presence version 8.x.  
- Supports deployments where all clusters have not yet been upgraded to Cisco Unified Communications Manager 9.  

`_collab-edge` | Provides the location of Cisco VCS Expressway or Cisco Expressway-E. The client can retrieve service profiles from Cisco Unified Communications Manager to determine the authenticator. | - Supports deployments with Expressway for Mobile and Remote Access.  

### How the Client Locates Services

The following steps describe how the client locates services with SRV records:

1. The client's host computer or device gets a network connection.  
   When the client's host computer gets a network connection, it also gets the address of a Domain Name System (DNS) name server from the DHCP settings.

2. User starts the client.

3. The client gets the address of the DNS name server from the DHCP settings.

4. The client issues an HTTP query to a Central Authentication Service (CAS) URL for the Cisco Webex Messenger service. This query enables the client to determine if the domain is a valid Cisco Webex domain.

5. The client queries the name server for the following SRV records in order of priority:
   - `_cisco-uds`
   - `_cuplogin`
   - `_collab-edge`

The client caches the results of the DNS query to load on subsequent launches.

The following is an example of an SRV record entry:

```
_cisco_uds._tcp.DOMAIN SRV service location:  
priority = 0  
weight = 0  
port = 8443  
svr hostname=192.168.0.26
```
Client Issues HTTP Query

In addition to querying the name server for SRV records to locate available services, the client sends an HTTP query to the CAS URL for the Cisco WebEx Messenger service. This request enables the client to determine cloud-based deployments and authenticate users to the Cisco WebEx Messenger service.

When the client gets a domain from the user, it appends that domain to the following HTTP query:

http://loginp.webexconnect.com/cas/FederatedSSO?org=

For example, if the client gets example.com as the domain from the user, it issues the following query:

http://loginp.webexconnect.com/cas/FederatedSSO?org=example.com

That query returns an XML response that the client uses to determine if the domain is a valid Cisco WebEx domain.

If the client determines the domain is a valid Cisco WebEx domain, it prompts users to enter their Cisco WebEx credentials. The client then authenticates to the Cisco WebEx Messenger service and retrieves configuration and UC services configured in Cisco WebEx Org Admin.

If the client determines the domain is not a valid Cisco WebEx domain, it uses the results of the query to the name server to locate available services.

---

**Note**

The client will use any configured system proxies when sending the HTTP request to the CAS URL. Proxy support for this request has the following limitations:

- Proxy Authentication is not supported.
- Wildcards in the bypass list are not supported. Use example.com instead of *.example.com for example.

---

Cisco UDS SRV Record

In deployments with Cisco Unified Communications Manager version 9 and later, the client can automatically discover services and configuration with the _cisco-uds SRV record.

The following figure shows how the client uses the _cisco-uds SRV record.
1. The client queries the domain name server for SRV records.
2. The domain name server returns the \_cisco-uds SRV record.
3. The client locates the user's home cluster.
   As a result, the client can retrieve the device configuration for the user and automatically register telephony services.

**Important**

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

If you do not configure ILS, you must manually configure remote cluster information, similar to the Extension Mobility Cross Cluster (EMCC) remote cluster setup. For more information on remote cluster configurations, see the Cisco Unified Communications Manager Features and Services Guide.

4. The client retrieves the user's service profile.
   The user's service profile contains the addresses and settings for UC services and client configuration.
   The client also determines the authenticator from the service profile.
5. The client signs the user into the authenticator.
The following is an example of the _cisco-uds SRV record:

```
_cisco-uds._tcp.example.com SRV service location:
priority = 6
weight = 30
port = 8443
svr hostname = cucm3.example.com

_cisco-uds._tcp.example.com SRV service location:
priority = 2
weight = 20
port = 8443
svr hostname = cucm2.example.com

_cisco-uds._tcp.example.com SRV service location:
priority = 1
weight = 5
port = 8443
svr hostname = cucm1.example.com
```

Related Topics
Remote Cluster Configuration on Cisco Unified Communications Manager 10.0

**CUP Login SRV Record**

Cisco Jabber can automatically discover and connect to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service with the _cuplogin SRV record.

The following figure shows how the client uses the _cuplogin SRV record.

*Figure 7: CUP SRV Record Login Flow*

1. The client queries the domain name server for SRV records.
2. The name server returns the _cuplogin SRV record.

As a result, Cisco Jabber can locate the presence server and determine that Cisco Unified Presence is the authenticator.
3. The client prompts the user for credentials and authenticates to the presence server.

4. The client retrieves service profiles from the presence server.

Tip

The _cuplogin SRV record also sets the default server address on the Advanced Settings window.

The following is an example of the _cuplogin SRV record:

```plaintext
_cuplogin._tcp.example.com        SRV service location:
priority    = 8
weight      = 50
port        = 8443
svr hostname= cup3.example.com

_cuplogin._tcp.example.com        SRV service location:
priority    = 5
weight      = 100
port        = 8443
svr hostname= cup1.example.com

_cuplogin._tcp.example.com        SRV service location:
priority    = 7
weight      = 4
port        = 8443
svr hostname= cup2.example.com
```

**Manual Connection Settings**

Manual connection settings provide a fallback mechanism when Service Discovery is not used.

When you start Cisco Jabber, you can specify the authenticator and server address in the Advanced settings window. The client caches the server address to the local application configuration that loads on subsequent starts.

Cisco Jabber prompts users to enter these advanced settings on the initial start as follows:

- **On-Premises with Cisco Unified Communications Manager release 9.x and Later** — If the client cannot get the authenticator and server addresses from the service profile.

- **Cloud-Based or On-Premises with Cisco Unified Communications Manager release 8.x** — If you do not set the authenticator in the bootstrap file. The client also prompts users to enter server addresses in the Advanced settings window if you do not set server addresses in the bootstrap file or with SRV records.

Settings that you enter in the Advanced settings window take priority over any other sources including SRV records and bootstrap settings.

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

**Manual Connection Settings for On-Premises Deployments**

Users can set Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service as the authenticator and specify the server address in the Advanced settings window.
You can automatically set the default server address with the `_cuplogin` SRV record.

The following diagram illustrates how the client uses manual connection settings in on-premises deployments:

1. Users manually enter connection settings in the **Advanced settings** window.
2. The client authenticates to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.
3. The client retrieves service profiles from the presence server.

### Manual Connection Settings for On-Premises Deployments in Phone Mode

Users can set Cisco Unified Communications Manager as the authenticator and specify the following server addresses in the **Advanced settings** window:

- TFTP server
- CTI server
- CCMCIP server

The following diagram illustrates how the client uses manual connection settings in phone mode deployments:
1. Users manually enter connection settings in the Advanced settings window.

2. The client authenticates to Cisco Unified Communications Manager and gets configuration.

3. The client retrieves device and client configuration.

**Manual Connection Settings for Cloud-Based Deployments**

Users can set the Cisco WebEx Messenger service as the authenticator and specify the CAS URL for login in the Advanced settings window.

The following diagram illustrates how the client uses manual connection settings in cloud-based deployments:

1. Users manually enter connection settings in the Advanced settings window.
2. The client authenticates to the Cisco WebEx Messenger service.
3. The client retrieves configuration and services.

**Automatic Connection Setting for Service Discovery**

Users can select the **Automatic** option in the **Advanced settings** window to discover servers automatically. The Automatic option allows users change from manually setting the service connection details to using service discovery. For example, on the initial launch, you manually set the authenticator and specify a server address in the **Advanced settings** window.

The client always checks the cache for manual settings. The manual settings take higher priority over SRV records, and for Cisco Jabber for Windows, the bootstrap file. For this reason, if you decide to deploy SRV records and use service discovery, you override the manual settings from the initial launch.

**Installer Switches: Cisco Jabber for Windows**

When you install Cisco Jabber, you can specify the authenticator and server addresses. The installer saves these details to a bootstrap file. When users launch the client for the first time, it reads the bootstrap file. The bootstrap file takes priority if service discovery is deployed.

Bootstrap files provide a fallback mechanism for service discovery in situations where service discovery has not been deployed and where you do not want users to manually specify their connection settings.

The client only reads the bootstrap file on the initial launch. After the initial launch, the client caches the server addresses and configuration, and then loads from the cache on subsequent launches.

We recommend that you do not use a bootstrap file, and instead use service discovery, in on-premises deployments with Cisco Unified Communications Manager release 9.x and later.

**Bootstrap Settings for On-Premises Deployments**

The following table lists the argument values for various deployment types.

<table>
<thead>
<tr>
<th>Product Mode</th>
<th>Server Releases</th>
<th>Argument Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full UC (Default Mode)</td>
<td>Release 9 and later:</td>
<td>Use the following installer switches and values:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager</td>
<td>• AUTHENTICATOR=CUP</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager IM and Presence Service</td>
<td>• CUP_ADDRESS= &lt;presence_server_address&gt;</td>
</tr>
<tr>
<td>Full UC (Default Mode)</td>
<td>Release 8.x:</td>
<td>Use the following installer switches and values:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager</td>
<td>• AUTHENTICATOR=CUP</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Presence</td>
<td>• CUP_ADDRESS= &lt;presence_server_address&gt;</td>
</tr>
</tbody>
</table>
The following diagram illustrates how the client uses bootstrap settings in on-premises deployments:

When users start the client for the first time, the following occurs:

1. The client retrieves settings from the bootstrap file.
   The client starts in default mode and determines that Cisco Unified Communications Manager IM and Presence Service is the authenticator. The client also gets the address of the presence server, unless Service Discovery results dictate otherwise.

2. The client authenticates to Cisco Unified Communications Manager IM and Presence Service.
3. The client retrieves service profiles from the presence server.

**Bootstrap Settings for On-Premises Deployments in Phone Mode**

During installation, you set values for arguments as follows:

- Set `CUCM` as the value for `AUTHENTICATOR`.
- Set `phone_mode` as the value for `PRODUCT_MODE`.
- Set the TFTP server address as the value for TFTP.
- Set the CTI server address as the value for CTI.
- Set the CCMCIP server address as the value for CCMCIP.

Cisco Unified Communications Manager release 9.x and earlier—If you enable Cisco Extension Mobility, the Cisco Extension Mobility service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the *Feature and Services* guide for your Cisco Unified Communications Manager release.

The following diagram illustrates how the client uses bootstrap settings in phone mode deployments:

When users start the client for the first time, the following occurs:

1. The client retrieves settings from the bootstrap file.
The client starts in phone mode and determines that Cisco Unified Communications Manager is the authenticator. The client also gets the addresses for the TFTP and CTI servers, unless Service Discovery results dictate otherwise.

2. The client authenticates to Cisco Unified Communications Manager and gets configuration.
3. The client retrieves device and client configuration.

**Bootstrap Settings for Cloud-Based Deployments**

During installation, you set values for arguments as follows:

- Set `WEBEX` as the value for `AUTHENTICATOR`.

The following diagram illustrates how the client uses bootstrap settings in cloud-based deployments:

![Diagram](image)

When users start the client for the first time, the following occurs:

1. The client retrieves settings from the bootstrap file.
   
   The client starts in default mode and determines that the Cisco WebEx Messenger service is the authenticator, unless Service Discovery results dictate otherwise.

2. The client authenticates to the Cisco WebEx Messenger service.

3. The client retrieves configuration and services.
Cloud-Based SSO

In cloud-based deployments, Cisco Jabber supports SSO with the Cisco WebEx Messenger service. The following steps describe the login flow for cloud-based SSO after users start Cisco Jabber:

1. Cisco Jabber sends a login request to the Cisco WebEx Messenger service.
2. The Cisco WebEx Messenger service redirects Cisco Jabber to the domain where your identity provider resides.
3. Cisco Jabber follows the redirect and requests a login token from the identity provider.
4. The identity provider gives a login token to Cisco Jabber.
5. Cisco Jabber passes that login token to the Cisco WebEx Messenger service.

As a result, Cisco Jabber authenticates with the Cisco WebEx Messenger service. The following diagram illustrates the login flow for cloud-based SSO:

Figure 8: Cloud-Based SSO Login Flow
The identity provider must be Security Assertion Markup Language (SAML) compliant. Cisco Jabber has been tested with, and supports, the following products as identity providers:

- PingFederate
- Microsoft Active Directory Federation Services (ADFS)
- CA SiteMinder
- Oracle Access Manager

**Related Topics**

WebEx Single Sign-On Documentation
Command Line Arguments, on page 83

---

**Enable Cloud-Based SSO**

The client detects Cisco WebEx as the authentication source using one of the supported deployment methods: service discovery, installer switches, or manual configuration.

For Cisco Jabber for Windows, you must specify the `SSO_ORG_DOMAIN` argument during installation to enable Cisco Jabber for Windows for SSO in cloud-based deployments.

**Related Topics**

Command Line Arguments, on page 83

---

**Expressway for Mobile and Remote Access Deployments**

Expressway for Mobile and Remote Access for Cisco Unified Communications Manager allows users to access their collaboration tools from outside the corporate firewall without a VPN client. Using Cisco collaboration gateways, the client can connect securely to your corporate network from remote locations such as public Wi-Fi networks or mobile data networks.

You set up Expressway for Mobile and Remote Access as follows:

1. Set up servers to support Expressway for Mobile and Remote Access using Cisco Expressway-E and Cisco Expressway-C.*
   1. See the following documents to set up the Cisco Expressway servers:
      - *Cisco Expressway Basic Configuration Deployment Guide*
      - *Mobile and Remote Access via Cisco Expressway Deployment Guide*

     * If you currently deploy a Cisco TelePresence Video Communications Server (VCS) environment, you can set up Expressway for Mobile and Remote Access. For more information, see *Cisco VCS Basic Configuration (Control with Expressway) Deployment Guide* and *Mobile and Remote Access via Cisco VCS Deployment Guide*.

2. Add any relevant servers to the whitelist for your Cisco Expressway-C server to ensure that the client can access services that are located inside the corporate network.
To add a server to the Cisco Expressway-C whitelist, use the **HTTP server allow** setting. This list can include the servers on which you host voicemail or contact photos.

2. Configure an external DNS server that contains the `collab-edge` DNS SRV record to allow the client to locate the Expressway for Mobile and Remote Access server.

3. 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, ensure that you configure the Voice Services Domain. The Voice Services Domain allows the client to locate the DNS server that contains the `collab-edge` record.

---

### Important

In most cases, users can sign in to the client for the first time using Expressway for Mobile and Remote Access to connect to services from outside the corporate firewall. In the following cases, however, users must perform initial sign in while on the corporate network:

- If the voice services domain is different from the services domain. In this case, users must be inside the corporate network to get the correct voice services domain from the jabber-config.xml file.
- If the client needs to complete the CAPF enrollment process, which is required when using a secure or mixed mode cluster.

---

**Figure 9: How the Client Connects to the Expressway for Mobile and Remote Access**

The following diagram illustrates the architecture of an Expressway for Mobile and Remote Access environment.

![Expressway Architecture Diagram](image)

---

**Related Topics**

- Cisco Expressway Configuration Guides
- Cisco VCS Configuration Guides
Supported Services

The following table summarizes the services and functionality that are supported when the client uses Expressway for Mobile and Remote Access to remotely connect to Cisco Unified Communications Manager.

**Table 4: Summary of supported services for Expressway for Mobile and Remote Access**

<table>
<thead>
<tr>
<th>Service</th>
<th>Supported</th>
<th>Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Directory</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDS directory search</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>LDAP directory search</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Directory photo resolution</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>* Using HTTP white list on Cisco Expressway-C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intradomain federation</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>* Contact search support depends on the format of your contact IDs. For more information, see the note below.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interdomain federation</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Instant Messaging and Presence</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>On-premises</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cloud</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Chat</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Group chat</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>High Availability: On-premises deployments</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>File transfer: On-premises deployments</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>File transfer: Cloud deployments</td>
<td>X</td>
<td>Desktop clients, some file transfer features are supported for mobile clients.</td>
</tr>
<tr>
<td>Video desktop share - BFCP</td>
<td>X</td>
<td>(Cisco Jabber for mobile clients only support BFCP receive.)</td>
</tr>
</tbody>
</table>
### Supported Services

<table>
<thead>
<tr>
<th>Service</th>
<th>Supported</th>
<th>Unsupported</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audio and Video</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio and video calls</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>* Cisco Unified</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications Manager 9.1(2) and later</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deskphone control mode (CTI)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Remote Desktop Control</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Extend and connect</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Session persistency</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Early media</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Self Care Portal access</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Voicemail</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visual voicemail</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>* Using HTTP white list on Cisco Expressway-C</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cisco WebEx Meetings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>On-premises</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cloud</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cisco WebEx desktop share</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>Installation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installer update</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>* Using HTTP white list on Cisco Expressway-C</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Customization</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom HTML tabs</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>* Using HTTP white list on Cisco Expressway-C</td>
<td></td>
<td>(Desktop clients only)</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>End-to-end encryption</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Supported</td>
<td>Unsupported</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------</td>
<td>------------</td>
</tr>
<tr>
<td>CAPF enrollment</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Troubleshooting</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem report generation</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Problem report upload</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td><strong>High Availability (failover)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audio and Video services</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Voicemail services</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>IM and Presence services</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

**Directory**

When the client connects to services using Expressway for Mobile and Remote Access, it supports directory integration with the following limitations.

- **LDAP contact resolution** — The client cannot use LDAP for contact resolution when outside of the corporate firewall. Instead, the client must use UDS for contact resolution.

  When users are inside the corporate firewall, the client can use either UDS or LDAP for contact resolution. If you deploy LDAP within the corporate firewall, Cisco recommends that you synchronize your LDAP directory server with Cisco Unified Communications Manager to allow the client to connect with UDS when users are outside the corporate firewall.

- **Directory photo resolution** — To ensure that the client can download contact photos, you must add the server on which you host contact photos to the white list of your Cisco Expressway-C server. To add a server to Cisco Expressway-C white list, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.

- **Intradomain federation** — When you deploy intradomain federation and the client connects with Expressway for Mobile and Remote Access from outside the firewall, contact search is supported only when the contact ID uses one of the following formats:
  - sAMAccountName@domain
  - UserPrincipalName (UPN)@domain
  - EmailAddress@domain
  - employeeNumber@domain
  - telephoneNumber@domain

- **Interdomain federation using XMPP** — The client does not support interdomain federation with XMPP standard-based environments such as Google Talk when it connects with Expressway for Mobile and Remote Access from outside the firewall.
Instant Messaging and Presence

When the client connects to services using Expressway for Mobile and Remote Access, it supports instant messaging and presence with the following limitations.

File transfer — The client does not support file transfer including screen capture with Cisco Unified Communications Manager IM and Presence Service deployments. File Transfer is supported only with Cisco WebEx cloud deployments with desktop clients. Managed File Transfer is supported with Cisco Unified Communication IM and Presence when Cisco Jabber is connected to Cisco Unified services using Expressway. Peer-to-Peer files transfer is not supported.

Audio and Video Calling

When the client connects to services using Expressway for Mobile and Remote Access, it supports voice and video calling with the following limitations.

• Cisco Unified Communications Manager — Expressway for Mobile and Remote Access supports video and voice calling with Cisco Unified Communications Manager Version 9.1.2 and later. Expressway for Mobile and Remote Access is not supported with Cisco Unified Communications Manager Version 8.x.

• Deskphone control mode (CTI) — The client does not support deskphone control mode (CTI), including extension mobility.

• Extend and connect — The client cannot be used to:
  • Make and receive calls on a Cisco IP Phone in the office.
  • Perform mid-call control such as hold and resume on a home phone, hotel phone, or Cisco IP Phone in the office.

• Session Persistency — The client cannot recover from audio and video calls drop when a network transition occurs. For example, if a user starts a Cisco Jabber call inside their office and then they walk outside their building and lose Wi-Fi connectivity, the call drops as the client switches to use Expressway for Mobile and Remote Access.

• Early Media — Early Media allows the client to exchange data between endpoints before a connection is established. For example, if a user makes a call to a party that is not part of the same organization, and the other party declines or does not answer the call, Early Media ensures that the user hears the busy tone or is sent to voicemail.

  When using Expressway for Mobile and Remote Access, the user does not hear a busy tone if the other party declines or does not answer the call. Instead, the user hears approximately one minute of silence before the call is terminated.

• Self care portal access — Users cannot access the Cisco Unified Communications Manager Self Care Portal when outside the firewall. The Cisco Unified Communications Manager user page cannot be accessed externally.

  Cisco Expressway-E proxies all communications between the client and unified communications services inside the firewall. However, the Cisco Expressway-E does not proxy services that are accessed from a browser that is not part of the Cisco Jabber application.

Voicemail

Voicemail service is supported when the client connects to services using Expressway for Mobile and Remote Access.
To ensure that the client can access voicemail services, you must add the voicemail server to the white list of your Cisco Expressway-C server. To add a server to Cisco Expressway-C white list, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.

**Cisco WebEx Meetings**

When the client connects to services using Expressway for Mobile and Remote Access, it supports only cloud-based conferencing using Cisco WebEx Meetings Center.

The client cannot access the Cisco WebEx Meetings Server or join or start on-premises Cisco WebEx meetings.

**Installation**

When the client connects to services using Expressway for Mobile and Remote Access, it supports installer updates.

To ensure that the client can download installer updates, you must add the server that hosts the installer updates to the white list of your Cisco Expressway-C server. To add a server to the Cisco Expressway-C white list, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.

**Customization**

When the client connects to services using Expressway for Mobile and Remote Access, it supports custom HTML tab configuration for desktop clients.

To ensure that the client can download the custom HTML tab configuration, you must add the server that hosts the custom HTML tab configuration to the white list of your Cisco Expressway-C server. To add a server to the Cisco Expressway-C whitelist, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.

**Security**

When the client connects to services using Expressway for Mobile and Remote Access, it supports most security features with the following limitations.

- **Initial CAPF enrollment** — Certificate Authority Proxy Function (CAPF) enrollment is a security service that runs on the Cisco Unified Communications Manager Publisher that issues certificates to Cisco Jabber (or other clients). To successfully enrol for CAPF, the client must connect from inside the firewall or using VPN.

- **End-to-end encryption** — When users connect through Expressway for Mobile and Remote Access and participate in a call:
  - Media is encrypted on the call path between the Cisco Expressway-C and devices that are registered to the Cisco Unified Communications Manager using Expressway for Mobile and Remote Access.
• Media is not encrypted on the call path between the Cisco Expressway-C and devices that are registered locally to Cisco Unified Communications Manager, if either Cisco Jabber or an internal device is not configured with Encrypted security mode.

• Media is encrypted on the call path between the Expressway-C and devices that are registered locally to Cisco Unified Communications Manager, if both Cisco Jabber and internal device are configured with Encrypted security mode.

Troubleshooting

Problem report upload — When the desktop client connects to services using Expressway for Mobile and Remote Access, it cannot send problem reports because the client uploads problem reports over HTTP to a specified internal server.

To work around this issue, users can save the report locally and send the report in another manner.

High Availability (failover)

High Availability means that if the client fails to connect to the primary server, it fails over to a secondary server with little or no interruption to the service. In relation to high availability being supported on the Expressway for Mobile and Remote Access, high availability refers to the server for the specific service failing over to a secondary server (such as Instant Messaging and Presence), and not the Cisco Expressway-E server itself failing over.

Some services are available on the Expressway for Mobile and Remote Access that are not supported for high availability. This means that if users are connected to the client from outside the corporate network and the instant messaging and presence server fails over, the services will continue to work as normal. However, if the audio and video server or voicemail server fails over, those services will not work as the relevant servers do not support high availability.

Deployment in a Virtual Environment

You can deploy Cisco Jabber for Windows in virtual environments using the following software:

• Citrix XenDesktop 7.5
• Citrix XenDesktop 7.1
• Citrix XenDesktop 7.0
• Citrix XenDesktop 5.6
• Citrix XenApp 7.5 Enterprise Edition for Windows Server 2008 R2 Standard Service Pack 1 64 bit, published desktop
• Citrix XenApp 6.5 Feature Pack 1 Enterprise Edition for Windows Server 2008 R2 Standard Service Pack 1 64 bit, published desktop
• Citrix XenApp 6.5 Enterprise Edition for Windows Server 2008 R2 Standard Service Pack 1 64 bit, published desktop
• VMware Horizon View 6.0
• VMware Horizon View 5.3
• VMware Horizon View 5.2

**Supported Features**

- Instant messaging and presence with other Cisco Jabber clients
- Desk phone control
- Voicemail
- Presence integration with Microsoft Outlook 2007, 2010 and 2013

---

**Note**

Cisco Jabber credentials caching is not supported when using Cisco Jabber in non-persistent virtual deployment infrastructure (VDI) mode.

---

**Softphones in Virtual Environments**

Use Cisco Virtualization Experience Media Engine (VXME) for softphone calls in a virtual environment.

**Roaming Profiles**

The client stores user data such as user call history and configuration store cache on the local machine for use when the user next signs in. In virtual environments, users do not always access the same virtual desktop. To guarantee a consistent user experience, these files need to be accessible every time the client is launched.

To preserve the user's personal settings in a virtual environment when roaming between hosted virtual desktops, use dedicated profile management solutions from Citrix and VMware.

Citrix Profile Management is a profile solution for Citrix environments. In deployments with random hosted virtual desktop assignments, Citrix Profile Management synchronizes each user's entire profile between the system it is installed on and the user store.

VMware View Persona Management preserves user profiles and dynamically synchronizes them with a remote profile repository. VMware View Persona Management does not require the configuration of Windows roaming profiles and can bypass Windows Active Directory in the management of View user profiles. Persona Management enhances the functionality of existing roaming profiles.

You can specify which files and folders to omit from synchronization by adding them to an exclusion list. To include a subfolder within an excluded folder, add the subfolder to an inclusion list.

To preserve the user's personal settings, do not exclude the following directories:

- `AppData\Local\Cisco`
- `AppData\Local\Jabber\WerxCPP`
- `AppData\Roaming\Cisco`
- `AppData\Roaming\Jabber\WerxCPP`

**Client Information Storage**

The client stores user information in the following locations:

C:\Users\username\AppData\Local\Cisco\Unified Communications\Jabber\CSF

<table>
<thead>
<tr>
<th>Folder Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Contacts</td>
<td>Contact cache files</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>History</td>
<td>Call history and chat history</td>
</tr>
<tr>
<td>Photo cache</td>
<td>Caches the directory photos locally</td>
</tr>
</tbody>
</table>

C:\Users\username\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF

<table>
<thead>
<tr>
<th>Folder Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config</td>
<td>Maintains users' Jabber configuration files and stores configuration store cache</td>
</tr>
<tr>
<td>Credentials</td>
<td>Stores encrypted user name and password file</td>
</tr>
</tbody>
</table>

**Related Topics**

[Calendar Integration](#), on page 10
CHAPTER 6

Install Cisco Jabber

Review the options for installation and learn about different methods for installing Cisco Jabber. Understand the requirements for successful deployments before you start the installation procedure.

• Methods of Installation, on page 75
• Use the Command Line, on page 76
• Run the MSI Manually, on page 77
• Create a Custom Installer, on page 78
• Deploy with Group Policy, on page 81
• Command Line Arguments, on page 83
• Installer Properties, on page 94
• Supported Languages, on page 95
• Cisco Media Services Interface, on page 95
• Uninstall Cisco Jabber for Windows, on page 97

Methods of Installation

Cisco Jabber for Windows provides an MSI installation package. You must be logged in as an administrator to complete installation. You can use this installation package in the following ways:

Use the Command Line

Specify arguments in a command line window to set installation properties.

Choose this option if you plan to install multiple instances.

Run the MSI Manually

Run the MSI manually on the file system of the client workstation and then specify connection properties when you start the client.

Choose this option if you plan to install a single instance for testing or evaluation purposes.

Create a Custom Installer

Open the default installation package, specify the required installation properties, and then save a custom installation package.

Choose this option if you plan to distribute an installation package with the same installation properties.
Deploy with Group Policy

Install the client on multiple computers in the same domain.

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.

**Cisco Unified Communications Manager, Release 8.x in Default Mode**

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP CUP_ADDRESS=1.2.3.4
```

Where:

- `CLEAR=1` — Deletes any existing bootstrap file.
- `AUTHENTICATOR=CUP` — Sets Cisco Unified Presence as the authenticator.
- `CUP_ADDRESS=1.2.3.4` — Sets 1.2.3.4 as the IP address of the presence server.
- `/quiet` — Specifies a silent installation.

**Cisco Unified Communications Manager, Release 8.x in Phone Mode**

If you are integrating with UDS when you are installing in phone mode, you must first define the `<PresenceDomain>` parameter.

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 PRODUCT_MODE=Phone_Mode AUTHENTICATOR=CUCM TFTP=1.2.3.4 CTI=5.6.7.8
```
Where:

CLEAR=1 — Deletes any existing bootstrap file.
PRODUCT_MODE=Phone_Mode — Sets the client to phone mode.
AUTHENTICATOR=CUCM — Sets Cisco Unified Communications Manager as the authenticator.
TFTP=1.2.3.4 — Sets 1.2.3.4 as the IP address of the TFTP server that hosts the client configuration.
CTI=5.6.7.8 — Sets 5.6.7.8 as the IP address of the CTI server.
/quiet — Specifies a silent installation.

Cisco WebEx Messenger Service

msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=WEBEX
Where:

CLEAR=1 — Deletes any existing bootstrap file.
AUTHENTICATOR=WEBEX — Sets the Cisco WebEx Messenger service as the authenticator.
/quiet — Specifies a silent installation.

Cisco WebEx Messenger Service with SSO

msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=WEBEX
SSO_ORG_DOMAIN=example.com
Where:

CLEAR=1 — Deletes any existing bootstrap file.
AUTHENTICATOR=WEBEX — Sets the Cisco WebEx Messenger service as the authenticator.
SSO_ORG_DOMAIN=example.com — Sets example.com as the single sign-on (SSO) domain.
/quiet — Specifies a silent installation.

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

Step 1
Launch CiscoJabberSetup.msi.
The installation program opens a window to guide you through the installation process.

Step 2
Follow the steps to complete the installation process.

Step 3
Start Cisco Jabber for Windows.

Step 4
Select Manual setup and sign in.
The Advanced settings window opens.

Step 5
Specify values for the connection settings properties.

Step 6
Select Save.
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>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Get the Default Transform File, on page 78</td>
<td>You must have the default transform file to modify the installation package with Microsoft Orca.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Create Custom Transform Files, on page 79</td>
<td>Transform files contain installation properties that you apply to the installer.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Transform the Installer, on page 79</td>
<td>Apply a transform file to customize the installer.</td>
</tr>
</tbody>
</table>

**Related Topics**

Microsoft Windows SDK for Windows 7 and .NET Framework 4

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 79

**Related Topics**

Software Downloads
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 78

Procedure

Step 1  Start Microsoft Orca.
Step 2  Open CiscoJabberSetup.msi and then apply CiscoJabberProperties.msi.
Step 3  Specify values for the appropriate installer properties.
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 79

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 79

Procedure

Step 1  Start Microsoft Orca.

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  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.

Related Topics
   Installer Properties, on page 94

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>Step 1 Set a Language Code, on page 81</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>Step 2 Deploy the Client with Group Policy, on page 82</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.

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 82*

**Related Topics**

*Supported Languages, on page 95*

---

**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 81*

**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.

### Command Line Arguments

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

### Override Argument

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

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.

- 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.
- Cisco Unified Communications Manager, Release 8.x — You can specify phone mode during installation if you set Cisco Unified Communications Manager as the authenticator. The client reads the bootstrap file on the initial launch and determines it should start in phone mode. The client then gets Cisco Unified Communications Manager as the authenticator from the bootstrap file or manual settings. After the user signs in, the client does not require a restart.

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.

**Change Product Modes with Cisco Unified Communications Manager Version 8.x**
To change product modes with Cisco Unified Communications Manager version 8.x, you must reinstall Cisco Jabber for Windows to change the authenticator.

**Change Default Mode > Phone Mode**
Set the following arguments, at a minimum:
- CLEAR=1 to delete any existing bootstrap file.
- AUTHENTICATOR=CUCM to set the authenticator to Cisco Unified Communications Manager.
- PRODUCT_MODE=Phone_Mode to set phone mode as the product mode.

**Change Phone Mode > Default Mode**
Set the following arguments, at a minimum:
- CLEAR=1 to delete any existing bootstrap file.
- AUTHENTICATOR= one of the following:
  - CUP to set the authenticator to Cisco Unified Presence or Cisco Unified Communications Manager.
  - WEBEX to set the authenticator to the Cisco WebEx Messenger service.

**Authentication Arguments**
The following table describes 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>CUP</td>
<td>Specifies the source of authentication for the client. This value is used if Service Discovery fails.</td>
</tr>
<tr>
<td></td>
<td>CUCM</td>
<td>Set one of the following as the value:</td>
</tr>
<tr>
<td></td>
<td>Webex</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CUP—Cisco Unified Communications Manager IM and Presence Service. On-premises deployments in the default product mode. The default product mode can be either full UC or IM only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CUCM—Cisco Unified Communications Manager. On-premises deployments in phone mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Webex—Cisco Webex Messenger Service. Cloud-based or hybrid cloud-based deployments.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In on-premises deployments with Cisco Unified Communications Manager version 9.x and later, you should deploy the _cisco-uds SRV record. The client can then automatically determine the authenticator.</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>
<tr>
<td>TFTP</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 (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>
<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>
</tbody>
</table>
### Authentication Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| CTI        | IP address    | Sets the address of your CTI server. Specify this argument if:  
|            | Hostname      | • You set Cisco Unified Communications Manager as the authenticator.  
|            | FQDN          | • Users have desk phone devices and require a CTI server.  |
|            |               |                                                                                                                                          |
| CCMCIP     | IP address    | Sets the address of your CCMCIP server. Specify this argument if:  
|            | Hostname      | • You set Cisco Unified Communications Manager as the authenticator.  
|            | FQDN          | • The address of your CCMCIP server is not the same as the TFTP server address.  
|            |               | The client can locate the CCMCIP server with the TFTP server address if both addresses are the same.  
|            |               |                                                                                                                                          |
|            |               | Cisco Unified Communications Manager release 9.x and earlier—If you enable Cisco Extension Mobility, the **Cisco Extension Mobility** service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the *Feature and Services* guide for your **Cisco Unified Communications Manager** release. |
| SERVICES_DOMAIN | Domain       | Sets the value of the domain where the DNS SRV records for Service Discovery reside.  
|            |               | 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.  
|            |               | If this argument is not specified and Service Discovery fails, the user will be prompted for services domain information.  |
|            |               |                                                                                                                                          |
In Hybrid Deployments the domain required to discover Webex via CAS lookup may 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 will use 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:
- CUP
- Webex
- CUCM

Lists the services that you want Jabber to exclude from Service Discovery. For example, you may have done a trial with Webex which means that your company domain is registered on Webex, but you do not want Jabber users to authenticate using Webex. You want Jabber to authenticate with an on-premises CUP CUCM server. In this case set:

- `EXCLUDED_SERVICES=WEBEX`

Possible values are CUP, CUCM, Webex

To exclude more than one service, use comma separated values. For example, to exclude CUP and CUCM, specify: `EXCLUDED_SERVICES=CUP,CUCM`. To exclude all services, specify: `EXCLUDED_SERVICES=CUP,CUCM,WEBEX`

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

### 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 command line arguments that are common to all deployments:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LANGUAGE</td>
<td>LCID in decimal</td>
<td>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 <em>LCID for Languages</em> 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 uses the regional language for the current user as the default. From Release 11.1(1) onwards, 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 <strong>Control Panel &gt; Region and Language &gt; Change the date, time, or number format &gt; Formats tab &gt; Format dropdown.</strong></td>
</tr>
<tr>
<td>FORGOT_PASSWORD_URL</td>
<td>URL</td>
<td>Specifies the URL where users can reset lost or forgotten passwords. This argument is optional but recommended. <strong>Note</strong> In cloud-based deployments, you can specify a forgot password URL using the Cisco WebEx Administration Tool. However, the client cannot retrieve that forgot password URL until users sign in.</td>
</tr>
</tbody>
</table>
### Common Installation 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>Applies to Release 11.1(1) onwards. 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>TFTP_FILE_NAME</td>
<td>Filename</td>
<td>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. <strong>Remember</strong> You can specify group configuration files in the <strong>Cisco Support Field</strong> on the CSF device configuration on Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td>LOGIN_RESOURCE</td>
<td>WBX</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>MUT</td>
<td>• WBX—Users can sign in to one instance of Cisco Jabber for Windows at a time. Cisco Jabber for Windows appends the <strong>wbxconnect</strong> suffix to the user's JID. Users cannot sign in to any other Cisco Jabber client that uses the <strong>wbxconnect</strong> suffix.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>
### SSO Arguments

This section describes the command line arguments you can use to deploy Cisco Jabber for Windows with single sign on (SSO) capabilities.

#### Cloud-Based SSO Arguments

The arguments in the following table apply to cloud-based deployments only:

<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>
<tr>
<td>CLICK2X</td>
<td>DISABLE</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>
<tr>
<td>Telemetry_Enabled</td>
<td>true/false</td>
<td>Specifies whether analytics data is gathered. The default value is true. To improve your experience and product performance, Cisco Jabber may collect and send non-personally identifiable usage and performance data to Cisco. The aggregated data is used by Cisco to understand trends in how Jabber clients are being used and how they are performing. Full details on what analytics data Cisco Jabber does and does not collect can be found in the Cisco Jabber Supplement to Cisco’s On-Line Privacy Policy at <a href="http://www.cisco.com/web/siteassets/legal/privacy_02Jun10.html">http://www.cisco.com/web/siteassets/legal/privacy_02Jun10.html</a>.</td>
</tr>
<tr>
<td>Argument</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SSO_ORG_DOMAIN</td>
<td>Domain name</td>
<td>Specifies the domain name for the Cisco WebEx Org that contains the URL for the SSO service. Cisco Jabber for Windows uses this argument to retrieve the URL of the SSO service from the Org. When Cisco Jabber for Windows gets the SSO service URL, it can request login tokens to authenticate with Cisco WebEx Messenger. Note: You specify the URL for the SSO service as the value of the Customer SSO Service Login URL in the Cisco WebEx Administration Tool.</td>
</tr>
</tbody>
</table>

**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.
Supported Languages

Cisco Jabber for Windows 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.

The following table lists the languages that Cisco Jabber for Windows supports.

<table>
<thead>
<tr>
<th>Arabic</th>
<th>French</th>
<th>Romanian</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulgarian</td>
<td>Hebrew</td>
<td>Russian</td>
</tr>
<tr>
<td>Catalan</td>
<td>Hungarian</td>
<td>Serbian</td>
</tr>
<tr>
<td>Croatian</td>
<td>Italian</td>
<td>Slovak</td>
</tr>
<tr>
<td>Czech</td>
<td>Japanese</td>
<td>Slovakian</td>
</tr>
<tr>
<td>Danish</td>
<td>Korean</td>
<td>Swedish</td>
</tr>
<tr>
<td>German</td>
<td>Norwegian</td>
<td>Thai</td>
</tr>
<tr>
<td>Greek</td>
<td>Dutch</td>
<td>Turkish</td>
</tr>
<tr>
<td>English</td>
<td>Polish</td>
<td>Chinese - China</td>
</tr>
<tr>
<td>Spanish</td>
<td>Portuguese - Brazil</td>
<td>Chinese - Taiwan</td>
</tr>
<tr>
<td>Finnish</td>
<td>Portuguese - Portugal</td>
<td></td>
</tr>
</tbody>
</table>

Note: Cisco Jabber for Windows does not support Locale IDs for all sub-languages. For example, if you specify French - Canada, Cisco Jabber for Windows uses French - France.

See the following documentation for more information about Locale IDs:
- Microsoft Windows Locale Code Identifier (LCID) Reference
- Locale IDs Assigned by Microsoft

Related Topics
Microsoft Windows Locale Code Identifier (LCID) Reference
Locale IDs Assigned by Microsoft

Cisco Media Services Interface

Cisco Jabber for Windows supports Cisco Media Services Interface version 4.1.2 for Microsoft Windows 7 and later.

Cisco Jabber for Mac supports Cisco Media Services Interface version 4.0.2 or later.

Traffic Marking

Cisco Media Services Interface provides a service that works with Cisco Prime Collaboration Manager and Cisco Mediant-enabled routers to ensure that Cisco Jabber can send audio media and video media on your network with minimum latency or packet loss.
Before Cisco Jabber sends audio media or video media, it checks for Cisco Media Services Interface.

- If the service exists on the computer, Cisco Jabber provides flow information to Cisco Media Services Interface.
  
  The service then signals the network so that routers classify the flow and provide priority to the Cisco Jabber traffic.

- If the service does not exist, Cisco Jabber does not use it and sends audio media and video media as normal.

---

**Note**
Cisco Jabber checks for Cisco Media Services Interface for each audio call or video call.

---

**Desk Phone Video Capabilities**

You must install Cisco Media Services Interface to enable desk phone video capabilities. Cisco Media Services Interface provides a driver that enables Cisco Jabber for Windows to do the following:

- Discover the desk phone device.

  - Establish and maintain a connection to the desk phone device using the CAST protocol.

---

**Prepare Your Network**

To install Cisco Media Service Interface for traffic marking, you must prepare your network.

**Procedure**

1. **Step 1** Install Cisco Prime Collaboration manager.
2. **Step 2** Install routers or switches enabled for Cisco Medianet where appropriate.
3. **Step 3** Configure your network to handle the metadata attributes that Cisco Media Service Interface applies to applications.

Not all devices on your network must support Cisco Medianet. The first hop should prioritize traffic based on the metadata attributes from Cisco Media Service Interface. As the traffic traverses the network, all other devices should also prioritize that traffic unless you configure policies on those devices to handle the traffic differently.

---

**Install Cisco Media Services Interface**

**Procedure**

1. **Step 1** Download the Cisco Media Services Interface installation program from the download site on cisco.com.
Step 2

Install Cisco Media Services Interface on each computer on which you install Cisco Jabber. See the appropriate Cisco Medianet documentation for installing Cisco Media Services Interface.

Related Topics
- Download software
- Medianet Knowledge Base Portal

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

Step 1
Open a command line window.

Step 2
Enter the following command:

`msiexec.exe /x path_to_CiscoJabberSetup.msi`

For example,

`msiexec.exe /x C:\Windows\Installer\CiscoJabberSetup.msi /quiet`

Where `/quiet` specifies a silent uninstall.

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

Step 1
Find the product code.

a) Open the Microsoft Windows registry editor.
b) Locate the following registry key: `HKEY_CLASSES_ROOT\Installer\Products`c) Select `Edit > Find`.d) Enter Cisco Jabber in the **Find what** text box in the **Find** window and select **Find Next**.e) Find the value of the **ProductIcon** key.
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.
CHAPTER 7

Configure Cisco Jabber

Learn how to configure Cisco Jabber and review the configuration parameters you can set.

• Introduction to Client Configuration, on page 99
• Configure Service Profiles, on page 100
• Create and Host Client Configuration Files, on page 106
• Configuration File Structure, on page 113
• Summary of Configuration Parameters, on page 114
• Example Configuration, on page 116
• Client Parameters, on page 117
• Options Parameters, on page 119
• Phone Parameters, on page 122
• Policies Parameters, on page 125
• Presence Parameters, on page 132
• Service Credentials Parameters, on page 133
• Voicemail Parameters, on page 134
• Configure Automatic Updates, on page 134
• Problem Reporting, on page 136
• Custom Embedded Tabs, on page 136

Introduction to Client Configuration

Cisco Jabber can retrieve configuration settings from the following sources:

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

  Applies to on-premises deployments only.

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

  Applies to on-premises deployments only.
• Cisco Unified Communications Manager IM and Presence Service — You can enable instant messaging and presence capabilities and configure certain settings such as presence subscription requests.

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

Applies to on-premises deployments only.

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

Applies to on-premises and cloud-based deployments.

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

Applies to cloud-based deployments only.

## Configure Service Profiles

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

### Important

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

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

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

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

### Related Topics

Remote Cluster Configuration on Cisco Unified Communications Manager 10.0

## Set Parameters on Service Profile

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

### Parameters in Service Profiles

Learn which configuration parameters you can set in service profiles. Review the corresponding parameters in the client configuration file.
### IM and Presence Service Profile

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Product type** | Provides the source of authentication to Cisco Jabber and has the following values:  
  - Unified CM (IM and Presence Service) — Cisco Unified Communications Manager IM and Presence Service is the authenticator.  
  - WebEx (IM and Presence Service) — The Cisco WebEx Messenger service is the authenticator.  
  
  **Note** As of this release, the client issues an HTTP query in addition to the query for SRV records. The HTTP query allows the client to determine if it should authenticate to the Cisco WebEx Messenger service.  
  As a result of the HTTP query, the client connects to the Cisco WebEx Messenger service in cloud-based deployments before getting the _cisco-uds SRV record. Setting the value of the **Product type** field to **WebEx** may have no practical effect if the WebEx service has already been discovered by a CAS lookup.  
  - Not set — If the service profile does not contain an IM and presence service configuration, the authenticator is Cisco Unified Communications Manager. |
| **Primary server** | Specifies the address of your primary presence server.  
  - On-Premises Deployments — You should specify the fully qualified domain name (FQDN) of Cisco Unified Communications Manager IM and Presence Service.  
  - Cloud-Based Deployments — The client uses the following URL as default when you select **WebEx** as the value for the **Product type** parameter:  
    https://loginp.webexconnect.com/cas/auth.do  
    This default URL overrides any value that you set. |
Voicemail Profile

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

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

Conferencing Profile

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

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

Directory Profile

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

CTI Profile

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

<table>
<thead>
<tr>
<th>CTI Service Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTI server</td>
<td>Specifies connection settings for the CTI server.</td>
</tr>
</tbody>
</table>

Add Cisco Unified Communications Manager Services

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

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

**Step 2**  
Select **User Management > User Settings > UC Service**.  
The **Find and List UC Services** window opens.

**Step 3**  
Select **Add New**.  
The **UC Service Configuration** window opens.

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

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

---

**What to do next**

Add your UC services to service profiles.

---

**Create Service Profiles**

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

**Procedure**

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

**Step 2**  
Select **User Management > User Settings > Service Profile**.  
The **Find and List UC Services** window opens.

**Step 3**  
Select **Add New**.  
The **Service Profile Configuration** window opens.

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

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

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

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

---

**What to do next**

Apply service profiles to end user configuration.
Apply Service Profiles

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

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Open the <strong>Cisco Unified CM Administration</strong> interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select <strong>User Management &gt; End User</strong>. The <strong>Find and List Users</strong> window opens.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the appropriate search criteria to find existing users and then select a user from the list. The <strong>End User Configuration</strong> window opens.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Locate the <strong>Service Settings</strong> section.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select a service profile to apply to the user from the <strong>UC Service Profile</strong> drop-down list. <strong>Important Cisco Unified Communications Manager release 9.x only</strong>: If the user has only IIM and Presence Service capabilities (IM only), you must select <strong>Use Default</strong>. For IM only users, Cisco Unified Communications Manager release 9.x always applies the default service profile regardless of what you select from the <strong>UC Service Profile</strong> drop-down list.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Apply any other configuration as appropriate and then 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 CSFKenzi. The client retrieves CSFKenzi.cnf.xml from Cisco Unified Communications Manager when Adam signs in. The client then looks for the following in CSFKenzi.cnf.xml:

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

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

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

**Note**

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

Step 1  Associate users with devices.
   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.

Set Parameters on Phone Configuration for Desktop Clients

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

Enterprise Phone Configuration
   Applies to the entire cluster.

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

Common Phone Profile Configuration
   Applies to groups of devices and takes priority over the cluster configuration.

Cisco Unified Client Services Framework (CSF) Phone Configuration
   Applies to individual CSF devices and takes priority over the group configuration.

Parameters in Phone Configuration

The following table lists the configuration parameters you can set in the Product Specific Configuration Layout section of the phone configuration and maps corresponding parameters from the client configuration file:
<table>
<thead>
<tr>
<th>Desktop Client Settings Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Video Calling</strong></td>
<td>Enables or disables video capabilities.</td>
</tr>
<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><strong>File Types to Block in File Transfer</strong></th>
<th>Restricts users from transferring specific file types.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set a file extension as the value, for example, .exe.</td>
<td>Use a semicolon to delimit multiple values, for example, .exe;.msi;.rar;.zip</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Automatically Start in Phone Control</strong></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><strong>Jabber For Windows Software Update Server URL</strong></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>
<tbody>
<tr>
<td></td>
<td>In hybrid cloud-based deployments, you should use the Cisco WebEx Administration Tool to configure automatic updates.</td>
</tr>
</tbody>
</table>

| **Problem Report Server URL** | Specifies the URL for the custom script that allows users to submit problem reports. |

---

**Create and Host Client Configuration Files**

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

In cloud-based deployments, you should configure the client with the Cisco WebEx Administration Tool. However, you can optionally set up a TFTP server to configure the client with settings that are not available in Cisco WebEx Administration Tool.
In most environments, the client does not require any configuration to connect to services. You should create a configuration file only if you require custom content such as:

- Embedded HTML tabs
- Automatic updates
- Problem reporting
- User policies and options

Client Configuration Files

Before you deploy configuration files, review the differences between global and group configuration files. To successfully deploy configuration files you should also review the requirements for configuration files such as supported encoding.

Global Configuration Files

Global configuration files apply to all users. The client downloads the global configuration file from your TFTP server during the login sequence.

The default name for the global configuration file is `jabber-config.xml`.

Group Configuration Files

- Group configuration files are supported on Cisco Jabber for Windows and on Cisco Jabber for mobile devices.
- Group configuration files apply to subsets of users. Group configuration files take priority over global configuration files.

Group Configuration File Names

You specify the name of the group configuration files in the Cisco Support Field on the CSF, BOT, TCT, or TAB device configuration in Cisco Unified Communications Manager.

If you remove the name of the group configuration file in the CSF device configuration on Cisco Unified Communications Manager, the client detects the change, prompts the users to sign out, and loads the global configuration file. You can remove the name of the group configuration file in the CSF, BOT, TCT, or TAB device configuration by deleting the entire `configurationFile=group_configuration_file_name.xml` string or by deleting the group configuration filename from the string.

If users have desk phone devices only, use the following command line argument to specify unique names configuration files for different groups during installation:

```
TFTP_FILE_NAME
```
Configuration File Requirements

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

Tip
Open your configuration file in Microsoft Internet Explorer to see if any characters or entities are not valid.

- If Internet Explorer displays the entire XML structure, your configuration file does not contain invalid characters or entities.
- If Internet Explorer displays only part of the XML structure, your configuration file most likely contains invalid characters or entities.

Specify Your TFTP Server Address

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

Attention
If Cisco Jabber gets the _cisco-uds SRV record from a DNS query, it can automatically locate the user's home cluster. As a result, the client can also locate the Cisco Unified Communications Manager TFTP service.

You do not need to specify your TFTP server address if you deploy the _cisco-uds SRV record.

Specify Your TFTP Server on Cisco Unified Presence

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

Procedure

Step 1
Open the Cisco Unified Presence Administration interface.

Step 2
Select Application > Cisco Jabber > Settings.

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

The Cisco Jabber Settings window opens.
Step 3 Locate the fields to specify TFTP servers in one of the following sections, depending on your version of Cisco Unified Presence:
- Cisco Jabber Security Settings
- CUPC Global Settings

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

Step 5 Select Save.

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

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

Procedure

Step 1 Open the Cisco Unified CM IM and Presence Administration interface.
Step 2 Select Application > Legacy Clients > Settings.
The Legacy Client Settings window opens.
Step 3 Locate the Legacy Client Security Settings section.
Step 4 Specify the IP address of your primary and backup TFTP servers in the following fields:
- Primary TFTP Server
- Backup TFTP Server
- Backup TFTP Server

Step 5 Select Save.

Specify TFTP Servers in Phone Mode

If you deploy the client in phone mode you can provide the address of the TFTP server as follows:
- Users manually enter the TFTP server address when they start the client.
- You specify the TFTP server address during installation with the TFTP argument.
Specify TFTP Servers with the Cisco WebEx Administration Tool

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

**Procedure**

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

Create Global Configurations

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

**Before you begin**

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

**Procedure**

1. **Step 1** Create a file named **jabber-config.xml** with any text editor.
   - Use lowercase letters in the filename.
   - Use UTF-8 encoding.
2. **Step 2** Define the required configuration parameters in **jabber-config.xml**.
3. **Step 3** Host the group configuration file on your TFTP server.

   If your environment has multiple TFTP servers, ensure that the configuration file is the same on all TFTP servers.
Create Group Configurations

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

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

Before you begin

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

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

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

Procedure

Step 1

Create an XML group configuration file with any text editor.

The group configuration file can have any appropriate name; for example, jabber-groupa-config.xml.

Step 2

Define the required configuration parameters in the group configuration file.

Step 3

Add the group configuration file to applicable CSF devices.

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

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Open the Cisco Unified OS Administration interface on Cisco Unified Communications Manager.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Software Upgrades &gt; TFTP File Management.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Upload File.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Browse in the Upload File section.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select the configuration file on the file system.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Do not specify a value in the Directory text box in the Upload File section.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Select Upload File.</td>
</tr>
</tbody>
</table>

Restart Your TFTP Server

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

Procedure

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

What to do next

To verify that the configuration file is available on your TFTP server, open the configuration file in any browser. Typically, you can access the global configuration file at the following URL:

http://tftp_server_address:6970/jabber-config.xml
Configuration File Structure

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

**XML Declaration**

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

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

**Root Element**

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

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

**Group Elements**

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

**Group Elements and Parameters**

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

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Contains configuration parameters for the client.</td>
</tr>
<tr>
<td>Directory</td>
<td>Contains configuration parameters for directory integration.</td>
</tr>
<tr>
<td>Options</td>
<td>Contains configuration parameters for user options.</td>
</tr>
<tr>
<td>Phone</td>
<td>Contains configuration parameters for phone services.</td>
</tr>
<tr>
<td>Policies</td>
<td>Contains configuration parameters for policies.</td>
</tr>
<tr>
<td>Presence</td>
<td>Contains configuration parameters for presence options.</td>
</tr>
<tr>
<td>Voicemail</td>
<td>Contains configuration parameters for the voicemail service.</td>
</tr>
</tbody>
</table>

**XML Structure**

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

```xml
<Client>
  <parameter>value</parameter>
</Client>
<Directory>
  <parameter>value</parameter>
</Directory>
```
Summary of Configuration Parameters

The following table lists all the parameters you can include in the client configuration:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Group Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrtLogServerUrl</td>
<td>Client</td>
</tr>
<tr>
<td>UpdateUrl</td>
<td>Client</td>
</tr>
<tr>
<td>jabber-plugin-config</td>
<td>Client</td>
</tr>
<tr>
<td>Forgot_Password_URL</td>
<td>Client</td>
</tr>
<tr>
<td>Persistent_Chat_Enabled</td>
<td>Client</td>
</tr>
<tr>
<td>Mention_P2PChat</td>
<td>Client</td>
</tr>
<tr>
<td>Mention_GroupChat</td>
<td>Client</td>
</tr>
<tr>
<td>Mention_PersistentChat</td>
<td>Client</td>
</tr>
<tr>
<td>Disable_IM_History</td>
<td>Client</td>
</tr>
<tr>
<td>Set_Status_Away_On_Inactive</td>
<td>Options</td>
</tr>
<tr>
<td>Set_Status_Inactive_Timeout</td>
<td>Options</td>
</tr>
<tr>
<td>Set_Status_Away_On_Lock_OS</td>
<td>Options</td>
</tr>
<tr>
<td>StartCallWithVideo</td>
<td>Options</td>
</tr>
<tr>
<td>Start_Client_On_Start_OS</td>
<td>Options</td>
</tr>
<tr>
<td>AllowUserCustomTabs</td>
<td>Options</td>
</tr>
<tr>
<td>ShowContactPictures</td>
<td>Options</td>
</tr>
<tr>
<td>ShowOfflineContacts</td>
<td>Options</td>
</tr>
<tr>
<td>DockedWindowVisible</td>
<td>Options</td>
</tr>
<tr>
<td>DockedWindowPosition</td>
<td>Options</td>
</tr>
<tr>
<td>DeviceAuthenticationPrimaryServer</td>
<td>Phone</td>
</tr>
<tr>
<td>DeviceAuthenticationBackupServer</td>
<td>Phone</td>
</tr>
<tr>
<td>Parameter</td>
<td>Group Element</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>TftpServer1</td>
<td>Phone</td>
</tr>
<tr>
<td>TftpServer2</td>
<td>Phone</td>
</tr>
<tr>
<td>CtiServer1</td>
<td>Phone</td>
</tr>
<tr>
<td>CtiServer2</td>
<td>Phone</td>
</tr>
<tr>
<td>useCUCMGroupForCti</td>
<td>Phone</td>
</tr>
<tr>
<td>CcmcipServer1</td>
<td>Phone</td>
</tr>
<tr>
<td>CcmcipServer2</td>
<td>Phone</td>
</tr>
<tr>
<td>Meeting_Server_Address</td>
<td>Phone</td>
</tr>
<tr>
<td>Meeting_Server_Address_Backup</td>
<td>Phone</td>
</tr>
<tr>
<td>Meeting_Server_Address_Backup2</td>
<td>Phone</td>
</tr>
<tr>
<td>EnableVideo</td>
<td>Policies</td>
</tr>
<tr>
<td>InitialPhoneSelection</td>
<td>Policies</td>
</tr>
<tr>
<td>UserDefinedRemoteDestinations</td>
<td>Policies</td>
</tr>
<tr>
<td>enableLocalAddressBookSearch</td>
<td>Policies</td>
</tr>
<tr>
<td>EnableAccessoriesManager</td>
<td>Policies</td>
</tr>
<tr>
<td>BlockAccessoriesManagerPlugins</td>
<td>Policies</td>
</tr>
<tr>
<td>ForceFontSmoothing</td>
<td>Policies</td>
</tr>
<tr>
<td>Screen_Capture_ENABLED</td>
<td>Policies</td>
</tr>
<tr>
<td>File_Transfer_ENABLED</td>
<td>Policies</td>
</tr>
<tr>
<td>Disallowed_File_Transfer_TYPES</td>
<td>Policies</td>
</tr>
<tr>
<td>EnableBFCPVideoDesktopShare</td>
<td>Policies</td>
</tr>
<tr>
<td>Meetings_ENABLED</td>
<td>Policies</td>
</tr>
<tr>
<td>Telephony_ENABLED</td>
<td>Policies</td>
</tr>
<tr>
<td>Voicemail_ENABLED</td>
<td>Policies</td>
</tr>
<tr>
<td>EnableTelProtocolHandler</td>
<td>Policies</td>
</tr>
<tr>
<td>EnableSaveChatToFile</td>
<td>Policies</td>
</tr>
<tr>
<td>EnableSIPURIDialling</td>
<td>Policies</td>
</tr>
<tr>
<td>DirectoryURI</td>
<td>Policies</td>
</tr>
<tr>
<td>ForceC2XDirectoryResolution</td>
<td>Policies</td>
</tr>
<tr>
<td>ServiceDiscoveryExcludedServices</td>
<td>Policies</td>
</tr>
<tr>
<td>VoiceServicesDomain</td>
<td>Policies</td>
</tr>
<tr>
<td>LoginResource</td>
<td>Presence</td>
</tr>
</tbody>
</table>
Example Configuration

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

```xml
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Client>
    <PrtLogServerUrl>http://server_name:port/path/prt_script.php</PrtLogServerUrl>
    <jabber-plugin-config>
      <browser-plugin>
        <page refresh="true" preload="true">
          <tooltip>Cisco</tooltip>
          <icon>http://www.cisco.com/web/fw/i/logo.gif</icon>
          <url>www.cisco.com</url>
        </page>
      </browser-plugin>
    </jabber-plugin-config>
  </Client>
  <Options>
    <Set_Status_Inactive_Timeout>20</Set_Status_Inactive_Timeout>
    <StartCallWithVideo>false</StartCallWithVideo>
  </Options>
  <Policies>
    <Disallowed_File_Transfer_Types>.exe;.msi</Disallowed_File_Transfer_Types>
  </Policies>
  <Directory>
    <PrimaryServerName>dir.example.com</PrimaryServerName>
    <SearchBase1>ou=staff,dc=example,dc=com</SearchBase1>
    <ConnectionUsername>ad_jabber_access@example.com</ConnectionUsername>
    <ConnectionPassword>jabber</ConnectionPassword>
    <PhotoUriSubstitutionEnabled>True</PhotoUriSubstitutionEnabled>
    <PhotoUriWithToken>http://example.com/photo/sAMAccountName.jpg</PhotoUriWithToken>
  </Directory>
</config>
```
Client Parameters

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrtLogServerUrl</td>
<td>URL</td>
<td>Specifies the custom script for submitting problem reports.</td>
</tr>
<tr>
<td>UpdateUrl</td>
<td>URL</td>
<td>Specifies the URL to the automatic updates XML definition file on your HTTP server. The client uses this URL to retrieve the update XML file. In hybrid cloud-based deployments, you should use the Cisco WebEx Administration Tool to configure automatic updates.</td>
</tr>
<tr>
<td>jabber-plugin-config</td>
<td>Plug-in definition</td>
<td>Contains plug-in definitions such as custom embedded tabs that display HTML content.</td>
</tr>
<tr>
<td>Forgot_Password_URL</td>
<td>URL</td>
<td>Specifies the URL of your web page for users to reset or retrieve forgotten passwords. In hybrid cloud-based deployments, you should use the Cisco WebEx Administration Tool to direct users to the web page to reset or retrieve forgotten passwords.</td>
</tr>
<tr>
<td>Persistent_Chat_Enabled</td>
<td>true/false</td>
<td>Specifies whether the Persistent Chat feature is available in the client. true: If the value is set to true, the Persistent Chat interface is shown in the client. false (default): The default value is assumed if the setting is not present in the configuration file.</td>
</tr>
<tr>
<td>Mention_P2PChat</td>
<td>true/false</td>
<td>Specifies whether mentions are enabled in person to person chat. true (default): Enables mentions in person to person chat. false: Disables mentions in person to person chat.</td>
</tr>
<tr>
<td>Mention_GroupChat</td>
<td>true/false</td>
<td>Specifies whether mentions are enabled in group chat. true (default): Enables mentions in group chat. false: Disables mentions in group chat.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mention_PersistentChat</td>
<td>true</td>
<td>Specifies whether mentions are enabled in persistent chat.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td>true (default)</td>
<td>Enables mentions in persistent chat.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>Disables mentions in persistent chat.</td>
</tr>
<tr>
<td>Disable_IM_History</td>
<td>true</td>
<td>Specifies whether to retain chat history after participants close the chat window.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td>true (default)</td>
<td>Note: This parameter is not available for IM-only deployments.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>Retain chat history:</td>
</tr>
<tr>
<td></td>
<td>true</td>
<td>• After participants close the chat window.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>• Until the participants sign out.</td>
</tr>
<tr>
<td></td>
<td>true</td>
<td>If the participants re-open the chat window, the last 99 messages show.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>Message archiving should be disabled on the server.</td>
</tr>
<tr>
<td>CachePasswordMobile</td>
<td>true</td>
<td>Specifies whether the password is remembered or not on the client side.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td>true (default)</td>
<td>The password is prefilled and Automatic sign-in is shown.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>Users can allow the client to cache their password.</td>
</tr>
<tr>
<td></td>
<td>true</td>
<td>This option allows users to automatically sign in when the client starts.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>After the client successfully registers to the Cisco Unified Communications Manager, the password field is empty and Automatic sign-in is not shown.</td>
</tr>
<tr>
<td></td>
<td>true</td>
<td>Users cannot allow the client to cache their password.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>Users must enter their password each time the client starts.</td>
</tr>
<tr>
<td></td>
<td>true</td>
<td>Note: The client displays Automatic sign-in on first sign-in, or if the user clears the application data.</td>
</tr>
</tbody>
</table>
Options Parameters

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set_Status_Away_On_Inactive</td>
<td>true</td>
<td>Specifies if the availability status changes to <code>Away</code> when users are inactive.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>true (default)</strong></td>
<td>Availability status changes to <code>Away</code> when users are inactive.</td>
</tr>
<tr>
<td></td>
<td><strong>false</strong></td>
<td>Availability status does not change to <code>Away</code> when users are inactive.</td>
</tr>
<tr>
<td>Set_Status_Inactive_Timeout</td>
<td>Number of minutes</td>
<td>Sets the amount of time, in minutes, before the availability status changes to <code>Away</code> if users are inactive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 15.</td>
</tr>
<tr>
<td>Set_Status_Away_On_Lock_OS</td>
<td>true</td>
<td>Specifies if the availability status changes to <code>Away</code> when users lock their operating systems.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>true (default)</strong></td>
<td>Availability status changes to <code>Away</code> when users lock their operating systems.</td>
</tr>
<tr>
<td></td>
<td><strong>false</strong></td>
<td>Availability status does not change to <code>Away</code> when users lock their operating systems.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>StartCallWithVideo</td>
<td>true</td>
<td>Specifies how calls start when users place calls. Calls can start with audio only or audio and video.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>true (default)</strong></td>
<td>Calls always start with audio and video.</td>
</tr>
<tr>
<td></td>
<td><strong>false</strong></td>
<td>Calls always start with audio only.</td>
</tr>
<tr>
<td>Important</td>
<td></td>
<td>Server settings take priority over this parameter in the client configuration file. However, if users change the default option in the client user interface, that setting takes priority over both the server and client configurations.</td>
</tr>
<tr>
<td>Configure this setting on the server as follows:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cisco Unified Presence</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Open the <strong>Cisco Unified Presence Administration</strong> interface.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Select <strong>Application &gt; Cisco Jabber &gt; Settings</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Select or clear the <strong>Always begin calls with video muted</strong> parameter and then select <strong>Save</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cisco Unified Communications Manager version 9.x and higher</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Open the <strong>Cisco Unified CM Administration interface</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Select <strong>System &gt; Enterprise Parameters</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Set a value for the <strong>Never Start Call with Video</strong> parameter and then select <strong>Save</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Start_Client_On_Start_OS</td>
<td>true</td>
<td>Specifies if the client starts automatically when the operating system starts.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>true</strong></td>
<td>The client starts automatically.</td>
</tr>
<tr>
<td></td>
<td><strong>false (default)</strong></td>
<td>The client does not start automatically.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AllowUserCustomTabs</td>
<td>true/false</td>
<td>Specifies if users can create their own custom embedded tabs.</td>
</tr>
<tr>
<td></td>
<td>true (default)</td>
<td>Users can create custom embedded tabs.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>Users cannot create custom embedded tabs.</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>This parameter affects only custom embedded tabs that users create.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If you allow users to create custom embedded tabs, they cannot modify or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>remove the tabs that you define in the client configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If you do not allow users to create custom embedded tabs, the tabs that</td>
</tr>
<tr>
<td></td>
<td></td>
<td>you define are still available to users.</td>
</tr>
<tr>
<td>ShowContactPictures</td>
<td>true/false</td>
<td>Specifies if contact pictures display in the contact list.</td>
</tr>
<tr>
<td></td>
<td>true (default)</td>
<td>Contact pictures display in the contact list.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>Contact pictures do not display in the contact list.</td>
</tr>
<tr>
<td>ShowOfflineContacts</td>
<td>true/false</td>
<td>Specifies if offline contacts display in the contact list.</td>
</tr>
<tr>
<td></td>
<td>true (default)</td>
<td>Offline contacts display in the contact list.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>Offline contacts do not display in the contact list.</td>
</tr>
<tr>
<td>DockedWindowVisible</td>
<td>TRUE/FALSE</td>
<td>Specifies if the docked window displays when the client starts.</td>
</tr>
<tr>
<td></td>
<td>true (default)</td>
<td>The docked window displays when the client starts.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>The docked window does not display when the client starts.</td>
</tr>
</tbody>
</table>
### Phone Parameters

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DockedWindowPosition</td>
<td>TopCenter</td>
<td>Sets the position of the docked window on the user's screen.</td>
</tr>
<tr>
<td></td>
<td>TopLeft</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TopRight</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>TopCenter (default)</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The position of the docked window is at the top center of the screen.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>TopLeft</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The position of the docked window is at the top left of the screen.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>TopRight</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The position of the docked window is at the top right of the screen.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeviceAuthenticationPrimaryServer</td>
<td>Hostname</td>
<td>Specifies the address of the primary instance of Cisco Unified Communications Manager to which users authenticate in phone mode deployments. Set one of the following as the value:</td>
</tr>
<tr>
<td></td>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FQDN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hostname (hostname)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IP address (123.45.254.1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FQDN (hostname.domain.com)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This parameter can only be used in Cisco Jabber 9.6 and 9.7.</td>
</tr>
</tbody>
</table>

<p>| DeviceAuthenticationBackupServer | Hostname       | Specifies the address of the backup instance of Cisco Unified Communications Manager to which users authenticate in phone mode deployments. Set one of the following as the value: |
|                                  | IP address     |                                                                             |
|                                  | FQDN           |                                                                             |
|                                  |                | • Hostname (hostname)                                                       |
|                                  |                | • IP address (123.45.254.1)                                                 |
|                                  |                | • FQDN (hostname.domain.com)                                                |
|                                  |                | This parameter can only be used in Cisco Jabber 9.6 and 9.7.                |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| TftpServer1 | Hostname, IP address, FQDN | Specifies the address of the primary Cisco Unified Communications Manager TFTP service where device configuration files reside. Set one of the following as the value:  
  - Hostname (*hostname*)  
  - IP address (*123.45.254.1*)  
  - FQDN (*hostname.domain.com*)  
  You should set this parameter in the client configuration only if:  
  - You deploy the client in phone mode.  
  - The TFTP server address for the device configuration is different to the TFTP server address for the client configuration.  
  During installation, you should set the address of the TFTP server where the client configuration file resides with the following argument: TFTP. |
<p>| TftpServer2 | Hostname, IP address, FQDN | Specifies the address of the secondary Cisco Unified Communications Manager TFTP service. This parameter is optional. |
| CtiServer1  | Hostname, IP address, FQDN | Specifies the address of the primary CTI server. You should specify a CTI server address in the client configuration if users have desk phone devices. |
| CtiServer2  | Hostname, IP address, FQDN | Specifies the address of the secondary CTI server. This parameter is optional. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| useCUCMGroupForCti         | true     | Specifies if the Cisco Unified CM Group handles load balancing for CTI servers. Set one of the following values: true.
|                            | false    | The Cisco Unified CM Group does not handle CTI load balancing.              |
|                            |          | You should set this value in phone mode deployments only. In full UC mode, the presence server automatically handles CTI load balancing. false (default)
| CcmcipServer1              | Hostname | Specifies the address of the primary CCMCIP server. This parameter is required: |
|                            | IP address| • Only if the address of your CCMCIP server is not the same as the TFTP server address. |
|                            | FQDN     | If the address of the CCMCIP server is the same as the TFTP server address, the client can use the TFTP server address to connect to the CCMCIP server. |
|                            |          | • In deployments with Cisco Unified Communications Manager version 8. |
|                            |          | In deployments with Cisco Unified Communications Manager version 9 and higher, the client can discover the CCMCIP server if you provision the _cisco-uds SRV record. |
|                            |          | Cisco Unified Communications Manager release 9.x and earlier—If you enable Cisco Extension Mobility, the Cisco Extension Mobility service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the Feature and Services guide for your Cisco Unified Communications Manager release. |
| CcmcipServer2              | Hostname | Specifies the address of the secondary CCMCIP server. This parameter is optional. |
|                            | IP address|                                                                             |
|                            | FQDN     |                                                                             |
### Policies Parameters

Policies parameters let you control specific client functionality.

#### On-Premises Policies

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen_Capture_Enabled</td>
<td>true</td>
<td>Specifies if users can take screen captures.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td><strong>true (default)</strong></td>
<td></td>
<td><strong>true (default)</strong> Users can take screen captures.</td>
</tr>
<tr>
<td><strong>false</strong></td>
<td></td>
<td><strong>false</strong> Users cannot take screen captures.</td>
</tr>
</tbody>
</table>

---

**Parameter**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meeting_Server_Address</td>
<td>Cisco WebEx meetings site URL</td>
<td>Specifies the primary Cisco WebEx meeting site URL for users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The client populates this meeting site in the user's host account on the <strong>Options</strong> window. Users can enter their credentials to set up the host account and access their Cisco WebEx meetings, if the meeting site requires credentials. <strong>Important</strong> If you specify an invalid meeting site, users cannot add, or edit, any meetings sites in the client user interface. This parameter is optional.</td>
</tr>
<tr>
<td>Meeting_Server_Address_Backup</td>
<td>Cisco WebEx meetings site URL</td>
<td>Specifies the secondary Cisco WebEx meeting site URL for users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This parameter is optional.</td>
</tr>
<tr>
<td>Meeting_Server_Address_Backup2</td>
<td>Cisco WebEx meetings site URL</td>
<td>Specifies the tertiary Cisco WebEx meeting site URL for users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This parameter is optional.</td>
</tr>
</tbody>
</table>

**Related Topics**

[TFTP Server Address](#), on page 89
### Common Policies

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| File_Transfer_Enabled         | true/false  | Specifies if users can transfer files to each other.  
  **true** *(default)*  
  Users can transfer files to each other.  
  **false**  
  Users cannot transfer files to each other. |
| Disallowed_File_Transfer_Types | File extension | Restricts users from transferring specific file types.  
  Set file extensions as the value, for example, `.exe`.  
  Use a semicolon to delimit multiple file extensions, for example, `.exe;.msi;.rar;.zip`. |

**Related Topics**

- [Common Policies](#), on page 126
- [Cisco WebEx Policies](#), on page 132
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserDefinedRemoteDestinations</td>
<td>true</td>
<td>Lets users add, edit, and delete remote destinations through the client interface. Use this parameter to change the default behavior when you provision Extend and Connect capabilities. By default, if a user's device list contains only a CTI remote device, the client does not let that user add, edit, or delete remote destinations. This occurs to prevent users from modifying dedicated remote devices that you assign. However, if the user's device list contains a software device or a desk phone device, the client lets users add, edit, and delete remote destinations. <strong>true</strong> Users can add, edit, and delete remote destinations. <strong>false (default)</strong> Users cannot add, edit, and delete remote destinations.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>enableLocalAddressBookSearch</td>
<td>true</td>
<td>Lets users search for and add local Microsoft Outlook contacts to their contact lists. <strong>true (default)</strong> Users can search for and add local contacts to their contact lists. <strong>false</strong> Users cannot search for or add local contacts to their contact lists.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>EnableAccessoriesManager</td>
<td>true</td>
<td>Enables the accessories API in the client. This API lets accessory vendors create plugins to enable call management functionality for devices such as headsets. <strong>true (default)</strong> Enable the accessories API. <strong>false</strong> Disable the accessories API.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td>BlockAccessoriesManagerPlugins</td>
<td>Plugin library</td>
<td>Disables specific Accessories Manager plugins from third party vendors such as Jabra or Logitech. You should set the name of the plugin DLL file as the value. Use a comma to separate multiple values, for example, on Microsoft Windows: <code>&lt;BlockAccessoriesManagerPlugins&gt;</code> JabraJabberPlugin.dll, lucpcisco.dll &lt;/BlockAccessoriesManagerPlugins&gt; There is no default value.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>ForceFontSmoothing</td>
<td>true</td>
<td>Specifies if the client applies anti-aliasing to smooth text.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>true (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The client applies anti-aliasing to text.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The operating system applies anti-aliasing to text.</td>
</tr>
<tr>
<td>EnableBFCPVideoDesktopShare</td>
<td>true</td>
<td>Enables BFCP video desktop sharing capabilities.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>true (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enables BFCP video desktop sharing on the client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disables BFCP video desktop sharing.</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>BFCP video desktop sharing is enabled on the server as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- On Cisco Unified Communications Manager version 8.x and lower, you must select the Allow Presentation Sharing using BFCP checkbox.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- On Cisco Unified Communications Manager version 9.x and higher, BFCP video desktop sharing is enabled by default.</td>
</tr>
<tr>
<td>MeetingsEnabled</td>
<td>true</td>
<td>Enables meetings capabilities in the client. Works in conjunction with the CalendarIntegrationType parameter.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>true (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enables meetings capabilities, allowing you to create meetings and get reminders to join meetings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>false</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disables meetings capabilities and user interface.</td>
</tr>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Value</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CalendarIntegrationType</td>
<td>0</td>
<td>This parameter works in conjunction with the Meetings_Enabled parameter.</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Disables calendar integration in the Meetings tab of the client user interface. If you disable this parameter, the Meetings tab in the client is empty, but the Meetings tab remains on the hub window.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 Enables calendar integration in the Meetings tab of the client user interface.</td>
</tr>
<tr>
<td>Telephony_Enabled</td>
<td>true</td>
<td>Enables audio and video capabilities and user interface in the client.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>true (default) Enables audio and video capabilities and user interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>false Disables audio and video capabilities and user interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you are upgrading to this release, and your client is enabled for IM-only mode, then you must set this parameter to false. If you do not set this parameter in IM-only mode deployments, then users may see disabled telephony capabilities on their user interface.</td>
</tr>
<tr>
<td>Voicemail_Enabled</td>
<td>true</td>
<td>Enables voicemail capabilities and user interface in the client.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>true (default) Enables voicemail capabilities and user interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>false Disables voicemail capabilities and user interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you are upgrading to this release, and your client is enabled for IM-only mode, then you must set this parameter to false. If you do not set this parameter in IM-only mode deployments, then users may see disabled telephony capabilities on their user interface.</td>
</tr>
<tr>
<td>EnableTelProtocolHandler</td>
<td>true</td>
<td>Specifies if the client registers as the protocol handler for the tel: URI.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>true (default) The client registers as the protocol handler for the tel: URI.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>false The client does not register as the protocol handler for the tel: URI.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EnableSaveChatToFile</td>
<td>true</td>
<td>Allows users to save their chats to the file system as HTML.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>Users cannot save their chats to file.</td>
</tr>
<tr>
<td></td>
<td><strong>true (default)</strong></td>
<td>Users can save their chats to file.</td>
</tr>
<tr>
<td></td>
<td><strong>false</strong></td>
<td>Users cannot save their chats to file.</td>
</tr>
<tr>
<td>EnableSIPURIDialling</td>
<td>true</td>
<td>Enables URI dialing with Cisco Jabber and allows users to make calls with URIs.</td>
</tr>
<tr>
<td></td>
<td><strong>true</strong></td>
<td>Users can make calls with URIs.</td>
</tr>
<tr>
<td></td>
<td><strong>false (default)</strong></td>
<td>Users cannot make calls with URIs.</td>
</tr>
<tr>
<td>DirectoryURI</td>
<td>Directory attribute</td>
<td>Specifies the directory attribute that holds the SIP URI for users.</td>
</tr>
<tr>
<td></td>
<td><strong>On-Premises Deployments</strong></td>
<td>Set one of the following as the value:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• mail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• msRTCSIP-PrimaryUserAddress</td>
</tr>
<tr>
<td></td>
<td><strong>Cloud-Based Deployments</strong></td>
<td>Set one of the following as the value:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• mail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• imaddress</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• workphone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• homephone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• mobilephone</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong></td>
<td>The value you specify must match the directory URI setting for users in Cisco Unified Communications Manager or the Cisco WebEx Administration Tool.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ForceC2XDirectoryResolution</td>
<td>true</td>
<td>Specifies if the client queries the directory to resolve contact information when users perform click-to-x actions.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>true (default)</strong></td>
<td>The client queries the directory when users perform click-to-x actions.</td>
</tr>
<tr>
<td></td>
<td><strong>false</strong></td>
<td>The client does not query the directory for click-to-x actions.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>This parameter does not take effect when users connect to the corporate network through Expressway for Mobile and Remote Access. In this case, UDS provides contact resolution and the client cannot query the directory.</td>
</tr>
<tr>
<td>ServiceDiscoveryExcludedServices</td>
<td>WEBEX, CUCM, CUP</td>
<td>Specifies whether to exclude certain services from Service Discovery.</td>
</tr>
<tr>
<td></td>
<td><strong>WEBEX</strong></td>
<td>When you set this value, the client:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Does not perform CAS lookup</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Looks for _cisco-uds, _cuplogin, and _collab-edge</td>
</tr>
<tr>
<td></td>
<td><strong>CUCM</strong></td>
<td>When you set this value, the client:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Does not look for _cisco_uds</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Looks for _cuplogin and _collab-edge</td>
</tr>
<tr>
<td></td>
<td><strong>CUP</strong></td>
<td>When you set this value, the client:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Does not look for _cuplogin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Looks for _cisco-uds_collab-edge</td>
</tr>
<tr>
<td></td>
<td><strong>You can specify multiple, comma-separated values to exclude multiple services. For example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;ServiceDiscoveryExcludedServices&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>WEBEX, CUCM</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;/ServiceDiscoveryExcludedServices&gt;</code></td>
</tr>
</tbody>
</table>
Cisco WebEx Policies

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

Related Topics
- On-Premises Policies, on page 125
- Common Policies, on page 126
- Using policy actions available in Cisco WebEx

Presence Parameters

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoginResource</td>
<td>multiResource</td>
<td>Controls user log in to multiple client instances.</td>
</tr>
<tr>
<td></td>
<td>wbxconnect</td>
<td>multiResource (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Users can log in to multiple instances of the client at the same time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wbxconnect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Users can log in to one instance of the client at a time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The client appends the wbxconnect suffix to the user's JID. Users cannot log in to any other Cisco Jabber client that uses the wbxconnect suffix.</td>
</tr>
</tbody>
</table>
Service Credentials Parameters

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

### Voicemail Service Credentials

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoiceMailService_UseCredentialsFrom</td>
<td>phone</td>
<td>Specifies that the client uses the phone service credentials to access voicemail services. Ensure the user's phone service credentials match their voicemail service credentials. If you set this configuration, users cannot specify voicemail service credentials in the client interface. This parameter is not set by default. You should set this parameter in the following deployments only:   - Hybrid cloud-based deployments.   - Phone mode deployments. In on-premises deployments, you should set the credentials source for voicemail services on the presence server.</td>
</tr>
</tbody>
</table>

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

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

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

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VVM_Mailstore_Server_0</td>
<td>Hostname</td>
<td>Specifies the address of your voicemail server. Set one of the following as the value:</td>
</tr>
<tr>
<td></td>
<td>IP address</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>

Related Topics

Service Credentials Parameters, on page 133

Configure Automatic Updates

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

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

Note

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

XML File Structure

XML files for automatic updates have the following structure:

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

The following is example XML file for automatic updates:

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

Before you begin

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

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Host the update installation program on your HTTP server.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Create an update XML file with any text editor.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Specify values in the XML as follows:</td>
</tr>
<tr>
<td></td>
<td>• name—Specify the following ID as the value of the name attribute for the App element:</td>
</tr>
<tr>
<td></td>
<td>• JabberWin—The update applies to Cisco Jabber for Windows.</td>
</tr>
<tr>
<td></td>
<td>• LatestBuildNum—Build number of the update.</td>
</tr>
<tr>
<td></td>
<td>• LatestVersion—Version number of the update.</td>
</tr>
<tr>
<td></td>
<td>• Mandatory—(Windows clients only) True or False. Determines whether users must upgrade their client version when prompted.</td>
</tr>
<tr>
<td></td>
<td>• Message—HTML in the following format:</td>
</tr>
<tr>
<td></td>
<td>• DownloadURL—URL of the installation package on your HTTP server.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Save and close your update XML file.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Host your update XML file on your HTTP server.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Specify the URL of your update XML file as the value of the UpdateUrl parameter in your configuration file.</td>
</tr>
</tbody>
</table>
Problem Reporting

**Applies to:** Cisco Jabber for Windows

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

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

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

**Before you begin**

Complete the following steps to prepare your environment:

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

The following is an example form that accepts problem reports:

```html
  <input type="file" name="zipFileName" id="zipFileName" />
  <input type="submit" name="submitBtn" id="submitBtn" value="Upload File" />
</form>
```

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Host your custom script on your HTTP server.</td>
</tr>
<tr>
<td>2</td>
<td>Specify the URL of your script as the value of the PrtLogServerUrl parameter in your configuration file.</td>
</tr>
</tbody>
</table>

**Custom Embedded Tabs**

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

**Note**

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

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

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>browser-plugin</td>
<td>Contains all definitions for custom embedded tabs. The value includes all custom tab definitions.</td>
</tr>
<tr>
<td>page</td>
<td>Contains one custom embedded tab definition.</td>
</tr>
<tr>
<td>refresh</td>
<td>Controls when the content refreshes.</td>
</tr>
<tr>
<td></td>
<td>• true — Content refreshes each time users select the tab.</td>
</tr>
<tr>
<td></td>
<td>• false (default) — Content refreshes when users restart the client or sign in.</td>
</tr>
<tr>
<td>preload</td>
<td>Controls when the content loads.</td>
</tr>
<tr>
<td></td>
<td>• true — Content loads when the client starts.</td>
</tr>
<tr>
<td></td>
<td>• false (default) — Content loads when users select the tab.</td>
</tr>
<tr>
<td>tooltip</td>
<td>Defines hover text for the custom embedded tab.</td>
</tr>
<tr>
<td></td>
<td>This parameter is optional. If you do not specify the hover text, the client will use <strong>Custom tab</strong>.</td>
</tr>
<tr>
<td></td>
<td>The value is string of unicode characters.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| icon      | Specifies an icon for the tab. You can specify a local or hosted icon as follows:  
  - Local icon—Specify the URL as follows:  
    file://file_path/icon_name  
  - Hosted icon—Specify the URL as follows: http://path/icon_name  
  You can use any icon that the client browser can render, including .JPG, .PNG, and .GIF formats.  
  This parameter is optional. If you do not specify an icon, the client loads the favicon from the HTML page. If no favicon is available, the client loads the default icon. |
| url       | Specifies the URL where the content for the embedded tab resides.  
  The client uses the browser rendering engine to display the content of the embedded tab. For this reason, you can specify any content that the browser supports.  
  This parameter is required. |

**User Custom Tabs**

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

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

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

**Note**

User custom embedded tabs are set to true by default.

**Custom Icons**

Icons for custom embedded tabs contain ten frames for each state within a single image file.

**Note**

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

- Dimensions: 20 x 20 pixels
- 1 pixel of padding between each frame. 1 pixel of padding results in a working icon space of 19 by 19 pixels.
- Transparent background
- PNG file format
Each frame of an icon represents the following states:

1. Normal
2. Pressed
3. Hover
4. Disabled
5. Focused
6. Selected and normal
7. Selected and pressed
8. Selected and hover
9. Selected and disabled
10. Selected and focused

The following is an example icon:

![Example Icon]

The following are the hexadecimal color codes for each frame of the preceding icon. Use these color codes for a consistent appearance with your custom icons.

1. #4f6b7c
2. #2aa6c7
3. #99b5c7
4. #FFFFFF
5. #19bae3
6. #19bae3
7. #2aa6c7
8. #99b5c7
9. #FFFFFF
10. #19bae3

### Chats and Calls from Custom Tabs

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

- Use the XMPP: or IM: protocol handler to start chats.
- Use the TEL: protocol handler to start audio and video calls.

#### Related Topics

- [Protocol Handlers](#), on page 25

### UserID Tokens

You can specify the `${UserID}` token as part of the value for the url parameter. When users sign in, the client replaces the `${UserID}` token with the username of the logged in user.
You can also specify the ${UserID} token in query strings; for example, www.cisco.com/mywebapp.op?url=${UserID}.

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

1. You specify the following in your custom embedded tab:
   <url>www.cisco.com/${UserID}/profile</url>
2. Mary Smith signs in. Her username is msmith.
3. The client replaces the ${UserID} token with Mary's username as follows:
   <url>www.cisco.com/msmith/profile</url>

### JavaScript Notifications

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

#### Notification Methods

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

- **SetNotificationBadge** — You call this method from the client in your JavaScript. This method takes a string value that can have any of the following values:
  - **Empty** — An empty value removes any existing notification badge.
  - A number from 1 to 999
  - Two digit alphanumeric combinations, for example, A1

- **onPageSelected()** — The client invokes this method when users select the custom embedded tab.
- **onPageDeselected()** — The client invokes this method when users select another tab.

#### Note

Not applicable for Jabber for iPhone and iPad

### Show Call Events in Custom Tabs

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

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

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

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

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

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

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

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

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

```javascript
function OnTelephonyConversationStateChanged(json) {
    console.log("OnTelephonyConversationStateChanged");
    try {
        var conversation = JSON.parse(json);
        console.log("conversation state= " + conversation.state);
        console.log("conversation acceptanceState= " + conversation.acceptanceState);
        console.log("conversation callType= " + conversation.callType);
        for (var i=0; i<conversation.remoteParticipants.length; i++) {
            console.log("conversation remoteParticipants[" + i + "]=");
            console.log("voiceMediaDisplayName= " + conversation.remoteParticipants[i].voiceMediaDisplayName);
            console.log("voiceMediaNumber= " + conversation.remoteParticipants[i].voiceMediaNumber);
            console.log("translatedNumber= " + conversation.remoteParticipants[i].translatedNumber);
            console.log("voiceMediaPhoneType= " + conversation.remoteParticipants[i].voiceMediaPhoneType);
            console.log("voiceMediaState= " + conversation.remoteParticipants[i].voiceMediaState);
        }
        console.log("conversation localParticipant= ");
        console.log(" voiceMediaDisplayName= " +
```
conversation.localParticipant.voiceMediaDisplayName);
    console.log(" voiceMediaNumber=" + conversation.localParticipant.voiceMediaNumber);
    console.log(" translatedNumber=" + conversation.localParticipant.translatedNumber);
    console.log(" voiceMediaPhoneType=" + conversation.localParticipant.voiceMediaPhoneType);
    console.log(" voiceMediaState=" + conversation.localParticipant.voiceMediaState);
  }
  catch(e) {
    console.log("cannot parse conversation:" + e.message);
  }

### Custom Embedded Tab Example

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

```xml
<config version="1.0">
  <Client>
    <jabber-plugin-config>
      <browser-plugin>
        <page refresh="true" preload="true">
          <tooltip>Cisco</tooltip>
          <icon>https://www.cisco.com/web/fw/i/logo.gif</icon>
          <url>https://www.cisco.com</url>
        </page>
      </browser-plugin>
    </jabber-plugin-config>
  </Client>
</config>
```
Integrate with Directory Sources

Cisco Jabber integrates with directory sources in on-premises deployments to query for and resolve contact information. Learn why you should enable synchronization and authentication between your directory source and Cisco Unified Communications Manager. Understand how directory integration works with certain contact sources. Review when you should configure the client for directory integration. Find configuration examples of specific integration scenarios.

- Set Up Directory Synchronization and Authentication, on page 143
- Contact Sources, on page 146
- Client Configuration for Directory Integration, on page 151
- Federation, on page 182

Set Up Directory Synchronization and Authentication

When you set up an on-premises deployment, you should configure Cisco Unified Communications Manager to do both of the following:

- Synchronize with the directory server.
- Authenticate with the directory server.

Synchronizing with the directory server replicates contact data from your directory to Cisco Unified Communications Manager.

Enabling authentication with the directory server lets Cisco Unified Communications Manager proxy authentication from the client to the directory server. In this way, users authenticate with the directory server, not with Cisco Unified Communications Manager or a presence server.

Related Topics

- Configuring Cisco Unified Communications Manager Directory Integration
Synchronize with the Directory Server

Directory server synchronization ensures that contact data in your directory server is replicated to Cisco Unified Communications Manager.

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

1. Open the Cisco Unified CM Administration interface.
2. Select System > LDAP > LDAP System.
   
   The LDAP System Configuration window opens.
3. Locate the LDAP System Information section.
4. Select Enable Synchronizing from LDAP Server.
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 userID.

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

1. Locate the LDAP Attribute for User ID drop-down list on the LDAP System Configuration window.
2. Specify an attribute for the user ID as appropriate and then select Save.
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 EDI parameter is `UserAccountName`.

```xml
<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.

---

### Perform Synchronization

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

**Before you begin**

If your environment includes a presence server, you should ensure the following feature service is activated and started before you synchronize with the directory server:

- Cisco Unified Presence — **Cisco UP Sync Agent**
- Cisco Unified Communications Manager IM and Presence Service — **Cisco Sync Agent**

This service keeps data synchronized between the presence server and Cisco Unified Communications Manager. When you perform the synchronization with your directory server, Cisco Unified Communications Manager then synchronizes the data with the presence server. However, the **Cisco Sync Agent** service must be activated and started.

**Procedure**

1. **Step 1** Select **System > LDAP > LDAP Directory**.
2. **Step 2** Select **Add New**.
   
   The **LDAP Directory** window opens.

3. **Step 3** Specify the required details on the **LDAP Directory** window.
   
   See the [Cisco Unified Communications Manager Administration Guide](#) for more information about the values and formats you can specify.

4. **Step 4** Create an LDAP Directory Synchronization Schedule to ensure that your information is synchronized regularly.
5. **Step 5** Select **Save**.
6. **Step 6** Select **Perform Full Sync Now**.
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.

### 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 <strong>Cisco Unified CM Administration</strong> interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select <strong>System &gt; LDAP &gt; LDAP Authentication</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>Use LDAP Authentication for End Users</strong>.</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**. |

### Contact Sources

In on-premises deployments, the client requires a contact source to resolve directory look ups for user information. You can use the following as a contact source:

**Enhanced Directory Integration**

Enhanced Directory Integration (EDI) is an LDAP-based contact source.

**Cisco Unified Communications Manager User Data Service**

Cisco Unified Communications Manager User Data Service (UDS) is a contact source on Cisco Unified Communications Manager.

UDS is used for contact resolution in the following cases:

- If you configure the DirectoryServerType parameter in the client configuration file to use “UDS”.

---

---
With this configuration, the client uses UDS for contact resolution when it is inside or outside of the corporate firewall.

• If you deploy Expressway for Mobile and Remote Access.

With this configuration, the client automatically uses UDS for contact resolution when it is outside of the corporate firewall.

---

**Note**

Cisco Jabber supports UDS using the following Cisco Unified Communications Manager versions:

• Cisco Unified Communications Manager Version 9.1(2) or later with the following COP file: cmterm-cucm-uds-912-5.cop.sgn.

• Cisco Unified Communications Manager Version 10.0(1). No COP file is required.

You can deploy approximately 50 percent of the maximum number of Cisco Jabber clients that your Cisco Unified Communications Manager node supports.

For example, if a Cisco Unified Communications Manager node can support 10,000 Cisco Jabber clients using an LDAP-based contact source, that same node can support 5,000 Cisco Jabber clients using UDS as a contact source.

---

**Enhanced Directory Integration**

EDI uses native Microsoft Windows APIs to retrieve contact data from the directory service.

The following are the default settings for on-premises deployments with EDI:

• Cisco Jabber integrates with Active Directory as the contact source.

• Cisco Jabber automatically discovers and connects to a Global Catalog.

---
In the preceding diagram, the client does the following by default:

1. Gets the DNS domain from the workstation and looks up the SRV record for the Global Catalog.
2. Retrieves the address of the Global Catalog from the SRV record.
3. Connects to the Global Catalog with the logged in user's credentials.

**Domain Name Retrieval**

Cisco Jabber for Windows retrieves the fully qualified DNS domain from the USERDNSDOMAIN environment variable on the client workstation.

After the client gets the DNS domain, it can locate the Domain Name Server and retrieve SRV records.

If the USERDNSDOMAIN environment variable is not present, you can deploy the LdapUserDomain configuration parameter to specify which domain to execute the request for the LDAP service. If that parameter is not configured, then Jabber uses the domain from the email address screen.

In some instances, the value of the USERDNSDOMAIN environment variable does not resolve to the DNS domain that corresponds to the domain of the entire forest. For example, when an organization uses a sub-domain or resource domain. In this case, the USERDNSDOMAIN environment variable resolves to a child domain, not the parent domain. As a result, the client cannot access information for all users in the organization.

If the USERDNSDOMAIN environment variable resolves to a child domain, you can use one of the following options to enable Cisco Jabber for Windows to connect to a service in the parent domain:

- Ensure that the Global Catalog or LDAP directory server can access all users in the organization.
- Configure your DNS server to direct the client to a server that can access all users in the organization when Cisco Jabber for Windows requests a Global Catalog or LDAP directory server.
- Configure Cisco Jabber for Windows to use the FQDN of the domain controller.

Specify the FQDN of the domain controller as the value of the PrimaryServerName parameter in your client configuration as follows:

```
<PrimaryServerName>parent-domain-fqdn</PrimaryServerName>
```

**Related Topics**

- Directory Connection Parameters, on page 160
- Configuring DNS for the Forest Root Domain
- Assigning the Forest Root Domain Name
- Deploying a GlobalNames Zone
- Support for DNS Namespace planning in Microsoft server products

**Directory Server Discovery**

Cisco Jabber can automatically discover and connect to the directory server if:

- The workstation on which you install Cisco Jabber automatically detects the workstation by determining the user domain.
- The workstation retrieves the server connection address from the DNS SRV record.
Cisco Unified Communications Manager User Data Service

User Data Service (UDS) is a REST interface on Cisco Unified Communications Manager that provides contact resolution.

UDS is used for contact resolution in the following cases:

- If you set the DirectoryServerType parameter to use a value of UDS in the client configuration file.
  With this configuration, the client uses UDS for contact resolution when it is inside or outside of the corporate firewall.

- If you deploy Expressway for Remote and Mobile Access.
  With this configuration, the client automatically uses UDS for contact resolution when it is outside of the corporate firewall.

You synchronize contact data into Cisco Unified Communications Manager from a directory server. Cisco Jabber then automatically retrieves that contact data from UDS.

Enable Integration with UDS

To enable integration with UDS, perform the following steps:
**Set UDS Service Parameters**

You can set service parameters for UDS on Cisco Unified Communications Manager.

**Procedure**

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

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

The **Enterprise Parameters Configuration** window opens.

**Step 3** Locate the **User Data Service Parameters** section.

**UDS Service Parameters**

Set values for the following service parameters to configure UDS:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable All User Search</td>
<td>Allows searches for all users in the directory (search with no last name, first name, or directory number specified). The default value is true.</td>
</tr>
<tr>
<td>User Search Limit</td>
<td>Limits the number of users returned in a query. The default value is 64.</td>
</tr>
</tbody>
</table>
### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Digits to Match</td>
<td>Specifies the number of digits to match when users search for phone numbers.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>To resolve PSTN numbers, set the value equal to the number of digits in the PSTN numbers. For example, if the PSTN numbers have 10 digits, set the value to 10.</td>
</tr>
</tbody>
</table>

### Contact Resolution with Multiple Clusters

For contact resolution with multiple Cisco Unified Communications Manager clusters, synchronize all users on the corporate directory to each cluster. Provision a subset of those users on the appropriate cluster.

For example, your organization has 40,000 users. 20,000 users reside in North America. 20,000 users reside in Europe. Your organization has the following Cisco Unified Communications Manager clusters for each location:

- cucm-cluster-na for North America
- cucm-cluster-eu for Europe

In this example, synchronize all 40,000 users to both clusters. Provision the 20,000 users in North America on cucm-cluster-na and the 20,000 users in Europe on cucm-cluster-eu.

When users in Europe call users in North America, Cisco Jabber retrieves the contact details for the user in Europe from cucm-cluster-na.

When users in North America call users in Europe, Cisco Jabber retrieves the contact details for the user in North America from cucm-cluster-eu.

### Client Configuration for Directory Integration

You can configure directory integration through service profiles using Cisco Unified Communications Manager release 9 or later or with the configuration file. Use this section to learn how to configure the client for directory integration.

When both a service profile and a configuration file are present, the following table describes which parameter value takes precedence.

<table>
<thead>
<tr>
<th>Service Profile</th>
<th>Configuration File</th>
<th>Which Parameter Value Takes Precedence?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter value is set</td>
<td>Parameter value is set</td>
<td>Service profile</td>
</tr>
<tr>
<td>Parameter value is set</td>
<td>Parameter value is blank</td>
<td>Service profile</td>
</tr>
<tr>
<td>Parameter value is blank</td>
<td>Parameter value is set</td>
<td>Configuration file</td>
</tr>
<tr>
<td>Parameter value is blank</td>
<td>Parameter value is blank</td>
<td>Service profile blank (default) value</td>
</tr>
</tbody>
</table>
Cisco Unified Presence, Release 8.x profiles cannot be used for directory integration.

**When to Configure Directory Integration**

Install Cisco Jabber for Windows on a workstation that is registered to an Active Directory domain. In this environment, you do not need to configure Cisco Jabber for Windows to connect to the directory. The client automatically discovers the directory and connects to a Global Catalog server in that domain.

Configure Cisco Jabber to connect to a directory services if you plan to use one of the following services as the contact source:

- Domain Controller
- Cisco Unified Communications Manager User Data Service
- OpenLDAP
- Active Directory Lightweight Directory Service
- Active Directory Application Mode

You can optionally configure directory integration to:

- Change the default attribute mappings.
- Adjust directory query settings.
- Specify how the client retrieves contact photos.
- Perform intradomain federation.

**Configure Directory Integration in a Service Profile**

With Cisco Unified Communications Manager version 9 and higher, you can provision users with service profiles and deploy the _cisco-uds SRV record on your internal domain name server.

The client can then automatically discover Cisco Unified Communications Manager and retrieve the service profile to get directory integration configuration.

To set up service discovery to support service profiles, you must:

- Deploy the _cisco-uds SRV record on your internal domain name server.
- Ensure that the client can resolve the domain name server address.
- Ensure that the client can resolve the hostname of Cisco Unified Communications Manager.
- Ensure that the client can resolve the fully qualified domain name (FQDN) for the Cisco Unified Communications Manager.
Cisco Jabber now supports Cisco Unified Communications Manager User Data Service (UDS). In addition to being able to deploy Cisco Jabber using LDAP to connect to Active Directory, Jabber can now alternatively be deployed with Cisco Unified Communications Manager User Data Services contact lookup service. Server scaling must be considered when using the UDS server. A Cisco Unified Communication node can support UDS contact service connections for 50% of the maximum device registrations supported by the server.

To configure directory integration in a service profile, do the following:

**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>Add a directory service.</td>
</tr>
<tr>
<td></td>
<td>a) Select User Management &gt; User Settings &gt; UC Service.</td>
</tr>
<tr>
<td></td>
<td>The Find and List UC Services window opens.</td>
</tr>
<tr>
<td></td>
<td>b) Select Add New.</td>
</tr>
<tr>
<td></td>
<td>The UC Service Configuration window opens.</td>
</tr>
<tr>
<td></td>
<td>c) Select Directory from the UC Service Type menu and then select Next.</td>
</tr>
<tr>
<td></td>
<td>d) Set all appropriate values for the directory service and then select Save.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Apply the directory service to a service profile.</td>
</tr>
<tr>
<td></td>
<td>a) Select User Management &gt; User Settings &gt; Service Profile.</td>
</tr>
<tr>
<td></td>
<td>The Find and List Service Profiles window opens.</td>
</tr>
<tr>
<td></td>
<td>b) Select Add New.</td>
</tr>
<tr>
<td></td>
<td>The Service Profile Configuration window opens.</td>
</tr>
<tr>
<td></td>
<td>c) Add the directory services to the directory profile.</td>
</tr>
<tr>
<td></td>
<td>d) Select Save.</td>
</tr>
</tbody>
</table>

**Directory Profile Parameters**

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

<table>
<thead>
<tr>
<th>Directory Service Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary server</strong></td>
<td>Specifies the address of the primary directory server. This parameter is required for manual connections where the client cannot automatically discover the directory server.</td>
</tr>
<tr>
<td><strong>Secondary server</strong></td>
<td>Specifies the address of the backup directory server.</td>
</tr>
</tbody>
</table>
### Directory Service Configuration

<table>
<thead>
<tr>
<th>Description</th>
<th>Directory Service Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies if the client uses UDS as a contact source.</td>
<td>Use UDS for Contact Resolution</td>
</tr>
<tr>
<td>True (Default)</td>
<td>Use UDS as a contact source. When this option is selected the following parameters in this table are not used.</td>
</tr>
<tr>
<td>False</td>
<td>Use EDI or BDI as a contact source. The following parameters are used to connect to the LDAP server.</td>
</tr>
</tbody>
</table>

By default, UDS provides contact resolution when users connect to the corporate network through Expressway for Mobile and Remote Access.

<table>
<thead>
<tr>
<th>Description</th>
<th>Directory Service Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies if the client uses the logged on username and password for LDAP contact resolution.</td>
<td>Use Logged On User Credential</td>
</tr>
<tr>
<td>If you have configured Active Directory (AD) SSO, this will take priority over this setting.</td>
<td></td>
</tr>
<tr>
<td>True (default)</td>
<td>Use logged on user credentials. This value maps to the values for the UseWindowsCredentials parameter for Windows clients, and the BDIUseJabberCredntials parameter for other clients.</td>
</tr>
<tr>
<td>False</td>
<td>Do not use logged on user credentials.</td>
</tr>
</tbody>
</table>

When you have SSO configured, Jabber uses those credentials before using the ConnectionUsername and ConnectionPassword parameters.

You must specify the logged on user credentials with the following parameters:

- ConnectionUsername
- ConnectionPassword

You must specify the logged on user credentials with the following parameters:

- EDI (Windows client)
  - ConnectionUsername
  - ConnectionPassword

- BDI (Mac, Android, iOS clients)
  - BDIClonectionUsername
  - BDIClonectionPassword
### Directory Service Configuration

<table>
<thead>
<tr>
<th>Directory Service Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Lets you manually specify a shared username that the client can use to authenticate with the directory server. By default, Cisco Jabber for Windows uses Integrated Windows Authentication when connecting to the directory server. You should use this parameter only in deployments where you cannot authenticate with the directory server using Microsoft Windows credentials. Use only a well-known or public set of credentials for an account that has read-only permissions.</td>
</tr>
<tr>
<td>Password</td>
<td>Lets you manually specify a shared password that the client can use to authenticate with the directory server. By default, Cisco Jabber for Windows uses Integrated Windows Authentication when connecting to the directory server. You should use this parameter only in deployments where you cannot authenticate with the directory server using Microsoft Windows credentials. Use only a well-known or public set of credentials for an account that has read-only permissions.</td>
</tr>
<tr>
<td>Search Base 1</td>
<td>Specifies a location in the directory server from which searches begin. In other words, a search base is the root from which the client executes a search. By default, the client searches from the root of the directory tree. You can specify the value of up to three search bases in your OU to override the default behavior. Active Directory does not typically require a search base. Specify search bases for Active Directory only for specific performance requirements. Specify a search base for directory servers other than Active Directory to create bindings to specific locations in the directory. <strong>Tip</strong> Specify an OU to restrict searches to certain user groups. For example, a subset of your users have instant messaging capabilities only. Include those users in an OU and then specify that as a search base.</td>
</tr>
</tbody>
</table>

---

### Directory Profile Parameters

**Search Base 1**  
The following parameters only apply to Cisco Jabber for Windows:

**Search Base 2**

**Search Base 3**
Summary of Directory Integration Configuration Parameters

This topic lists all the parameters you can specify to configure directory integration.

The following table lists the parameters you can use for attribute mapping with LDAP directory servers:

<table>
<thead>
<tr>
<th>Directory Service Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recursive Search on All Search Bases</strong></td>
<td>Select this option to perform a recursive search of the directory starting at the search base. Use recursive searches to allow the Cisco Jabber client contact search queries to search all of the LDAP directory tree from a given search context (search base). This is a common option when searching LDAP. This is a required field. The default value is True.</td>
</tr>
<tr>
<td><strong>Search Timeout</strong></td>
<td>Specifies the timeout period for directory queries in seconds. The default value is 5.</td>
</tr>
<tr>
<td><strong>Base Filter</strong></td>
<td>Specifies a base filter for Active Directory queries. Specify a directory subkey name only to retrieve objects other than user objects when you query the directory. The default value is (((&amp;(objectCategory=person)(&amp;objectClass=user))).)</td>
</tr>
<tr>
<td><strong>Predictive Search Filter</strong></td>
<td>Defines filters to apply to predictive search queries. You can define multiple, comma-separated values to filter search queries. The default value is ANR. When Cisco Jabber performs a predictive search, it issues a query using Ambiguous Name Resolution (ANR). This query disambiguates the search string and returns results that match the attributes that are set for ANR on your directory server. Important: Configure your directory server to set attributes for ANR if you want the client to search for those attributes.</td>
</tr>
</tbody>
</table>

**Attribute Mappings**

It is not possible to change the default attribute mappings in a service profile. If you plan to change any default attribute mappings, you must define the required mappings in a client configuration file.
### Attribute Mapping Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Attribute Mapping Parameters</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>CommonName</td>
<td>• CommonName</td>
<td>• Title</td>
</tr>
<tr>
<td>DisplayName</td>
<td>• DisplayName</td>
<td>• CompanyName</td>
</tr>
<tr>
<td>Firstname</td>
<td>• Firstname</td>
<td>• UserAccountName</td>
</tr>
<tr>
<td>Lastname</td>
<td>• Lastname</td>
<td>• DomainName</td>
</tr>
<tr>
<td>EmailAddress</td>
<td>• EmailAddress</td>
<td>• Location</td>
</tr>
<tr>
<td>SipUri</td>
<td>• SipUri</td>
<td>• Nickname</td>
</tr>
<tr>
<td>PhotoSource</td>
<td>• PhotoSource</td>
<td>• PostalCode</td>
</tr>
<tr>
<td>BusinessPhone</td>
<td>• BusinessPhone</td>
<td>• City</td>
</tr>
<tr>
<td>MobilePhone</td>
<td>• MobilePhone</td>
<td>• State</td>
</tr>
<tr>
<td>HomePhone</td>
<td>• HomePhone</td>
<td>• StreetAddress</td>
</tr>
<tr>
<td>OtherPhone</td>
<td>• OtherPhone</td>
<td></td>
</tr>
</tbody>
</table>

The following table lists the parameters you can use to connect to an LDAP directory server:

### Directory Server Connection Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Directory Server Connection Parameters</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectionType</td>
<td>• ConnectionType</td>
<td>• UseWindowsCredentials</td>
</tr>
<tr>
<td>PrimaryServerName</td>
<td>• PrimaryServerName</td>
<td>• ConnectionUsername</td>
</tr>
<tr>
<td>SecondaryServerName</td>
<td>• SecondaryServerName</td>
<td>• ConnectionPassword</td>
</tr>
<tr>
<td>ServerPort1</td>
<td>• ServerPort1</td>
<td>• UseSSL</td>
</tr>
<tr>
<td>ServerPort2</td>
<td>• ServerPort2</td>
<td>• UseSecureConnection</td>
</tr>
</tbody>
</table>

The following table lists the parameters you can use for contact resolution and directory queries with LDAP directory servers:

### Contact Resolution and Directory Query Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Contact Resolution and Directory Query Parameters</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>BaseFilter</td>
<td>• BaseFilter</td>
<td>• PhotoUriSubstitutionEnabled</td>
</tr>
<tr>
<td>PredictiveSearchFilter</td>
<td>• PredictiveSearchFilter</td>
<td>• PhotoUriSubstitutionToken</td>
</tr>
<tr>
<td>DisableSecondaryNumberLookups</td>
<td>• DisableSecondaryNumberLookups</td>
<td>• PhotoUriWithToken</td>
</tr>
<tr>
<td>PhoneNumberMasks</td>
<td>• PhoneNumberMasks</td>
<td>• UseSIPURIToResolveContacts</td>
</tr>
<tr>
<td>SearchTimeout</td>
<td>• SearchTimeout</td>
<td>• UriPrefix</td>
</tr>
<tr>
<td>UseWildcards</td>
<td>• UseWildcards</td>
<td>• IMAddresses</td>
</tr>
<tr>
<td>MinimumCharacterQuery</td>
<td>• MinimumCharacterQuery</td>
<td>• IMAddress</td>
</tr>
<tr>
<td>SearchBase1, SearchBase2,</td>
<td>• SearchBase1, SearchBase2, SearchBase3, SearchBase4, and SearchBase5</td>
<td>• UseWildcards</td>
</tr>
</tbody>
</table>
Summary of UDS Parameters

The following table lists the parameters you can use to connect to UDS and perform contact resolution and directory queries.

<table>
<thead>
<tr>
<th>UDS Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>• DirectoryServerType</td>
</tr>
<tr>
<td>• PresenceDomain</td>
</tr>
<tr>
<td>• UdsServer</td>
</tr>
<tr>
<td>• UdsPhotoUriWithToken</td>
</tr>
</tbody>
</table>

Directory Integration Parameters

The following sections lists details about the parameters you can configure for LDAP-based directory integration.

Attribute Mapping Parameters

The following table describes the parameters for mapping LDAP directory attributes:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Directory Attribute</th>
<th>Exists in Global Catalog by Default</th>
<th>Is Indexed by Default</th>
<th>Set for Ambiguous Name Resolution (ANR) by Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>CommonName</td>
<td>cn</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>DisplayName</td>
<td>displayName</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FirstName</td>
<td>givenName</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LastName</td>
<td>sn</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EmailAddress</td>
<td>mail</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SipUri</td>
<td>msRTCSIP-PrimaryUserAddress</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PhotoSource</td>
<td>thumbnailPhoto</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>BusinessPhone</td>
<td>telephoneNumber</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MobilePhone</td>
<td>mobile</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>HomePhone</td>
<td>homePhone</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>OtherPhone</td>
<td>otherTelephone</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>CompanyName</td>
<td>company</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>UserAccountName</td>
<td>sAMAccountName</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DomainName</td>
<td>userPrincipalName</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Location</td>
<td>co</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Nickname</td>
<td>displayName</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
You must index attributes on your LDAP directory server for the clients. This lets clients resolve contacts. To use the default attribute mappings, you must index the following attributes:

- sAMAccountName
- displayName
- sn
- name
- proxyAddresses
- mail
- department
- givenName
- telephoneNumber

Additionally, you must index the following attributes for secondary number queries:

- otherTelephone
- mobile
- homePhone

By default secondary number queries are enabled in Cisco Jabber for Windows. You can disable secondary number queries with the DisableSecondaryNumberLookups parameter.

Index msRTCSIP-PrimaryUserAddress for intradomain federation only.

Since Cisco Jabber for Windows connects to a Global Catalog server by default, you must ensure that all attributes reside on your Global Catalog server. You can replicate attributes to a Global Catalog server using an appropriate tool such as the Microsoft Active Directory Schema Snap-in. You can choose either to replicate or not to replicate attributes to your Global Catalog server:
• If you replicate attributes to your Global Catalog server, it generates traffic between Active Directory servers in the domain. For this reason, you should replicate attributes to your Global Catalog server only if the network traffic can handle extra load.

• If you do not want to replicate attributes to a Global Catalog server, configure Cisco Jabber to connect to a Domain Controller. In this case, the client queries single domains only when it connects to a Domain Controller.

Directory Connection Parameters

The following table describes parameters for configuring your LDAP directory connection:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectionType</td>
<td>0</td>
<td>Connect to a Global Catalog. This is the default value.</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Connect to a Domain Controller.</td>
</tr>
</tbody>
</table>

**Note**

Default ports are as follows:

- **Global Catalog**: 3268
- **Domain Controller**: 389
### Directory Connection Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrimaryServerName</td>
<td>IP address</td>
<td>Required parameter. Specifies the address of the primary directory server. This parameter is required for manual connections where the client cannot automatically discover the directory server.</td>
</tr>
<tr>
<td></td>
<td>FQDN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Each time the client starts, it attempts to connect to the primary server. The client attempts to connect to the secondary server if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The primary server is not available.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The primary server fails after the client connects to it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the connection to the secondary server is successful, the client keeps the connection to the secondary server until the next restart.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the secondary server fails while the client is connected to it, the client attempts to connect to the primary server.</td>
</tr>
<tr>
<td>SecondaryServerName</td>
<td>IP address</td>
<td>Specifies the address of the backup directory server. This parameter is required for manual connections where the client cannot automatically discover the directory server.</td>
</tr>
<tr>
<td></td>
<td>FQDN</td>
<td></td>
</tr>
<tr>
<td>ServerPort1</td>
<td>Port number</td>
<td>Specifies the port for the primary directory server.</td>
</tr>
<tr>
<td>ServerPort2</td>
<td>Port number</td>
<td>Specifies the port for the backup directory server.</td>
</tr>
<tr>
<td>UseWindowsCredentials</td>
<td>0</td>
<td>Specifies if the client uses Microsoft Windows usernames and passwords.</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Do not use Windows credentials. Specify credentials with the ConnectionUsername and ConnectionPassword parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 Use Windows credentials. This is the default value.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| ConnectionUsername   | Username | Lets you manually specify a shared username that the client can use to authenticate with the directory server. You should use this parameter only in deployments where you cannot authenticate with the directory server using Microsoft Windows credentials.  

**Important** The client transmits and stores this username as plain text.  
By default, the client uses Integrated Windows Authentication when connecting to the directory server. This parameter lets you manually specify a username in scenarios where it is not possible to authenticate with the directory server with the user's Microsoft Windows credentials.  
If you must use this parameter, you should use only a well-known or public set of credentials. The account that you use for integration should have read-only permissions to the directory. |
| ConnectionPassword   | Password | Lets you manually specify a shared password that the client can use to authenticate with the directory server. You should use this parameter only in deployments where you cannot authenticate with the directory server using Microsoft Windows credentials.  

**Important** The client transmits and stores this password as plain text.  
By default, the client uses Integrated Windows Authentication when connecting to the directory server. This parameter lets you manually specify a password in scenarios where it is not possible to authenticate with the directory server with the user's Microsoft Windows credentials.  
If you must use this parameter, you should use only a well-known or public set of credentials. The account that you use for integration should have read-only permissions to the directory. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UseSSL</td>
<td>0</td>
<td>Use SSL for secure connections to the directory.</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Use SSL.</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>Do not use SSL. This is the default value.</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

The SSL connection certificate must be present:
- In the Microsoft Windows certificate store.
- On the directory server to which the client connects.

To establish an SSL connection, the server presents the client with the certificate. The client then validates the certificate from the server against the certificate in the store on the client computer.

Default protocols and ports for SSL connections are as follows:

**Global Catalog**
- Protocol: TCP
- Port number: 3269

**Domain Controller**
- Protocol: TCP
- Port number: 636
Directory Query Parameters

The following table describes parameters for configuring how the client queries your LDAP directory:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BaseFilter</td>
<td>Base filter</td>
<td>Specifies a base filter for Active Directory queries. Specify a directory subkey name only to retrieve objects other than user objects when you query the directory. The default value is (&amp;(objectCategory=person)). Configuration files can contain only valid XML character entity references. Use &amp; instead of &amp; if you specify a custom base filter.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>PrediciveSearchFilter</td>
<td>Search filter</td>
<td>Defines filters to apply to predictive search queries. You can define multiple, comma-separated values to filter search queries. The default value is anr. When Cisco Jabber for Windows performs a predictive search, it issues a query using Ambiguous Name Resolution (ANR). This query disambiguates the search string and returns results that match the attributes that are set for ANR on your directory server. <strong>Important</strong> You must configure your directory server to set attributes for ANR if you want the client to search for those attributes.</td>
</tr>
<tr>
<td>DisableSecondaryNumberLookups</td>
<td>0, 1</td>
<td>Specifies whether users can search for alternative contact numbers if the work number is not available, such as the mobile, home, or other number. 0 Users can search for alternative contact numbers. This is the default value. 1 Users cannot search for alternative contact numbers.</td>
</tr>
<tr>
<td>SearchTimeout</td>
<td>Number of seconds</td>
<td>Specifies the timeout period for queries in seconds. The default value is 5.</td>
</tr>
<tr>
<td>UseWildcards</td>
<td>0, 1</td>
<td>Enables wildcard searches. 0 Do not use wildcards. This is the default value. 1 Use wildcards. If you use wildcards, it might take longer to search the directory.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MinimumCharacterQuery</td>
<td>Numerical value</td>
<td>Sets the minimum number of characters in a contact name to query the directory. For example, if you set 2 as the value of this parameter, the client searches the directory when users enter at least two characters in the search field. The default value is 3.</td>
</tr>
<tr>
<td>SearchBase1</td>
<td>Searchable organizational unit (OU) in the directory tree</td>
<td>Specifies a location in the directory server from which searches begin. In other words, a search base is the root from which the client executes a search. By default, the client searches from the root of the directory tree. You can specify the value of up to five search bases in your OU to override the default behavior. Active Directory does not typically require a search base. You should specify search bases for Active Directory only for specific performance requirements. You must specify a search base for directory servers other than Active Directory to create bindings to specific locations in the directory. <strong>Tip</strong> Specify an OU to restrict searches to certain user groups. For example, a subset of your users have instant messaging capabilities only. Include those users in an OU and then specify that as a search base.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Ambiguous Name Resolution for LDAP in Windows 2000
- LDAP Referrals
- Common Default Attributes Set for Active Directory and Global Catalog

**Base Filter Examples**

The following are example base filters you can use to look up specific locations or objects.

Find only specific groups:

```sql
(&(objectClass=user)(memberOf=cn=group-name,ou=Groups,dc=example,dc=com))
```

Find a nested group within a group:

```sql
(&(objectClass=user)(memberOf:search-oid:=cn=group-name,ou=Groups,dc=example,dc=com))
```

Find only enabled accounts and non-administrator accounts:
Phone Number Masks Parameter

Phone number masks parameter only applies to EDI. The following table describes the parameter to configure masks for phone number resolution:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PhoneNumberMasks</td>
<td>Mask string</td>
<td>Specifies masks to use when users search for phone numbers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, a user receives a call from +14085550100. In the directory, this number is +(1) 408 555 0100. The following mask resolves the number: +1408</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The length of mask strings cannot exceed the size restriction for registry subkey names.</td>
</tr>
</tbody>
</table>

Phone masks apply to phone numbers before the client searches your directory. If you configure phone masks correctly, directory searches succeed as exact query matches and prevent any impact to performance of your directory server.

The following table describes the elements you can include in a phone mask:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone number pattern</td>
<td>Provides a number pattern to retrieve phone numbers from your directory.</td>
</tr>
<tr>
<td></td>
<td>To add a phone mask, you specify a number pattern that applies to the mask.</td>
</tr>
<tr>
<td></td>
<td>For example, to specify a mask for searches that begin with +1408, you can use the following mask: +1408</td>
</tr>
<tr>
<td></td>
<td>To enable a mask to process phone numbers that have the same number of digits, but different patterns, use multiple masks with the same number of digits.</td>
</tr>
<tr>
<td></td>
<td>For example, your company has site A and site B. Each site maintains a separate directory in which the phone numbers have different formats, such as the following:</td>
</tr>
<tr>
<td></td>
<td>+(1) 408 555 0100</td>
</tr>
<tr>
<td></td>
<td>+1-510-5550101</td>
</tr>
<tr>
<td></td>
<td>The following mask ensures you can use both numbers correctly: +1408</td>
</tr>
<tr>
<td></td>
<td>####</td>
</tr>
<tr>
<td>Pipe symbol (I)</td>
<td>Separates number patterns and masks.</td>
</tr>
<tr>
<td></td>
<td>For example, +1408</td>
</tr>
</tbody>
</table>
### Contact Photo Parameters

The following table describes parameters for configuring how the client retrieves contact photos from an LDAP directory:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PhotoUriSubstitutionEnabled</td>
<td>true</td>
<td>Specifies if photo URI substitution is enabled.</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td>Specifies if photo URI substitution is disabled. This is the default value.</td>
</tr>
</tbody>
</table>

**Wildcard character**

Substitutes one or more characters for a subset of possible matching characters. Any wildcard character can exist in a phone mask.

For example, an asterisk (*) represents one or more characters and can apply to a mask as follows: `+3498|+###*###*###*####`. Using this mask with the wildcard, a phone number search can match any of the following formats:

- `+34(98)555 0199`
- `+34 98 555-0199`
- `+34-(98)-555.0199`

**Reverse mask**

Applies a number pattern from right to left.

For example, a mask of `+3498|R+34 (98) 559 ####` applied to `+34985590199` results in `+34 (98) 559 0199`.

You can use both forward and reverse masks.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PhotoUriSubstitutionToken</td>
<td>Directory attribute</td>
<td>Specifies a directory attribute to insert in the photo URI; for example, <code>sAMAccountName</code>. Only the following attributes are supported for use with the PhotoUriSubstitutionToken parameter:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Common Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Display Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• First Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Last Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Nickname</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Email Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Photo Source</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Business Phone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mobile Phone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Home Phone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Preferred Phone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Other Phone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Title</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Company Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User Account Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Domain Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Location</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Post Code</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• State</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• City</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Street</td>
</tr>
</tbody>
</table>
Specifies a photo URI with a directory attribute as a variable value; for example, http://staffphoto.example.com/sAMAccountName.jpg.

The parameter applies to LDAP directory integrations.

To configure photo URI substitution, you set the directory attribute as the value of PhotoUriSubstitutionToken.

**Restriction** The client must be able to retrieve the photos from the web server without credentials.

### Related Topics

- [Contact Photo Formats and Dimensions](#), on page 171

### Contact Photo Retrieval with EDI

Cisco Jabber retrieves and displays contact photos with the following methods.

#### Note

When you change a photo in the Active Directory, the photo can take up to 24 hours to refresh in Cisco Jabber.

### URI substitution

Cisco Jabber dynamically builds a URL to contact photos with a directory attribute and a URL template.

To use this method, set the following values in your configuration file:

1. Specify `true` as the value of the PhotoUriSubstitutionEnabled parameter.
2. Specify a directory attribute to use as a dynamic token as the value of the PhotoUriSubstitutionToken parameter; for example,
   
   
   `<PhotoUriSubstitutionToken>sAMAccountName</PhotoUriSubstitutionToken>`

3. Specify the URL and the dynamic token as the value of the PhotoUriWithToken parameter; for example,
   
   `<PhotoUriWithToken>http://staffphoto.example.com/sAMAccountName.jpg</PhotoUriWithToken>`

With the example values in the preceding steps, the `sAMAccountName` attribute might resolve to `msmith` in your directory. Cisco Jabber then takes this value and replaces the token to build the following URL: `http://staffphoto.example.com/msmith.jpg`.

### Binary objects

Cisco Jabber retrieves the binary data for the photo from your database.

If using binary objects from Active Directory, PhotoUriWithToken should not be set.

To use this method to retrieve contact photos, specify the attribute that contains the binary data as the value of the PhotoSource parameter in the configuration; for example,

 `<PhotoSource>jpegPhoto</PhotoSource>`
PhotoURL attribute

Cisco Jabber retrieves a URL from a directory attribute.

To use this method to retrieve contact photos, specify the attribute that contains the photo URL as the value of the PhotoSource parameter in the configuration; for example,

```xml
<PhotoSource>photoUri</PhotoSource>
```

Contact Photo Formats and Dimensions

To achieve the best result with Cisco Jabber, your contact photos should have specific formats and dimensions. Review supported formats and optimal dimensions. Learn about adjustments the client makes to contact photos.

Contact Photo Formats

Cisco Jabber supports the following formats for contact photos in your directory:

- JPG
- PNG
- BMP
- GIF

---

Important

Cisco Jabber does not apply any modifications to enhance rendering for contact photos in GIF format. As a result, contact photos in GIF format might render incorrectly or with less than optimal quality. To obtain the best quality, use PNG format for your contact photos.

---

Contact Photo Dimensions

Tip

The optimum dimensions for contact photos are 128 pixels by 128 pixels with an aspect ratio of 1:1. 128 pixels by 128 pixels are the maximum dimensions for local contact photos in Microsoft Outlook.

The following table lists the different dimensions for contact photos in Cisco Jabber.

<table>
<thead>
<tr>
<th>Location</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio call window</td>
<td>128 pixels by 128 pixels</td>
</tr>
<tr>
<td>Invitations and reminders, for example:</td>
<td></td>
</tr>
<tr>
<td>• Incoming call windows</td>
<td>64 pixels by 64 pixels</td>
</tr>
<tr>
<td>• Meeting reminder windows</td>
<td></td>
</tr>
</tbody>
</table>
Contact Photo Adjustments

Cisco Jabber adjusts contact photos as follows:

- **Resizing**—If contact photos in your directory are smaller or larger than 128 pixels by 128 pixels, the client automatically resizes the photos. For example, contact photos in your directory are 64 pixels by 64 pixels. When Cisco Jabber retrieves the contact photos from your directory, it resizes the photos to 128 pixels by 128 pixels.

  **Tip**  
  Resizing contact photos can result in less than optimal resolution. For this reason, use contact photos that are 128 pixels by 128 pixels so that the client does not automatically resize them.

- **Cropping**—Cisco Jabber automatically crops nonsquare contact photos to a square aspect ratio, or an aspect ratio of 1:1 where the width is the same as the height.

- **Portrait orientation**—If contact photos in your directory have portrait orientation, the client crops 30 percent from the top and 70 percent from the bottom.

  For example, if contact photos in your directory have a width of 100 pixels and a height of 200 pixels, Cisco Jabber needs to crop 100 pixels from the height to achieve an aspect ratio of 1:1. In this case, the client crops 30 pixels from the top of the photos and 70 pixels from the bottom of the photos.

- **Landscape orientation**—If contact photos in your directory have landscape orientation, the client crops 50 percent from each side.

  For example, if contact photos in your directory have a width of 200 pixels and a height of 100 pixels, Cisco Jabber needs to crop 100 pixels from the width to achieve an aspect ratio of 1:1. In this case, the client crops 50 pixels from the right side of the photos and 50 pixels from the left side of the photos.

- **Rounding**—Cisco Jabber rounds the corners of contact photos after retrieving them from your directory.

UDS Parameters

The following table provides details about the parameters you can use in the configuration file to connect to UDS and perform contact resolution and directory queries.
Contact Photo Retrieval with UDS

Cisco Unified Communications Manager User Data Service (UDS) dynamically builds a URL for contact photos with a directory attribute and a URL template.

To resolve contact photos with UDS, you specify the format of the contact photo URL as the value of the UdsPhotoUriWithToken parameter. You also include a %%uid%% token to replace the contact username in the URL, for example,

<UdsPhotoUriWithToken>http://server_name/%%uid%%.jpg</UdsPhotoUriWithToken>
Integrate with Directory Sources

Contact Photo Formats and Dimensions

UDS substitutes the %%uid%% token with the value of the userName attribute in UDS. For example, a user named Mary Smith exists in your directory. The value of the userName attribute for Mary Smith is msmith. To resolve the contact photo for Mary Smith, Cisco Jabber takes the value of the userName attribute and replaces the %%uid%% token to build the following URL: http://staffphoto.example.com/msmith.jpg

Note

When you change a photo in the Active Directory, the photo can take up to 24 hours to refresh in Cisco Jabber.

Important

• If you deploy Expressway for Mobile and Remote Access, the client automatically uses UDS for contact resolution when users connect to services from outside the corporate network. When you set up UDS contact resolution for Expressway for Mobile and Remote Access, you must add the web server on which you host the contact photos to the HTTP server allow list in your Cisco Expressway-C server configuration. The HTTP server allow list enables the client to access web services inside the corporate network.

• All contact photos must follow the format of the URL you specify as the value of UdsPhotoUriWithToken.

Contact Photo Formats and Dimensions

To achieve the best result with Cisco Jabber, your contact photos should have specific formats and dimensions. Review supported formats and optimal dimensions. Learn about adjustments the client makes to contact photos.

Contact Photo Formats

Cisco Jabber supports the following formats for contact photos in your directory:

• JPG
• PNG
• BMP
• GIF

Important

Cisco Jabber does not apply any modifications to enhance rendering for contact photos in GIF format. As a result, contact photos in GIF format might render incorrectly or with less than optimal quality. To obtain the best quality, use PNG format for your contact photos.

Contact Photo Dimensions

Tip

The optimum dimensions for contact photos are 128 pixels by 128 pixels with an aspect ratio of 1:1. 128 pixels by 128 pixels are the maximum dimensions for local contact photos in Microsoft Outlook.

The following table lists the different dimensions for contact photos in Cisco Jabber.
Integrate with Directory Sources

## Contact Photo Adjustments

Cisco Jabber adjusts contact photos as follows:

<table>
<thead>
<tr>
<th>Location</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio call window</td>
<td>128 pixels by 128 pixels</td>
</tr>
<tr>
<td>Invitations and reminders, for example:</td>
<td>64 pixels by 64 pixels</td>
</tr>
<tr>
<td>• Incoming call windows</td>
<td></td>
</tr>
<tr>
<td>• Meeting reminder windows</td>
<td></td>
</tr>
<tr>
<td>Lists of contacts, for example:</td>
<td>32 pixels by 32 pixels</td>
</tr>
<tr>
<td>• Contact lists</td>
<td></td>
</tr>
<tr>
<td>• Participant rosters</td>
<td></td>
</tr>
<tr>
<td>• Call history</td>
<td></td>
</tr>
<tr>
<td>• Voicemail messages</td>
<td></td>
</tr>
</tbody>
</table>

**Contact Photo Adjustments**

Cisco Jabber adjusts contact photos as follows:

- **Resizing**—If contact photos in your directory are smaller or larger than 128 pixels by 128 pixels, the client automatically resizes the photos. For example, contact photos in your directory are 64 pixels by 64 pixels. When Cisco Jabber retrieves the contact photos from your directory, it resizes the photos to 128 pixels by 128 pixels.

  ![Tip]

  Resizing contact photos can result in less than optimal resolution. For this reason, use contact photos that are 128 pixels by 128 pixels so that the client does not automatically resize them.

- **Cropping**—Cisco Jabber automatically crops nonsquare contact photos to a square aspect ratio, or an aspect ratio of 1:1 where the width is the same as the height.

- **Portrait orientation**—If contact photos in your directory have portrait orientation, the client crops 30 percent from the top and 70 percent from the bottom.

  For example, if contact photos in your directory have a width of 100 pixels and a height of 200 pixels, Cisco Jabber needs to crop 100 pixels from the height to achieve an aspect ratio of 1:1. In this case, the client crops 30 pixels from the top of the photos and 70 pixels from the bottom of the photos.

- **Landscape orientation**—If contact photos in your directory have landscape orientation, the client crops 50 percent from each side.

  For example, if contact photos in your directory have a width of 200 pixels and a height of 100 pixels, Cisco Jabber needs to crop 100 pixels from the width to achieve an aspect ratio of 1:1. In this case, the client crops 50 pixels from the right side of the photos and 50 pixels from the left side of the photos.

- **Rounding**—Cisco Jabber rounds the corners of contact photos after retrieving them from your directory.
Directory Server Configuration Examples

This section describes supported integration scenarios and provides example configurations.

Domain Controller Connection

To connect to a Domain Controller, set the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectionType</td>
<td>1</td>
</tr>
</tbody>
</table>

The following is an example configuration:

```xml
<Directory>
  <ConnectionType>1</ConnectionType>
</Directory>
```

Manual Server Connection

To manually connect to a directory server, set the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrimaryServerName</td>
<td>FQDN, IP address</td>
</tr>
<tr>
<td>ServerPort1</td>
<td>Port number</td>
</tr>
<tr>
<td>SecondaryServerName</td>
<td>FQDN, IP address</td>
</tr>
<tr>
<td>ServerPort2</td>
<td>Port number</td>
</tr>
</tbody>
</table>

The following is an example configuration:

```xml
<Directory>
  <PrimaryServerName>primary-server-name.domain.com</PrimaryServerName>
  <ServerPort1>1234</ServerPort1>
  <SecondaryServerName>secondary-server-name.domain.com</SecondaryServerName>
  <ServerPort2>5678</ServerPort2>
</Directory>
```

UDS Integration

To integrate with UDS, set the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DirectoryServerType</td>
<td>UDS</td>
</tr>
<tr>
<td>UdsServer</td>
<td>IP address of the UDS server</td>
</tr>
<tr>
<td>UdsPhotoUriWithToken</td>
<td>Contact photo URL</td>
</tr>
</tbody>
</table>
Integrate with Directory Sources

LDAP Integration with Expressway for Mobile and Remote Access

When you deploy Expressway for Mobile and Remote Access with an LDAP directory integration, the client uses:

- LDAP when inside the corporate firewall
- UDS when outside the corporate firewall

LDAP is the default configuration, so it is not necessary to include the DirectoryServerType parameter in your client configuration file.

To ensure that the client can resolve contact photos from both inside and outside your corporate firewall, set the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PhotoUriWithToken</td>
<td>Contact photo URL when inside the corporate firewall</td>
</tr>
<tr>
<td>BDIPhotoUriWithToken</td>
<td>Contact photo URL when inside the corporate firewall</td>
</tr>
<tr>
<td>UdsPhotoUriWithToken</td>
<td>Contact photo URL when outside the corporate firewall</td>
</tr>
</tbody>
</table>

The following is an example configuration:

```xml
<Directory>
    <PhotoUriWithToken>http://photo.example.com/sAMAccountName.jpg</PhotoUriWithToken>
    <BDIPhotoUriWithToken>http://photo.example.com/sAMAccountName.jpg</BDIPhotoUriWithToken>
    <UdsPhotoUriWithToken>http://server-name/%uid%.jpg</UdsPhotoUriWithToken>
</Directory>
```
Simple Authentication for Cisco Jabber for Windows

Simple authentication lets you connect to a directory server using simple binds, as in the following example configuration:

```
<UseWindowsCredentials>0</UseWindowsCredentials>
<UseSSL>0</UseSSL>
<UseSecureConnection>0</UseSecureConnection>
<ConnectionUsername>username</ConnectionUsername>
<ConnectionPassword>password</ConnectionPassword>
```

This configuration specifies that the client:

- Does not use Microsoft Windows credentials.
- Does not use SSL.
- Uses simple authentication.
- Uses custom credentials.

As a result of the simple bind, the client transmits the credentials in the payload of the bind request in plain text.

Simple Authentication with SSL for Cisco Jabber for Windows

Enable SSL in directory server connections with the UseSSL parameter. You can use SSL to encrypt credentials when you use simple authentication, as in the following example configuration:

```
<UseWindowsCredentials>0</UseWindowsCredentials>
<UseSSL>1</UseSSL>
<UseSecureConnection>0</UseSecureConnection>
<ConnectionUsername>username</ConnectionUsername>
<ConnectionPassword>password</ConnectionPassword>
```

This configuration specifies that the client:

- Does not use Microsoft Windows credentials.
- Uses SSL.
- Uses simple authentication.
- Uses custom credentials.

As a result, the client uses SSL to encrypt the credentials in the client configuration.

OpenLDAP Integration

You can integrate with OpenLDAP using anonymous binds or authenticated binds.

Anonymous Binds for Cisco Jabber for Windows

To integrate with OpenLDAP using anonymous binds, set the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectionType</td>
<td>1</td>
</tr>
</tbody>
</table>
### Parameter	Value

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrimaryServerName</td>
<td>IP address</td>
</tr>
<tr>
<td></td>
<td>Hostname</td>
</tr>
<tr>
<td>UseWindowsCredentials</td>
<td>0</td>
</tr>
<tr>
<td>UseSecureConnection</td>
<td>1</td>
</tr>
<tr>
<td>SearchBase1</td>
<td>Root of the directory service or the organizational unit (OU)</td>
</tr>
<tr>
<td>UserAccountName</td>
<td>Unique identifier such as UID or CN</td>
</tr>
<tr>
<td>BaseFilter</td>
<td>Object class that your directory service uses; for example, inetOrgPerson.</td>
</tr>
<tr>
<td>PredictiveSearchFilter</td>
<td>UID or other search filter</td>
</tr>
</tbody>
</table>

The following is an example configuration:

```
<Directory>
  <ConnectionType>1</ConnectionType>
  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <UseWindowsCredentials>0</UseWindowsCredentials>
  <UseSecureConnection>1</UseSecureConnection>
  <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
  <UserAccountName>uid</UserAccountName>
  <BaseFilter>(&amp;(objectClass/inetOrgPerson))</BaseFilter>
  <PredictiveSearchFilter>uid</PredictiveSearchFilter>
</Directory>
```

### Authenticated Binds for Cisco Jabber for Windows

To integrate with OpenLDAP using authenticated binds, set the following parameters:

### Parameter	Value

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectionType</td>
<td>1</td>
</tr>
<tr>
<td>PrimaryServerName</td>
<td>IP address</td>
</tr>
<tr>
<td></td>
<td>Hostname</td>
</tr>
<tr>
<td>UserWindowsCredentials</td>
<td>0</td>
</tr>
<tr>
<td>UseSecureConnection</td>
<td>0</td>
</tr>
<tr>
<td>SearchBase1</td>
<td>Root of the directory service or the organizational unit (OU)</td>
</tr>
<tr>
<td>UserAccountName</td>
<td>Unique identifier such as UID or CN</td>
</tr>
<tr>
<td>BaseFilter</td>
<td>Object class that your directory service uses; for example, inetOrgPerson.</td>
</tr>
<tr>
<td>PredictiveSearchFilter</td>
<td>UID or other search filter</td>
</tr>
</tbody>
</table>
AD LDS Integration

You can integrate with AD LDS or ADAM using specific configurations.

Anonymous Binds

To integrate with AD LDS or ADAM using anonymous binds, set the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrimaryServerName</td>
<td>IP address</td>
</tr>
<tr>
<td></td>
<td>Hostname</td>
</tr>
<tr>
<td>ServerPort1</td>
<td>Port number</td>
</tr>
<tr>
<td>UseWindowsCredentials</td>
<td>0</td>
</tr>
<tr>
<td>UseSecureConnection</td>
<td>1</td>
</tr>
<tr>
<td>SearchBase1</td>
<td>Root of the directory service or the organizational unit (OU)</td>
</tr>
</tbody>
</table>

The following is an example configuration:

```xml
<Directory>
  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <ServerPort1>50000</ServerPort1>
  <UseWindowsCredentials>0</UseWindowsCredentials>
  <UseSecureConnection>1</UseSecureConnection>
  <SearchBase1>dc=adam,dc=test</SearchBase1>
</Directory>
```

Windows Principal User Authentication

To integrate with AD LDS or ADAM using authentication with the Microsoft Windows principal user, set the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectionUsername</td>
<td>Username</td>
</tr>
<tr>
<td>ConnectionPassword</td>
<td>Password</td>
</tr>
</tbody>
</table>

The following is an example configuration:

```xml
<Directory>
  <ConnectionType>1</ConnectionType>
  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <UserWindowsCredentials>0</UserWindowsCredentials>
  <UseSecureConnection>0</UseSecureConnection>
  <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
  <BaseFilter>(&amp;(objectClass=inetOrgPerson)</BaseFilter>
  <PredictiveSearchFilter>uid</PredictiveSearchFilter>
  <ConnectionUsername>cn=lds-read-only-user,dc=cisco,dc=com</ConnectionUsername>
  <ConnectionPassword>password</ConnectionPassword>
</Directory>
```
### AD LDS Principal User Authentication

To integrate with AD LDS or ADAM using authentication with the AD LDS principal user, set the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrimaryServerName</td>
<td>IP address&lt;br&gt;Hostname</td>
</tr>
<tr>
<td>ServerPort1</td>
<td>Port number</td>
</tr>
<tr>
<td>UseWindowsCredentials</td>
<td>0</td>
</tr>
<tr>
<td>UseSecureConnection</td>
<td>1</td>
</tr>
<tr>
<td>ConnectionUsername</td>
<td>Username</td>
</tr>
<tr>
<td>ConnectionPassword</td>
<td>Password</td>
</tr>
<tr>
<td>UserAccountName</td>
<td>Unique identifier such as UID or CN</td>
</tr>
<tr>
<td>SearchBase1</td>
<td>Root of the directory service or the organizational unit (OU)</td>
</tr>
</tbody>
</table>

The following is an example configuration:

```xml
<Directory>
  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <ServerPort1>50000</ServerPort1>
  <UseWindowsCredentials>0</UseWindowsCredentials>
  <UseSecureConnection>1</UseSecureConnection>
  <ConnectionUsername>cn=administrator,dc=cisco,dc=com</ConnectionUsername>
  <ConnectionPassword>password</ConnectionPassword>
  <UserAccountName>cn</UserAccountName>
  <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
</Directory>
```
<Directory>
<PrimaryServerName>11.22.33.456</PrimaryServerName>
<ServerPort1>50000</ServerPort1>
<UseWindowsCredentials>0</UseWindowsCredentials>
<UseSecureConnection>0</UseSecureConnection>
<ConnectionUsername>cn=administrator,dc=cisco,dc=com</ConnectionUsername>
<ConnectionPassword>password</ConnectionPassword>
<UserAccountName>cn</UserAccountName>
<SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
</Directory>

Federation

Federation lets Cisco Jabber users communicate with users who are provisioned on different systems and who are using client applications other than Cisco Jabber.

Interdomain Federation

Interdomain federation enables Cisco Jabber users in an enterprise domain to share availability and send instant messages with users in another domain.

• Cisco Jabber users must manually enter contacts from another domain.

• Cisco Jabber supports federation with the following:
  • Microsoft Office Communications Server
  • Microsoft Lync
  • IBM Sametime
  • XMPP standard-based environments such as Google Talk

Note
Expressway for Mobile and Remote Access doesn’t enable XMPP Interdomain federation itself. Cisco Jabber clients connecting over Expressway for Mobile and Remote Access can use XMPP Interdomain federation if it has been enabled on Cisco Unified Communications Manager IM and Presence.

• AOL Instant Messenger

You configure interdomain federation for Cisco Jabber on Cisco Unified Communications Manager IM and Presence Service. See the appropriate server documentation for more information.

Related Topics
Integration Guide for Configuring Cisco Unified Presence Release 8.6 for Interdomain Federation
Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager
Intradomain Federation

Intradomain federation enables users within the same domain to share availability and send instant messages between Cisco Unified Communications Manager IM and Presence Service and Microsoft Office Communications Server, Microsoft Live Communications Server, or another presence server.

Intradomain federation allows you to migrate users to Cisco Unified Communications Manager IM and Presence Service from a different presence server. For this reason, you configure intradomain federation for Cisco Jabber on the presence server. See the following for more information:

- Cisco Unified Communications Manager IM and Presence Service: Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager

Configure Intradomain Federation for BDI or EDI

In addition to configuring intradomain federation on the presence server, you might need to specify some configuration settings in the Cisco Jabber configuration files.

To resolve contacts during contact search or retrieve contact information from your directory, Cisco Jabber requires the contact ID for each user. Cisco Unified Communications Manager IM & Presence server uses a specific format for resolving contact information that does not always match the format on other presence servers such as Microsoft Office Communications Server or Microsoft Live Communications Server.

The parameters that you use to configure intradomain federation depend on whether you use Enhanced Directory Integration (EDI) or Basic Directory Integration (BDI). EDI uses native Microsoft Windows APIs to retrieve contact data from the directory service and is only used by Cisco Jabber for Windows. For BDI, the client retrieves contact data from the directory service and is used by Cisco Jabber for Mac, Cisco Jabber for Android, and Cisco Jabber for iPhone and iPad.

Procedure

**Step 1**

Set the value of the relevant parameter to true:

- For BDI: BDIUseSipUriToResolveContacts
- For EDI: UseSIPURIToResolveContacts

**Step 2**

Specify an attribute that contains the Cisco Jabber contact ID that the client uses to retrieve contact information. The default value is msRTCSIP-PrimaryUserAddress, or you can specify another attribute in the relevant parameter:

- For BDI: BDISipUri
- For EDI: SipUri
When you deploy intradomain federation and the client connects with Expressway for Mobile and Remote Access from outside the firewall, contact search is supported only when the contact ID uses one of the following formats:

- sAMAccountName@domain
- UserPrincipalName (UPN)@domain
- EmailAddress@domain
- employeeNumber@domain
- phoneNumber@domain

**Note**

In the UriPrefix parameter, specify any prefix text that precedes each contact ID in the relevant SipUri parameter.

**Example:**

For example, you specify msRTCSIP-PrimaryUserAddress as the value of SipUri. In your directory the value of msRTCSIP-PrimaryUserAddress for each user has the following format: sip:username@domain.

- For BDI: BDIUriPrefix
- For EDI: UriPrefix

**Example**

The following XML snippet provides an example of the resulting configuration for BDI:

```xml
<Directory>
  <BDIUseSIPURIToResolveContacts>true</BDIUseSIPURIToResolveContacts>
  <BDISipUri>non-default-attribute</BDISipUri>
  <BDIUriPrefix>sip:</BDIUriPrefix>
</Directory>
```

The following XML snippet provides an example of the resulting configuration for EDI:

```xml
<Directory>
  <UseSIPURIToResolveContacts>true</UseSIPURIToResolveContacts>
  <SipUri>non-default-attribute</SipUri>
  <UriPrefix>sip:</UriPrefix>
</Directory>
```

**Related Topics**

- Example of Intradomain Federation, on page 184

**Example of Intradomain Federation**

The following example shows how to create intradomain federation contacts using the following BDI or EDI parameters and example values:
For BDI: SipUri
For EDI: SipURI
Value: msRTCSIP-PrimaryUserAddress

For BDI: UseSIPURIToResolveContacts
For EDI: UseSIPURIToResolveContacts
Value: true

For BDI: UriPrefix
For EDI: UriPrefix
Value: sip

For the user Mary Smith, the directory contains sip:msmith@domain.com as the value of the msRTCSIP-PrimaryUserAddress attribute.

The following workflow describes how the client connects to your directory to resolve contact information for Mary Smith:

1. Your presence server passes msmith@domain.com to the client.
2. The client adds sip: to msmith@domain.com and then queries your directory.
3. sip:msmith@domain.com matches the value of the msRTCSIP-PrimaryUserAddress attribute.
4. The client retrieves contact information for Mary Smith.

When Cisco Jabber users search for Mary Smith, the client removes the sip: prefix from sip:msmith@domain.com to get her contact ID.

**Related Topics**
- Configure Intradomain Federation for BDI or EDI, on page 183
Example of Intradomain Federation
Customize Cisco Jabber for Windows

Review what features you can customize after installation. Learn how to change these features to meet your organizational requirements.

- Custom Emoticons, on page 187
- Create Custom Embedded Tabs, on page 191

Custom Emoticons

Applies to: Cisco Jabber for Windows

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

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Create a file named emoticonDefs.xml with any text editor.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Specify the emoticon definitions as appropriate in emoticonDefs.xml.</td>
</tr>
<tr>
<td></td>
<td>See Emoticon Definitions for more information on the structure and available parameters for emoticonDefs.xml.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Save and close emoticonDefs.xml.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Save emoticonDefs.xml in the appropriate directory on the file system.</td>
</tr>
</tbody>
</table>

Cisco Jabber for Windows loads emoticon definitions from the following directories on the file system:

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

- Dimensions: 17 x 17 pixels
- Transparent background
- PNG file format
- RGB colors
• The directory can differ depending on your operating system
  • For 32-bit operating systems:
    • Program Files\Cisco Systems\Cisco Jabber\Emoticons
    • Program Files\Cisco Systems\Cisco Jabber\CustomEmoticons
  • For 64-bit operating systems:
    • Program Files(x86)\Cisco Systems\Cisco Jabber\Emoticons
    • Program Files(x86)\Cisco Systems\Cisco Jabber\CustomEmoticons

The Emoticons folder contains the default emoticons for Cisco Jabber for Windows and the default emoticonDefs.xml.

The CustomEmoticons folder does not exist by default. Administrators can create this folder to contain custom emoticon definitions to include in organizational deployments.

Emoticons that you define in the CustomEmoticons folder take precedence over emoticon definitions in the default Emoticons folder.

• %USERPROFILE%\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\CustomEmoticons

This folder contains custom emoticon definitions for individual instances of Cisco Jabber for Windows.

Emoticons that you define in this directory take precedence over emoticon definitions in the CustomEmoticons folder in the installation directory.

Step 5
Restart Cisco Jabber for Windows.

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

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

1. User A defines a custom emoticon in emoticonDefs.xml.
   The custom emoticon definition exists only on User A’s local file system.

2. User A sends that custom emoticon to User B.

3. User B receives only the default key for the custom emoticon. User B does not receive the icon.

Emoticon Definitions
Cisco Jabber for Windows loads emoticon definitions from emoticonDefs.xml.
The following XML snippet shows the basic structure for the emoticon definitions file:
The following table describes the elements and attributes for defining custom emoticons:

<table>
<thead>
<tr>
<th>Element or attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>emoticons</td>
<td>This element contains all emoticon definitions.</td>
</tr>
<tr>
<td>emoticon</td>
<td>This element contains the definition of an emoticon.</td>
</tr>
<tr>
<td>defaultKey</td>
<td>This attribute defines the default key combination that renders the emoticon. Specify any key combination as the value. This attribute is required. defaultKey is an attribute of the emoticon element.</td>
</tr>
<tr>
<td>image</td>
<td>This attribute specifies the filename of the emoticon image. Specify the filename of the emoticon as the value. The emoticon image must exist in the same directory as <code>emoticonDefs.xml</code>. This attribute is required. Cisco Jabber for Windows supports any icon that Internet Explorer can render, including <code>.jpeg</code>, <code>.png</code>, and <code>.gif</code>. image is an attribute of the emoticon element.</td>
</tr>
<tr>
<td>text</td>
<td>This attribute defines the descriptive text that displays in the Insert emoticon dialog box. Specify any string of unicode characters. This attribute is optional. text is an attribute of the emoticon element.</td>
</tr>
<tr>
<td>order</td>
<td>This attribute defines the order in which emoticons display in the Insert emoticon dialog box. Specify an ordinal number beginning from 1 as the value. order is an attribute of the emoticon element. This attribute is required. However, if the value of hidden is <code>true</code> this parameter does not take effect.</td>
</tr>
</tbody>
</table>
### Emoticon Definitions

<table>
<thead>
<tr>
<th>Element or attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| hidden                | This attribute specifies whether the emoticon displays in the **Insert emoticon** dialog box. Specify one of the following as the value:  
| true                  | Specifies the emoticon does not display in the **Insert emoticon** dialog box. Users must enter the key combination to render the emoticon.  
| false                 | Specifies the emoticon displays in the **Insert emoticon** dialog box. Users can select the emoticon from the **Insert emoticon** dialog box or enter the key combination to render the emoticon. This is the default value.  
|                       | This attribute is optional. hidden is an attribute of the emoticon element. |
| alt                   | This element enables you to map key combinations to emoticons. Specify any key combination as the value. For example, if the value of defaultKey is :), you can specify : -) as the value of alt so that both key combinations render the same emoticon. This element is optional. |

---

**Remember**

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

- :callme
- :telephone

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

**Emoticon Definition Example**

```xml
<emoticons>
    <emoticon defaultKey=":)"> image="Emoticons_Smiling.png" text="Smile" order="1">
        <alt>:-)</alt>
        <alt>^_</alt>
    </emoticon>
    <emoticon defaultKey=":)" image="Emoticons_Frowning.png" text="Frown" order="2">
        <alt>:-p</alt>
    </emoticon>
</emoticons>
```
Create Custom Embedded Tabs

You create custom embedded tabs to display HTML content in the client interface.

You define custom embedded tabs as part of your client configuration file. See the Custom Embedded Tabs section for more information.

Related Topics

Custom Embedded Tabs, on page 136
Appendix

Review additional information that can help you successfully deploy or troubleshoot Cisco Jabber for Windows.

- Migrate Your Unified Communications Server Infrastructure, on page 193
- ADSI Error Codes, on page 196

Migrate Your Unified Communications Server Infrastructure

To migrate your unified communications infrastructure, you upgrade your presence server from Cisco Unified Presence version 8.x to Cisco Unified Communications Manager IM and Presence Service version 9.x or higher. You also upgrade Cisco Unified Communications Manager from version 8.x to version 9.x or higher.

Before you begin the migration effort, you should understand the architectural differences in the server versions and how this change impacts the client.

Differences in Server Infrastructures

The key to a successful migration is understanding the differences in the server infrastructures and how these differences impact the client.

Version 8.x Server Infrastructure

In the version 8.x server infrastructure, Cisco Unified Presence is the primary source of authentication and configuration.

You provision users with services and provide the location of servers, including the TFTP and CCMCIP services, on Cisco Unified Presence. Those details reside in the server database. When the client gets the location of Cisco Unified Presence from the _cuplogin SRV record, the client authenticates users and retrieves the details from the database through an interface on Cisco Unified Presence. In this way, the client retrieves configuration and services from the presence server after users sign in.

Version 9.x Server Infrastructure

In the version 9.x server infrastructure, Cisco Unified Communications Manager is the main source of configuration for users.

You define configuration on Cisco Unified Communications Manager in service profiles that you apply to users, groups, or clusters. That configuration holds the location of services that you provision to users as well as other client specific settings. Those details reside in the server database. When the client gets the
The _cisco-uds SRV record, it can discover the user's home cluster. The client can also discover the TFTP and CCMCIP services, get the devices configured for the user, and register the configured devices. The client also then retrieves the service profile that contains additional service configuration and client configuration.

After the client gets the service profile, it can determine the authenticator to which users sign in.

The following diagram illustrates the differences between the version 8.x infrastructure and the version 9.x infrastructure:

**Summary of Differences in Server Infrastructures**

The following table highlights the main differences between the version 8.x infrastructure and the version 9.x infrastructure:

<table>
<thead>
<tr>
<th>Version 8.x Server Infrastructure</th>
<th>Version 9.x Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>You deploy the _cuplogin SRV record.</td>
<td>You deploy the _cisco-uds SRV record.</td>
</tr>
<tr>
<td>The client gets configuration from Cisco Unified Presence.</td>
<td>The client gets configuration from Cisco Unified Communications Manager.</td>
</tr>
</tbody>
</table>
Cisco Unified Presence is the primary source of authentication. Cisco Unified Communications Manager is the primary source of authentication.

After the client gets the service profile, it determines which of the following authenticators users should sign in to:

- **Cisco Unified Communications Manager IM and Presence Service**
  - Full UC and IM only deployments.
- **Cisco Unified Communications Manager**
  - Phone mode deployments.
- **Cisco WebEx service**
  - Cloud-based deployments.

You can configure directory integration and additional client settings in client configuration files.

You must configure directory integration and some client settings in the service profile.

You must provision users with telephony capabilities with TFTP and CCMCIP services.

The client discovers TFTP and UDS services when it finds the user's home cluster.

**Remember**
- UDS replaces CCMCIP in the Cisco Unified Communications Manager version 9.x infrastructure. You do not need to provision users with CCMCIP profiles.

The client gets the device configuration and registers devices after sign in.

The client gets the device configuration and registers devices before sign in.

---

### Upgrade Servers from Version 8.x to Version 9.x or Higher

To upgrade servers from version 8.x to version 9.x or higher, you should take a phased approach. Upgrade your server infrastructure first and leave existing configuration in place. After you upgrade all servers across your infrastructure, you should then migrate service profiles from Cisco Unified Presence to Cisco Unified Communications Manager. When all users have service profiles on Cisco Unified Communications Manager version 9.x, you can deploy the `_cisco-uds` SRV record.

The steps to migrate your unified communication server infrastructure are as follows:

**Procedure**

**Step 1**
Upgrade your server infrastructure.

You should perform the required steps to upgrade each node in the cluster, one cluster at a time.

Leave existing configuration for users until you have upgraded servers across all clusters. The client can retrieve existing configuration, including settings you define for services in Cisco Unified Presence, from Cisco Unified Communications Manager IM and Presence Service using the `_cuplogin` SRV record.

**Step 2**
Provision users with service profiles on Cisco Unified Communications Manager.

**Step 3**
Deploy the `_cisco-uds` SRV record.
When you verify that all users in the deployment can successfully sign in and get all provisioned services, you should remove the `_cuplogin` SRV record.

## ADSI Error Codes

Cisco Jabber for Windows uses Microsoft Active Directory Service Interfaces (ADSI) for directory integration. You should refer to the ADSI error codes to help troubleshoot directory integration issues.

See the following Microsoft documentation for information about ADSI error codes:

- *Error Codes for ADSI 2.5* at [http://support.microsoft.com/kb/242076](http://support.microsoft.com/kb/242076)