Cisco Jabber for Mac 9.6 Installation and Configuration Guide

First Published: April 16, 2014

Last Modified: June 06, 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Introduction

Cisco Jabber 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

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

Release Notes

http://www.cisco.com/en/US/partner/products/ps11764/prod_release_notes_list.html

End-User Guides

http://www.cisco.com/en/US/partner/products/ps11764/products_user_guide_list.html

Licensing Information

http://www.cisco.com/en/US/partner/products/ps11764/products_licensing_information_listing.html

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.

http://www.cisco.com/cisco/web/support/index.html

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

CHAPTER 2

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 Mac

Installed RAM

2 GB RAM

Free Physical Memory

1 GB

Free Disk Space

300 MB

CPU Speed and Type

Intel Core 2 Duo or later processors in any of the following Apple hardware:

- Mac Pro
- MacBook Pro (including Retina Display model)
- MacBook
- MacBook Air
- iMac
- Mac Mini

I/O Ports

USB 2.0 for USB camera and audio devices.

Software Requirements

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

Operating Systems for Cisco Jabber for Mac

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

- Apple OS X Lion Version 10.7.4 (or later)
- Apple OS X Mountain Lion 10.8.1 (or later)
- Apple OS X Mavericks 10.9 (or later)

This version of Cisco Jabber for Mac is not supported on Apple OS X Yosemite 10.10

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

Cisco Jabber supports the following on-premises servers:

- Cisco Unified Communications Manager version 8.0(1) or later
- Cisco Unified Presence version 8.0(3) or later
- Cisco Unity Connection version 8.5 or later
- Cisco WebEx Meetings Server version 2.0 or later
- Cisco Expressway Series for Cisco Unified Communications Manager
    - Cisco Expressway-E Version 8.1.1
    - Cisco Expressway-C Version 8.1.1

- Cisco TelePresence Video Communication Server
  - Cisco VCS Expressway Version 8.1.1
  - Cisco VCS Control Version 8.1.1

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

Restriction Cisco Jabber requires an active connection to the presence server to successfully fall back to Cisco Unified Survivable Remote Site Telephony.

Refer to the *Cisco Unified SCCP and SIP SRST System Administrator Guide* for information about configuring Cisco Unified Survivable Remote Site Telephony at: http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide.html

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.

Cisco Jabber supports high availability with the following servers:

Cisco Unified Presence version 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 IM and Presence version 9.0 and higher

Use the following Cisco Unified Communications IM and Presence 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 Re-Login Parameters

In Cisco Unified Presence and Cisco Unified Communications IM and Presence, 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

8.6: How To Configure High Availability Cisco Unified Presence Deployments
8.6: High Availability Client Login Profiles
8.6: Configuring the Advanced Service Parameters for the Server Recovery Manager
8.6: Impact of Failover to Cisco Unified Presence Clients and Services
9.0(1): High Availability IM and Presence deployments configuration
9.0(1): High Availability client login profiles
9.0(1): Configure advanced service parameters for Server Recovery Manager
9.0(1): Impact of failover to IM and Presence clients and services

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 Service (UDS)

  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.

- OpenLDAP

Restriction Directory integration with OpenLDAP requires you to define specific parameters in a Cisco Jabber configuration file. See *LDAP Directory Servers* for more information.

Local Contacts in Mac Address Book

Cisco Jabber allows users search for and add local contacts in the Mac Address book.

To search for local contacts in Mac Address book with the client, users must install the Address Book plug-in:

1. Select **Jabber** > **Install Mac Address Book Plug-In**.

To enable the Address Book plug-in:

1. Select **Jabber** > **Preferences** > **General** > **Enable "Mac Address Plug-in"**.
2. Restart the client for this to take effect.

To communicate with local contacts in Mac Address book 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 Mac Address book, local contacts must have phone numbers.

CTI Servitude

Cisco Jabber for Windows and Cisco Jabber for Mac support Computer Telephony Integration (CTI) servitude, or CTI control of Cisco Jabber from a third party application.

For more information on CTI servitude, see the CTI documentation for the appropriate version of Cisco Unified Communications Manager.

See the following sites on the Cisco Developer Network for more information about creating applications for CTI control through Cisco Unified Communications Manager APIs:

- Cisco TAPI: http://developer.cisco.com/web/tapi/home
- Cisco JTAPI: http://developer.cisco.com/web/jtapi/home

Ports and Protocols for Cisco Jabber for Windows and Cisco Jabber for Mac

The following table lists outbound ports and protocols that Cisco Jabber uses:

Port	Protocol	Description
443	TCP (XMPP and HTTPS)	XMPP traffic to the Cisco 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.
389	UDP / TCP	LDAP directory server
636	LDAPS	LDAP directory server (secure)
3268	TCP	Global Catalog server
3269	LDAPS	Global Catalog server (secure)
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
37200	SOCKS5 Bytestreams	Peer to peer file transfers. In on-premises deployments, the client also uses this port to send screen captures.
5060	UDP/TCP	Session Initiation Protocol (SIP) call signalling

Port	Protocol	Description
5061	TCP	Secure SIP call signalling

Ports for Additional Services and Protocols

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

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

CTI Supported Devices

Cisco Jabber supports the same CTI devices as Cisco Unified Communications Manager version 8.6(1). See the *CTI Supported Device Matrix* in the *CTI Supported Devices* topic.

Related Topics

CTI Supported Devices

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

Supported Audio Codecs

- G.722.1
  - G.722.1 32k
  - G.722.1 24k

Note G.722.1 is supported on Cisco Unified Communications Manager 8.6.1 or later.

- G.711
  - G.711 A-law

    - G.711 u-law
- G.729a

Supported Video Codecs

- 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	Description	Cisco Unified Communications Manager Versions
ciscocm.installcsfdevicetype.cop.sgn	Adds the CSF device type to Cisco Unified Communications Manager. For more information, see *Software Requirements*.	7.1.3
ciscocm.addcsfsupportfield.cop.sgn	Adds the **CSF Support Field** field for group configuration files. For more information, see *Create Group Configurations*.	8.6.x and lower
cmterm-cupc-dialrule-wizard-0.1.cop.sgn	Publishes application dial rules and directory lookup rules to Cisco Jabber. For more information, see *Publish Dial Rules*.	All supported versions

Related Topics

Download software

Availability Presence on Client

For on-premise deployments, the Cisco Jabber for Mac client displays the **In a meeting (according to my calendar)** checkbox on the **Preferences** > **Status** window.

The client displays the 'In a meeting' availability status when events occur in your calendar:

'In a meeting' availability status comes from Microsoft Exchange

Requires Cisco Unified Presence and Microsoft Exchange integration or Cisco Unified Communications IM and Presence and Microsoft Exchange integration. Applies to on-premise deployments.

Availability status changes to 'In a meeting' if events occur in your calendar when:

Deployment	Select In a meeting (according to my calendar)	Do Not Select In a meeting (according to my calendar)
You enable integration between Cisco Unified Presence and Microsoft Exchange or Cisco Unified Communications IM and Presence and Microsoft Exchange.	Cisco Unified Presence or Cisco Unified Communications IM and Presence sets availability status	Availability status does not change

Note **In a meeting** availability status refers to calendar meetings that are created using the Cisco Unified Presence and Microsoft Exchange integration or Cisco Unified Communications IM and Presence and Microsoft Exchange integration. **In a WebEx meeting** availability status refers to Cisco WebEx meetings. The client does not display other availability statuses from other calendar sources (such as Microsoft Outlook for Mac).

Instant Message Encryption

Cisco Jabber uses TLS to secure 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-premise deployments:

Connection	Protocol	Negotiation Certificate	Expected Encryption Algorithm
Client to server	XMPP over TLS	X.509 Public Key Infrastructure certificate	AES 256 bit

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 Presence

- Cisco Unified Communications IM and Presence

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 Presence and Cisco Unified Communications IM and Presence:

Version	Key Length
Cisco Unified Communications IM and Presence versions 9.0.1 and higher	2048 bit
Cisco Unified Presence versions 8.6.4 and higher	2048 bit
Cisco Unified Presence versions lower than 8.6.4	1024 bit

XMPP Encryption

Cisco Unified Presence and Cisco Unified Communications IM and Presence both use 256 bit length session keys 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 Presence or Cisco Unified Communications IM and Presence. See the following documents for more information about security settings:

- Cisco Unified Presence: *Configuring Security on Cisco Unified Presence*
- Cisco Unified Communications IM and Presence: *Security configuration on IM and Presence*

Instant Message Logging

If required, 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 Presence and Cisco Unified Communications IM and Presence do not encrypt instant messages 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 you log.

See the following documents for more information about compliance:

- Cisco Unified Presence: *Instant Messaging Compliance Guide*
- Cisco Unified Communications IM and Presence: *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*.

For more information about X509 Public Key Infrastructure certificates, see the *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* document.

Related Topics

Instant Messaging Compliance Guide
Configuring Security on Cisco Unified Presence
Instant Messaging Compliance for IM and Presence Service

Internet X.509 Public Key Infrastructure Certificate and CRLProfile
Next Generation Encryption

Cloud-Based Encryption

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

Connection	Protocol	Negotiation Certificate	Expected Encryption Algorithm
Client to server	XMPP within TLS	X.509 Public Key Infrastructure certificate	AES 128 bit

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 length session keys encrypted with the AES algorithm to secure instant message traffic between Cisco Jabber and the Cisco WebEx Messenger service.

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 it logs.

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*.

For more information about X509 Public Key Infrastructure certificates, see the *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* document.

Related Topics

Client to Client Encryption
Internet X.509 Public Key Infrastructure Certificate and CRLProfile
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 you can set with these policies:

Policy combination	Client to client encryption	When the remote client supports AES encryption	When the remote client does not support AES encryption
Support AES Encoding For IM = false **Support No Encoding For IM** = true	No	Cisco Jabber sends unencrypted instant messages. Cisco Jabber does not negotiate a key exchange. As a result, other clients do not send Cisco Jabber encrypted instant messages.	Cisco Jabber sends and receives unencrypted instant messages.
Support AES Encoding For IM = true **Support No Encoding For IM** = true	Yes	Cisco Jabber sends and receives encrypted instant messages. Cisco Jabber displays an icon to indicate instant messages are encrypted.	Cisco Jabber sends encrypted instant messages. Cisco Jabber receives unencrypted instant messages.
Support AES Encoding For IM = true **Support No Encoding For IM** = false	Yes	Cisco Jabber sends and receives encrypted instant messages. Cisco Jabber displays an icon to indicate instant messages are encrypted.	Cisco Jabber does not send or receive instant messages to the remote client. Cisco Jabber displays an error message when users attempt to send instant messages to the remote client.

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 the *About Encryption Levels* topic in the Cisco WebEx documentation.

Related Topics

About Encryption Levels

Local Chat History

If you enable local chat history, Cisco Jabber for Mac does not archive instant messages in an encrypted format. In order to restrict access to chat history, Cisco Jabber saves archives to the following directory: `~/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/History/uri.db`.

For on-premises deployment, 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.

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

Cisco Media Services Interface provides a Mac daemon 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.

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.

Specify a Port Range on the SIP Profile

To specify a port range for the client to use for RTP traffic, do the following:

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
9.0.x: SIP profile setup

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

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.

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 on the Client

For some configurations there is an option to enable differentiated services for calls in the Cisco Jabber for Mac client.

Important This option is enabled by default. Cisco recommends not disabling this option unless you are experiencing issues in the following scenarios:

- You can hear or see other parties, but you cannot be heard or seen
- You are experiencing unexpected Wi-Fi disconnection issues

Disabling differentiated service for calls may degrade voice and video quality.

Procedure

Step 1 Select **Jabber > Preferences > Calls > Advanced**

Step 2 Select **Enable Differentiated Service for Calls**.

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 protocol handlers with the OSX launch services database to enable click-to-call or click-to-IM functionality from web browsers or other applications.

Click to Call protocol handlers - Starts an audio or video call with Cisco Jabber:

- TEL:
- SIP:

- CiscoTEL:

Click to IM protocol handlers - Starts an instant message and opens a chat window in Cisco Jabber:

- XMPP:
- Jabber:
- CiscoIM:

Audio and Video Performance Reference

Attention 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.

Bit Rates for Audio for Cisco Jabber for Windows and Cisco Jabber for Mac

The following table describes bit rates for audio:

Codec	RTP payload in kilobits (kbits) per second	Actual bitrate (kbits per second)	Notes
g.722.1	24/32	54/62	High quality compressed
g.711	64	80	Standard uncompressed
g.729a	8	38	Low quality compressed

Bit Rates for Video for Cisco Jabber for Windows and Cisco Jabber for Mac

The following table describes bit rates for video with g.711 audio:

Resolution	Pixels	Measured bit rate (kbits per second) with g.711 audio
w144p	256 x 144	156
w288p This is the default size of the video rendering window for Cisco Jabber.	512 x 288	320
w448p	768 x 448	570
w576p	1024 x 576	890
720p	1280 x 720	1300

Notes about the preceding table:

- This table does not list all possible resolutions.
- The measured bit rate is the actual bandwidth used (RTP payload + IP packet overhead).

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:

Audio	Interactive video (Main video)
Cisco Jabber uses the maximum audio bit rate	Cisco Jabber allocates the remaining bit rate as follows: The maximum video call bit rate minus the audio bit rate.

Performance Expectations for Bandwidth for Cisco Jabber for Windows and Cisco Jabber for Mac

Cisco Jabber for Mac 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:

Upload speed	Audio	Audio + Interactive video (Main video)
125 kbps under VPN	At bandwidth threshold for g.711. Sufficient bandwidth for g.729a and g.722.1.	Insufficient bandwidth for video.
384 kbps under VPN	Sufficient bandwidth for any audio codec.	w288p (512 x 288) at 30 fps
384 kbps in an enterprise network	Sufficient bandwidth for any audio codec.	w288p (512 x 288) at 30 fps
1000 kbps	Sufficient bandwidth for any audio codec.	w576p (1024 x 576) at 30 fps
2000 kbps	Sufficient bandwidth for any audio codec.	w720p30 (1280 x 720) at 30 fps

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.

CHAPTER 3

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, page 23

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.

Related Topics

Server Setup Guide

CHAPTER 4

Set Up 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 validates those certificates against certificates in the Keychain.

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

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

Required Certificates

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

Server	Certificate
Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service	`HTTP (Tomcat)` `XMPP`
Cisco Unified Communications Manager	`HTTP (Tomcat)`
Cisco Unity Connection	`HTTP (Tomcat)`
Cisco WebEx Meetings Server	`HTTP (Tomcat)`

Server	Certificate
Cisco VCS Expressway Cisco Expressway-E	`Server certificate` (used for HTTP and XMPP)

Important Notes

- You should apply the most recent Service Update (SU) for Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service before you begin the certificate signing process.
- The required certificates apply to all server versions.
- Each node in a cluster, subscribers and publishers, 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

Step 1 Generate a Certificate Signing Request (CSR) on each server that can present a certificate to the client.

Step 2 Submit each CSR to the CA.

Step 3 Upload the certificates that the CA issues to each server.

Certificate Signing Request Formats and Requirements

Public CAs typically require CSRs to conform to specific formats. For example, a public CA might only accept CSRs that:

- 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.

Likewise, 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

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.

You may get invalid certificate messages in either of the below scenarios:

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

To ensure that your certificates are validated when you get a certificate issued by a Certificate Authority (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.
- The identity of the server that presents the certificate matches the identity of the server specified in the certificate.

Note 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, 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 throughout your environment.

Provide XMPP Domain to Clients

The client identifies `XMPP` certificates using the XMPP domain, rather than 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 Select **Save**.

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.

Cancel

The client:

- Does not save the certificate.
- Does not connect to the server.

Continue

The client will connect, but when the user restarts the client they are prompted to accept the certificate again.

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 server, 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.

Cloud-Based Servers

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

- `CAS`
- `WAPI`

Important 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. The root certificate for Cisco WebEx Messenger is the DST Root CA X3 certificate. If your operating system does not contain this certificate you must provide the root certificate.

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, you can find more information for the root certificate on the Apple support website at *http://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.

Important

- Cisco recommends that you update all profile photo URLs that contain an IP address as the server name. You should 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 Cisco Jabber.

You can complete the following steps 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 Replace IP addresses with the Cisco WebEx domain in the **userProfilePhotoURL** field as appropriate.

Step 3 Save the CSV file.

Step 4 Import the CSV file with the Cisco WebEx Administration Tool.

CHAPTER 5

Deployment Options

Learn about options for deploying Cisco Jabber.

On-Premises Deployments

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

Product Modes

For all deployments, the user's primary authentication is to a presence server. You must provision users with instant messaging and presence capabilities as the base for your deployment. You can then provision users with additional services, depending on your requirements.

Full UC

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.

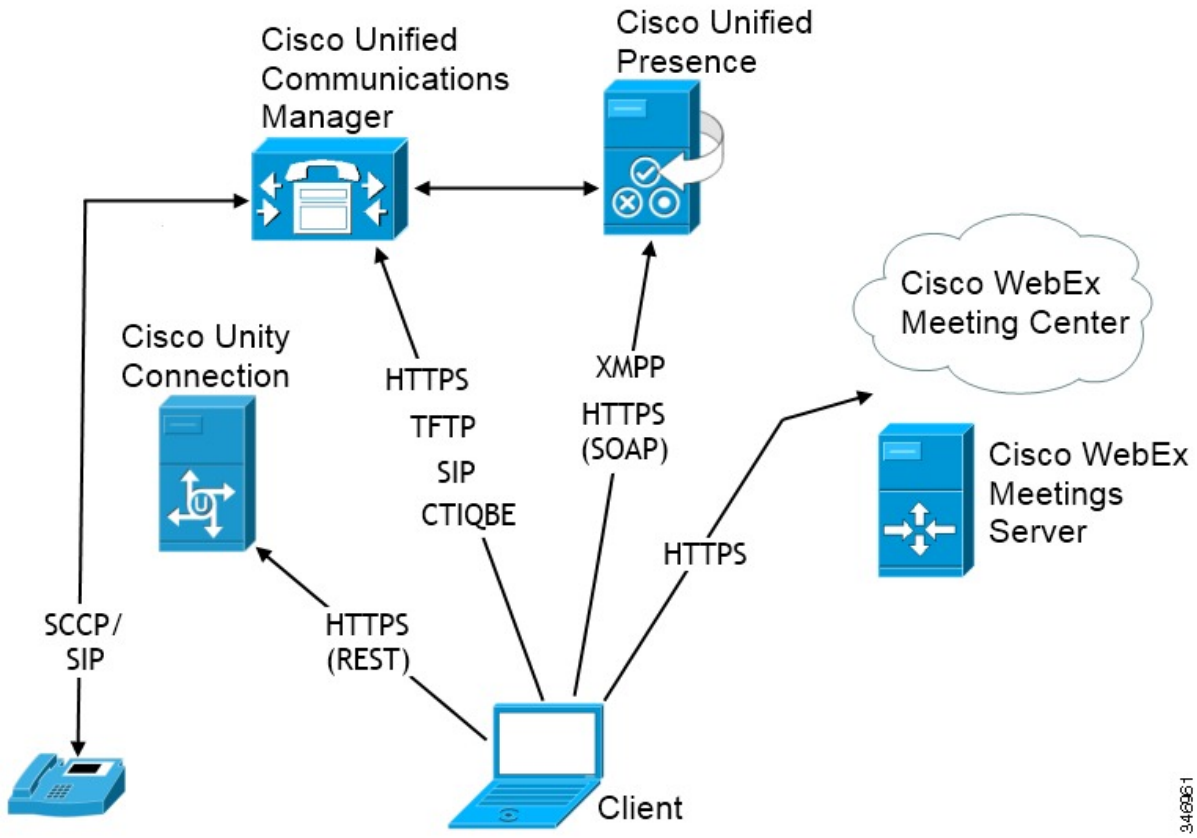
Default Mode Diagrams

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

Diagram with Cisco Unified Presence

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

Figure 1: 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 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 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.

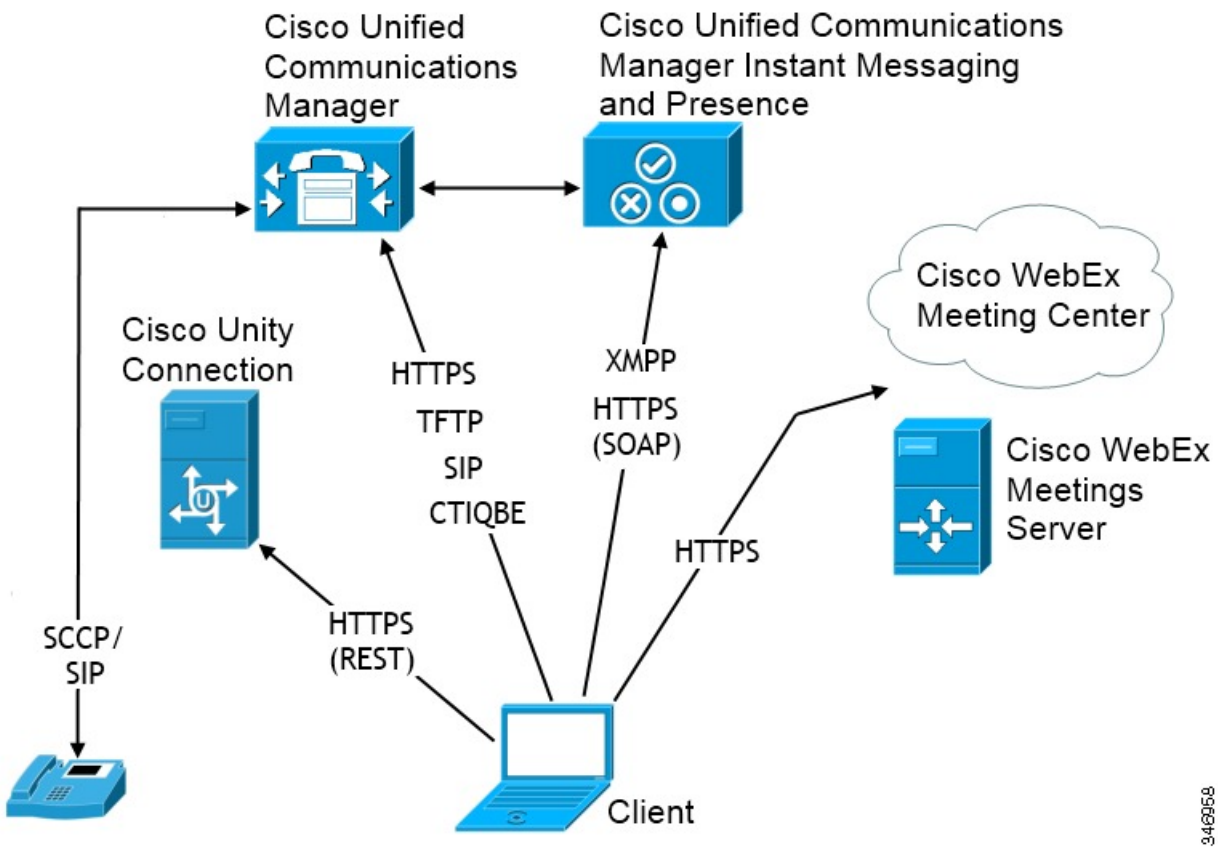
Related Topics

Integrate with Directory Sources, on page 95

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 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 95

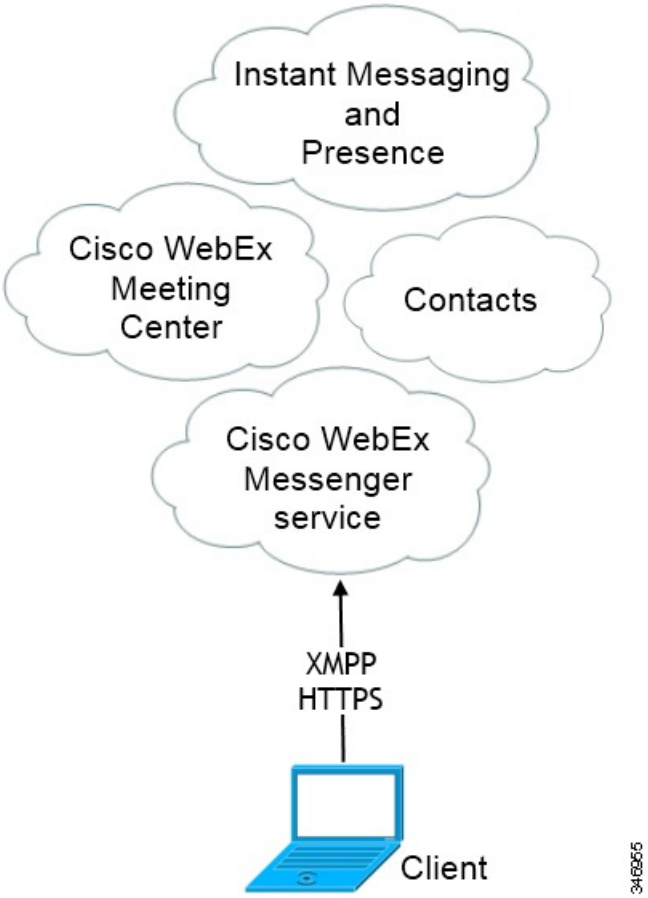
Cloud-Based Deployments

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.

Cloud-Based Diagram

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

Figure 3: 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.

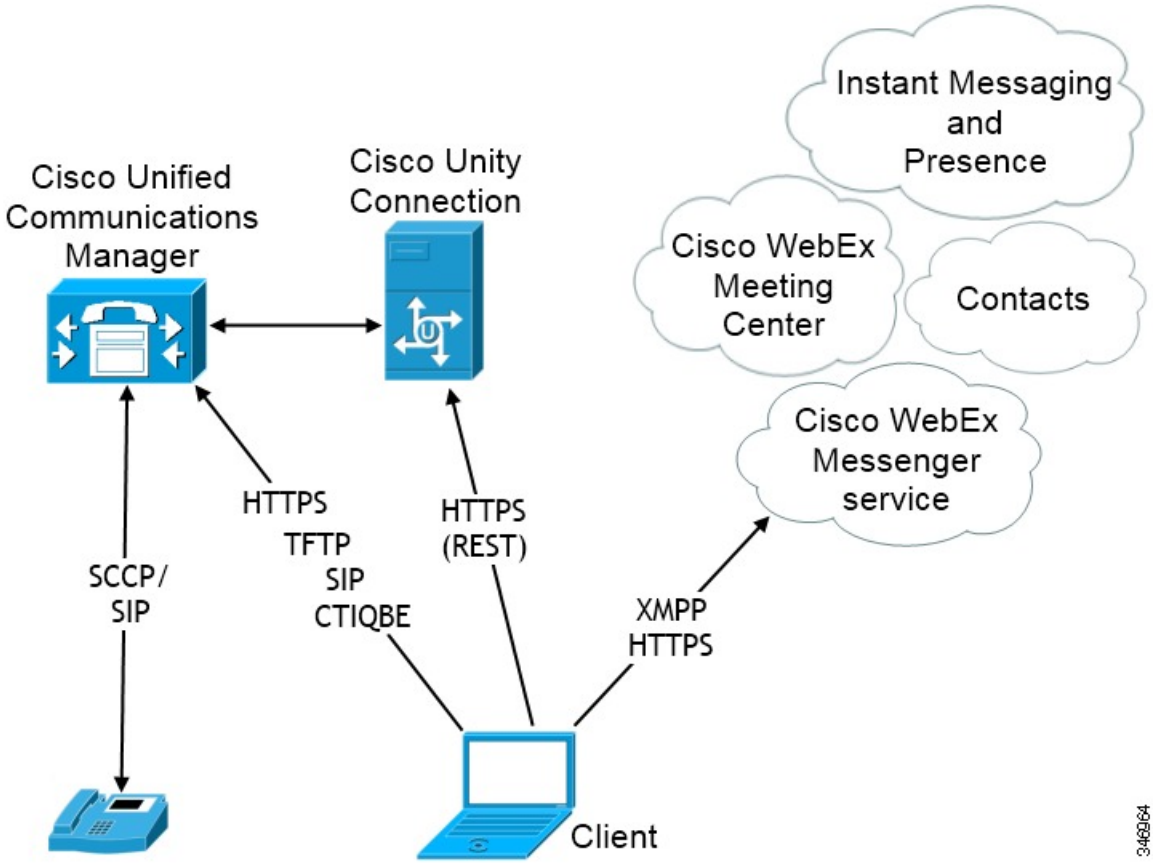
Conferencing

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 4: 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 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:

URL Configuration

Users are sent an email from their administrators. The email contains a URL that will configure the domain needed for service discovery.

Service Discovery

The client automatically locates and connects to services.

Manual Connection Settings

Users manually enter connection settings in the client user interface.

Recommended Connection Methods

The method 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.

On-Premises Deployments for Cisco Jabber for Mac

Product Mode	Server Versions	Discovery Method
Full UC (Default Mode)	Version 9 and higher: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds.<domain>`
Full UC (Default Mode)	Version 8.x: • Cisco Unified Communications Manager • Cisco Unified Presence	A DNS SRV request against `_cuplogin.<domain>`

Hybrid Cloud-Based Deployments

Server Versions	Connection Method
Cisco WebEx Messenger	HTTPS request against `http://loginp.webexconnect.com/cas/FederatedSSO?org=<domain>`

Cloud-Based Deployments

Deployment Type	Connection Method
Enabled for single sign-on (SSO)	Cisco WebEx Administration Tool
Not enabled for SSO	Cisco WebEx Administration Tool

Sources of Authentication

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

There are three possible sources of authentication, as follows:

Cisco Unified 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.

How the Client Gets an Authenticator

Cisco Jabber looks for an authenticator as follows:

1. Client checks cache for manual settings.

   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.

4. Client checks cache for service discovery.

   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.

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

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:

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

Important Migrating from Cisco Unified Presence 8.x to Cisco Unified Communications IM and Presence 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 IM and Presence 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 you can deploy and explains the purpose and benefits of each record:

SRV Record	Purpose	Why You Deploy
`_cisco-uds`	Provides the location of Cisco Unified Communications Manager version 9.0 and higher. 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 CCMCIP profiles or 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.
`_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.

SRV Record	Purpose	Why You Deploy
`_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 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 DNS name server from the DHCP settings.

2 The user employs one of the following methods to discover the service during the first sign-in:

Manual

The user starts Cisco Jabber and then inputs an email-like address on the welcome screen.

URL Configuration

URL configuration allows users to click on a link to cross-launch Cisco Jabber without manually inputting an email.

To create a URL configuration link, you include:

ServicesDomain

The domain that Cisco Jabber uses for service discovery.

VoiceServiceDomain

For a hybrid deployment, the domain that Cisco Jabber uses to retrieve the DNS SRV records can be different from the ServicesDomain that is used to discover Cisco WebEx domain.

ServiceDiscoveryExcludedServices

In certain deployment scenarios services can be excluded from the service discovery process. These values can be a combination of the following:

- WEBEX
- CUCM
- CUP

Note When all three parameters are included, service discovery will not happen and the user will be prompted to manually enter connection settings.

Create the link in the following format:

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

Examples:

- `ciscojabber://provision?servicesdomain=example.com`
- `ciscojabber://provision?servicesdomain=example.com &VoiceServicesDomain=VoiceServices.example.com`
- `ciscojabber://provision?servicesdomain=example.com &ServiceDiscoveryExcludeServices=WEBEX,CUP`

Provide the link to users using email or a web site.

Note If your organization uses a mail application that supports cross launching proprietary protocols or custom links, you can provide the link to users using email, otherwise provide the link to users using a web site.

3. The client gets the address of the DNS name server from the DHCP settings.
4. The client issues an HTTP query to a 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:

```
_cuplogin._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 theCisco 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.

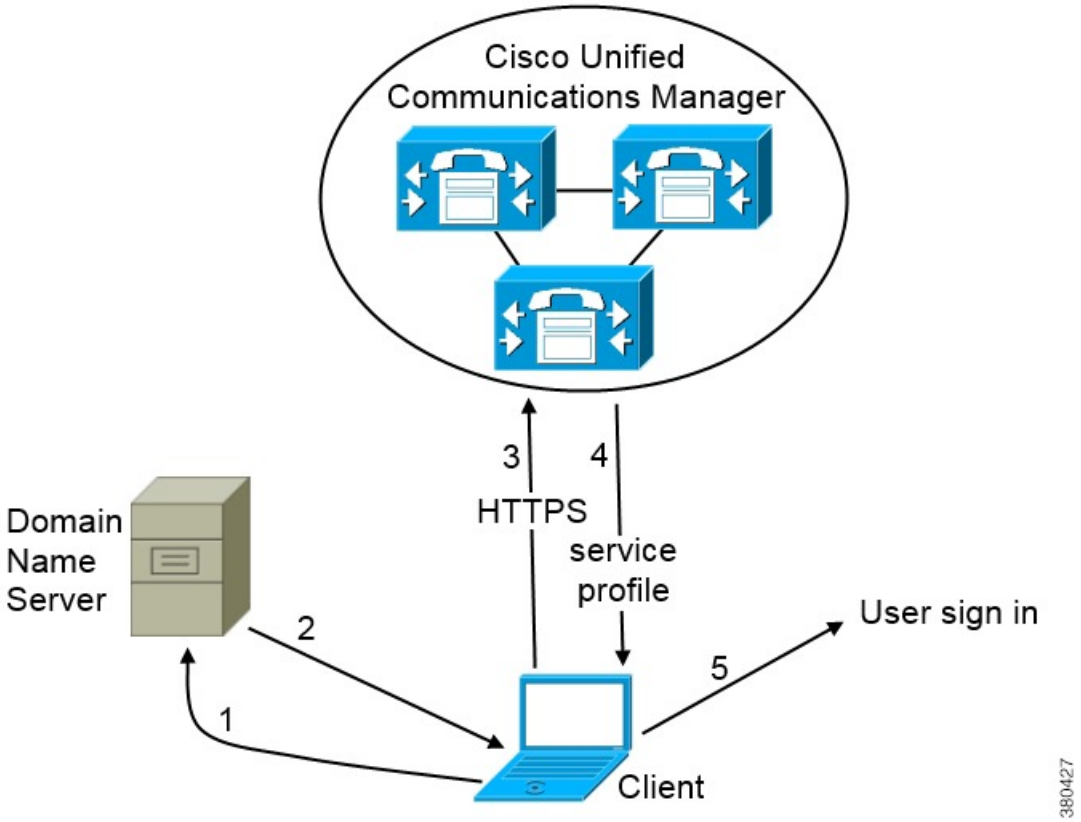
Note The client will use any configured system proxies when sending the HTTP request to the CAS URL. Proxy support for this request has the following limitations :

- 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 higher, the client can automatically discover services and configuration with the following SRV record: `_cisco-uds`.

The following image illustrates how the client uses the `_cisco-uds` SRV record:



1 The client queries the domain name server for SRV records.

2 The name server returns the `_cisco-uds` SRV record.

3 The client locates the user's home cluster.

As a result of automatically locating the user's home cluster, 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, 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.

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 in to the authenticator.

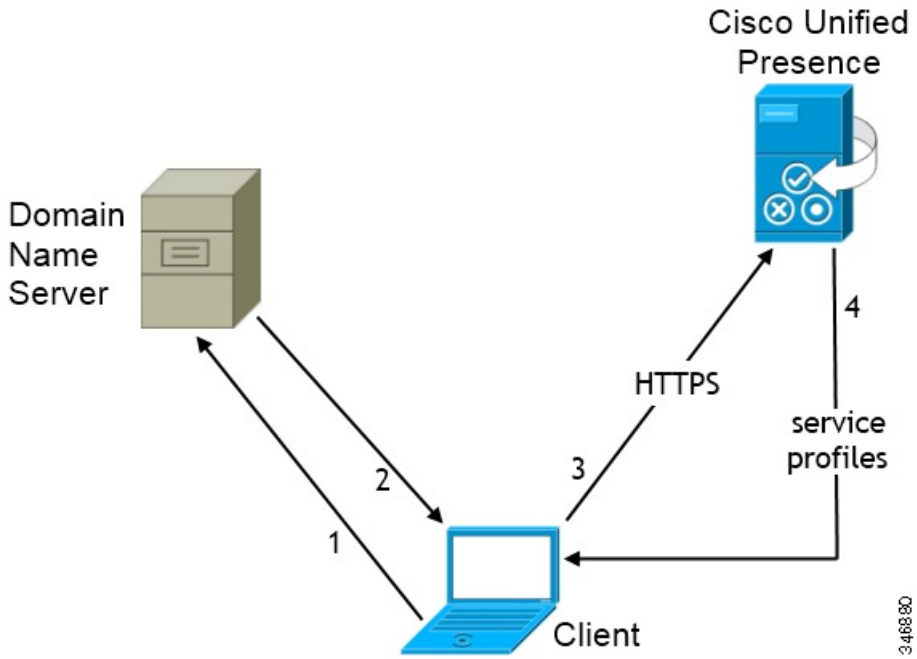
The following is an example of the `_cisco-uds` SRV record:

```
_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
```

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 following SRV record: `_cuplogin`.

The following image illustrates how the client uses the `_cuplogin` SRV record:



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:

```
_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 for Service Discovery in situations where Service Discovery has not been deployed.

When you launch Cisco Jabber, you can specify the authenticator and server addresses in the **Advanced Settings** window. The client then caches the server addresses to the local application configuration that it loads on subsequent launches.

Cisco Jabber prompts users to enter settings in the **Advanced Settings** window on the initial launch as follows:

On-Premises with Cisco Unified Communications Manager Version 9.x and Higher

If the client cannot get the authenticator and server addresses from the service profile.

Cloud-Based or On-Premises with Cisco Unified Communications Manager Version 8.x

The client also prompts users to enter server addresses in the **Advanced Settings** window if you do not set server addresses with SRV records.

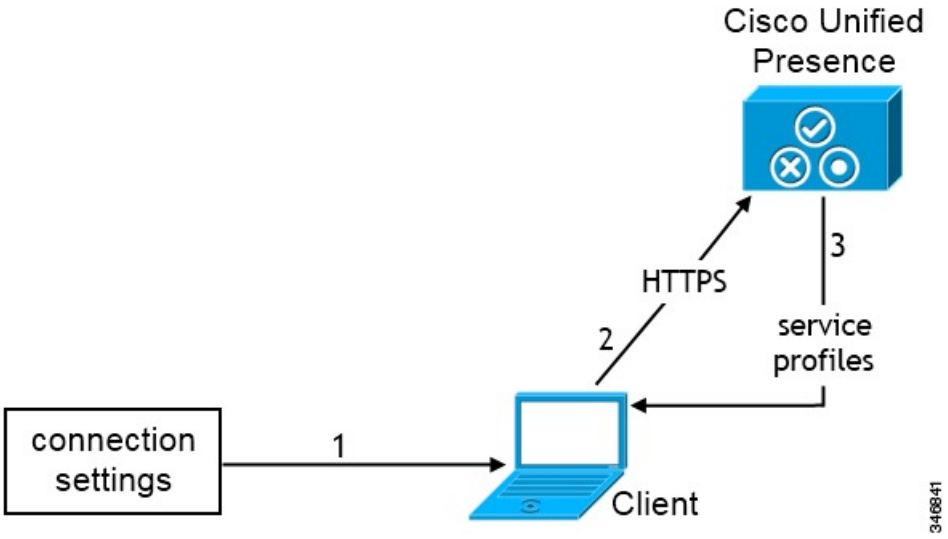
Settings that you enter in the **Advanced Settings** window take priority over any other sources including SRV records.

Manual Connection Settings for On-Premises Deployments

Users can set Cisco Unified Presence as the authenticator and specify the server address in the **Advanced Settings** window.

Remember 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.

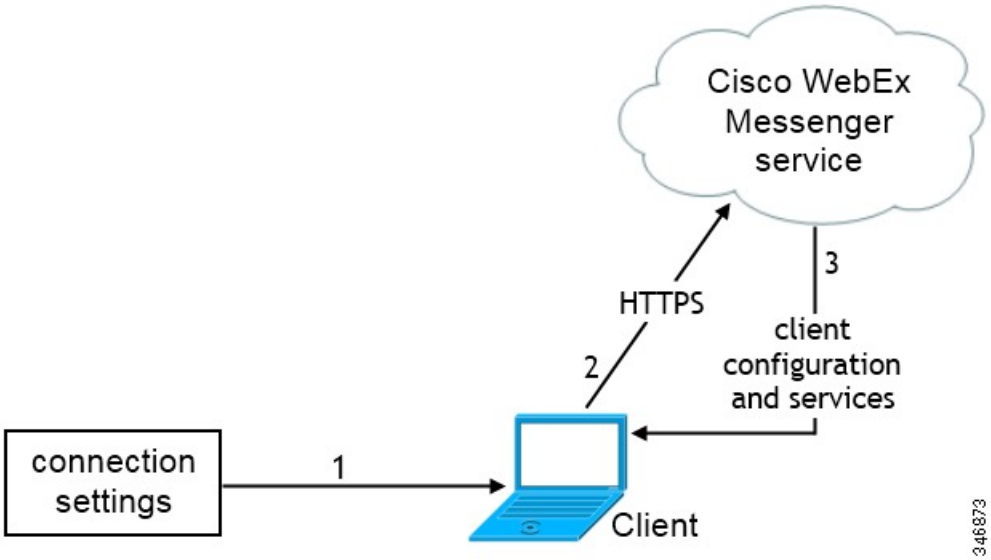
2 The client authenticates to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.

3 The client retrieves service profiles from the presence server.

Manual Connection Settings for 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.

Manual Connection Settings for Service Discovery

Users can select the **Automatic** option in the **Advanced Settings** window to discover servers automatically.

This option lets 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 also take higher priority over SRV records. For this reason, if you decide to deploy SRV records and use service discovery, you must override the manual settings from the initial launch.

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 must do the following to set up the Expressway for Mobile and Remote Access feature:

1. Set up servers to support Expressway for Mobile and Remote Access using Cisco Expressway-E and Cisco Expressway-C.*
   a. 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 Communication 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*.

   b. 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 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.

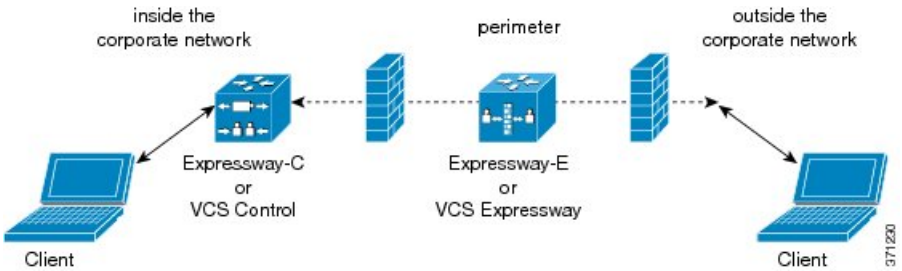
   The Voice Services Domain allows the client to locate the DNS server that contains the `_collab-edge` record.

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.

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

Figure 5: Cisco Jabber for Windows and Mac Architecture Diagram



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 1: Summary of supported services for Expressway for Mobile and Remote Access

Service		Supported	Unsupported
Directory			
	UDS directory search	x	
	LDAP directory search		x
	Directory photo resolution	x * Using HTTP whitelist on Cisco Expressway-C	

Service		Supported	Unsupported
	Intradomain federation	x * Contact search support depends of the format of your contact IDs. For more information, see the note below.	
	Interdomain federation	x	
Instant Messaging and Presence			
	On-premises	x	
	Cloud	x	
	Chat	x	
	Group Chat	x	
	High Availability: On-premises deployments	x	
	File Transfer: On-premises deployments		x
	File Transfer: Cloud deployments	x (Desktop clients only)	
Audio and Video			
	Audio and video calls	x * Cisco Unified Communications Manager 9.1(2) and later	
	Deskphone control mode (CTI)		x
	Extend and Connect		x
	Session persistency		x
	Early media		x
	Self Care Portal access		x
Voicemail			
	Visual voicemail	x * Using HTTP whitelist on Cisco Expressway-C	
Cisco WebEx Meetings			

Service		Supported	Unsupported
	On-premises		x
	Cloud	x	
	Cisco WebEx Desktop Share	x	
Security			
	End-to-end encryption		x
	CAPF enrollment		x
Troubleshooting			
	Problem report generation	x	
	Problem report upload		x

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 whitelist of your Cisco Expressway-C server. To add a server to Cisco Expressway-C whitelist, 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
- UserPrincipleName (UPN)@domain
- EmailAddress@domain
- employeeNumber@domain
- telephoneNumber@domain

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.

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 users start 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.

The 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.

Note To ensure that the client can access voicemail services, you must add the voicemail server to the whitelist of your Cisco Expressway-C server. To add a server to Cisco Expressway-C whitelist, 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 Meeting Center.

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

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.

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 HTTPS to a specified internal server.

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

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.

Install Cisco Media Services Interface

Procedure

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

Traffic Marking

Cisco Media Services Interface provides a Mac daemon 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.

Prepare Your Network

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

Procedure

Step 1 Install Cisco Prime Collaboration Manager.

Step 2 Install routers or switches enabled for Cisco Medianet where appropriate.

Step 3 Configure your network to handle the metadata attributes that Cisco Media Services 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 Services 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

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

Distribute the Cisco Jabber for Mac client

Visit the Cisco Software Center to download the Cisco Jabber for Mac client.

In cloud-based deployments, when the Cisco Jabber client connects to the Cisco WebEx Messenger server, it checks for the latest version. If a new version exists, the Cisco Jabber client prompts the user to upgrade.

CHAPTER 7

Configure Cisco Jabber

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

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 version 9 and higher. 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 version 9 and higher. 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 Presence or 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.

If you do not use service discovery with Cisco Unified Communications Manager version 9 and higher, the client retrieves UC services from Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.

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 Client on Cisco Unified Communications Manager

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

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.

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 Profile

The following table lists the configuration parameters you can set in the instant messaging and presence profile:

IM and Presence Service Configuration	Description
Product type	Provides the source of authentication to Cisco Jabber and has the following values: **Unified CM (IM and Presence)** Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service is the authenticator. **WebEx (IM and Presence)** 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.

IM and Presence Service Configuration	Description
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 Presence or 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:

Voicemail Service Configuration	Description
Voicemail server	Specifies connection settings for the voicemail server.
Credentials source for voicemail service	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.

Conferencing Profile

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

Conferencing Service Configuration	Description
Conferencing server	Specifies connection settings for the conferencing server.
Credentials source for web conference service	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.

Directory Profile

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

CTI Profile

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

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

Add UC Services

Add UC services to specify the address, ports, protocols and other settings for services such as instant messaging and presence, 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 UC 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 version 9.x only, users who have only instant messaging capabilities (IM only) must use the default service profile. For this reason, you should set the service profile as the default if you plan to apply the service profile to IM only users.

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

What to Do Next

Apply service profiles to end user configuration.

Apply Service Profiles

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

Procedure

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

Step 2 Select **User Management** > **End User**.
The **Find and List Users** window opens.

Step 3 Enter the appropriate search criteria to find existing users and then select a user from the list.
The **End User Configuration** window opens.

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

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

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

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

Associate Users with Devices

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

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

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

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

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

Procedure

Step 1 Associate users with devices.

a) Open the **Unified CM Administration** interface.
b) Select **User Management** > **End User**.
c) Find and select the appropriate user.
The **End User Configuration** window opens.
d) Select **Device Association** in the **Device Information** section.
e) Associate the user with devices as appropriate.
f) Return to the **End User Configuration** window and then select **Save**.

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

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

Create 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.

Important 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:

- 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`.

Note Do not rename the jabber-config.xml file. The client does not support jabber-config.xml files with a different name.

Group Configuration Files

Note Group configuration files are supported on Cisco Jabber for Windows only.

Group configuration files apply to subsets of users. Group configuration files take priority over global configuration files.

Cisco Jabber retrieves group configuration files after users sign in to their phone account in the client for the first time. The client then prompts the users to sign out. During the second login sequence, the client downloads the group configuration file from your TFTP server.

Cisco Jabber loads group configuration files as follows:

Users are not signed in

1. Users sign in and then the client notifies the users about the change to their configuration settings.
2. Users sign out.
3. Users sign in and then the client loads the group configuration settings.

Users are signed in and use software phones for calls

1. The client notifies the users about the change to their configuration settings.
2. Users sign out.
3. Users sign in and then the client loads the group configuration settings.

Users are signed in and use desk phones for calls

1. Users sign out.
2. Users sign in and then the client notifies the users about the change to their configuration settings.
3. Users sign out.
4. Users sign in and then the client loads the group configuration settings.

If users select the option to use software phones for calls before they sign out, the client notifies the users to sign out and then sign in again to load the group configuration settings.

Group Configuration File Names

You specify the name of the group configuration files in the **Cisco Support Field** on the CSF 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 device configuration by deleting the entire `configurationFile=`*`group_configuration_file_name.xml`* string or by deleting the group configuration filename from the string.

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 `&` 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 Version 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 Version 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 Version 8.x, complete the steps to specify the address of your TFTP server on Cisco Unified Communications Manager IM and Presence Service. If you are using Cisco Unified Communications Manager Version 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 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 Administration Tool.

Procedure

Step 1 Open the Cisco WebEx Administration Tool.

Step 2 Select the **Configuration** tab.

Step 3 Select **Unified Communications** in the **Additional Services** section.
The **Unified Communications** window opens.

Step 4 Select the **Clusters** tab.

Step 5 Select the appropriate cluster from the list.
The **Edit Cluster** window opens.

Step 6 Select **Advanced Server Settings** in the **Cisco Unified Communications Manager Server Settings** section.

Step 7 Specify the IP address of your primary TFTP server in the **TFTP Server** field.

Step 8 Specify the IP address of your backup TFTP servers in the **Backup Server #1** and **Backup Server #2** fields.

Step 9 Select **Save**.
The **Edit Cluster** window closes.

Step 10 Select **Save** in the **Unified Communications** window.

Create Global Configurations

Configure the client for all users in your deployment.

Remember If your environment has multiple TFTP servers, you must ensure that the configuration file is the same on all TFTP servers.

Procedure

Step 1 Create a file named `jabber-config.xml` with any text editor.

- Use lowercase letters in the filename.
- Use utf-8 encoding.

Step 2 Define the required configuration parameters in `jabber-config.xml`.

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.

Step 3 Host the group configuration file on your TFTP server.

Create Group Configurations

Apply different client configurations to different sets of users.

If you provision users with CSF devices, you specify the group configuration file names in the **Cisco Support Field** field on the device configuration.

If users do not have CSF devices, set a unique configuration file name for each group during installation with the TFTP_FILE_NAME argument.

Before You Begin

The **Cisco Support Field** field does not exist on Cisco Unified Communications Manager version 8.6.x or lower. You must apply a COP file as follows:

1. Download the Cisco Jabber administration package.
2. Copy `ciscocm.addcsfsupportfield.cop` from the Cisco Jabber administration package to your file system.
3. Deploy `ciscocm.addcsfsupportfield.cop` on Cisco Unified Communications Manager.

   See the Cisco Unified Communications Manager documentation for instructions on deploying COP files.

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

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`.

- Use lowercase letters in the filename.
- Use utf-8 encoding.

Step 2 Define the required configuration parameters in the group configuration file.

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.

Step 3 Specify the name of the group configuration file.

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.
The **Phone Configuration** window opens.
d) Navigate to **Product Specific Configuration Layout** > **Desktop Client Settings**.
e) Enter `configurationfile=`*`group_configuration_file_name.xml`* in the **Cisco Support Field** field.
For example, enter the following: `configurationfile=groupa-config.xml`

Use a semicolon to delimit multiple entries. Do not add more than one group configuration file. The client uses only the first group configuration in the **Cisco Support Field** field.
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`.

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

Step 1 Open the **Cisco Unified OS Administration** interface on Cisco Unified Communications Manager.

Step 2 Select **Software Upgrades** > **TFTP File Management**.

Step 3 Select **Upload File**.

Step 4 Select **Browse** in the **Upload File** section.

Step 5 Select the configuration file on the file system.

Step 6 Do not specify a value in the **Directory** text box in the **Upload File** section.
You should leave an empty value in the **Directory** text box so that the configuration file resides in the default directory of the TFTP server.

Step 7 Select **Upload File**.

Restart Your TFTP Server

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

Procedure

Step 1 Open the **Cisco Unified Serviceability** interface on Cisco Unified Communications Manager.

Step 2 Select **Tools** > **Control Center - Feature Services**.

Step 3 Select **Cisco Tftp** from the **CM Services** section.

Step 4 Select **Restart**.
A window displays to prompt you to confirm the restart.

Step 5 Select **OK**.
The **Cisco Tftp Service Restart Operation was Successful** status displays.

Step 6 Select **Refresh** to ensure the **Cisco Tftp** service starts successfully.

What to Do Next

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

Configuration File Structure

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

XML Declaration

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

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

Root Element

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

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

Group Elements

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

Group Elements

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

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

Related Topics

Summary of Configuration Parameters, on page 78

XML Structure

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

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

```
<Phone>
  <parameter>value</parameter>
</Phone>
<Policies>
  <parameter>value</parameter>
</Policies>
<Presence>
  <parameter>value</parameter>
</Presence>
<Voicemail>
  <parameter>value</parameter>
</Voicemail>
```

Summary of Configuration Parameters

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

Parameter	Group Element
Forgot_Password_URL	Client
Set_Status_Away_On_Inactive	Options
Set_Status_Inactive_Timeout	Options
Set_Status_Away_On_Lock_OS	Options
StartCallWithVideo	Options
ShowContactPictures	Options
ShowOfflineContacts	Options
DeviceAuthenticationPrimaryServer	Phone
DeviceAuthenticationBackupServer	Phone
TftpServer1	Phone
TftpServer2	Phone
CtiServer1	Phone
CtiServer2	Phone
useCUCMGroupForCti	Phone
CcmcipServer1	Phone
CcmcipServer2	Phone
Meeting_Server_Address	Phone
Meeting_Server_Address_Backup	Phone
Meeting_Server_Address_Backup2	Phone
EnableDSCPPacketMarking	Phone
EnableVideo	Policies
InitialPhoneSelection	Policies

Parameter	Group Element
UserDefinedRemoteDestinations	Policies
Screen_Capture_Enabled	Policies
File_Transfer_Enabled	Policies
Disallowed_File_Transfer_Types	Policies
Meetings_Enabled	Policies
Telephony_Enabled	Policies
Voicemail_Enabled	Policies
EnableSIPURIDialling	Policies
BDIDirectoryURI	Policies
ServiceDiscoveryExcludedServices	Policies
VoiceServicesDomain	Policies
LoginResource	Presence
PresenceServerAddress	Presence
PresenceServerURL	Presence
VoiceMailService_UseCredentialsFrom	Voicemail
VVM_Mailstore_Server_0	Voicemail

Related Topics

Group Elements, on page 77
Client Parameters, on page 79
Options Parameters, on page 80
Phone Parameters, on page 82
Policies Parameters, on page 85
Presence Parameters, on page 91
Service Credentials Parameters, on page 92
Voicemail Parameters, on page 92
Integrate with Directory Sources, on page 95

Client Parameters

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

Parameter	Value	Description
Forgot_Password_URL	URL	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.

Related Topics

Summary of Configuration Parameters, on page 78

Options Parameters

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

Parameter	Value	Description
Set_Status_Away_On_Inactive	true false	Specifies if the availability status changes to **Away** when users are inactive. **true (default)** Availability status changes to **Away** when users are inactive. **false** Availability status does not change to **Away** when users are inactive.
Set_Status_Inactive_Timeout	Number of minutes	Sets the amount of time, in minutes, before the availability status changes to **Away** if users are inactive. The default value is 15.
Set_Status_Away_On_Lock_OS	true false	Specifies if the availability status changes to **Away** when users lock their operating systems. **true (default)** Availability status changes to **Away** when users lock their operating systems. **false** Availability status does not change to **Away** when users lock their operating systems.

Parameter	Value	Description
StartCallWithVideo	true false	Specifies how calls start when users place calls. Calls can start with audio only or audio and video. **true (default)** Calls always start with audio and video. **false** Calls always start with audio only. **Important** Server settings take priority over this parameter in the client configuration file. However, if users change the default option in the client user interface, that setting takes priority over both the server and client configurations. Configure this setting on the server as follows: **Cisco Unified Presence** 1 Open the **Cisco Unified Presence Administration** interface. 2 Select **Application** > **Cisco Jabber** > **Settings**. 3 Select or clear the **Always begin calls with video muted** parameter and then select **Save**. **Cisco Unified Communications Manager version 9.x and higher** 1 Open the **Cisco Unified CM Administration** interface. 2 Select **System** > **Enterprise Parameters**. 3 Set a value for the **Never Start Call with Video** parameter and then select **Save**.
ShowContactPictures	true false	Specifies if contact pictures display in the contact list. **true (default)** Contact pictures display in the contact list. **false** Contact pictures do not display in the contact list.

Parameter	Value	Description
ShowOfflineContacts	true false	Specifies if offline contacts display in the contact list. **true (default)** Offline contacts display in the contact list. **false** Offline contacts do not display in the contact list.

Related Topics

Summary of Configuration Parameters, on page 78

Phone Parameters

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

Parameter	Value	Description
DeviceAuthenticationPrimaryServer	Hostname IP address FQDN	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: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*)
DeviceAuthenticationBackupServer	Hostname IP address FQDN	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: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*)

Parameter	Value	Description
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.
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.

Parameter	Value	Description
useCUCMGroupForCti	true false	Specifies if the Cisco Unified CM Group handles load balancing for CTI servers. Set one of the following values: **true** The Cisco Unified CM Group handles CTI load balancing. You should set this value in phone mode deployments only. In full UC mode, the presence server automatically handles CTI load balancing. **false (default)** The Cisco Unified CM Group does not handle CTI load balancing.
CcmcipServer1	Hostname IP address FQDN	Specifies the address of the primary CCMCIP server. This parameter is required: • Only if the address of your CCMCIP server is not the same as the TFTP server address. 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.
CcmcipServer2	Hostname IP address FQDN	Specifies the address of the secondary CCMCIP server. This parameter is optional.

Parameter	Value	Description
Meeting_Server_Address	Cisco WebEx meetings site URL	Specifies the primary Cisco WebEx meeting site URL for users. The client populates the meeting site in the user's host account on the **Preferences** > **Meetings** window. Users can enter their credentials to set up the host account and access their meetings site, if the Cisco WebEx meeting site requires credentials. **Important** If you specify an invalid meeting site, users cannot add, or edit, any meetings sites in the client user interface. This parameter is optional.
Meeting_Server_Address_Backup	Cisco WebEx meetings site URL	Specifies the secondary Cisco WebEx meeting site URL for users. This parameter is optional.
Meeting_Server_Address_Backup2	Cisco WebEx meetings site URL	Specifies the tertiary Cisco WebEx meeting site URL for users. This parameter is optional.
EnableDSCPPacketMarking	true false	Specifies if DSCP marking is applied to the packets: **true (default)** DSCP marking is enabled and the checkbox in the client is not shown. **false** DSCP marking is not made to packets and the checkbox in the client is not shown.

Related Topics

Summary of Configuration Parameters, on page 78
TFTP Server Address

Policies Parameters

Policies parameters let you control specific client functionality.

Related Topics

Summary of Configuration Parameters, on page 78

On-Premises Policies

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

Parameter	Value	Description
Screen_Capture_Enabled	true false	Specifies if users can take screen captures. **true (default)** Users can take screen captures. **false** Users cannot take screen captures.
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`.

Common Policies

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

Parameter	Value	Description
EnableVideo	true false	Enables or disables video capabilities. **true (default)** Users can make and receive video calls. **false** Users cannot make or receive video calls.

Parameter	Value	Description
InitialPhoneSelection	deskphone softphone	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. **deskphone** Use the desk phone device for calls. **softphone (default)** Use the software phone (CSF) device for calls. The client selects devices in the following order: **1** Software phone devices **2** Desk phone devices If you do not provision users with software phone devices, the client automatically selects desk phone devices.
UserDefinedRemoteDestinations	true false	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. **true** Users can add, edit, and delete remote destinations. **false (default)** Users cannot add, edit, and delete remote destinations.
Meetings_Enabled	true false	Enables meetings capabilities and user interface in the client. **true (default)** Enables meetings capabilities and user interface. **false** Disables meetings capabilities and user interface.

Parameter	Value	Description
Telephony_Enabled	true false	Enables audio and video capabilities and user interface in the client. **true (default)** Enables audio and video capabilities and user interface. **false** Disables audio and video capabilities and user interface. 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.
Voicemail_Enabled	true false	Enables voicemail capabilities and user interface in the client. **true (default)** Enables voicemail capabilities and user interface. **false** Disables voicemail capabilities and user interface.
EnableSIPURIDialling	true false	Enables URI dialing with Cisco Jabber and allows users to make calls with URIs. **true** Users can make calls with URIs. **false (default)** Users cannot make calls with URIs.

Parameter	Value	Description
BDIDirectoryURI	Directory attribute	Specifies the directory attribute that holds the SIP URI for users. **On-Premises Deployments** Set one of the following as the value: • mail • msRTCSIP-PrimaryUserAddress **Cloud-Based Deployments** Set one of the following as the value: • mail • imaddress • workphone • homephone • mobilephone The mail attribute is used by default. **Important** The value you specify must match the directory URI setting for users in Cisco Unified Communications Manager or the Cisco WebEx Administration Tool.

Parameter	Value	Description

ServiceDiscoveryExcludedServices	WEBEX
	CUCM
	CUP
		Specifies whether to exclude certain services from Service Discovery.
		WEBEX
		When you set this value, the client:
		• Does not perform CAS lookup
		• Looks for `_cisco-uds`, `_cuplogin`, and `_collab-edge`
		CUCM
		When you set this value, the client:
		• Does not look for `_cisco_uds`
		• Looks for `_cuplogin` and `_collab-edge`
		CUP
		When you set this value, the client:
		• Does not look for `_cuplogin`
		• Looks for `_cisco-uds_collab-edge`
		You can specify multiple, comma-separated values to exclude multiple services. For example:
		`<ServiceDiscoveryExcludedServices>`
		`WEBEX,CUCM`
		`</ServiceDiscoveryExcludedServices>`

VoiceServicesDomain	FQDN	Specifies the Fully Qualified Domain Name that represents the DNS domain where the DNS SRV records for *_collab-edge* and *_cisco-uds* are configured. **Example:** Given the following DNS SRV records: • *_collab-edge.*_tls.voice.example.com • *_cisco-uds.*_tcp.voice.example.com The *VoiceServicesDomain* value would be *voice.example.com*.

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

Using policy actions available in Cisco WebEx
Using policy actions available in Cisco WebEx

Presence Parameters

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

Parameter	Value	Description
LoginResource	multiResource wbxconnect	Controls user log in to multiple client instances. **multiResource (default)** Users can log in to multiple instances of the client at the same time. **wbxconnect** Users can log in to one instance of the client at a time. 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.
PresenceServerAddress	Hostname IP address FQDN	Specifies the address of a presence server for on-premises deployments. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*)
PresenceServerURL	CAS URL	Specifies the Central Authentication Service (CAS) URL for the Cisco WebEx Messenger service. The following is an example of a URL you can set as the value: `https://loginp.webexconnect.com/cas/sso/ex_org/orgadmin.app`

Related Topics

Summary of Configuration Parameters, on page 78

Service Credentials Parameters

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

Voicemail Service Credentials

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

Parameter	Value	Description
VoiceMailService_UseCredentialsFrom	phone	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 hybrid cloud-based deployments only. In on-premises deployments, you should set the credentials source for voicemail services on the presence server.

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

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

Related Topics

Summary of Configuration Parameters, on page 78
Voicemail Parameters, on page 92

Voicemail Parameters

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

Key	Value	Description
VVM_Mailstore_Server_0	Hostname IP address FQDN	Specifies the address of your voicemail server. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*)

Related Topics

Summary of Configuration Parameters, on page 78
Service Credentials Parameters, on page 92

CHAPTER 8

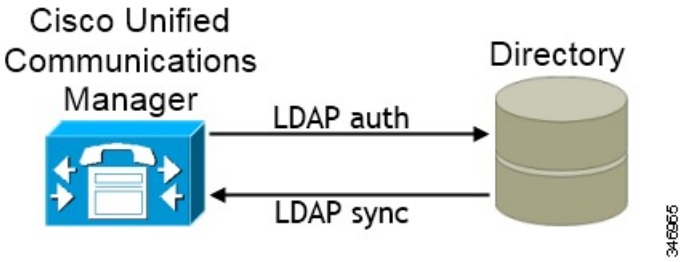
Integrate with Directory Sources

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

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
Server Setup Guide

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

The first step to synchronize with a directory server is to enable synchronization on Cisco Unified Communications Manager.

Procedure

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

Step 2 Select **System** > **LDAP** > **LDAP System**.
The **LDAP System Configuration** window opens.

Step 3 Locate the **LDAP System Information** section.

Step 4 Select **Enable Synchronizing from LDAP Server**.

Step 5 Select the type of directory server from which you are synchronizing data from the **LDAP Server Type** drop-down list.

What to Do Next

Specify an LDAP attribute for the user ID.

Populate User ID and Directory URI

When you synchronize your LDAP directory server with Cisco Unified Communications Manager, you can populate the end user configuration tables in both the Cisco Unified Communications Manager and the Cisco Unified Communications Manager IM and Presence Service databases with attributes that contain values for the following:

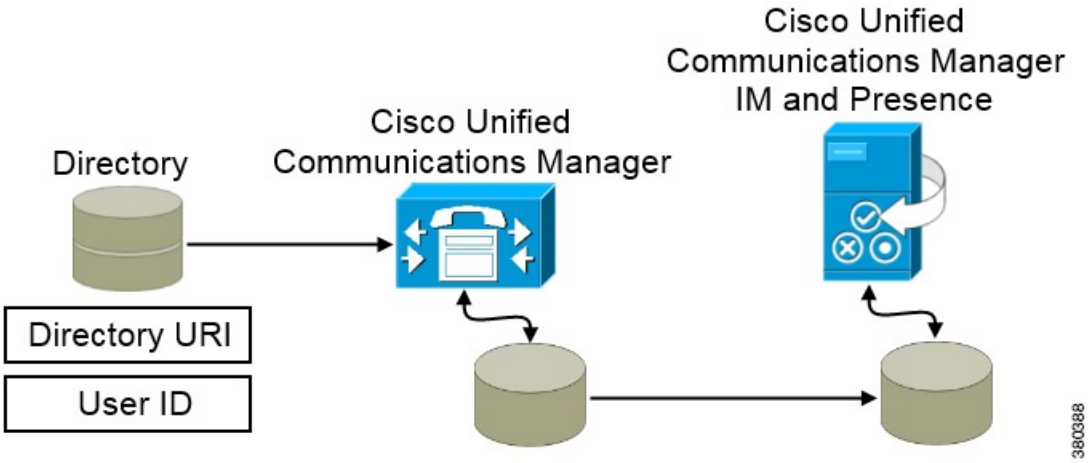
User ID

You must specify a value for the user ID on Cisco Unified Communications Manager. This value is required for the default IM address scheme and for users to log in. The default value is sAMAccountName.

Directory URI

You should specify a value for the directory URI if you plan to:

- Enable URI dialing in Cisco Jabber.



When Cisco Unified Communications Manager synchronizes with the directory source, it retrieves the values for the directory URI and user ID and populates them in the end user configuration table in the Cisco Unified Communications Manager database.

The Cisco Unified Communications Manager database then synchronizes with the Cisco Unified Communications Manager IM and Presence Service database. As a result, the values for the directory URI and user ID are populated in the end user configuration table in the Cisco Unified Communications Manager IM and Presence Service database.

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

Step 1 Locate the **LDAP Attribute for User ID** drop-down list on the **LDAP System Configuration** window.

Step 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`, you must specify the attribute as the value for the parameter in your client configuration file as follows:

The BDI parameter is `BDIUserAccountName`.

```
<BDIUserAccountName>attribute-name</BDIUserAccountName>
```

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

Specify an LDAP Attribute for the Directory URI

On Cisco Unified Communications Manager version 9.0(1) and higher, you can populate the directory URI from an attribute in the directory. The default attribute is `msRTCSIP-primaryuseraddress`.

Procedure

Step 1 Select **System** > **LDAP** > **LDAP Directory**.
Remember To add or edit an LDAP directory, you must first enable synchronization.

Step 2 Select the appropriate LDAP directory or select **Add New** to add an LDAP directory.

Step 3 Locate the **Standard User Fields To Be Synchronized** section.

Step 4 Select the appropriate LDAP attribute for the **Directory URI** drop-down list.

Step 5 Select **Save**.

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

Step 1 Select **System** > **LDAP** > **LDAP Directory**.

Step 2 Select **Add New**.
The **LDAP Directory** window opens.

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.

Step 4 Select **Save**.

Step 5 Select **Peform Full Sync Now**.

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

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

Authenticate with the Directory Server

You should configure Cisco Unified Communications Manager to authenticate with the directory server. When users log in to the client, the presence server routes that authentication to Cisco Unified Communications Manager. Cisco Unified Communications Manager then proxies that authentication to the directory server.

Procedure

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

Step 2 Select **System** > **LDAP** > **LDAP Authentication**.

Step 3 Select **Use LDAP Authentication for End Users**.

Step 4 Specify LDAP credentials and a user search base as appropriate.
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:

Basic Directory Integration

Basic Directory Integration (BDI) 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.

Basic Directory Integration

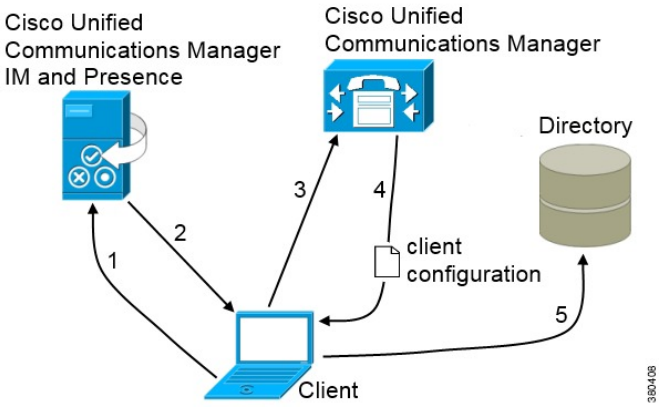
When using Basic Directory Integration (BDI), the client retrieves contact data from the directory service as follows.

1. The client connects to the Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service server.
2. The client gets the LDAP profile configuration section in the service profile from the Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service server.

   The service profile contains the location of Cisco Unified Communications Manager (TFTP) server. Depending on your configuration, the service profile can also contain the credentials to authenticate with the directory.
3. The client connects to the Cisco Unified Communications Manager server.
4. The client downloads the client configuration file from the Cisco Unified Communications Manager server.

   The client configuration file contains the location of the directory. Depending on your configuration, the client configuration file can also contain the credentials to authenticate with the directory.

5 The client uses the directory location and the authentication credentials to connect to the directory.



Authentication with Contact Sources

BDI requires users to authenticate with the directory source to resolve contacts. You can use the following methods to authenticate with the contact source, in order of priority:

Specify credentials in Cisco Unified Presence or Cisco Unified Communications Manager

Specify credentials in a profile on the server. The client can then retrieve the credentials from the server to authenticate with the directory.

This method is the most secure option for storing and transmitting credentials.

Set common credentials in the client configuration file

You specify a shared username and password in the client configuration file. The client can then authenticate with the directory server.

Important The client transmits and stores these credentials as plain text.

You should use only a well-known or public set of credentials. The credentials should also be linked to an account that has read-only permissions.

Use anonymous binds

Configure the client to connect to the directory source with anonymous binds.

Specify LDAP Directory Configuration on Cisco Unified Presence

If your environment includes Cisco Unified Presence version 8.x, you can specify directory configuration in the LDAP profile. The client can then get the directory configuration from the server to authenticate with the directory source.

Complete the steps to create an LDAP profile that contains authentication credentials, and then assign that profile to users.

Procedure

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

Step 2 Select **Application** > **Cisco Unified Personal Communicator** > **LDAP Profile**.

Step 3 Select **Add New**.

Step 4 Specify a name and optional description for the profile in the following fields:

- **Name**
- **Description**

Step 5 Specify a distinguished name for a user ID that is authorized to run queries on the LDAP server. Cisco Unified Presence uses this name for authenticated bind with the LDAP server.

Step 6 Specify a password that the client can use to authenticate with the LDAP server in the following fields:

- **Password**
- **Confirm Password**

Step 7 Select **Add Users to Profile** and add the appropriate users to the profile.

Step 8 Select **Save**.

What to Do Next

Specify any additional BDI information in the client configuration file.

Specify LDAP Directory Configuration on Cisco Unified Communications Manager

If your environment includes Cisco Unified Communications Manager version 9.x and higher, you can specify credentials when you add a directory service. The client can then get the configuration from the server to authenticate with the directory source.

Complete the steps to add a directory service, apply the directory service to the service profile, and specify the LDAP authentication configuration for the directory service.

Procedure

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

Step 2 Add a directory service as follows:

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

b) Select **Add New**.
The **UC Service Configuration** window opens.

c) In the **Add a UC Service** section, select **Directory** from the **UC Service Type** drop-down list.

d) Select **Next**.

e) Specify details for the directory service as follows:

Product Type

Select **Directory**.

Name

Enter a descriptive name for the server, for example, PrimaryDirectoryServer.

Description

Enter an optional description.

Hostname/IP Address

Enter the address of the directory server in one of the following formats:

- Hostname
- IP Address
- FQDN

Protocol Type

Select one of the following protocols from the following drop-down list:

- TCP
- UDP

f) Select **Save**.

Step 3 Apply the directory service to your service profile as follows:

a) Select **User Management** > **User Settings** > **Service Profile**.
The **Find and List Service Profiles** window opens.

b) Find and select your service profile.
The **Service Profile Configuration** window opens.

c) In the **Directory Profile** section, select up to three services from the following drop-down lists:

- **Primary**
- **Secondary**
- **Tertiary**

d) Specify the credentials that the client can use to authenticate with the LDAP server in the following fields:

- **Username**
- **Password**

e) Select **Save**.

Set Credentials in the Client Configuration

You can set credentials in the client configuration with the following parameters:

- BDIConnectionUsername
- BDIConnectionPassword

Important The client transmits and stores these credentials as plain text.

You should use only a well-known or public set of credentials. The credentials should also be linked to an account that has read-only permissions.

The following is an example configuration:

```
<Directory>
  <BDIConnectionUsername>admin@example.com</BDIConnectionUsername>
  <BDIConnectionPassword>password</BDIConnectionPassword>
</Directory>
```

Use Anonymous Binds

To use anonymous binds, you set the following parameters in the client configuration file:

Parameter	Value
DirectoryServerType	BDI
BDIPrimaryServerName	IP address FQDN
BDIEnableTLS	True
BDISearchBase1	Searchable organizational unit (OU) in the directory tree
BDIBaseFilter	Object class that your directory service uses; for example, inetOrgPerson
BDIPredictiveSearchFilter	uid or other search filter A search filter is optional.

The following is an example configuration:

```
<Directory>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIEnableTLS>True</BDIEnableTLS>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
  <BDIBaseFilter>(&amp;(objectClass=inetOrgPerson)</BDIBaseFilter>
  <BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>
</Directory>
```

Cisco Unified Communications Manager 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:

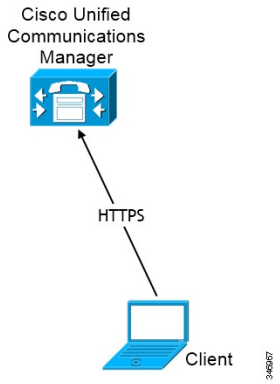
- If you set the DirectoryServerType parameter to use a value of UDS in the client configuration file.

  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 Mobile and Remote 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:

Procedure

Step 1 Create your directory source in Cisco Unified Communications Manager.

Step 2 Synchronize the contact data to Cisco Unified Communications Manager.
After the synchronization occurs, your contact data resides in Cisco Unified Communications Manager.

Step 3 For manual connections, specify the IP address of the Cisco Unified Communications Manager User Data Service server to ensure that the client can discover the server.
The following is an example configuration for the Cisco Unified Communications Manager User Data Service server:

```
<UdsServer>11.22.33.444</UdsServer>
```

Step 4 Configure the client to retrieve contact photos with UDS.
The following is an example configuration for contact photo retrieval:

```
<UdsPhotoUriWithToken>http://server_name.domain/%%uid%%.jpg</UdsPhotoUriWithToken>
```

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:

Parameter	Description
Enable All User Search	Allows searches for all users in the directory (search with no last name, first name, or directory number specified). The default value is true.
User Search Limit	Limits the number of users returned in a query. The default value is 64.
Number of Digits to Match	Specifies the number of digits to match when users search for phone numbers. **Tip** To resolve PSTN numbers, you should set the value as equal to the number of digits in the PSTN numbers. For example, if the PSTN numbers have 10 digits, set the value to 10.

Contact Resolution with Multiple Clusters

For contact resolution with multiple Cisco Unified Communications Manager clusters, you should synchronize all users on the corporate directory to each cluster. You should then 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, you should synchronize all 40,000 users to both clusters. You then 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

Directory integration can be configured through Service Profiles using Cisco Unified Communications Manager 9 or higher or with the configuration file. Use this section to learn how to configure the client for directory integration.

Note In instances where a Service Profile and the configuration file are present, settings in the Service Profile take priority.

Note Cisco Unified Presence 8 profiles cannot be used for directory integration.

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

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

Step 2 Add a directory service.

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

b) Select **Add New**.
The **UC Service Configuration** window opens.

c) Select **Directory** from the **UC Service Type** menu and then select **Next**.

d) Set all appropriate values for the directory service and then select **Save**.

Step 3 Apply the directory service to a service profile.

a) Select **User Management** > **User Settings** > **Service Profile**.
The **Find and List Service Profiles** window opens.

b) Select **Add New**.
The **Service Profile Configuration** window opens.

c) Add the directory services to the directory profile.

d) Select **Save**.

Directory Profile Parameters

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

Directory Service Configuration	Description
Primary server	Specifies the address of the primary directory server. This parameter is required for manual connections where the client cannot automatically discover the directory server.
Secondary server	Specifies the address of the backup directory server.
Use UDS for Contact Resolution	Specifies if the client uses UDS as a contact source. **Note** By default, UDS provides contact resolution when users connect to the corporate network through Expressway for Mobile and Remote Access.
Use Logged On User Credential	Specifies if the client uses the logged on username and password. **True** Use credentials. This is the default value. **False** Do not use credentials. Specify credentials with the BDIConnectionUsername and BDIConnectionPassword parameters.

Directory Service Configuration	Description
Username	Lets you manually specify a shared username that the client can use to authenticate with the directory server. If you must use this parameter, you should use only a well-known or public set of credentials. The credentials should also be linked to an account that has read-only permissions.
Password	Lets you manually specify a shared password that the client can use to authenticate with the directory server. If you must use this parameter, you should use only a well-known or public set of credentials. The credentials should also be linked to an account that has read-only permissions.
Search Base 1	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. 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. **Tip** 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.
Base Filter	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 `(&(objectCategory=person)`.
Predictive Search Filter	Defines filters to apply to predictive search queries. You can define multiple, comma-separated values to filter search queries. The default value is ANR.

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.

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:

Attribute Mapping Parameters	
• BDICommonName • BDIDisplayName • BDIFirstname • BDILastname • BDIEmailAddress • BDISipUri • BDIPhotoSource • BDIBusinessPhone • BDIMobilePhone • BDIHomePhone • BDIOtherPhone • BDIDirectoryUri	• BDITitle • BDICompanyName • BDIUserAccountName • BDIDomainName • BDICountry • BDILocation • BDINickname • BDIPostalCode • BDICity • BDIState • BDIStreetAddress

The following table lists the parameters you can use to connect to an LDAP directory server:

Directory Server Connection Parameters	
• BDILDAPServerType • BDIPresenceDomain • BDIPrimaryServerName • BDIServerPort1	• BDIUseJabberCredentials • BDIConnectionUsername • BDIConnectionPassword • BDIEnableTLS

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	
• BDIBaseFilter • BDIUseANR • BDIPredictiveSearchFilter • BDISearchBase1	• BDIPhotoUriSubstitutionEnabled • BDIPhotoUriSubstitutionToken • BDIPhotoUriWithToken • BDIUseSIPURIToResolveContacts • BDIUriPrefix • BDIDirectoryUri • BDIDirectoryUriPrefix

Summary of UDS Parameters

The following table lists the parameters you can use to connect to UDS and perform contact resolution and directory queries.

UDS Parameters
• DirectoryServerType • PresenceDomain • UdsServer • UdsPhotoUriWithToken

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:

Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
BDICommonName	cn	Yes	Yes	No
BDIDisplayName	displayName	Yes	Yes	Yes
BDIFirstname	givenName	Yes	Yes	Yes

Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
BDILastname	sn	Yes	Yes	Yes
BDIEmailAddress	mail	Yes	Yes	Yes
BDISipUri **Note** The client uses this parameter for intradomain federation, not URI dialing.	msRTCSIP-PrimaryUserAddress	Yes	Yes	Yes
BDIPhotoSource	thumbnailPhoto	No	No	No
BDIBusinessPhone	telephoneNumber	Yes	No	No
BDIMobilePhone	mobile	Yes	No	No
BDIHomePhone	homePhone	Yes	No	No
BDIOtherPhone	otherTelephone	Yes	No	No
BDIDirectoryUri **Note** The client uses this parameter for URI dialing.	mail	Yes	No	No
BDITitle	title	Yes	No	No
BDICompanyName	company	Yes	Yes	No
BDIUserAccountName	sAMAccountName	Yes	Yes	Yes
BDIDomainName	dn	Yes	Yes	No
BDICountry	co	Yes	No	No
BDILocation	location	Yes	No	No
BDINickname	displayName	Yes	Yes	Yes
BDIPostalCode	postalCode	Yes	No	No
BDICity	l	Yes	Yes	No
BDIState	st	Yes	Yes	No
BDIStreetAddress	streetAddress	Yes	No	No

Attributes on the Directory Server

You must index attributes on your LDAP directory server so that the client can resolve contacts.

If you use the default attribute mappings, ensure the following attributes are indexed:

- sAMAccountName
- displayName
- sn
- name
- proxyAddresses
- mail
- department
- givenName
- telephoneNumber

  Additionally, ensure you index the following attributes for secondary number queries:

  - otherTelephone
  - mobile
  - homePhone

- msRTCSIP-PrimaryUserAddress

  You should index msRTCSIP-PrimaryUserAddress for intradomain federation only.

Directory Connection Parameters

The following table describes parameters for configuring your LDAP directory connection:

Parameter	Value	Description
BDILDAPServerType	AD OpenLDAP	Specifies the type of LDAP directory server to which the client connects. **AD** Connect to Active Directory. This is the default value. **OpenLDAP** Connect to OpenLDAP.

Parameter	Value	Description
BDIPresenceDomain	Domain of the presence server	Required parameter. Specifies the domain of the presence server. The client appends this domain to the user ID to create an IM address. For example, a user named Adam McKenzie has the following user ID: `amckenzie`. You specify `example.com` as the presence server domain. When the user logs in, the client constructs the following IM address for Adam McKenzie: `amckenzie@example.com`.
BDIPrimaryServerName	IP address FQDN	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. **Note** Each time the client starts, it attempts to connect to the primary server. The client attempts to connect to the secondary server if: • The primary server is not available. • The primary server fails after the client connects to it. If the connection to the secondary server is successful, the client keeps the connection to the secondary server until the next restart. If the secondary server fails while the client is connected to it, the client attempts to connect to the primary server.
BDIServerPort1	Port number	Specifies the port for the primary directory server.

Parameter	Value	Description
BDIUseJabberCredentials	true false	Specifies whether the client can use the presence server credentials to sign in to the directory server. **True** The client searches for the username and password in this order: **1** Client configuration file (BDIConnectionUsername and BDIConnectionPassword) **2** Presence server If the credentials are not present, the client tries to sign in anonymously. **False** This is the default value. The client tries to sign in using the values of BDIConnectionUsername and BDIConnectionPassword in client configuration file. If those parameters are not present, the client tries to sign in anonymously.
BDIConnectionUsername	Username	Lets you manually specify a shared username that the client can use to authenticate with the directory server. **Important** The client transmits and stores this username as plain text. 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.
BDIConnectionPassword	Password	Lets you manually specify a shared password that the client can use to authenticate with the directory server. **Important** The client transmits and stores this password as plain text. 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.

Parameter	Value	Description
BDIEnableTLS	true false	Use TLS to secure directory connections. **true** Use TLS. **false** Do not use TLS. This is the default value.

Directory Query Parameters

The following table describes parameters for configuring how the client queries your LDAP directory:

Parameter	Value	Description
BDIBaseFilter	Base filter	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 `(&(objectCategory=person))`. Configuration files can contain only valid XML character entity references. Use `&` instead of `&` if you specify a custom base filter.
BDIUseANR	true false	Specifies if Cisco Jabber issues a query using Ambiguous Name Resolution (ANR) when it performs a predictive search. **true** Use ANR for predictive search. This is the default value. **false** Do not use ANR for predictive search. You should set the value to false if you integrate with a directory source other than Active Directory. **Important** You must configure your directory server to set attributes for ANR if you want the client to search for those attributes.

Parameter	Value	Description
BDIPredictiveSearchFilter	Search filter	Defines filters to apply to predictive search queries. You can define multiple, comma-separated values to filter search queries.
BDISearchBase1	Searchable organizational unit (OU) in the directory tree	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. **Tip** 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.

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:

```
(&amp;(objectClass=user)(memberOf=cn=group-name,ou=Groups,dc=example,dc=com))
```

Find a nested group within a group:

```
(&amp;(objectClass=user)(memberOf:search-oid:=cn=group-name,ou=Groups,dc=example,dc=com))
```

Find only enabled accounts and non-administrator accounts:

```
(&amp;(objectCategory=person)(objectClass=user)(!(userAccountControl:search-oid:=2))
(!(sAMAccountName=*_dbo))(!(sAMAccountName=*-admin)))
```

Contact Photo Parameters

The following table describes parameters for configuring how the client retrieves contact photos from an LDAP directory:

Parameter	Value	Description
BDIPhotoUriSubstitutionEnabled	true false	Specifies if photo URI substitution is enabled. **true** Photo URI substitution is enabled. **false** Specifies if photo URI substitution is disabled. This is the default value.

Parameter	Value	Description
BDIPhotoUriSubstitutionToken	Directory attribute	Specifies a directory attribute to insert in the photo URI; for example, `sAMAccountName`. Only the following attributes are supported for use with the PhotoURISubstitutionToken parameter: • Common Name • Display Name • First Name • Last Name • Nickname • Email Address • Photo Source • Business Phone • Mobile Phone • Home Phone • Preferred Phone • Other Phone • Title • Company Name • User Account Name • Domain Name • Location • Post Code • State • City • Street

Parameter	Value	Description
BDIPhotoUriWithToken	URI	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 BDIPhotoUriSubstitutionToken. **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 121

Contact Photo Retrieval with BDI

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 BDIPhotoUriSubstitutionEnabled parameter.
2. Specify a directory attribute to use as a dynamic token as the value of the BDIPhotoUriSubstitutionToken parameter; for example,
   `<BDIPhotoUriSubstitutionToken>sAMAccountName</BDIPhotoUriSubstitutionToken>`
3. Specify the URL and the dynamic token as the value of the BDIPhotoUriWithToken parameter; for example,
   `<BDIPhotoUriWithToken>http://staffphoto.example.com/sAMAccountName.jpg</BDIPhotoUriWithToken>`

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, BDIPhotoUriWithToken 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 BDIPhotoSource parameter in the configuration; for example,
`<BDIPhotoSource>jpegPhoto</BDIPhotoSource>`

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 BDIPhotoSource parameter in the configuration; for example,
`<BDIPhotoSource>photoUri</BDIPhotoSource>`

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.

Related Topics

Contact Photo Parameters, on page 118

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, you should 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.

The following table lists the different dimensions for contact photos in Cisco Jabber:

Location	Dimensions
Audio call window	128 pixels by 128 pixels

Location	Dimensions
Invitations and reminders, for example: • Incoming call windows • Meeting reminder windows	64 pixels by 64 pixels
Lists of contacts, for example: • Contact lists • Participant rosters • Call history • Voicemail messages	32 pixels by 32 pixels

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 upwards to 128 pixels by 128 pixels.

Tip Resizing contact photos can result in less than optimal resolution. For this reason, you should use contact photos that are 128 pixels by 128 pixels so that the client does not automatically resize them.

Cropping

Cisco Jabber automatically crops non-square 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.

UDS Parameters

The following table provides details about the parameters you can use to connect to UDS and perform contact resolution and directory queries.

Parameter	Value	Description
PresenceDomain	Domain of the presence server	Required parameter. Specifies the domain of the presence server. The client appends this domain to the user ID to create an IM address. For example, a user named Adam McKenzie has the following user ID: `amckenzie`. You specify `example.com` as the presence server domain. When the user logs in, the client constructs the following IM address for Adam McKenzie: `amckenzie@example.com`.
UdsServer	IP address FQDN	Specifies the address of the Cisco Unified Communications Manager User Data Service (UDS) server. This parameter is required for manual connections where the client cannot automatically discover the UDS server.

Parameter	Value	Description
UdsPhotoUriWithToken	URI	Specifies a photo URI with a directory attribute as a variable value; for example, `http://www.photo/url/path/%%uid%%.jpg`. This parameter applies to UDS directory integrations. You must specify this parameter to download contact photos in either of the following cases: • If you configure the DirectoryServerType parameter 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. **Restriction** The client must be able to retrieve the photos from the web server without credentials.

Contact Photo Retrieval with UDS

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>`

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.

Related Topics

Contact Photo Parameters, on page 118

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, you should 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.

The following table lists the different dimensions for contact photos in Cisco Jabber:

Location	Dimensions
Audio call window	128 pixels by 128 pixels

Location	Dimensions
Invitations and reminders, for example: • Incoming call windows • Meeting reminder windows	64 pixels by 64 pixels
Lists of contacts, for example: • Contact lists • Participant rosters • Call history • Voicemail messages	32 pixels by 32 pixels

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 upwards to 128 pixels by 128 pixels.

Tip Resizing contact photos can result in less than optimal resolution. For this reason, you should use contact photos that are 128 pixels by 128 pixels so that the client does not automatically resize them.

Cropping

Cisco Jabber automatically crops non-square 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.

Directory Server Configuration Examples

This section describes supported integration scenarios and provides example configurations.

UDS Integration

To integrate with UDS, set the following parameters.

Parameter	Value
DirectoryServerType	UDS
UdsServer	IP address of the UDS server
UdsPhotoUriWithToken	Contact photo URL

Note Configure the DirectoryServerType parameter to UDS only if you want to use UDS for all contact resolution (that is, from inside and outside the corporate firewall).

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>UDS</DirectoryServerType>
  <UdsServer>11.22.33.444</UdsServer>
  <UdsPhotoUriWithToken>http://server-name/%%uid%%.jpg</UdsPhotoUriWithToken>
</Directory>
```

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

Note 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.

Parameter	Value
BDIPhotoUriWithToken	Contact photo URL when inside the corporate firewall
UdsPhotoUriWithToken	Contact photo URL when outside the corporate firewall

The following is an example configuration:

```
<Directory>
  <BDIPhotoUriWithToken>http://staffphoto.example.com/sAMAccountName.jpg
      </BDIPhotoUriWithToken>
  <UdsPhotoUriWithToken>http://server-name/%%uid%%.jpg</UdsPhotoUriWithToken>
</Directory>
```

OpenLDAP Integration

You can integrate with OpenLDAP using anonymous binds or authenticated binds.

Anonymous Binds for Mobile Clients and Cisco Jabber for Mac

To integrate with OpenLDAP using anonymous binds, set the following parameters:

Parameter	Value
BDILDAPServerType	OpenLDAP
BDIPrimaryServerName	IP address Hostname
BDIEnableTLS	True
BDISearchBase1	Root of the directory service or the organizational unit (OU)
BDIServerPort1	The port for the primary directory server
BDIUserAccountName	Unique identifier such as uid or cn

Parameter	Value
BDIBaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
(Optional) BDIPredictiveSearchFilter	uid or other search filter

The following is an example configuration:

```
<Directory>
  <BDILDAPServerType>OpenLDAP</BDILDAPServerType>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIEnableTLS>True</BDIEnableTLS>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
  <BDIServerPort1>636/3269</BDIServerPort1>
  <BDIUserAccountName>uid</BDIUserAccountName>
  <BDIBaseFilter>(&amp;(objectClass=inetOrgPerson)</BDIBaseFilter>
  <BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>
</Directory>
```

Authenticated Binds for Mobile Clients and Cisco Jabber for Mac

To integrate with OpenLDAP using authenticated binds, set the following parameters:

Parameter	Value
BDILDAPServerType	OpenLDAP
BDIPrimaryServerName	IP address Hostname
BDIEnableTLS	False
BDISearchBase1	Root of the directory service or the organizational unit (OU)
BDIServerPort1	The port for the primary directory server
BDIUserAccountName	Unique identifier such as uid or cn
BDIBaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
(Optional) BDIPredictiveSearchFilter	uid or other search filter
BDIConnectionUsername	Username
BDIConnectionPassword	Password

The following is an example configuration:

```
<Directory>
  <BDILDAPServerType>OpenLDAP</BDILDAPServerType>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIEnableTLS>False</BDIEnableTLS>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
  <BDIServerPort1>389/3268</BDIServerPort1>
  <BDIUserAccountName>uid</BDIUserAccountName>
  <BDIBaseFilter>(&amp;(objectClass=inetOrgPerson)</BDIBaseFilter>
```

```
  <BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>
  <BDIConnectionUsername>cn=administrator,dc=cisco,dc=com</BDIConnectionUsername>
  <BDIConnectionPassword>password</BDIConnectionPassword>
</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
  - AOL Instant Messenger

You configure interdomain federation for Cisco Jabber on Cisco Unified Presence or 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 Presence and Microsoft Office Communications Server, Microsoft Live Communications Server, or other presence server.

Intradomain federation allows you to migrate users to Cisco Unified Presence or Cisco Unified Communications IM and Presence from a different presence server. For this reason, you configure intradomain federation for Cisco Jabber on the presence server. See the following documents for more information:

- Cisco Unified Presence: *Integration Guide for Configuring Partitioned Intradomain Federation for Cisco Unified Presence Release 8.6 and Microsoft LCS/OCS*
- Cisco Unified Communications IM and Presence: *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 Presence 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

Note 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
- UserPrincipleName (UPN)@domain
- EmailAddress@domain
- employeeNumber@domain
- telephoneNumber@domain

Step 3 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 BDISipUri. In your directory the value of `msRTCSIP-PrimaryUserAddress` for each user has the following format: `sip:`*`username@domain`*.

- For BDI: BDIUriPrefix

- For EDI: UriPrefix

The following XML snippet provides an example of the resulting configuration for BDI:

```
<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:

```
<Directory>
  <UseSIPURIToResolveContacts>true</UseSIPURIToResolveContacts>
  <SipUri>non-default-attribute</SipUri>
  <UriPrefix>sip:</UriPrefix>
</Directory>
```

Example of Intradomain Federation

Intradomain Federation using BDI or EDI

The following example shows how to create intradomain federation contacts using the following BDI or EDI parameters and example values:

For BDI: BDISipUri

For EDI: SipURI

Value: msRTCSIP-PrimaryUserAddress

For BDI: BDIUseSIPURIToResolveContacts

For EDI: UseSIPURIToResolveContacts

Value: true

For BDI: BDIUriPrefix

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.