Planning Guide for Cisco Jabber 14.0

First Published: 2021-03-25

Last Modified: 2022-01-06

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

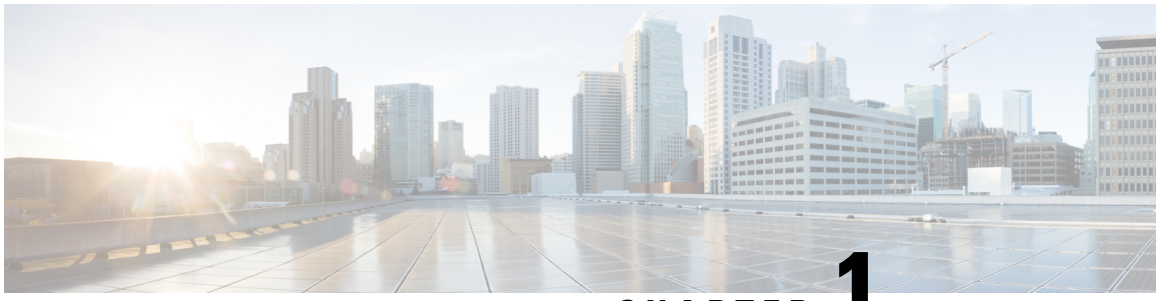
CONTENTS

New and Changed Information

New and Changed Information

Date	Status	Description	Location
December 2021	New	Added information about location awareness for E911 calls.	Location awareness for Enhanced 911 support
October 2021	Updated	EMM clients now support APNs on iOS.	Enterprise Mobility Management Deployments
September 2021	Updated	Added Monterey support	Operating System for Cisco Jabber for Mac
	Updated	Add new supported hardware	Hardware Requirements for Cisco Jabber for Android
	Updated	Clarified that list of IdPs showed only the ones we test, not all the supported ones.	Supported Identity Providers
March 2021		Initial Publication	
	Updated	Added macOS Big Sur	Operating System for Cisco Jabber for Mac
	Updated	Add new supported hardware	Hardware Requirements for Cisco Jabber for Android

New and Changed Information



CHAPTER 1

Requirements

Server Requirements

The following software requirements are common to all Cisco Jabber clients in this release:

Service	Software Requirement	Supported Version
IM and Presence	Cisco Unified Communications Manager IM and Presence Service	10.5(2) and later (Minimum) 11.5(1) SU2 or later (Recommended)
	Webex Messenger	
Telephony	Cisco Unified Communications Manager	10.5(2) and later (Minimum) 11.5(1) SU3 or later (Recommended)
	Cisco Unified Survivable Remote Site Telephony	Unified SIP SRST 12.8 and later
Contact Search	LDAP directory	LDAP v3 compliant directory such as Microsoft Active directory 2008 R2 and Open LDAP 2.4 or later
Voicemail	Cisco Unity Connection	10.5 and later
Multiline	Cisco Unified Contact Center Express	11.6

Service	Software Requirement	Supported Version
Conferencing	Cisco Meeting Server	2.2 and later
	Cisco TelePresence Server	3.1 and later
	Cisco TelePresence MCU	4.3 and later
	Cisco ISR PVDM3	Cisco Unified Communications Manager 9.x and later
	Cloud CMR	Webex Meetings Server with Collaboration Meeting Room
	Webex Meetings Server	2.8 MR1 and later
	Webex Meetings Center	WBS33 and later
Remote Access	Cisco Adaptive Security Appliance Only applies to Cisco Jabber for Android.	8.4(1) and later
	Cisco AnyConnect Secure Mobility Client Cisco Jabber for Android and Cisco Jabber for iPhone and iPad clients only.	Platform-dependent
	Cisco Expressway C	X8.10.1 and later
	Cisco Expressway E	X8.10.1 and later.

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

Operating System Requirements

Operating Systems for Cisco Jabber for Windows

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

- Microsoft Windows 10 (desktop mode)
- Microsoft Windows 8.1 (desktop mode)
- Microsoft Windows 8 (desktop mode)

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

Windows 10 Servicing Options

Cisco Jabber for Windows supports the following Windows 10 servicing options:

- Current Branch (CB)
- Current Branch for Business (CBB)
- Long-Term Servicing Branch (LTSB)—with this option, it is your responsibility to ensure that any relevant service updates are deployed.

For more information about Windows 10 servicing options, see the following Microsoft documentation:https://technet.microsoft.com/en-us/library/mt598226(v=vs.85).aspx.

Note Cisco Jabber installs the required files to the following directories by default:

- %temp%\Cisco Systems\Cisco Jabber-Bootstrap.properties file and installation log
- %LOCALAPPDATA%\Cisco\Unified Communications-Logs and temporary telemetry data
- %APPDATA%\Cisco\Unified Communications-Cached configurations and account credentials
- %ProgramFiles%\Cisco Systems\Cisco Jabber-Installation files for x86 Windows
- %ProgramFiles(x86)%\Cisco Systems\Cisco Jabber-Installation files for x64 Windows

Operating System for Cisco Jabber for Mac

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

- macOS Catalina 10.15 or later
- macOS Mojave 10.14 or later
- macOS High Sierra 10.13 (or later)
- macOS Sierra 10.12 (or later)
- macOC Big Sur
- macOS Monterey

Operating Systems for Cisco Jabber for Android

Refer to the Play Store for the latest supported operating system version information.

Note Cisco Jabber for Android is available as a 32-bit app and a 64-bit app. If your Android device has a 64-bit OS, you get a faster and richer experience by running the 64-bit Jabber client.

You cannot install the 64-bit app on a 32-bit OS. If you use the 32-bit app on most 64-bit platforms, you get a notification to upgrade to the 64-bit app.

Note If Cisco Jabber is installed on Android 6.0 Marshmallow OS or later, and if it is kept idle:

- The network connection to Cisco Jabber is disabled.
- The users do not receive any calls or messages.

Tap **Change Settings** and ignore battery optimization to receive calls and messages.

Last Jabber Release for Android 5.x Support

Cisco Jabber 12.8 is the last release that supports devices running Android 5.x.

The next Jabber release will end support for all devices that cannot upgrade to Android 6.x.

Operating Systems for Cisco Jabber for iPhone and iPad

Refer to the App Store for the latest supported operating system version information.

Important Cisco supports only the current App Store version of Cisco Jabber for iPhone and iPad. Defects found in any Cisco Jabber for iPhone and iPad release are evaluated against current versions.

Hardware Requirements

Hardware Requirements for Desktop Clients

Requirement	Cisco Jabber for Windows	Cisco Jabber for Mac
Installed RAM	2-GB RAM	2-GB RAM
Free physical memory	128 MB	1 GB
Free disk space	256 MB	300 MB

Requirement	Cisco Jabber for Windows	Cisco Jabber for Mac
CPU speed and type	AMD Mobile Sempron Processor 3600+ 2 GHz Intel Core 2 Duo Processor T7400 @ 2. 16 GHz	Intel Core 2 Duo or later processors in any of the following Apple hardware: • iMac 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.	USB 2.0 for USB camera and audio devices

CTI Supported Devices

To view the list of Computer Telephony Integration (CTI) supported devices for your Unified Communications Manager:

1. From the **Cisco Unified Reporting** page, select **Unified CM Phone Feature List** from the **System Reports** menu.
2. After opening the report, select **CTI controlled** from the **Feature** drop-down list.

Hardware Requirements for Cisco Jabber for Android

Minimum requirements for Android devices:

Android Operating System	CPU	Display
6.0 or later	1.5 GHz dual-core Recommended: 1.2-GHz quad-core or higher	For two-way video: 480p x 800p or higher. For IM only: 320p x 480p or higher.

Cisco Jabber for Android supports Full UC mode in the devices with these OS versions:

Table 1: Supported Android Devices

Device	Model	Minimum Android OS Version	Notes
Ascom	Myco 3	10.0	

Device	Model	Minimum Android OS Version	Notes
BlackBerry	Priv	6.0.1	If you remove Jabber from the recently viewed apps list and you keep the device idle for some time, then Jabber becomes inactive.
Fujitsu	Arrows M357	6.0.1	

Device	Model	Minimum Android OS Version	Notes
Google	Nexus 5	6.0	
	Nexus 5X	6.0	
	Nexus 6	6.0	
	Nexus 6P	6.0	For Google Nexus 6P with Android OS version 6.x or 7.0, your administrator must set your Jabber phone service as a secure phone service. Otherwise, your device might not respond. No action is required for Android OS version 7.1 or later.
	Nexus 7	6.0	
	Nexus 9	6.0	
	Pixel	7.0	
	Pixel C	6.0	
	Pixel XL	7.0	
	Pixel 2	8.0	During a Jabber call, if the user switches audio from the mobile device to a headset, momentary audio issues are possible.
	Pixel 2 XL	8.0	During a Jabber call, if the user switches audio from the mobile device to a headset, momentary audio issues are possible.
	Pixel 3	8.0	If you use the attached headset with the phone, then there might be some issues with the audio for few seconds.
	Pixel 3 XL	8.0	If you use the attached headset with the phone, then there might be some issues with the audio for few seconds.
	Pixel 4	10.0	
	Pixel 4 XL	10.0	
	Pixel 4a 5G	10.0	
	Pixel 5	11.0	

Device	Model	Minimum Android OS Version	Notes
Honeywell Dolphin	CT50	6.0	
	CT40	7.1.1	
	CT60	7.1.1 and 8.1	We only support the CT60 with Android OS 7.1.1 and 8.1.
HTC	10	6.0	
	A9	6.0	
	M8	6.0	
	M9	6.0	
	X9	6.0	
Huawei [1]	Honor 7	6.0	
	Mate 8	6.0	
	Mate 9	6.0	
	Nova	7.0	
	Mate 10	8.0	
	Mate 10 Pro	8.0	
	P8	6.0	
	P9	6.0	
	P10	7.0	
	P10 Plus	7.0	
	P20	8.0	
	P20 Pro	8.0	
	Mate20	8.0	
	Mate20 Pro	8.0	
	P30	9.0	
	P30 Pro	9.0	

Device	Model	Minimum Android OS Version	Notes
LG	G3	6.0	
	G4	6.0	
	G5	6.0	
	G6	7.0	
	V10	6.0	
	V30	8.0	
Motorola	Moto G4	6.0	
	Moto G5	7.0	
	Moto G6	8.0	
	Moto Z Droid	6.0	
Nokia	6.1	8.0	
	8.1	8.1	
OnePlus	One	6.0	
	5	8.0	
	5T	8.0	
	6	9.0	
	6T	9.0	
	7T	10.0	
	8	11.0	
	8 Pro	11.0	
	8T	11.0	

Device	Model	Minimum Android OS Version	Notes
Samsung	All	6.0	• Devices that can't upgrade to Android OS 6.x or later are no longer supported. • Enable the auto-run option for Jabber. For Android OS 6.x and later, you can find the auto-run option under **App Smart Manager**. • Jabber delays the incoming call notification pop-up on Samsung Galaxy Tab Pro 8.4 (Model T320UEU1AOC1) for Canada. • Jabber delays reconnecting to the network on a Samsung Xcover 3 when it loses Wi-Fi connectivity. • There's an audio quality issue in Samsung devices with chipset Exynos 7580. The audio becomes unclear when the device screen is off. Here is the device list: • Samsung Galaxy A3 2016 • Samsung Galaxy A5 2016 • Samsung Galaxy A7 2016 • Samsung Galaxy S5 Neo • Samsung Galaxy J7 • Samsung Galaxy View
Seuic	Cruise 1	9.0	
Sonim	XP8	7.1.1	

Device	Model	Minimum Android OS Version	Notes
Sony Xperia	XZ	7.0	
	XZ1	8.0	
	XZ2	8.0	
	XZ3	9.0	
	Z2	6.0	
	Z2 tablet	6.0	
	Z3	6.0	Sony Xperia Z3 (Model SO-01G) with Android OS 5.0.2 has poor audio on Jabber calls.
	Z3 Tablet Compact	6.0	
	Z3+/Z4	6.0	Video call is unstable on Sony Z3+/Z4. Try disabling your self-video for a video call. Otherwise, make a voice call only.
	Z4 TAB	6.0	
	Z5 Premium and Z5	6.0	
	Xperia 5 Mark II	11.0	

Device	Model	Minimum Android OS Version	Notes
Xiaomi	4C	6.0	Only the 32-bit version runs on these devices.
	MAX	6.0	
	Mi 4	6.0	
	Mi 5	6.0	
	Mi 5s	7.0	
	Mi 6	7.0	
	Mi 8	8.0	
	Mi 9	9.0	
	Mi 10	10.0	
	Mi 10 Ultra	10.0	
	Pocophone	8.0	
	Mi Note	6.0	Only the 32-bit version runs on these devices.
	Mi Note 2	7.0	
	Mi MIX 2	8.0	
	Mi A1	8.0	
	Redmi Note 3	6.0	
	Redmi Note 4X	6.0.1	
	Redmi Note 5	8.0	
	Redmi Note 6 Pro	8.1	
Zebra	TC75X	6.0	
	TC51	6.0	

[1] Because of changes in EMUI 10, incoming call toasts might not appear when your device is locked. In Jabber, go to **Settings** > **Notifications** and select **Banners**.

Jabber Support for Samsung Knox

Cisco Jabber for Android supports Samsung Knox as follows:

Knox Version	Samsung Devices
2.6	Note 4 Note 5 Note Edge S5 S6 S6 Edge S6 Edge Plus S7 S7 Edge Note 10.1 (2014 Edition)
2.7.1	Galaxy Note5
3.1	Galaxy A5 (2017)
3.2	Galaxy On5 (2016)
3.3	Galaxy S10

Note When you run Cisco Jabber for Android inside Samsung Know, the security design of Samsung Knox requires you to unlock Knox first. You can't answer or decline a call with Jabber until you unlock Knox.

Jabber Supports Samsung Dex

Cisco Jabber for Android supports Samsung Dex in Samsung S8, S8 Plus, and Note 8.

Support Policy on Earlier Android Versions for Cisco Jabber

Due to an Android kernel issue, Cisco Jabber can’t register to the Cisco Unified Communications Manager on some Android devices. To resolve this problem, try the following:

Upgrade the Android kernel to 3.10 or later version.

Set the Cisco Unified Communications Manager to use mixed mode security, enable secure SIP call signaling, and use port 5061. See the *Cisco Unified Communications Manager Security Guide* for your release for instructions on configuring mixed mode with the Cisco CTL Client. You can locate the security guides in the Cisco Unified Communications Manager Maintain and Operate Guides. This solution applies to the following supported devices:

Device Model	Operating System
HTC M8	Android OS 6.0 or later
HTC M9	Android OS 6.0 or later

Device Model	Operating System
Sony Xperia Z2	Android OS 6.0 or later and kernel version earlier than 3.10.49. If the device's Android OS is 6.0 or later and kernel version is 3.10.49 or later, then the device can support nonsecure mode.
Sony Xperia Z2 tablet	
Sony Xperia Z3	
Sony Xperia Z3 Tablet Compact	
Xiaomi Mi4	Android OS 6.0 or later
Xiaomi Mi Note	Android OS 6.0 or later
Honeywell Dolphin CT50	Android OS 6.0 or later

Supported Bluetooth Devices

Bluetooth Devices	Dependencies
Cisco 561	
Cisco 562	
Plantronics Voyager Legend	
Plantronics Voyager Legend UC	
Plantronics Voyager edge UC	
Plantronics Voyager edge	
Plantronics PLT focus	
Plantronics BackBeat 903+	If you use a Samsung Galaxy S4, you can experience problems due to compatibility issues between these devices.
Jabra Motion	Upgrade Jabra Motion Bluetooth headset to firmware version 3.72 or above. The Jabra Motion Bluetooth headsets with firmware version 3.72 or above supports Cisco Jabber call control.
Jabra Wave+	
Jabra Biz 2400	
Jabra Easygo	
Jabra PRO 9470	
Jabra Speak 510	
Jabra Supreme UC	

Bluetooth Devices	Dependencies
Jabra Stealth	
Jabra Evolve 65 UC Stereo	
Jawbone ICON for Cisco Bluetooth Headset	If you use a Samsung Galaxy S4, you can experience problems due to compatibility issues between these devices.

Bluetooth limitations:

- Using a Bluetooth device on a Samsung Galaxy SIII may cause distorted ringtone and distorted call audio.
- If a user disconnects and reconnects the Bluetooth Headset during a Jabber call, then the user can't hear the audio. This limitation applies to Smartphones with versions earlier to Android 5.0 OS.
- In Sony Z4 / LG G4 /Devices with OS Android 6.0, users can experience audio loss when switching to a Bluetooth headset after starting a Jabber call. As a workaround, switch the audio output to a speaker and then switch back to Bluetooth. Or connect the Bluetooth headset before making a Cisco Jabber call.

Supported Android Wear

Cisco Jabber runs on all Android wear devices with Android OS 5.0 or later and Google service 8.3 or later. We test Cisco Jabber on these Android Wear devices:

- Fossil Gen 3 SmartWatch
- Huawei watch
- LG G Watch R
- LG Watch Urbane
- Moto 360
- Moto 360 (2nd Gen)
- Samsung Gear Live
- Sony SmartWatch 3

Note The Cisco Jabber installer for Android wear devices is separate from the main Jabber APK file. Users get the Android wear installer from the Google Play store when they pair the wear device with a mobile device.

Supported Chromebook Models

Chromebook must have Chrome OS version 53 or later. Users can download Cisco Jabber for Android from Google Play Store.

- HP Chromebook 13 G1 Notebook PC
- Google Chromebook Pixel

- Google Chromebook Pixelbook
- Samsung Chromebook Pro
- Asus C302

Hardware Requirements for Cisco Jabber for iPhone and iPad

The following Apple devices are supported for Cisco Jabber for iPhone and iPad on iOS iOS 13.x and iPadOS. The devices that are not upgraded to these versions are not supported.

Apple Device	Version
iPad	5th, 6th, and 7th generation
iPad Air	Air 2 and Air 3
iPad Pro	9.7 and 10.5 inch 12.9 inch, 1st, 2nd and 3rd generation
iPad mini	Mini 4 and mini 5
iPhone	6s, 6s Plus, 7, 7 Plus , 8, 8 Plus, X, Xs, Xs Max, 11, 11 Pro, 11 Pro Max, XR and SE
iPod touch	6th generation
Apple Watch	WatchOS 5 running on Apple Watch and Apple Watch 2, 3 and 4.

The following Bluetooth headsets are supported on iPhone and iPad:

Manufacturer	Model(s)
Apple	AirPod
Cisco	561, 562
Jabra	BIZ 2400, Easygo, Evolve 65 UC Stereo, EXTREME 2, Motion[2], PRO 9470, Speak 450 for Cisco, Speak 510, Stealth Supreme UC, Wave +
Jawbone	ICON for Cisco Bluetooth Headset
Plantronics	Voyager Edge, Voyager Edge UC, Voyager Legend, Voyager Legend UC
Sony Eriksson	MW-600

[2] Supports Bluetooth control for Cisco Jabber calls. This feature is only supported with firmware version 3.72.

Network Requirements

When using Cisco Jabber over your corporate Wi-Fi network, we recommend that you do the following:

- Design your Wi-Fi network to eliminate gaps in coverage as much as possible, including in areas such as elevators, stairways, and outside corridors.
- Ensure that all access points assign the same IP address to the mobile device. Calls are dropped if the IP address changes during the call.
- Ensure that all access points have the same service set identifier (SSID). Hand-off may be much slower if the SSIDs do not match.
- Ensure that all access points broadcast their SSID. If the access points do not broadcast their SSID, the mobile device may prompt the user to join another Wi-Fi network, which interrupts the call.
- Ensure that the Enterprise firewall is configured to allow the passage of Session Traversal Utilities for NAT (STUN) packets.

Conduct a thorough site survey to minimize network problems that could affect voice quality. We recommend that you do the following:

- Verify nonoverlapping channel configurations, access point coverage, and required data and traffic rates.
- Eliminate rogue access points.
- Identify and mitigate the impact of potential interference sources.

For more information, see the following documentation:

- The “VoWLAN Design Recommendations” section in the *Enterprise Mobility Design Guide*.
- The *Cisco Unified Wireless IP Phone 7925G Deployment Guide*.
- The *Capacity Coverage & Deployment Considerations for IEEE 802.11g* white paper.
- The *Solutions Reference Network Design (SRND)* for your Cisco Unified Communications Manager release.

IPv6 Requirements

Cisco Jabber is fully IPv6 ready, it works as normal in pure IPv6 and hybrid networks with the limitations listed in this section. Cisco Collaboration solutions does not currently fully support IPv6. For example, Cisco VCS Expressway for Mobile and Remote Access has limitations in pure IPv6 networks that require NAT64/DNS64 to be deployed in mobile carrier networks. Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence don't currently support HTTPS in pure IPv6 networks.

This feature is configured in Jabber using the IP_Mode parameter to set the protocol to IPv4, IPv6, or Dual Stacks. Dual Stacks is the default setting. The IP_Mode parameter can be included in Jabber Client Configuration (refer to the latest version of the *Parameters Reference Guide for Cisco Jabber*), the bootstrap for Windows, and the URL configuration for Mac and Mobile clients.

The network IP protocol used by Jabber when connecting to services is determined by the following factors:

- The Jabber Client Configuration IP_Mode parameter.
- The client operating system IP capabilities.
- The server operating system IP capabilities.
- The availability of a DNS record for IPv4 and IPv6.
- Cisco Unified Communications Manager SIP setting for softphone devices configuration for IPv4, IPv6, or both. The SIP connection setting for softphone devices must match the Jabber IP_Mode parameter setting to make a successful connection.
- Underlying network IP capabilities.

On Cisco Unified Communications Manager, the IP capability is determined by generic server settings and device-specific settings. The following table lists the expected Jabber connections given the various settings, this list assumes that the DNS records for IPv4 and IPv6 are both configured.

When the Client OS, Server OS, and Jabber IP_Mode parameter are set to Two Stacks, Jabber will use either IPv4 or IPv6 address for connections with the server in accordance with RFC6555.

Client OS	Server OS	Jabber IP_Mode parameter	Jabber Connection outcome
IPv4 Only	IPv4 Only	IPv4-Only	IPv4 Connection
		IPv6-Only	Connection Failure
		Two Stacks	IPv4 Connection
IPv4 Only	IPv6 Only	IPv4-Only	Connection Failure
		IPv6-Only	Connection Failure
		Two Stacks	Connection Failure
IPv6 Only	IPv4 Only	IPv4-Only	Connection Failure
		IPv6-Only	Connection Failure
		Two Stacks	Connection Failure
IPv6 Only	IPv6 Only	IPv4-Only	Connection Failure
		IPv6-Only	IPv6 Connection
		Two Stacks	IPv6 Connection
IPv4 Only	Two Stacks	IPv4-Only	IPv4 Connection
		IPv6-Only	Connection Failure
		Two Stacks	IPv4 Connection

Client OS	Server OS	Jabber IP_Mode parameter	Jabber Connection outcome
IPv6 Only	Two Stacks	IPv4-Only	Connection Failure
		IPv6-Only	IPv6 Connection
		Two Stacks	IPv6 Connection
Two Stacks	IPv4 Only	IPv4-Only	IPv4 Connection
		IPv6-Only	Connection Failure
		Two Stacks	IPv4 Connection
Two Stacks	IPv6 Only	IPv4-Only	Connection Failure
		IPv6-Only	IPv6 Connection
		Two Stacks	IPv6 Connection
Two Stacks	Two Stacks	IPv4-Only	IPv4 Connection
		IPv6-Only	IPv6 Connection
		Two Stacks	IPv6 Connection

When you use Jabber in IPv6-Only mode, NAT64/DNS64 is required to connect to an IPv4 infrastructure, such as Webex Messenger service, Cisco VCS Expressway for Mobile and Remote Access, and Cisco Webex Platform service.

Desktop device support is available for IPv6-only on-premises deployments. All Jabber mobile devices must be configured as Two Stacks.

For more details about IPv6 deployment, see the IPv6 Deployment Guide for Cisco Collaboration Systems Release 12.0.

Limitations

- HTTPS Connectivity
  - In an On-Premises deployment, Cisco Jabber supports IPv4 only and Two Stacks modes to connect to Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service. These servers do not currently support IPv6 HTTPS connections.

    Cisco Jabber can connect using HTTPS to Cisco Unity Connection for Voicemail using IPv6 only mode.

- Webex Messenger Limitations
  - Webex Messenger is not supported on IPv6.

- Telephony Limitations
  - When you upgrade user devices on Cisco Unified Communications Manager to either Two Stacks or IPv6 only, the corresponding Jabber client must be upgraded to 11.6 or later.

- When an installation includes IPv4 endpoints and IPv6 endpoints, we recommend that you use a hardware MTP to bridge the Audio and Video between these devices. This is supported on hardware MTP with Cisco IOS version 15.5. For example, a Cisco 3945 router must run the following T-train build: c3900e-universalk9-mz.SPA.155-2.T2.bin.
- At present we do not have a solution roadmap to support IPv4 and IPv6 simultaneously in Cisco endpoints including Jabber. Cisco Unified Communications Manager supports the current functionality which is IPv4-Only and IPv6-Only. An MTP is required to support calls between IPv4-only and IPv6-only endpoints, or IPv4-only or IPv6-only Gateways.
- Jabber to Jabber calls are not supported on IPv6.

- File Transfer Limitations
  - Advanced File Transfer—When the client is configured for Two Stacks and Cisco Unified Communications Manager IM and Presence Service is Two Stacks enabled, advanced file transfer is supported on the following Cisco Unified Communications Manager IM and Presence Service versions:
    - 10.5.2 SU2
    - 11.0.1 SU2
    - 11.5
  - Person to Person file transfer—For on-premises deployment person to person file transfer between IPv4 and IPv6 clients is not supported. If you have a network configuration with both IPv4 and IPv6 clients, we recommend configuring advanced file transfer.

- Mobile and Remote Access Limitations
  - Cisco VCS Expressway for Mobile and Remote Access doesn't support IPv6.
  - If Cisco Unified Communications Manager is configured for an IPv6 SIP connection, you can't connect to Cisco Unified Communications Manager using Cisco VCS Expressway for Mobile and Remote Access to use telephony services.

Requirements to Support IPv6 in Android

Android OS Requirement

Android 5.0 and later

Network Requirements

- IPv4 Only mode (Android accepts only IPv4 address)
- Dual Stack with SLAAC (Android accepts both IPv4 and IPv6 address)
- NAT64 or DNS64 (server uses IPv4 address and client uses IPv6 address)

Limitations

- DHCPv6 Limitation

- DHCPv6 is not supported on an Android device.

- Android OS Limitation
  - Android OS does not support IPv6-only network. For more information on this limitation, see the Android developer link.

Ports and Protocols

The client uses the ports and protocols listed in the following table. If you plan to deploy a firewall between the client and a server, configure the firewall to allow these ports and protocols.

	Port	Application Layer Protocol	Transport Layer Protocol	Description
Configuration				
	6970	HTTP	TCP	Connect to the TFTP server to download client configuration files.
	6972	HTTPS	TCP	Connects to the TFTP server to download client configuration files securely for Cisco Unified Communications Manager release 11.0 and later.
	53	DNS	UDP	Hostname resolution.
	3804	CAPF	TCP	Issues Locally Significant Certificates (LSC) to IP phones. This port is the listening port for Cisco Unified Communications Manager Certificate Authority Proxy Function (CAPF) enrollment.
	8443	HTTPS		Traffic to Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service.
	8191	SOAP	TCP	Connects to local port to provide Simple Object Access Protocol (SOAP) web services.
Directory Integration—For LDAP contact resolution, one of these ports is used based on your LDAP configuration.				
	389	LDAP	TCP	LDAP TCP (UDP) Connects to an LDAP directory service.
	3268	LDAP	TCP	Connects to a Global Catalog server for contact searches.
	636	LDAPS	TCP	LDAPS TCP Connects securely to an LDAP directory service.
	3269	LDAPS	TCP	LDAPS TCP Connects securely to the Global Catalog server.
Instant Messaging and Presence				

	Port	Application Layer Protocol	Transport Layer Protocol	Description
	443	XMPP	TCP	XMPP traffic to the Webex Messenger service. The client sends XMPP through this port in cloud-based deployments only. If port 443 is blocked, the client falls back to port 5222.
	5222	XMPP	TCP	Connects to Cisco Unified Communications Manager IM and Presence Service for instant messaging and presence.
	37200	SOCKS5 Bytestream	TCP	Peer to Peer file transfer, In on-premises deployments, the client also uses this port to send screen captures.
	7336	HTTPS	TCP	MFT File transfer (On-Premises only).
Communication Manager Signaling				
	2748	CTI	TCP	Computer Telephony Interface (CTI) used for desk phone control.
	5060	SIP	TCP	Provides Session Initiation Protocol (SIP) call signaling.
	5061	SIP over TLS	TCP	SIP over TCP Provides secure SIP call signaling. (Used if Secure SIP is enabled for device.)
	3000-3999	FECC	UDP	Far end camera control (FECC).
	5070-6070	BFCP	UDP	Binary Floor Control Protocol (BFCP) for video screen sharing capabilities.
Voice or Video Media Exchange				
	16384-32766	RTP/SRTP	UDP	Cisco Unified Communications Manager media port range used for audio, video, and BFCP video desktop share.
	33434-33598	RTP/SRTP	UDP	Cisco Hybrid Services (Jabber to Jabber calling) media port range used for audio and video.
	8000	RTP/SRTP	TCP	Used by Jabber Desk Phone Video Interface. The interface enables users to receive video that's transmitted to their desk phone through the Jabber client.
Unity Connection				
	7080	HTTP	TCP	Used for Cisco Unity Connection to receive notifications of voice messages (new message, message update, and message deleted).
	7443	HTTPS	TCP	Used for Cisco Unity Connection to securely receive notifications of voice messages (new message, message update, and message deleted).
	8443	HTTPS	TCP	Connects to Cisco Unity Connection for configuration.
	443	HTTPS	TCP	Connects to Cisco Unity Connection for voicemail.

	Port	Application Layer Protocol	Transport Layer Protocol	Description
Webex Meetings				
	80	HTTP	TCP	Connects to Webex Meetings Center for meetings.
	443	HTTPS	TCP	Connects to Webex Meetings Center for meetings.
	8443	HTTPS	TCP	Web access to Cisco Unified Communications Manager and includes connections for the following: • Cisco Unified Communications Manager IP Phone (CCMCIP) server for assigned devices • User Data Service (UDS) for contact resolution
Accessories Manager				
	8001		TCP	In Cisco Jabber for Windows and Mac, Sennheiser plugin uses this port for Localhost traffic for call controls.

Ports for Other Services and Protocols

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

- For Cisco Unified Communications Manager, Cisco Unified Communications Manager IM and Presence Service, see the *TCP and UDP Port Usage Guide*.
- For Cisco Unity Connection, see the *System Administration Guide*.
- For Webex Meetings Server, see the *Administration Guide*.
- For Cisco Meeting Server, see *Cisco Meeting Server Release 2.6 and 2.7: Single Combined Meeting Server Deployments*.
- For Webex services, see the *Administrator's Guide*.
- For Expressway for Mobile and Remote Access, refer to *Cisco Expressway IP Port Usage for Firewall Traversal*.
- For file transfer port usage, see the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

Supported Codecs

Type	Codec	Codec Type	Cisco Jabber for Android	Cisco Jabber for iPhone and iPad	Cisco Jabber for Mac	Cisco Jabber for Windows
Audio	G.711	A-law	Yes Supports normal mode.		Yes	Yes
		µ-law/Mu-law	Yes Supports normal mode.		Yes	Yes
	G.722		Yes		Yes	Yes
	G.722.1	24 kb/s and 32 kb/s	Yes Supports normal mode.		Yes	Yes
	G.729		Does not support Visual Voicemail with G.729; however, you can access voice messages using G.729 and the **Call Voicemail** feature.		No	No
	G.729a		Yes Minimum requirement for low-bandwidth availability. Only codec that supports low-bandwidth mode. Supports normal mode.		Yes	Yes
	Opus		Yes		Yes	Yes
Video	H.264/AVC	Baseline profile	Yes		Yes	Yes
		High profile	No		Yes	Yes
Voicemail	G.711	A-law	Yes		Yes	Yes
		µ-law / Mu-law (default)	Yes		Yes	Yes
	PCM linear		Yes		Yes	Yes

If users have issues with voice quality when using Cisco Jabber for Android or Cisco Jabber for iPhone and iPad, they can turn low-bandwidth mode on and off in the client settings.

Virtual Environment Requirements

Software Requirements

To deploy Cisco Jabber for Windows in a virtual environment, select from the following supported software versions:

Software	Supported Versions
Citrix XenDesktop	7.9, 7.8, 7.6, 7.5, 7.1
Citrix XenApp	7.9 published apps and desktop 7.8 published apps and desktop 7.6 published apps and desktop 7.5 published desktop 6.5 published desktop
VMware Horizon View	6.x to 8.x

Softphone Requirements

For softphone calls, use Jabber Softphone for VDI. For more information, see **Release Notes for Cisco Jabber Softphone for VDI Release 12.9**

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.

Media Assure

Ensure quality of real-time media on all network types so that your meetings aren't interrupted because of poor media quality. Media Assure can relieve up to 25% packet loss.

Media Assure is supported for video on Cisco Unified Communications Manager Release 10.x or later and for audio and video on Cisco Unified Communications Manager Release 11.5 or later.

For Expressway for Mobile and Remote Access deployments, Media Assure requires Cisco Expressway Release 8.8.1 or later.

For minor to severe network conditions Jabber can:

- Temporarily limit bandwidth on streams.
- Re-sync video.

- Pace packets to avoid unnecessary congestion based burst losses.
- Provide resilience mechanisms by using upfront SDP signaling from first media packet.
- Protect packet loss.
- Avoid congestion based loss because of over production of media.
- Improve protection of low frame rate / low bit rate streams.
- Support authenticated and encrypted FEC.

Fast Lane Support

Fast Lane support ensures that business critical applications are prioritized on the network, even during high traffic. Jabber supports Fast Lane for Voice and Video traffic. For iOS 10, when the access point (AP) fast lane feature is used, the DSCP value configured on Cisco Unified Communications Manager will not be used anymore; whereas for iOS 11 that does not support the fast lane feature, Jabber will continue using the DSCP value configured on Cisco Unified Communications Manager.

Irrespective of the DSCP configuration on Cisco Unified Communications Manager, if your wireless AP supports the fast lane feature, then Jabber automatically sets the following DSCP and user priority (UP) values:

- For audio calls or the audio portion in a video call, DSCP is set to 0x2e and UP is set to 6.
- For the video portion in a video call, DSCP is set to 0x22 and UP is set to 5.
- If your AP does not support fast lane or does not use it, DSCP values are automatically set to that designated by Cisco Unified Communications Manager.

Prerequisites:

- WLC running AireOS 8.3 and higher
- AP1600/2600 Series Access Points, AP1700/2700 Series Access Points, AP3500 Series Access Points, AP3600 Series Access Points + 11ac Module, WSM, Hyperlocation module, 3602P, AP3700 Series Access Points + WSM, 3702P, OEAP600 Series OfficeExtend Access Points, AP700 Series Access Points, AP700W Series Access Points, AP1530 Series Access Points, AP1550 Series Access Points, AP1570 Series Access Points, and AP1040/1140/1260 Series Access Points
- iOS device running on iOS 11 or later.

Audio Bit Rates for Cisco Jabber Desktop Clients

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

Codec	RTP (kbits/second)	Actual bit rate (kbits/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

Audio Bit Rates for Cisco Jabber Mobile Clients

The following audio bit rates apply to Cisco Jabber for iPad and iPhone and Cisco Jabber for Android.

Codec	Codec bit rate (kbits/second)	Network Bandwidth Utilized (kbits/second)
g.711	64	80
g.722.1	32	48
g.722.1	24	40
g.729a	8	24

Video Bit Rates for Cisco Jabber Desktop Clients

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

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
1080p	1920 x 1080	2500-4000

Note The measured bit rate is the actual bandwidth used (RTP payload + IP packet overhead).

Video Bit Rates for Cisco Jabber for Android

Video	Resolution	Bandwidth
HD	1280 x 720	1024
VGA	640 x 360	512
CIF	488x211	310

Note To send and receive HD video during calls:

- Configure the maximum bit rate for video calls higher than 1024 kbps in Cisco Unified Communications Manager.
- Enable DSCP on a router to transmit video RTP package with high priority.

Video Bit Rates for Cisco Jabber for iPhone and iPad

The client captures and transmits at 20 fps.

Resolution	Pixels	Bit rate (kbits/second) with g.711 audio
w144p	256 x 144	290
w288p	512 x 288	340
w360p	640 x 360	415
w720p	1280 x 720	1024

Presentation Video Bit Rates

Cisco Jabber captures at 8 fps and transmits at 2–8 fps.

The values in this table do not include audio.

Pixels	Estimated wire bit rate at 2 fps (kbits per second)	Estimated wire bit rate at 8 fps (kbits per second)
720 x 480	41	164
704 x 576	47	188
1024 x 768	80	320
1280 x 720	91	364
1280 x 800	100	400
1920 x 1080	150-300	500-1000

In Release 12.5, we changed the bit rate allocation to improve the main video quality when your total video bandwidth is under 300 kb. But, that change also set the maximum bit rate for the main video at 450 kilobits/sec.

At higher total video bandwidths, you might see lower resolution, compared to earlier releases, in the main video.

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:

Desktop sharing session	Audio	Interactive video (Main video)	Presentation video (Desktop sharing video)
No	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.	—
Yes	Cisco Jabber uses the maximum audio bit rate.	Cisco Jabber allocates half of the remaining bandwidth after subtracting the audio bit rate.	Cisco Jabber allocates half of the remaining bandwidth after subtracting the audio 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.

Bandwidths

Region configuration on Cisco Unified Communications Manager can limit the bandwidth available to the client.

Use regions to limit the bandwidth that is used for audio and video calls within a region and between existing regions by specifying the transport-independent maximum bit rates for audio and for video calls. For more information on region configuration, see the Cisco Unified Communications Manager documentation for your release.

Bandwidth Performance Expectations for Cisco Jabber Desktop Clients

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

Upload speed	Audio	Audio + Interactive video (Main video)
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

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

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

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

Bandwidth Performance Expectations for Cisco Jabber for Android

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

Upload speed	Audio	Audio + Interactive Video (Main Video)
125 kbps under VPN	At bandwidth threshold for g.711. Insufficient bandwidth for video. Sufficient bandwidth for g.729a and g.722.1.	Insufficient bandwidth for video.
256 kbps	Sufficient bandwidth for any audio codec.	Transmission rate (Tx) — 256 x 144 at 15 fps Reception rate (Rx) — 256 x 144 at 30 fps
384 kbps under VPN	Sufficient bandwidth for any audio codec.	Tx — 640 x 360 at 15 fps Rx — 640 x 360 at 30 fps
384 kbps in an enterprise network	Sufficient bandwidth for any audio codec.	Tx — 640 x 360 at 15 fps Rx — 640 x 360 at 30 fps

Note Due to device limitations, the Samsung Galaxy SII and Samsung Galaxy SIII devices cannot achieve the maximum resolution listed in this table.

Bandwidth Performance Expectations for Cisco Jabber for iPhone and iPad

The client 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.

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

Upload speed	Audio	Audio + Interactive Video (Main Video)
125 kbps under VPN	At bandwidth threshold for g.711. Insufficient bandwidth for video. Sufficient bandwidth for g.729a and g.722.1.	Insufficient bandwidth for video.
290 kbps	Sufficient bandwidth for any audio codec.	256 x144 at 20 fps
415 kbps	Sufficient bandwidth for any audio codec.	640 x 360 at 20 fps
1024 kbps	Sufficient bandwidth for any audio codec.	1280 x 720 at 20 fps

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.

H.264 Profile Impact on Bandwidth

In earlier releases, we only supported the H.264 Baseline profile. In Release 12.8, we added support for H.264 High profile for the desktop clients. You cannot use High profile for VDI or mobile clients.

High profile can deliver the same video quality with up to 10% less bandwidth. Alternately, you can achieve better video quality with the same bandwidth.

Jabber defaults to the H.264 Baseline profile. To enable the High profile, us the H264HighProfileEnable parameter.

Call Management Records

At the end of a call, Jabber sends call performance and quality information to Cisco Unified Communications Manager. Cisco Unified Communications Manager uses these metrics to populate the Cisco Unified Communications Manager Call Management Record (CMR). Cisco Jabber sends the following information for both audio and video calls:

- Number of packets sent and received.
- Number of octets sent and received.
- Number of packets lost.
- Average jitter.

The client also sends the following video specific information:

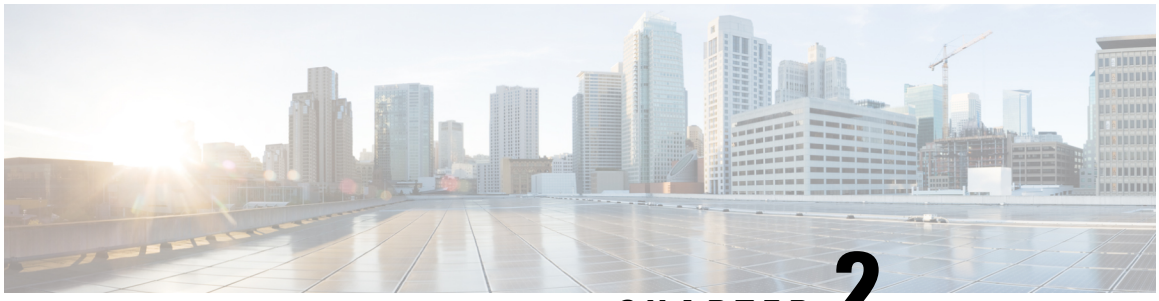
- Codec sent and received.
- Resolution sent and received.
- Framerate sent and received.
- Average round-trip time (RTT)

The client sends the following audio specific information:

- Concealed seconds.
- Severely concealed seconds.

The metrics appear in the Cisco Unified Communications Manager CMR record output in plain text format, this data can be read directly or consumed by a telemetry or analytics application.

For more information about configuring Cisco Unified Communications Manager CMR records, see the *Call Management Records* chapter of the *Call Detail Records Administration Guide* for your release of Cisco Unified Communications Manager.



CHAPTER 2

Deployment Scenarios

On-Premises Deployment

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

You can deploy Cisco Jabber in the following modes:

- **Full UC**—To deploy full UC mode, enable instant messaging and presence capabilities, provision voicemail and conferencing capabilities, and provision users with devices for audio and video.
- **IM-Only**—To deploy IM-only mode, enable instant messaging and presence capabilities. Do not provision users with devices.
- **Phone-Only Mode**—In Phone-Only mode, the user's primary authentication is to Cisco Unified Communications Manager. To deploy phone-only mode, provision users with devices for audio and video capabilities. You can also provision users with additional services such as voicemail.

The default product mode is one in which the user's primary authentication is to an IM and presence server.

On-Premises Deployment with Cisco Unified Communications Manager IM and Presence Service

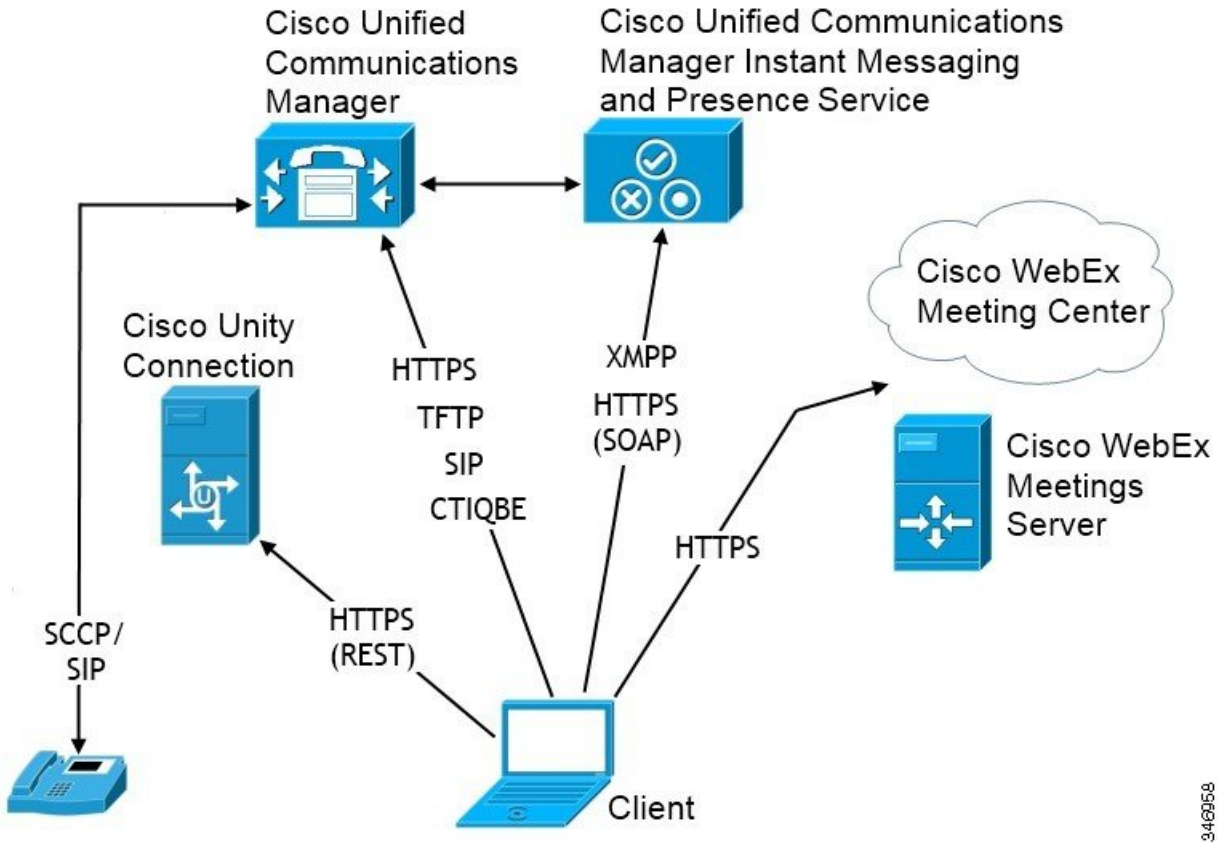
The following services are available in an on-premises deployment with Cisco Unified Communications Manager IM and Presence Service:

- **Presence**—Publish availability and subscribe to other users' availability through Cisco Unified Communications Manager IM and Presence Service.
- **IM**—Send and receive IMs through Cisco Unified Communications Manager IM and Presence Service.

- **File Transfers**—Send and receive files and screenshots through Cisco Unified Communications Manager IM and Presence Service.
- **Audio Calls**—Place audio calls through desk phone devices or computers through Cisco Unified Communications Manager.
- **Video**—Place video calls through Cisco Unified Communications Manager.
- **Voicemail**—Send and receive voice messages through Cisco Unity Connection.
- **Conferencing**—Integrate with one of the following:
  - Webex Meetings Center—Provides hosted meeting capabilities.
  - Webex Meetings Server—Provides on-premises meeting capabilities.

The following figure shows the architecture of an on-premises deployment with Cisco Unified Communications Manager IM and Presence Service.

Figure 1: On-Premises Deployment with Cisco Unified Communications Manager IM and Presence Service



Computer Telephony Integration

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

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

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

- Cisco TAPI: https://developer.cisco.com/site/jtapi/overview/
- Cisco JTAPI: https://developer.cisco.com/site/jtapi/overview/

On-Premises Deployment in Phone Mode

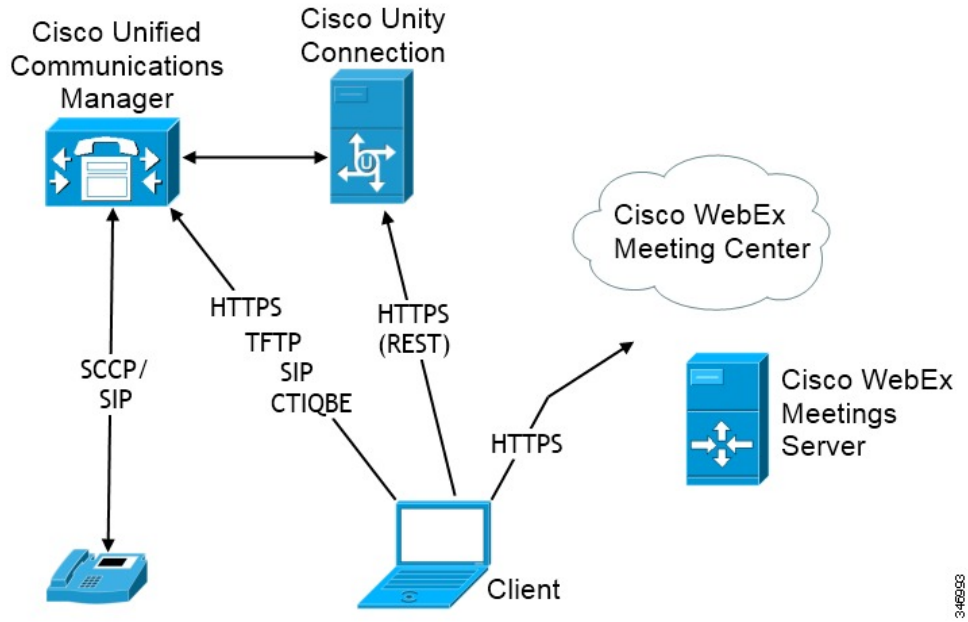
The following services are available in a phone mode deployment:

- **Contact**—This is applicable for mobile clients only. Cisco Jabber updates the contact information from the phone's contact address book.
- **Audio Calls**—Place audio calls through desk phone devices or on computers through Cisco Unified Communications Manager.
- **Video**—Place video calls through Cisco Unity Connection.
- **Voicemail**—Send and receive voice messages through Cisco Unity Connection.
- **Conferencing**—Integrate with one of the following:
  - **Webex Meetings Center**—Provides hosted meeting capabilities.
  - **Webex Meetings Server**—Provides on-premises meeting capabilities.

Note Cisco Jabber for Android and Cisco Jabber for iPhone and iPad do not support conferencing in phone mode.

The following figure shows the architecture of an on-premises deployment in phone mode.

Figure 2: On-Premises Deployment in Phone Mode



Softphone

Softphone mode downloads the configuration file from the TFTP server and operates as a SIP registered endpoint. The client uses the CCMCIP or UDS service to get the device name to register with Cisco Unified Communications Manager.

Deskphone

Deskphone mode creates a CTI connection with Cisco Unified Communications Manager to control the IP Phone. The client uses CCMCIP to gather the information about devices associated with a user and creates a list of IP phones available for control by the client.

Cisco Jabber for Mac in deskphone mode doesn't support desk phone video.

Extend and Connect

Cisco Unified Communications Manager Extend and Connect capabilities enable users control calls on devices such as public switched telephone network (PSTN) phones and private branch exchange (PBX) devices. For more information, see the Extend and Connect feature for your Cisco Unified Communications Manager release.

We recommend that you use extend and connect capabilities with Cisco Unified Communications Manager 9.1(1) and later.

Phone Mode with Contacts Deployment

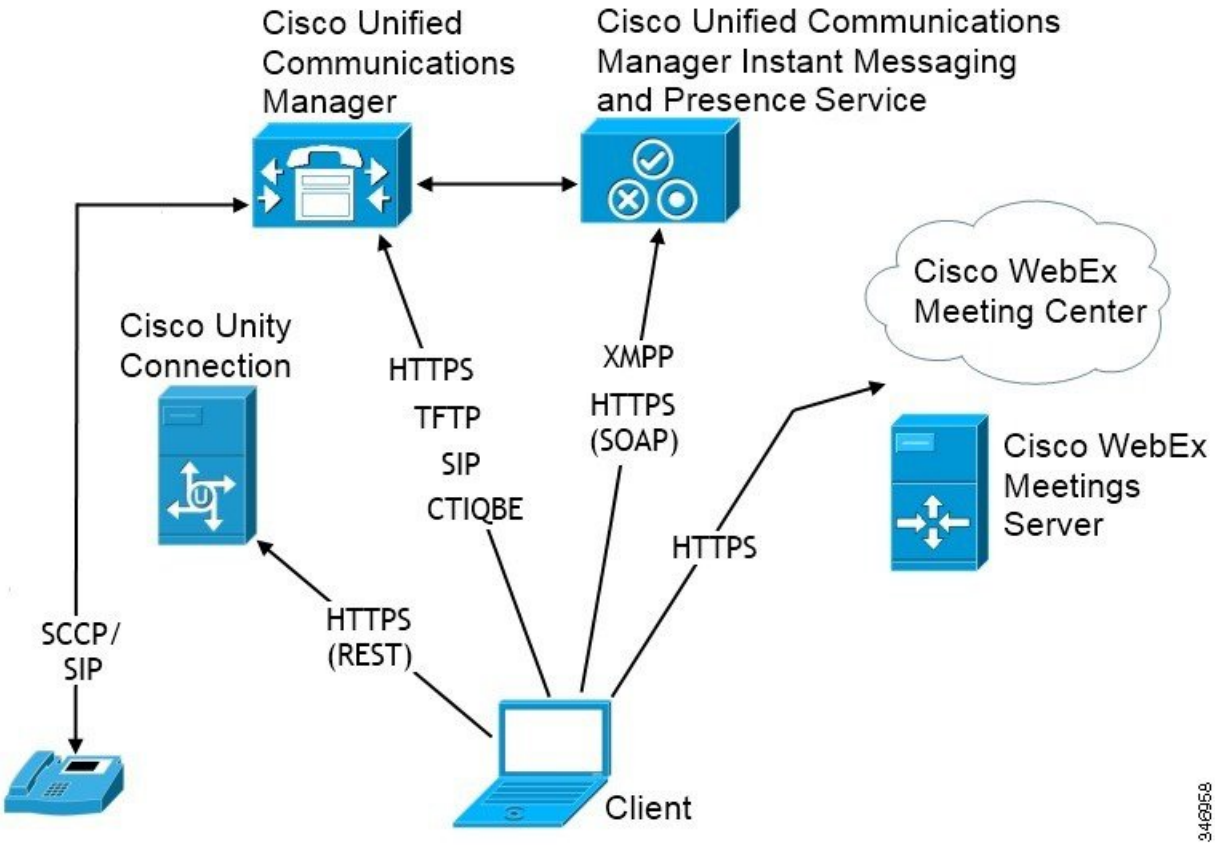
The following services are available in a phone mode with contacts deployment:

- **Contacts**—Contact information through Cisco Unified Communications Manager IM and Presence Service.

- **Presence**—Publish availability and subscribe to other users' availability through Cisco Unified Communications Manager IM and Presence Service.
- **Audio Calls**—Place audio calls through desk phone devices or computers through Cisco Unified Communications Manager.
- **Video**—Place video calls through Cisco Unified Communications Manager.
- **Voicemail**—Send and receive voice messages through Cisco Unity Connection.
- **Conferencing**—Integrate with one of the following:
  - Webex Meetings Center—Provides hosted meeting capabilities.
  - Webex Meetings Server—Provides on-premises meeting capabilities.

The following figure shows the architecture of an on-premises deployment with Cisco Unified Communications Manager IM and Presence Service.

Figure 3: Phone Mode with Contacts Deployment



Cloud-Based Deployments

A cloud-based deployment uses Webex to host services.

For cloud and hybrid deployments with Cisco Webex Messenger, you manage and monitor your cloud-based deployment using the Webex Administration Tool. You don't need to set up service profiles for your users.

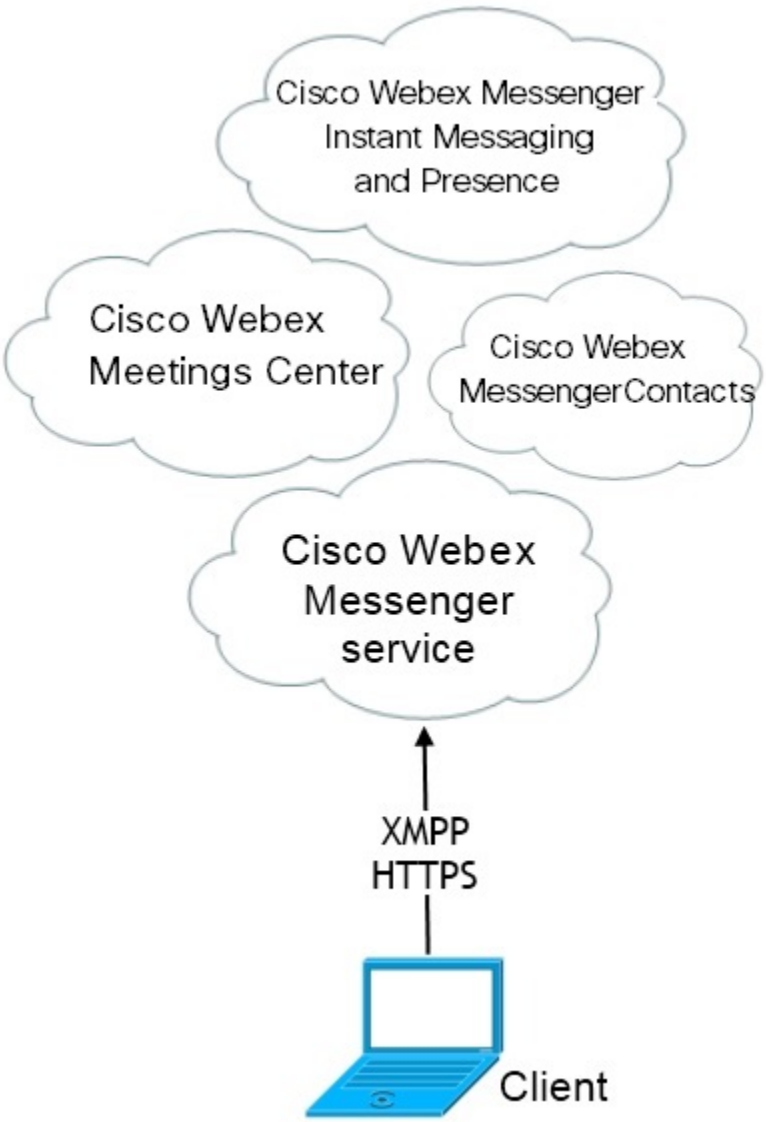
For cloud and hybrid deployments with Cisco Webex Platform service, you manage and monitor your deployment using the Cisco Control Hub.

Cloud-Based Deployment with Cisco Webex Messenger

The following services are available in a cloud-based deployment using Webex Messenger:

- **Contact Source**—Webex Messenger provides contact resolution.
- **Presence**—Webex Messenger lets users show their availability and see to other users' availability.
- **Instant Messaging**—Webex Messenger lets users send and receive instant messages.
- **Conferencing**—Webex Meetings Center provides hosted meeting capabilities.

The following figure shows the architecture of a cloud-based deployment.



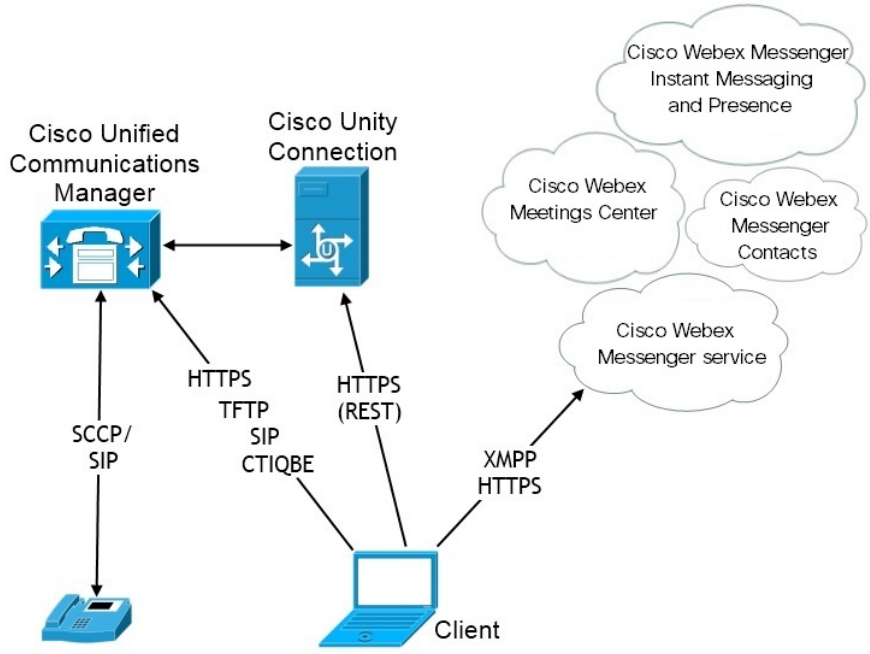
Hybrid Cloud-Based Deployment with Cisco Webex Messenger Service

The following services are available in a hybrid cloud-based deployment that uses Webex Messenger service:

- **Contact Source**—The Webex Messenger service provides contact resolution.
- **Presence**—The Webex Messenger service allows users to publish their availability and subscribe to other users' availability.
- **Instant Messaging**—The Webex Messenger service allows users to send and receive instant messages.
- **Audio**—Place audio calls through desk phone devices or computers through Cisco Unified Communications Manager.
- **Video**—Place video calls through Cisco Unified Communications Manager.

- **Conferencing**—Webex Meetings Center provides hosted meeting capabilities.
- **Voicemail**—Send and receive voice messages through Cisco Unity Connection.

The following figure shows the architecture of a hybrid cloud-based deployment.

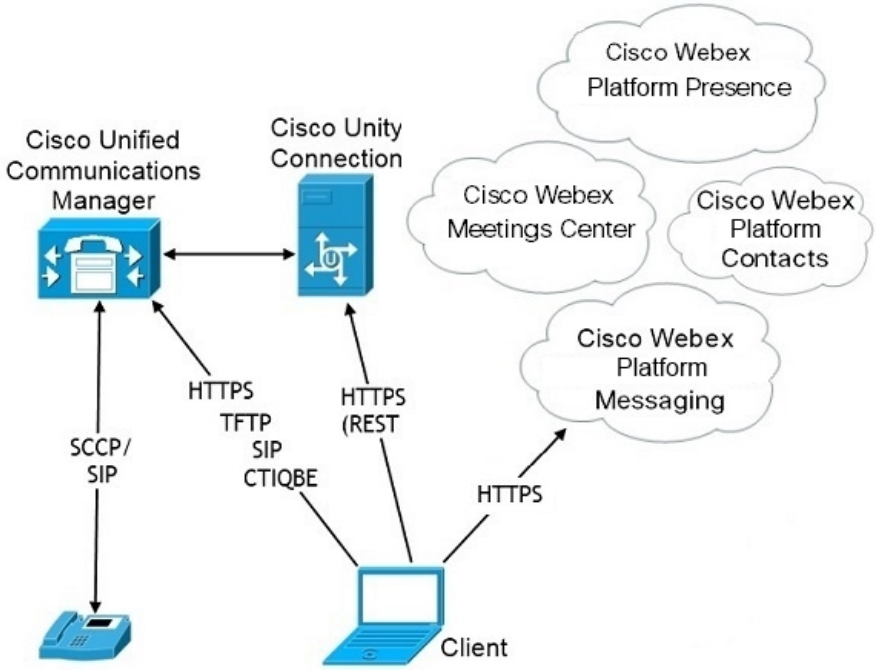


Hybrid Cloud-Based Deployment with Cisco Webex Platform Service

The following Jabber team messaging mode services are available in a Jabber hybrid cloud-based deployment with Cisco Webex Platform service:

- Contact Source—The Cisco Webex Platform service provides contacts.
- Presence—The Cisco Webex Platform service allows users to publish their availability and to view other users' availability.
- Messaging—The Cisco Webex Platform service allows users to send and receive messages.
- Audio—Make audio calls through desk phone devices or computers using Cisco UC Manager.
- Video—Make video calls using Cisco UC Manager.
- Conferencing—Webex Meetings Center provides hosted meeting capabilities.
- Voicemail—Send and receive voice messages through Cisco Unity Connection.

The following figure shows the architecture of a Jabber hybrid cloud-based deployment with Cisco Webex Platform service.



Contacts in Jabber Team Messaging Mode

Sign-In Flow

You must migrate your users' contacts while you enable team messaging mode in the Webex Control Hub.

This sign-in flow outlines the process for migrating users' contacts. The flow starts with the users being signed in to their current Jabber deployment. You enable Jabber team messaging mode and then migrate their contacts.

1. Users are signed into their current Jabber deployment, which connects to Cisco UC Manager IM&P or Cisco Webex Messenger.
2. The admin changes the configuration in the Webex Control Hub to enable Jabber team messaging mode, and optionally contact migration, and Jabber calls.
3. The next day, users sign into their current Jabber deployment. Within five minutes, Jabber performs the service discovery process, detecting that there is a Cisco Webex Platform service deployment for that user.
4. Jabber prompts the user to sign out of Jabber with the message, "Configuration changes detected."
5. Users sign back in again, this time authenticating to the Cisco Webex Platform service.
6. If you enabled contact migration, a message prompts the users to get their Jabber contacts. If they click Ok, then Jabber takes the contact list cache and uploads it to the Cisco Webex Platform service. If users selects **Cancel**, then Jabber doesn't migrate their contact list. They can later search for and add their contacts individually.

   During contact migration, Jabber only migrates contacts who are enabled for Cisco Webex Platform service. Jabber doesn't store custom contacts in Cisco Webex Platform service and can't add them to users' contact lists.

7. After Jabber connects to the Cisco Webex Platform service, it connects to Cisco UC Manager to download the service profile. If SSO is enabled on both Cisco Webex Platform service and UC Manager with different IdPs, or if SSO is only enabled on one, then users are prompted to enter their credentials. But, if SSO is on both with the same IdP, then no sign-in is necessary.

Deployment Considerations for Jabber Team Messaging Mode and Contact Migration

Your Cisco Webex Platform service org needs to have the same domain as the services domain. If they are different domains, then contact migration is not possible for users.

Deployment in a Virtual Environment

You can deploy Cisco Jabber for Windows in a virtual environment.

The following features are supported in a virtual environment:

- Instant messaging and presence with other Cisco Jabber clients
- Desk phone control
- Voicemail
- Presence integration with Microsoft Outlook 2007, 2010 and 2013
- Mobile and Remote Access (MRA)

Virtual Environment and Roaming Profiles

In a virtual environment, users do not always access the same virtual desktop. To guarantee a consistent user experience, these files must be accessible every time that the client is launched. Cisco Jabber stores user data in the following locations:

- `C:\Users\`*`username`*`\AppData\Local\Cisco\Unified Communications\Jabber\CSF`
  - **Contacts**—Contact cache files
  - **History**—Call and chat history
  - **Photo cache**—Caches the directory photos locally
- `C:\Users\`*`username`*`\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF`
  - **Config**—Maintains user configuration files and stores configuration store cache
  - **Credentials**—Stores encrypted username and password file

Because file encryption and decryption are linked to the Windows user profile, ensure that the following folders are accessible:

- `C:\Users\`*`username`*`\AppData\Roaming\Microsoft\Crypto`
- `C:\Users\`*`username`*`\AppData\Roaming\Microsoft\Credentials`
- `C:\Users\`*`username`*`\AppData\Local\Microsoft\Crypto`

- `C:\Users\username\AppData\local\Microsoft\Credentials`

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

If required, you can exclude files and folders from synchronization by adding them to an exclusion list. To synchronize a subfolder that is in an excluded folder, add the subfolder to an inclusion list.

To preserve personal user settings, do the following:

- Do not exclude the following directories:
  - `AppData\Local\Cisco`
  - `AppData\Local\JabberWerxCPP`
  - `AppData\Roaming\Cisco`
  - `AppData\Roaming\JabberWerxCPP`
- Use the following dedicated profile management solutions:
  - **Citrix Profile Management**—Provides a profile solution for Citrix environments. In deployments with random hosted virtual desktop assignments, Citrix profile management synchronizes each user's entire profile between the system it is installed on and the user store.
  - **VMware View Persona Management**—Preserves user profiles and dynamically synchronizes them with a remote profile repository. VMware View Persona Management does not require the configuration of Windows roaming profiles and can bypass Windows Active Directory in the management of VMware Horizon View user profiles. Persona Management enhances the functionality of existing roaming profiles.

Deploying Jabber Softphone for VDI

To deploy Jabber in a virtual environment with calling capabilities, you need to deploy Jabber Softphone for Virtual Desktop Infrastructure.

The workflow for deploying Jabber Softphone for VDI depends if you are deploying in an on-premises or hybrid environment, and follows Jabber deployment workflow up until application installation, at which point you follow Jabber Softphone for VDI deployment and installation workflows.

To get the on-premises deployment workflow for Jabber Softphone for VDI, see the *Full UC Deployment* workflow in the *Deployment and Installation Workflows* section of On-Premises Deployment for Cisco Jabber.

To get the hybrid deployment workflow for Jabber Softphone for VDI, see the *Hybrid Deployment using Webex Messenger* workflow in the *Workflows for Cloud and Hybrid Deployments* section of Cloud and Hybrid Deployments for Cisco Jabber.

Enterprise Mobility Management Deployments

Jabber supports two SDK-based clients for Enterprise Mobility Management (EMM) deployments:

- Cisco Jabber for Intune
- Cisco Jabber for BlackBerry

Your organization can deploy these clients to enforce policies for using Jabber on mobile devices in deployments that allow "Bring Your Own Device". For example, these policies can:

- Prevent the use of insecure jail-broken or rooted devices.
- Enforce minimum OS and app versions.
- Prevent users from copying data in Jabber and pasting it into another app.

Use the new EMMType parameter to control the Jabber clients on which your users can sign in.

Remember These clients follow a delayed release cycle. The clients release later than the corresponding releases of Jabber for Android and Jabber for iPhone and iPad.

EMM with Jabber for Intune

When you use the Jabber for Intune client in your deployment, your administrator configures your management policies in Microsoft Azure. Users download the new client from the App Store or Google Play Store. When the user runs the new client, it synchs with the policies that the administrator created.

Note For Android devices, users first install the Intune Company Portal. Then, they run the client through the portal.

The general process for setting up Jabber for Intune is:

1. Create a new Azure AD tenant.
2. Create new AD users or synch your on-premises AD users.
3. Create an Office 365 group or a Security group and add your users.
4. Add the Jabber for Intune client into Microsoft Intune.
5. Create and deploy your policies in Microsoft Intune.
6. Users sign in to the client and synch to receive your policies.

For details on these steps, see the Microsoft documentation.

This table lists the Microsoft Intune restrictions that we support in app protection policies for Cisco Jabber:

Restriction	Android	iPhone and iPad
Send data to other apps	Yes	Yes
Save copies of your organization's data	Yes	Yes
Cut, copy, and paste to other apps	Yes	Yes

Restriction	Android	iPhone and iPad
Screen captures	Yes	N/A
Maximum PIN attempts	Yes	Yes
Offline grace periods	Yes	Yes
Minimum app versions	Yes	Yes
Use on jailbroken or rooted devices	Yes	Yes
Minimum device OS version	Yes	Yes
Minimum patch version	Yes	N/A
Work (or school) account credentials for access	Yes	Yes
Recheck the access requirements	Yes	Yes

EMM with Jabber for BlackBerry

When you use the Jabber for BlackBerry client in your deployment, your administrator configures your management policies in the BlackBerry Unified Endpoint Management (UEM). Users download the new client from the App Store or Google Play Store. Jabber for BlackBerry is undergoing BlackBerry certification and isn't yet available in BlackBerry Marketplace.

Important Because the client is undergoing BlackBerry certification, we must grant access to your organization. To receive access, contact us (jabber-mobile-mam@cisco.com) and provide the Organization ID of your customer from their BlackBerry UEM server.

The new client has integrated the BlackBerry Dynamics SDK and can directly fetch the policies from BlackBerry UEM. The client bypasses BlackBerry Dynamics for connectivity and storage. The FIPS setting is not supported through the BlackBerry Dynamics SDK.

Your chat, voice, and video traffic bypasses the BlackBerry infrastructure. When the client isn't on-premises, it requires Mobile & Remote Access through a Cisco Expressway for all traffic.

Note Jabber for BlackBerry on Android requires Android 6.0 or above.

Jabber for BlackBerry on iOS requires iOS 11.0 or above.

For BlackBerry Dynamics, your administrator sets up policies in to control use of the Jabber for BlackBerry client.

The general process for setting up Jabber for BlackBerry is:

1. Create a server in the UEM.
2. Add the Jabber for BlackBerry client into BlackBerry Dynamics.

3. Create or import your users in BlackBerry Dynamics.

Note For Android users, you can optionally generate access keys in BlackBerry Dynamics.

4. Create and deploy your policies in UEM. Note the behavior of these settings on the Jabber for BlackBerry app configuration:
   - If you enable the optional DLP policy, BlackBerry requires that:
     - Use BlackBerry Works to send emails.
     - Use BlackBerry Access for SSO authentication in iOS devices. Enable **Use native browser** for iOS on Expressway and Unified Communications Manager. Then, add the **`ciscojabber`** scheme to the BlackBerry access policies in the BlackBerry UEM.
   - This list shows the Jabber parameters that are useful to set through app configuration in Jabber for BlackBerry deployments. See the *URL Configuration for Cisco Jabber for Android, iPhone, and iPad* section in the *Deployment Guide* for more details on these parameters:

Field	Supported on iOS	Supported on Android
Disable cross launch Webex Meetings [3]	Yes	Yes
Services Domain	Yes	Yes
Voice Services Domain	Yes	Yes
Service Discovery Excluded Services	Yes	Yes
Services Domain SSO Email Prompt	Yes	Yes
Invalid Certificate Behavior	Yes	Yes
Telephony Enabled	Yes	Yes
Allow Url Provisioning	Yes	Yes
IP Mode	Yes	Yes

[3] Enabling cross launch of Webex Meetings allows it to run as an exception in a BlackBerry Dynamics container that doesn't allow non-Dynamics apps.

5. Users sign in to the client.

For details on these steps, see the BlackBerry documentation.

This table lists the BlackBerry restrictions that we support in app protection policies for Cisco Jabber:

Group	Feature	Android	iPhone and iPad
IT policies	Wipe the device without network connectivity	Yes	Yes

Group	Feature	Android	iPhone and iPad
Activation	Allowed Version	Yes	Yes
BlackBerry Dynamics	Password	Yes	Yes
	Data leakage prevention - Don't allow copying data from BlackBerry Dynamics apps into non-BlackBerry Dynamics apps	Yes	Yes
	Data leakage prevention - Don't allow copying data from non-BlackBerry Dynamics apps into BlackBerry Dynamics apps	Yes	Yes
	Data leakage prevention - Don't allow screen captures on Android and Windows 10 devices	Yes	N/A
	Data leakage prevention - Don't allow screen recording and sharing on iOS devices	N/A	Yes
	Data leakage prevention - Don't allow custom keyboards on iOS devices	N/A	Yes
Enterprise Management Agent profile	Allow personal app collection	Yes	Yes
Compliance profile	Rooted OS or failed attestation	Yes	Yes
	Restricted OS version is installed	Yes	Yes
	Required security patch level isn't installed	Yes	N/A

IdP Connections in Jabber for BlackBerry

In Jabber for Android and iPhone and iPad deployments, the client connects to an Identity Provider (IdP) proxy in the DMZ. The proxy then passes the request to the IdP server behind the inner firewall.

In Jabber for BlackBerry, you have an alternate path available. If you enable the DLP policy in the BlackBerry UEM, clients on iOS devices can securely tunnel directly to the IdP server. To use this setup, configure your deployment as follows:

- Enable **Use native browser** for iOS on Expressway and Unified CM.
- Add the `ciscojabber` scheme to the BlackBerry access policies in the BlackBerry UEM.

Jabber for BlackBerry on the Android OS always connects to the IdP proxy for SSO.

If your deployment only contains devices running on iOS, you don't need an IdP proxy in the DMZ. But, if your deployment contains any devices running on Android OS, you require the IdP proxy.

App Transport Security on iOS

iOS includes the App Transport Security (ATS) feature. ATS requires that Jabber for BlackBerry and Jabber for Intune makes secure network connections over TLS with reliable certificates and encryption. ATS blocks connections to servers that don't have an X.509 digital certificate. The certificate must pass these checks:

- An intact digital signature
- A valid expiration date
- A name that matches the DNS name of the server
- A chain of valid certificates to a trusted anchor certificate from a CA

Note For more information on trusted anchor certificates that are part of iOS, see *Lists of available trusted root certificates in iOS* at https://support.apple.com/en-us/HT204132. A system administrator or user can also install their own trusted anchor certificate, as long as it meets the same requirements.

For more information on ATS, see *Preventing Insecure Network Connections* at https://developer.apple.com/documentation/security/preventing_insecure_network_connections.

Remote Access

Your users may need to access their work from a location that's outside the corporate network. You can provide them access to their work using one of the Cisco products for remote access.

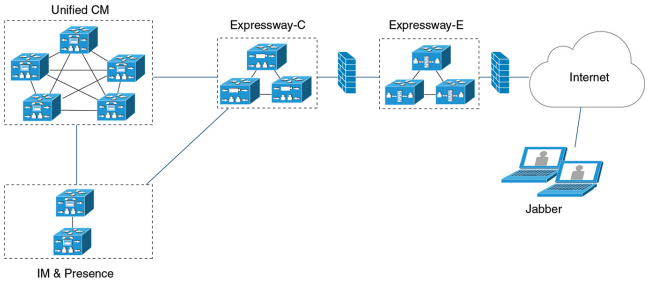
Jabber is not tested or validated with any third-party VPN client.

Expressway for Mobile and Remote Access

Expressway for Mobile and Remote Access for Cisco Unified Communications Manager allows users to access their collaboration tools from outside the corporate firewall without using a virtual private network (VPN). 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.

Figure 4: How the Client Connects to the Expressway for Mobile and Remote Access

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



First Time Signing into Jabber Using Expressway for Mobile and Remote Access

Applies to Cisco Jabber for mobile clients.

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, initially sign in while on the corporate network:

- If the voice services domain is different from the other services domain, then users must be inside the corporate network to get the correct voice services domain from the `jabber-config.xml` file. For a hybrid deployment, administrator can configure the VoiceServicesDomain parameter, refer to the latest version of the *Parameters Reference Guide for Cisco Jabber*. In this case, users are not required to sign in inside the corporate network.
- If Cisco Jabber must complete the CAPF enrollment process, which is required when using a secure or mixed mode cluster.

We do not support first-time sign-in on a public network if user is using a secure phone through Expressway for Mobile and Remote Access environment. If the configuration is for a secure profile with encrypted TFTP, then the first-time sign-in must be in on-premises to allow CAPF enrolment. First-time sign-in on a public network cannot be supported without Cisco Unified Communications Manager, Expressway for Mobile and Remote Access, and Cisco Jabber enhancements. However we do support:

- Encrypted TFTP, with first-time sign-in through on-premises.
- Unencrypted TFTP, with first-time sign-in through Expressway for Mobile and Remote Access or on-premises.

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 2: 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 white list on Cisco Expressway-C	
Intradomain federation	X * Contact search support depends on the format of your contact IDs. For more information, see the note below.	
Interdomain federation	X	

Service	Supported	Unsupported
Instant Messaging and Presence		
On-premises	X	
Cloud	X	
Chat	X	
Group chat	X	
Persistent chat	X	
High Availability: On-premises deployments	X	
File transfer: On-premises deployments	X Advanced options available for file transfer using Cisco Unified Communications Manager IM and Presence Service 10.5(2) or later, see the note below.	
File transfer: Cloud deployments	X	
Video screen share - BFCP	X (Cisco Jabber for mobile clients only support BFCP receive.)	
IM-Only Screen Share		x
Audio and Video		
Audio and video calls	X * Cisco Unified Communications Manager 9.1(2) and later	
Deskphone control mode (CTI) (desktop clients only)		X
Extend and connect (desktop clients only)		X
Remote desktop control (desktop clients only)		X
Silent Monitoring and Call Recording		X
Dial via Office - Reverse (mobile clients only)	X	
Session persistency		X
Early media		X
Self Care Portal access		X

Service	Supported	Unsupported
Graceful Registration	X * Applies to Cisco Jabber for Android. Jabber for Android supports graceful registration over Expressway for Mobile and Remote Access from Cisco Unified Communications Manager Release 10.5.(2) 10000-1.	
Shared line	X Prerequisites: • Cisco Expressway to X8.9.1 or later • Cisco Unified Communications Manager to 11.5 SU(2) or later	
Voicemail		
Visual voicemail	X * Using HTTP white list on Cisco Expressway-C	
Webex Meetings		
On-premises		X * Unsupported, except with an on-premises Cisco Webex Meeting Server from Jabber 11.6 forward.
Cloud	X	
Webex screen share (desktop clients only)	X	
Installation (Desktop clients)		
Installer update	X * Using HTTP white list on Cisco Expressway-C	X Not supported on Cisco Jabber for Mac
Customization		
Custom HTML tabs		X

Service	Supported	Unsupported
Enhanced911 Prompt	X * To ensure that the web page renders correctly for all Jabber clients operating outside the corporate network, the web page must be a static HTML page because the scripts and link tags are not supported by the E911NotificationURL parameter. For more inforation, see the latest *Parameter Reference Guide for Cisco Jabber*.	
Security		
ICE protocol for media	X	
CAPF enrollment		X
Single Sign-On	X	
Advanced Encryption Standard (AES) 256 and TLS1.2	X * Applies to Cisco Jabber for Android. Advanced encryption is supported only on corporate Wi-Fi	
Troubleshooting (Desktop clients only)		
Problem report generation	X	
Problem report upload		X
High Availability (failover)		
Audio and Video services		X
Voicemail services		X
IM and Presence services	X	
Contact search	X	
Contact resolution	X	
Configuration Management		
Fast Sign-in	X	
Authentication and Authorization		
O-Auth support for SSO Jabber users	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 white list of your Cisco Expressway-C server. To add a server to Cisco Expressway-C white list, use the **HTTP server allow** setting. For more information, see the relevant Cisco Expressway documentation.

- Intradomain federation — When you deploy intradomain federation and the client connects with Expressway for Mobile and Remote Access from outside the firewall, contact search is supported only when the contact ID uses one of the following formats:

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

- Interdomain federation using XMPP — Expressway for Mobile and Remote Access doesn't enable XMPP Interdomain federation itself. Cisco Jabber clients connecting over Expressway for Mobile and Remote Access can use XMPP Interdomain federation if it has been enabled on Cisco Unified Communications Manager IM and Presence.

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 has the following limitations for desktop and mobile clients:

- For Webex cloud deployments, file transfer is supported.
- For on-premises deployments with Cisco Unified Communication IM and Presence Service 10.5(2) or later, the **Managed File Transfer** selection is supported, however the **Peer-to-Peer** option is not supported.
- For on-premises deployments with Cisco Unified Communications Manager IM and Presence Service 10.0(1) or earlier deployments, file transfer is not supported.
- For Expressway for Mobile and Remote Access deployments with unrestricted Cisco Unified Communications Manager IM and Presence Server, Managed File Transfer is not supported.

Audio and Video Calling

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

- Cisco Unified Communications Manager — Expressway for Mobile and Remote Access supports video and voice calling with Cisco Unified Communications Manager Version 9.1.2 and later.
- Deskphone control mode (CTI) (Desktop clients only) — The client does not support deskphone control mode (CTI), including extension mobility.
- Extend and connect (Desktop clients only) — 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 (Desktop clients only) — Users cannot access the Cisco Unified Communications Manager Self Care Portal when outside the firewall. The Cisco Unified Communications Manager user page cannot be accessed externally.

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

Voicemail

Voicemail service is supported when the client connects to services using Expressway for Mobile and Remote Access.

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

Installation

Cisco Jabber for Mac — When the client connects to services using Expressway for Mobile and Remote Access, it doesn't support installer updates.

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

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

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 always encrypted on the call path between the Cisco Expressway-C and devices that are registered to the Cisco Unified Communications Manager using Expressway for Mobile and Remote Access.
  - Media is not encrypted on the call path between the Cisco Expressway-C and devices that are registered locally to Cisco Unified Communications Manager, if either Cisco Jabber or an internal device is not configured with Encrypted security mode.
  - Media is encrypted on the call path between the Expressway-C and devices that are registered locally to Cisco Unified Communication Manager, if both Cisco Jabber and internal device are configured with Encypted security mode.
  - In case where Cisco Jabber clients always connects through Expressway for Mobile and Remote access, CAPF enrollment is not required to achieve end-to-end encryption. However, Cisco Jabber devices must still be configured with encrypted security mode, and Cisco Unified Communications Manager must be enabled to support mixed mode.
  - You can configure ICE passthrough support on your Expressway-C or Expressway-E servers to ensure media sent over Jabber is encrypted when outside the corporate network. For more information on how to set it up, see the *Deployment Guide* for *Mobile and Remote Access through Cisco Expressway* .

Troubleshooting

Cisco Jabber for Windows only. 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.

High Availability (failover)

High Availability means that if the client fails to connect to the primary server, it fails over to a secondary server with little or no interruption to the service. In relation to high availability being supported on the Expressway for Mobile and Remote Access, high availability refers to the server for the specific service failing over to a secondary server (such as Instant Messaging and Presence).

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

Cisco AnyConnect Deployments

Cisco AnyConnect refers to a server-client infrastructure that enables the client to connect securely to your corporate network from remote locations such as Wi-Fi networks or mobile data networks.

The Cisco AnyConnect environment includes the following components:

- Cisco Adaptive Security Appliance — Provides a service to secure remote access.
- Cisco AnyConnect Secure Mobility Client — Establishes a secure connection to Cisco Adaptive Security Appliance from the user's device.

This section provides information that you should consider when deploying the Cisco Adaptive Security Appliance (ASA) with the Cisco AnyConnect Secure Mobility Client. Cisco AnyConnect is the supported VPN for Cisco Jabber for Android and Cisco Jabber for iPhone and iPad. If you use an unsupported VPN client, ensure that you install and configure the VPN client using the relevant third-party documentation.

For Samsung devices running Android OS 4.4.x, use Samsung AnyConnect version 4.0.01128 or later. For Android OS version above 5.0, you must use Cisco AnyConnect software version later than 4.0.01287.

Cisco AnyConnect provides remote users with secure IPsec (IKEv2) or SSL VPN connections to the Cisco 5500 Series ASA. Cisco AnyConnect can be deployed to remote users from the ASA or using enterprise software deployment systems. When deployed from the ASA, remote users make an initial SSL connection to the ASA by entering the IP address or DNS name in the browser of an ASA configured to accept clienteless SSL VPN connections. The ASA then presents a login screen in the browser window, if the user satisfies the login and authentication, it downloads the client that matches the computer operating system. After downloading, the client installs and configures itself and establishes an IPsec (IKEv2) or SSL connection to the ASA.

For information about requirements for Cisco Adaptive Security Appliance and Cisco AnyConnect Secure Mobility Client, see the *Software Requirements* topic.

Related Topics

Navigating the Cisco ASA Series Documentation
Cisco AnyConnect Secure Mobility Client

Deployment with Single Sign-On

You can enable your services with Security Assertion Markup Language (SAML) single sign-on (SSO). SAML SSO can be used in on-premises, cloud, or hybrid deployments.

The following steps describe the sign-in flow for SAML SSO after your users start their Cisco Jabber client:

1. The user starts the Cisco Jabber client. If you configure your Identity Provider (IdP) to prompt your users to sign in using a web form, the form is displayed within the client.
2. The Cisco Jabber client sends an authorization request to the service that it is connecting to, such as Webex Messenger service, Cisco Unified Communications Manager, or Cisco Unity Connection.
3. The service redirects the client to request authentication from the IdP.
4. The IdP requests credentials. Credentials can be supplied in one of the following methods:
   - Form-based authentication that contains username and password fields.
   - Kerberos for Integrated Windows Authentication (IWA) (Windows only)
   - Smart card authentication (Windows only)
   - Basic HTTP authentication method in which client offers the username and password when making an HTTP request.
5. The IdP provides a cookie to the browser or other authentication method. The IdP authenticates the identity using SAML, which allows the service to provide the client with a token.
6. The client uses the token for authentication to log in to the service.

Authentication Methods

The authentication mechanism impacts how a user signs on. For example, if you use Kerberos, the client does not prompt users for credentials, because your users already provided authentication to gain access to the desktop.

User Sessions

Users sign in for a *session*, which gives them a predefined period to use Cisco Jabber services. To control how long sessions last, you configure cookie and token timeout parameters.

Configure the IdP timeout parameters with an appropriate amount of time to ensure that users are not prompted to log in. For example, when Jabber users switch to an external Wi-Fi, are roaming, their laptops hibernate, or their laptop goes to sleep due to user inactivity. Users will not have to log in after resuming the connection, provided the IdP session is still active.

When a session has expired and Jabber is not able to silently renew it, because user input is required, the user is prompted to reauthenticate. This can occur when the authorization cookie is no longer valid.

If Kerberos or a Smart card is used, no action is needed to reauthenticate, unless a PIN is required for the Smart card; there is no risk of interruption to services, such as voicemail, incoming calls, or instant messaging.

Single Sign-On Requirements

SAML 2.0

Use SAML 2.0 to enable single sign-on (SSO) for Cisco Jabber clients using Cisco Unified Communications Manager services. SAML 2.0 isn't compatible with SAML 1.1. Select an IdP that uses the SAML 2.0 standard. Since the supported identity providers are compliant with SAML 2.0, you can use them to implement SSO.

Supported Identity Providers

We support IdPs that are Security Assertion Markup Language (SAML) compliant. We have tested the following identity providers:

- Ping Federate 6.10.0.4
- Microsoft Active Directory Federation Services (ADFS) 2.0
- Open Access Manager (OpenAM) 10.1

Note Ensure that you configure Globally Persistent cookies for use with OpenAM.

When you configure the IdP, the configured settings impact how you sign into the client. Parameters, such as the cookie type (persistent or session) or the authentication mechanism (Kerberos or Web form), determine how often you have to authenticate.

Cookies

To enable cookie sharing with the browser, use persistent cookies and not session cookies. Persistent cookies prompt the user to enter credentials one time in the client or in any other desktop application that uses Internet Explorer. Session cookies require that users enter their credentials every time that they launch the client. You configure persistent cookies as a setting on the IdP. If you're using Open Access Manager as your IdP, configure Globally Persistent cookies (and not Realm Specific Persistent Cookies).

When a user has successfully signed in to Cisco Jabber for iPhone and iPad using SSO credentials, cookies are saved in the iOS keychain by default. If cookies are in the iOS keychain, users don't need to enter sign in credentials for the next sign-in, unless the cookie expires during sign in. Cookies are deleted from iOS keychain in the following scenarios:

- Manually sign out of Cisco Jabber.
- Cisco Jabber is reset.
- After rebooting the iOS device
- Cisco Jabber is closed manually.

Note If you use the embedded Safari browser, Jabber can't control the cookies that Safari controls. Because Jabber can't clear these cookies, Jabber can only clear the SSO token in this case. If Safari has the user credentials in a persistent cookie, the cookie allows the user to avoid reentering their credentials when Jabber clears the SSO token.

If the iOS system stops Cisco Jabber for iPhone and iPad in the background, Jabber allows users to automatically sign in without entering a password.

Required Browsers

To share the authentication cookie (issued by IdP) between the browser and the client, specify one of the following browsers as your default browser:

Product	Required Browser
Cisco Jabber for Windows	Internet Explorer
Cisco Jabber for Mac	Safari
Cisco Jabber for iPhone and iPad	Safari
Cisco Jabber for Android	Chrome or Internet Explorer

Note An embedded browser can’t share a cookie with an external browser when using SSO with Cisco Jabber for Android.

Single Sign-On and Remote Access

For users that provide their credentials from outside the corporate firewall using Expressway Mobile and Remote Access, single sign-on has the following restrictions:

- Single sign-on (SSO) is available with Cisco Expressway 8.5 and Cisco Unified Communications Manager release 10.5.2 or later. You must either enable or disable SSO on both.
- You can't use SSO over the Expressway for Mobile and Remote Access on a secure phone.
- The Identity Provider used must have the same internal and external URL. If the URL is different, the user may be prompted to sign in again when changing between inside and outside the corporate firewall.

Location awareness for Enhanced 911 (Nomadic E911) support

To comply with the Ray Baum's Act in the United States, Jabber must report location information for emergency calls after January 6, 2022. *Nomadic E911* is the ability to report your actual location as you move. If you operate in the United States, almost all enterprises must enable this feature.

Wireless on-premises network

We already report wireless location when it's over on-premises network through Cisco Emergency Responder (CER) to your local Public Safety Answering Point (PSAP).

Other networks

We now support nomadic E911 as follows:

- **Mobile phones (Android and iPhone)**—Jabber always launches the native phone app to place the emergency call.
- **Desktop client and tablets**—If you oeprate in the United States, install the RedSky MyE911 app. Use MyE911 to report location information to your local PSAP.

Note You must create a RedSky account.

Server requirement

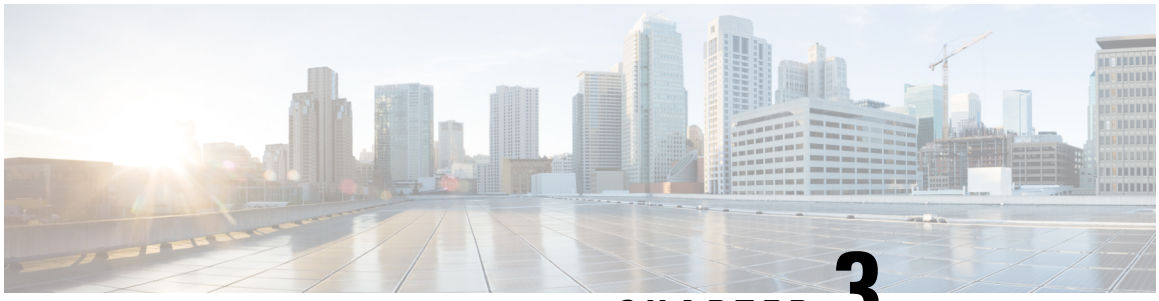
To pick up the routing logic change, update Cisco Emergency Responder (CER) to Release 12.5 SU6 or Release 14 SU2.

Note If you want the change before updating CER, you'll need to install a COP file for CER.

More information

See the following resources:

- "Wireless Location Monitoring Service" in the Feature Configuration for Cisco Jabber
- Cisco Emergency Responder Administration Guide
- RedSky E911 for Cisco



CHAPTER 3

User Management

Jabber IDs

Cisco Jabber uses a Jabber ID to identify the contact information in the contact source.

The default Jabber ID is created using the user ID and the presence domain.

For example, Adam McKenzie has a user ID of `amckenzie`, his domain is `example.com` and his Jabber ID is `amckenzie@example.com`.

The following characters are supported in a Cisco Jabber user ID or email address:

- Uppercase characters (A to Z)
- Lowercase characters (a to z)
- Numbers (0-9)
- Period (.)
- Hyphen (-)
- Underscore (_)
- Tilde (~)
- Hashtag (#)

When populating the contact list the client will search the contact source using the Jabber IDs to resolve the contacts and display the firstname, lastname, and any other contact information.

IM Address Scheme

Cisco Jabber 10.6 and later supports multiple presence domain architecture models for on premises deployments when the domains are on the same presence architecture, for example users in example-us.com and example-uk.com. Cisco Jabber supports flexible IM Address Scheme using Cisco Unified Communications Manager IM and Presence 10.x or later. The IM Address scheme is the Jabber ID that identifies the Cisco Jabber users.

To support multi domain models, all components of the deployment require the following versions:

- Cisco Unified Communications IM and Presence server nodes and call control nodes version 10.x or later.
- All clients running on Windows, Mac, IOS and Android version 10.6 or later.

Only deploy Cisco Jabber with multiple domain architecture in the following scenarios:

- Cisco Jabber 10.6 or later is deployed as a new installation to all users in your organization on all platforms (Windows, Mac, IOS and Android, including Android based IP Phones such as the DX series).
- Before making any domain or IM address changes on the presence server, Cisco Jabber is upgraded to version 10.6 or later for all users on all platforms (Windows, Mac, IOS and Android, including Android based IP Phones such as the DX series).

The available IM address schemes in the Advanced Presence Settings are:

- UserID@[Default Domain]
- Directory URI

UserID@[Default Domain]

The User ID field is mapped to an LDAP field. This is the default IM Address Scheme.

For example, user Anita Perez has an account name aperez and the User ID field is mapped to the sAMAccountName LDAP field. The address scheme used is aperez@example.com.

Directory URI

The Directory URI is mapped to the **mail** or **msRTCSIP-primaryuseraddress** LDAP fields. This option provides a scheme that is independent of the user ID for authentication.

For example, user Anita Perez has an account name aperez, the mail field is Anita.Perez@domain.com, the address scheme used is Anita.Perez@domain.com.

Service Discovery using Jabber IDs

Service discovery takes the Jabber ID entered in the format `[userid]@[domain.com]` and by default, extracts the `domain.com` portion of the Jabber ID to discover the services available. For a deployment where the presence domain is not the same as the service discovery domain, you can include the service discovery domain information during installation as follows:

- In Cisco Jabber for Windows this is done using the `SERVICES_DOMAIN` command line argument.

- In Cisco Jabber for Mac, Cisco Jabber for Android, or Cisco Jabber for iPhone and iPad the service discovery domain can be set using the `ServicesDomain` parameter used with URL configuration.

.

SIP URI

A SIP URI is associated with each user. The SIP URI can be an email address, an IMAddress, or a UPN.

The SIP URI is configured using the Directory URI field in Cisco Unified Communications Manager. These are the available options:

- mail
- msRTCSIP-primaryuseraddress

Users can search for contacts and dial contacts by entering a SIP URI.

LDAP User ID

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

User ID Planning for Federation

For federation, Cisco Jabber requires the contact ID or user ID for each user to resolve contacts during contact searches.

Set the attribute for the user ID in the SipUri parameter. The default value is `msRTCSIP-PrimaryUserAddress`. If there is a prefix to remove from your user ID you can set a value in the UriPrefix parameter, see the latest version of the *Parameters Reference Guide for Cisco Jabber*.

Proxy Addresses for User Contact Photos

Cisco Jabber accesses the photo server to retrieve contact photos. If your network configuration contains a Web Proxy, you need to ensure that Cisco Jabber can access the Photo Server.

Authentication and Authorization

Cisco Unified Communications Manager LDAP Authentication

LDAP authentication is configured on Cisco Unified Communications Manager to authenticate with the directory server.

When users sign 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.

Webex Messenger Login Authentication

Webex Messenger authentication is configured using the Webex Administration tool.

When users sign in to the client, the information is sent to the Webex Messenger and an authentication token is sent back to the client.

Single Sign-On Authentication

Single Sign on authentication is configured using an Identity Provider (IdP) and services.

When users sign in to the client, the information is sent to the IdP and once the credentials are accepted an authentication token is sent back to Cisco Jabber.

Certificate-Based Authentication for Cisco Jabber for iPhone and iPad

Cisco Jabber authenticates on the IdP server through a client certificate. This certificate authentication allows users to sign in to the servers without entering user credentials. The client uses the Safari framework to implement this feature.

Requirements

- Cisco Unified Communications Manager 11.5, IM and Presence Service 11.5, Cisco Unity Connection 11.5 and above.
- Expressway for Mobile and Remote Access server 8.9 and later.
- SSO enabled for the Unified Communications infrastructure.
- All server certificates are CA signed including Cisco Unified Communications Manager, IM and Presence Service, Cisco Unity Connection and IdP server. If the iOS device does use a trusted authority of OS, install the CA certificate before installing the Cisco Jabber app.
- Configure Native browser (embedded Safari) for SSO in Cisco Unified Communications Manager. For more information, refer to the section on certificate-based SSO authentication in *On-Premises Deployment for Cisco Jabber*.
- Configure Native browser (embedded Safari) for SSO in Expressway for Mobile and Remote Access server. For more information, see the Cisco Expressway installation guides at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.html.

You can deploy Cisco certificates on iOS devices through the EMM solution.

Recommendation—Cisco recommends using the EMM solution for deploying the certificate on iOS devices.

Certificate-Based Authentication for Cisco Jabber for Android

Cisco Jabber uses a client certificate to sign into single sign-on servers (Webex Messenger and on-premises).

Requirements

- Android OS 5.0 or later

- Single Sign-On is enabled
- Jabber client is supported over Mobile and Remote Access (MRA) and non-MRA deployment mode.
- Jabber always displays notifications for invalid certificates on Android 7.0 and later, even for installed custom CA-signed certificates on the Android OS. Apps that target Android 7.0 only trust system-provided certificates and no longer trust user-added Certificate Authorities.

Certificate Deployment

Cisco recommends using an EMM solution for deploying the certificate on an Android device.

Voicemail Authentication

Users need to exist on Cisco Unity Connection. Cisco Unity Connection supports multiple authentication types. If Cisco Unified Communications Manager and Cisco Unity Connection use the same authentication then we recommend that Cisco Jabber is configured to use the same credentials.

OAuth

You can set up Cisco Jabber to use the OAuth protocol to authorize users' access rights to services. If the user signs in to an OAuth-enabled environment, then there is no need to enter the credentials every time the user signs in. However, if the servers are not OAuth-enabled, then Jabber may not function appropriately.

If you're using Cisco Unified Communication Manager 12.5 or later, you can also enable SIP OAuth. It allows Jabber to authorize itself to SIP, which allows Jabber to connect to SIP service over TLS. It also allows Jabber to send media over a secure connection (sRTP). SIP OAuth means that CAPF enrollment is no longer necessary to enable secure SIP and media.

Prerequisites:

- OAuth Refresh tokens must be turned on across all of these components if deployed to be functional
- Cisco Unified Communication Manager, Cisco Unified Communication Manager Instant Messaging and Presence, and Cisco Unity Connection must be of version 11.5(SU3) or 12.0
- Cisco Expressway for Mobile and Remote Access version X8.10 or later
- For SIP OAuth: Cisco Unified Communication Manager 12.5 or later, Cisco Expressway for Mobile and Remote Access version X12.5 or later.

Before you configure OAuth, check the type of the deployment you have:

- If you have local authentication deployment, then IdP server is not required, and Cisco Unified Communication Manager is responsible for authentication.
- You can set up OAuth with or without SSO configured. If you're using SSO, ensure it is enabled for all services. If you have an SSO-enabled deployment, then deploy an IdP server, and IdP server is responsible for authentication.

You can enable OAuth on the following services for your users:

- Cisco Unified Communications Manager
- Cisco Expressway

- Cisco Unity Connection

By default, OAuth is disabled on these servers. To enable OAuth on these servers:

- For Cisco Unified Communications Manager and Cisco Unity Connection Servers, go to **Enterprise Parameter configuration** > **OAuth with refresh Login Flow**.
- For Cisco Expressway-C, go to **Configuration Unified Communication** > **Configuration Authorized by OAuth token with refresh**.

When OAuth is enabled or disabled on any of these servers, Jabber identifies it during configuration re-fetch interval, and lets the user sign out and sign in to Jabber.

During sign out, Jabber deletes user credentials stored in the cache, and then lets user sign in with regular sign-in flow, where Jabber fetches all the configuration information first, and then lets the user access Jabber services.

To configure OAuth on Cisco Unified Communication Manager:

1. Go to **Cisco Unified Communication Manager Admin** > **System** > **Enterprise Parameters** > **SSO Configuration**.
2. Set **O-Auth Access Token Expiry Timer(minutes)** to desired value.
3. Set **O-Auth Refresh Token Expiry Timer(days)** to desired value.
4. Click **Save** button.

To configure OAuth on Cisco Expressway:

1. Go to **Configuration** > **Unified Communications** > **Configuration** > **MRA Access Control**.
2. Set **O-Auth local authentication** to **On**.

To configure OAuth on Cisco Unity:

1. Go to **AuthZ Servers** and select **Add New**.
2. Enter the details in the all fields and select **Ignore Certificate Errors**.
3. Click **Save**.

Limitation

Jabber triggers automated intrusion protection

Conditions:

- Your Expressway for Mobile and Remote Access deployment is configured for authorization by OAuth token (with or without Refresh token).
- The Jabber user's access token is expired.

Jabber does one of these:

- Resumes from desktop hibernate
- Recovers network connection

- Attempts fast sign-in after it is signed out for several hours

Behavior:

- Some Jabber modules attempt to authorize at Expressway-E using the expired access token.
- The Expressway-E (correctly) denies these requests.
- If there are more than five such requests from a particular Jabber client, the Expressway-E blocks that IP address for ten minutes (by default).

Symptoms:

The affected Jabber clients' IP addresses are added to the blocked addresses list of Expressway-E, in the HTTP proxy authorization failure category. You can see these on **System** > **Protection** > **Automated detection** > **Blocked addresses.**.

Workaround:

There are two ways you can work around this issue; you can increase the detection threshold for that particular category, or you can create an exemption for the affected clients. We describe the threshold option here because the exemptions may be impractical in your environment.

1. Go to **System** > **Protection** > **Automated detection** > **Configuration**.
2. Click **HTTP proxy authorization failure**.
3. Change the **Trigger level** from 5 to 10. 10 must be enough to tolerate the Jabber modules that present expired tokens.
4. Save the configuration, which takes effect immediately.
5. Unblock any affected clients.

Multiple Resource Login

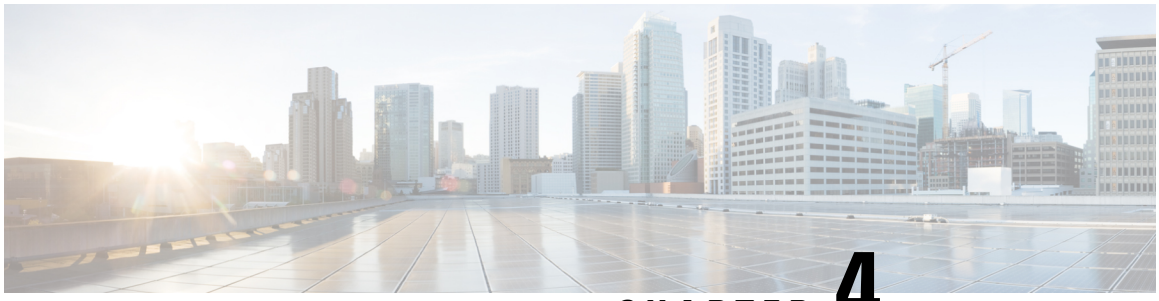
All Cisco Jabber clients register with one of the following central IM and Presence Service nodes when a user logs in to the system. This node tracks availability, contact lists, and other aspects of the IM and Presence Service environment.

- On-Premises Deployments: Cisco Unified Communications Manager IM and Presence Service.
- Cloud Deployments: Webex.

This IM and Presence Service node tracks all of the registered clients associated with each unique network user in the following order:

1. When a new IM session is initiated between two users, the first incoming message is broadcast to all of the registered clients of the receiving user.
2. The IM and Presence Service node waits for the first response from one of the registered clients.
3. The first client to respond then receives the remainder of the incoming messages until the user starts responding using another registered client.
4. The node then reroutes subsequent messages to this new client.

Note If there is no active resource when a user is logged into multiple devices, then priority is given to the client with the highest presence priority. If the presence priority is the same on all devices, then priority is given to the latest client the user logged in to.



CHAPTER 4

Service Discovery

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.

Cisco Webex Platform Service Discovery

Cisco Jabber sends an HTTPS request to Cisco Webex Platform Service to check whether the user is enabled for team messaging mode. If the user is enabled for team messaging, then Jabber continues to check for available on-premises services.

Cisco Webex Messenger Service Discovery

Cisco Jabber sends a cloud HTTP request to the CAS URL for the Webex Messenger service. Cisco Jabber authenticates users with Webex Messenger Service and connects to the available services.

The services are configured on Webex Administration Tool.

Cisco Intercluster Lookup Service

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

Expressway for Mobile and Remote Access Service Discovery

Expressway for Mobile and Remote Access enables remote users access services.

The client queries the name server for SRV records. With the `_collab-edge` SRV record the client connects to the internal network through Expressway for Mobile and Remote Access and discover services.

The name server returns the `_collab-edge` SRV record and the client gets the location of the Cisco Expressway-E server. The Cisco Expressway-E server then provides the client with the results of the query to the internal name server. This must include the `_cisco-uds` SRV record, the client then retrieves the service profiles from Cisco Unified Communication Manager

Note When your voice service domain is the same as the sign-in domain, don't configure voiceservicesdomain for MRA. Only configure voiceservicesdomain when the domains are different.

Recommended Connection Methods

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

Table 3: On-Premises Deployments for Cisco Jabber for Windows

Product Mode	Server Versions	Discovery Method	Non DNS SRV Record Method
Full UC (default mode)	Release 9.1.2 and later: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds .<domain>`	Use the following installer switches and values: • `AUTHENTICATOR=CUP` • `CUP_ADDRESS=` `<presence_server_address>`

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

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

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

Use the SERVICES_DOMAIN installer switch to specify the value of the domain where DNS records reside if you want users to bypass the email screen during the first login of a fresh installation.

Table 4: On-Premises Deployments for Cisco Jabber for Mac

Product Mode	Server Versions	Discovery Method
Full UC (default mode)	Release 9 and later: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds.<domain>`

Table 5: On-Premises Deployments for Cisco Jabber for Android and Cisco Jabber for iPhone and iPad

Product Mode	Server Versions	Discovery Method
Full UC (default mode)	Release 9 and later: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds .<domain>` and `_cuplogin.<domain>`
IM Only (default mode)	Release 9 and later: Cisco Unified Communications Manager IM and Presence Service	A DNS SRV request against `_cisco-uds .<domain>` and `_cuplogin.<domain>`
Phone mode	Release 9 and later: Cisco Unified Communications Manager	A DNS SRV request against `_cisco-uds.<domain>`

Note Cisco Unified Communications Manager version 9 and later can still discover full Unified Communications and IM-only services using the `_cuplogin` DNS SRV request but a `_cisco-uds` request will take precedence if it is present.

Table 6: Hybrid Cloud-Based Deployments

Server Versions	Connection Method
Webex Messenger	HTTPS request against `https://loginp.webexconnect.com/cas/FederatedSSO?org=<domain>`
Cisco Webex Platform service	HTTPS request against `atlas-a.wbx2.com`

Table 7: Cloud-Based Deployments

Deployment Type	Connection Method
Enabled for single sign-on (SSO)	Webex Administration Tool Bootstrap file to set the SSO_ORG_DOMAIN argument.
Not enabled for SSO	Webex Administration Tool

Sources of Authentication

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

Three possible sources of authentication are as follows:

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

How the Client Locates Services

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

1. The client's host computer or device gets a network connection.

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

2. 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.
   - Mobile Configuration Using Enterprise Mobility Management—As an alternative to URL configuration, you can configure Cisco Jabber using Enterprise Mobility Management (EMM) with Android for Work on Cisco Jabber for Android and with Apple Managed App Configuration on Cisco Jabber for iPhone and iPad. You need to configure the same parameters in the EMM console that are used for creating URL configuration link.

   To create a URL configuration link, you include the following:
   - ServicesDomain—The domain that Cisco Jabber uses for service discovery.
   - VoiceServicesDomain—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 the Cisco Jabber 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

Note When all three parameters are included, service discovery does not happen and the user is 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 &ServiceDiscoveryExcludedServices=WEBEX,CUCM`

Provide the link to users using email or a website.

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 website.

3. The client gets the address of the DNS name server from the DHCP settings.
4. The client issues an HTTP query to a Central Authentication Service (CAS) URL for the Webex Messenger service.

   This query enables the client to determine if the domain is a valid Webex domain.
5. The client queries the name server for the following SRV records in order of priority:
   - `_cisco-uds`
   - `_collab-edge`

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

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

The following is an example of an SRV record entry:

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

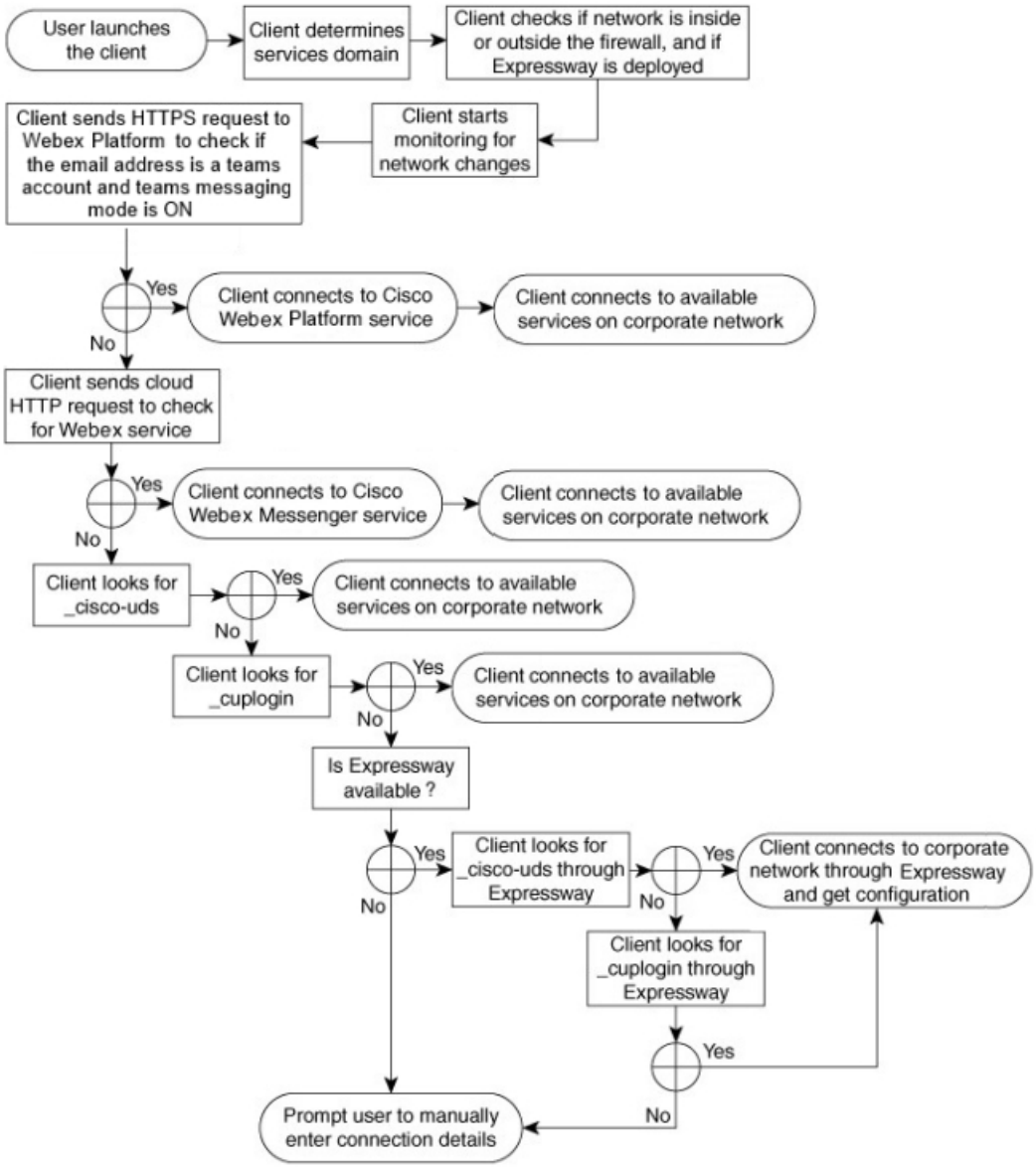
Method 1: Search For Services

We recommend that you use this method for how Cisco Jabber detects what services and features are available to users. Searching for services means that the client uses DNS service (SRV) records to determine which services are available to the client.

How the Client Discovers Available Services

The following figure shows the flow that the client uses to connect to services.

Figure 5: Login Flow for Service Discovery



To discover available services, the client does the following:

1. Checks if the network is inside or outside the firewall and if Expressway for Mobile and Remote Access is deployed. The client sends a query to the name server to get DNS Service (SRV) records.
2. Starts monitoring for network changes.

   When Expressway for Mobile and Remote Access is deployed, the client monitors the network to ensure that it can reconnect if the network changes from inside or outside the firewall.
3. Issues several HTTPS requests to Cisco Webex Platform Service to determine whether Jabber goes into team messaging mode. The request checks the user's email address to see whether the user has been enabled for team messaging in the Webex Control Hub.
4. Issues an HTTP query to a CAS URL for the Webex Messenger service.

   This query enables the client to determine if the domain is a valid Webex domain.

   When Expressway for Mobile and Remote Access is deployed, the client connects to Webex Messenger Service and uses Expressway for Mobile and Remote Access to connect to Cisco Unified Communications Manager. When the client launches for the first time the user will see a Phone Services Connection Error and will have to enter their credentials in the client options screen, subsequent launches will use the cached information.
5. Queries the name server to get DNS Service (SRV) records, unless the records exist in the cache from a previous query.

   This query enables the client to do the following:

   - Determine which services are available.
   - Determine if it can connect to the corporate network through Expressway for Mobile and Remote Access.

Client Issues an HTTP Query for Cisco Webex Messenger Service

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

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

```
https://loginp.webexconnect.com/cas/FederatedSSO?org=
```

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

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

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

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

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

When the client sends the HTTP request to the CAS URL, it uses configured system proxies.

For more information, see the *Configure Proxy Settings* section in the *Cisco Jabber Deployment and Installation Guide*.

Client Queries the Name Server

When the client queries a name server, it sends separate, simultaneous requests to the name server for SRV records.

The client requests the following SRV records in the following order:

- `_cisco-uds`
- `_collab-edge`

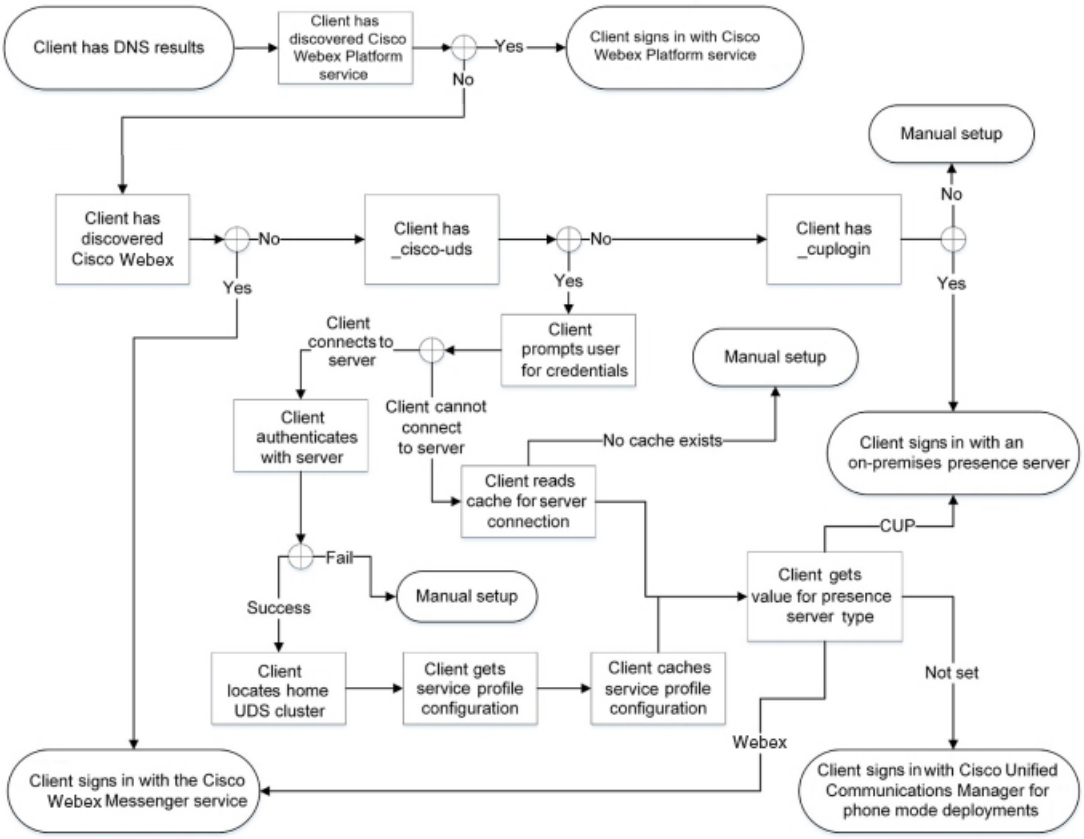
If the name server returns:

- `_cisco-uds`—The client detects it is inside the corporate network and connects to Cisco Unified Communications Manager.
- `_collab-edge`—The client attempts to connect to the internal network through Expressway for Mobile and Remote Access and discover services
- None of the SRV records—The client prompts users to manually enter setup and sign-in details.

Client Connects to Internal Services

The following figure shows how the client connects to internal services:

Figure 6: Client Connecting to Internal Services



When connecting to internal services, the goals are to determine the authenticator, sign users in, and connect to available services.

From the sign-in screen, users authenticate with one of these services:

- Cisco Webex Platform service—Cloud or hybrid deployments.
- Webex Messenger service—Cloud or hybrid deployments.
- Cisco Unified Communications Manager—On-premises deployments in phone mode.

The client connects to any services it discovers, which varies depending on the deployment.

1. If the client discovers that the user is enabled for team messaging mode, then the client does the following:
   a. Determines that Cisco Webex Platform service is the primary source of authentication.
   b. Automatically connects to Cisco Webex Platform Service.
   c. Prompts the user for credentials.
2. If the client discovers that the CAS URL lookup indicates a Webex user, the client does the following:
   a. Determines that the Webex Messenger service is the primary source of authentication.
   b. Automatically connects to the Webex Messenger service.

c. Prompts the user for credentials.

d. Retrieves client and service configuration.

3. If the client discovers a `_cisco-uds` SRV record, the client does the following:

Prompts the user for credentials to authenticate with Cisco Unified Communications Manager.

a. Locates the user's home cluster.

Locating the home cluster enables the client to automatically get the user's device list and register with Cisco Unified Communications Manager.

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

Important See the appropriate version of the *Cisco Unified Communications Manager Features and Services Guide* to learn how to configure ILS.

b. Retrieves the service profile.

The service profile provides the client with the authenticator as well as client and UC service configuration.

The client determines the authenticator from the value of the Product type field in the IM and presence profile, as follows:

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

As a result of the HTTP query, the client connects to the Webex Messenger service in cloud-based deployments. Setting the value of the **Product type** field to Webex does not effect if the client has already discovered the Webex service using 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.

c. Sign in to the authenticator.

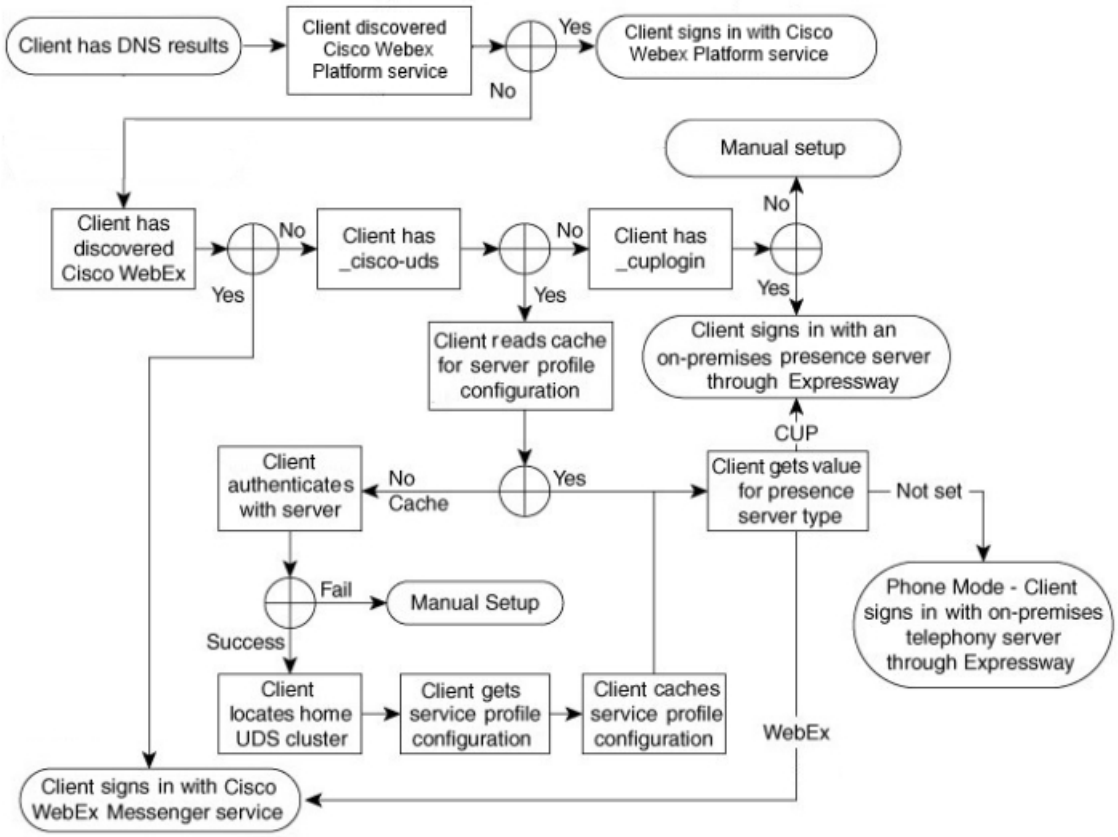
After the client signs in, it can determine the product mode.

Client Connects through Expressway for Mobile and Remote Access

If the name server returns the `_collab-edge` SRV record, the client attempts to connect to internal servers through Expressway for Mobile and Remote Access.

The following figure shows how the client connects to internal services when the client is connected to the network through Expressway for Mobile and Remote Access:

Figure 7: Client Connects through Expressway for Mobile and Remote Access



When the name server returns the `_collab-edge` SRV record, the client gets the location of the Cisco Expressway-E server. The Cisco Expressway-E server then provides the client with the results of the query to the internal name server.

Note The Cisco Expressway-C server looks up the internal SRV records and provides the records to the Cisco Expressway-E server.

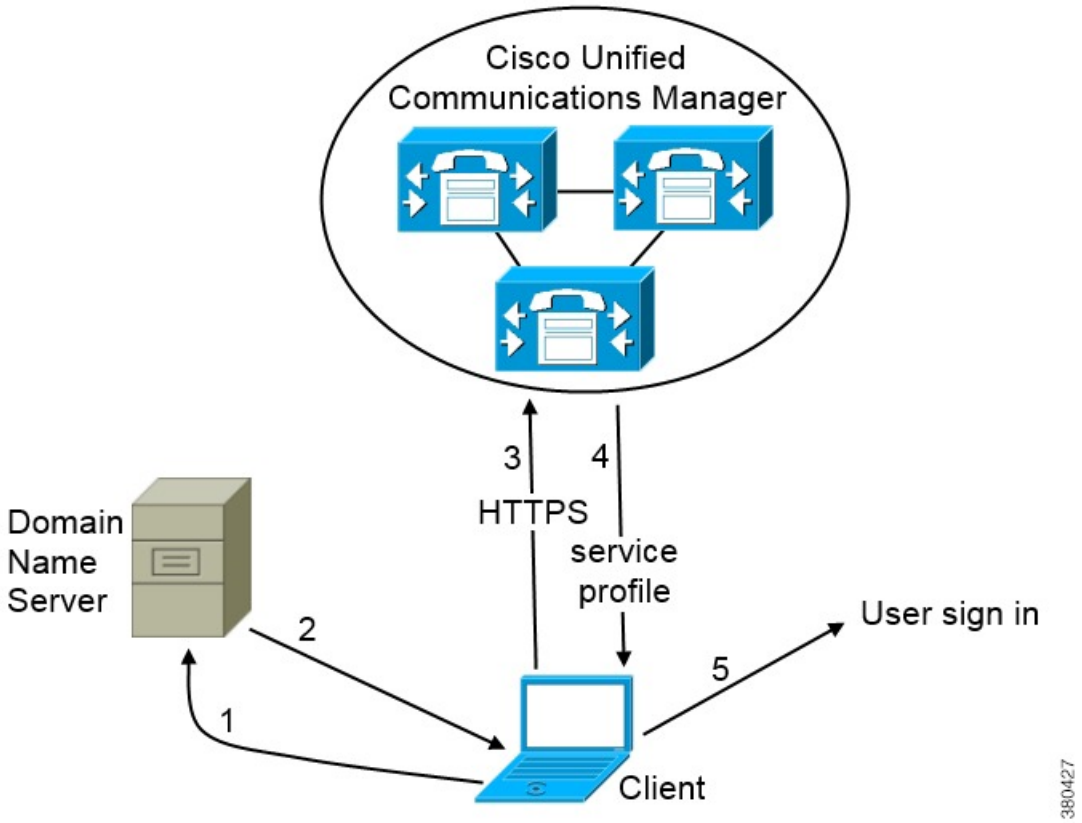
After the client gets the internal SRV records, which must include the `_cisco-uds`SRV record, it retrieves service profiles from Cisco Unified Communications Manager. The service profiles then provide the client with the user's home cluster, the primary source of authentication, and configuration.

Cisco UDS SRV Record

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

The following figure shows how the client uses the `_cisco-uds` SRV record.

Figure 8: UDS SRV Record Login Flow



1. The client queries the domain name server for SRV records.
2. The domain name server returns the `_cisco-uds` SRV record.
3. The client locates the user's home cluster.

   As a result, the client can retrieve the device configuration for the user and automatically register telephony services.

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

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

4. The client retrieves the user's service profile.

   The user's service profile contains the addresses and settings for UC services and client configuration.

   The client also determines the authenticator from the service profile.

5. The client signs the user in to the authenticator.

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

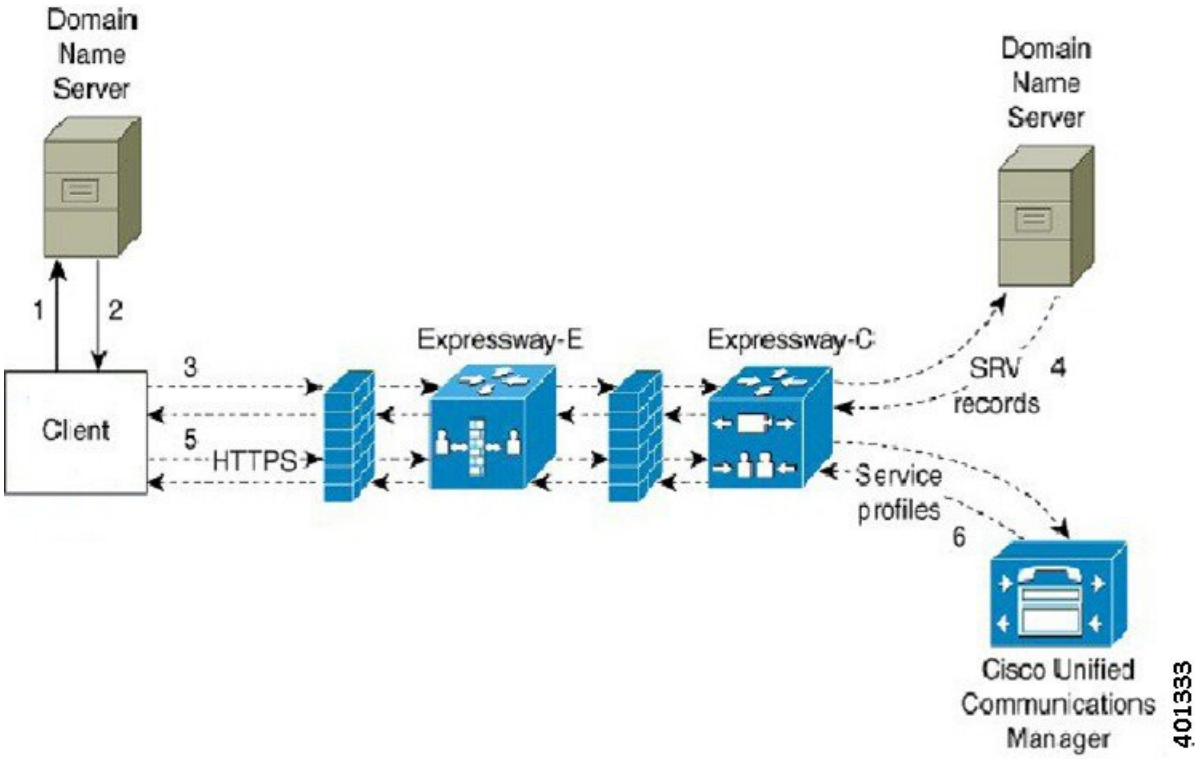
```
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 6
          weight         = 30
          port           = 8443
          svr hostname   = cucm3.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 2
          weight         = 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
```

Collaboration Edge SRV Record

Cisco Jabber can attempt to connect to internal servers through Expressway for Mobile and Remote Access to discover services with the following `_collab-edge` SRV record.

The following figure shows how the client uses the `_collab-edge` SRV record.

Figure 9: Collaboration Edge Record Login Flow



1. The client queries the external domain name server for SRV records.
2. The name server returns the `_collab-edge` SRV record and does not return the `_cuplogin` or `_cisco-uds` SRV records.

   As a result, Cisco Jabber can locate the Cisco Expressway-E server.
3. The client requests the internal SRV records (through Expressway) from the internal domain name server.

   These SRV records must include the `_cisco-uds` SRV record.
4. The client obtains the internal SRV records (through Expressway).

   As a result, the client can locate the Cisco Unified Communications Manager server.
5. The client requests the service profiles (through Expressway) from Cisco Unified Communications Manager.
6. The client retrieves the service profiles (through Expressway) from Cisco Unified Communications Manager.

   The service profile contains the user's home cluster, the primary source of authentication, and the client configuration.

DNS Configuration

How the Client Uses DNS

Cisco Jabber uses domain name servers to do the following:

- Determine whether the client is inside or outside the corporate network.
- Automatically discover on-premises servers inside the corporate network.
- Locate access points for Expressway for Mobile and Remote Access on the public Internet.

Note Android OS limitation: Android OS 4.4.2 and 5.0 using the DNS service can resolve only the domain name, but not the hostname.

For more information, see the Android developer link.

How the Client Finds a Name Server

Cisco Jabberlooks for DNS records from:

- Internal name servers inside the corporate network.
- External name servers on the public Internet.

When the client's host computer or device gets a network connection, the host computer or device also gets the address of a DNS name server from the DHCP settings. Depending on the network connection, that name server might be internal or external to the corporate network.

Cisco Jabber queries the name server that the host computer or device gets from the DHCP settings.

How the Client Gets a Services Domain

The services domain is discovered by the client in different ways.

New installation:

- User enters an address in the format `username@example.com` in the client user interface.
- User clicks on a configuration URL that includes the service domain. This option is only available in the following versions of the client:
  - Cisco Jabber for Android release 9.6 or later
  - Cisco Jabber for Mac release 9.6 or later
  - Cisco Jabber for iPhone and iPad release 9.6.1 or later
- The client uses installation switches in bootstrap files. This option is only available in the following version of the client:
  - Cisco Jabber for Windows release 9.6 or later

Existing installation:

- The client uses the cached configuration.
- User manually enters an address in the client user interface.

In hybrid deployments the domain required to discover Webex domain through Central Authentication Service (CAS) lookup may be different to the domain where the DNS records are deployed. In this scenario you set the ServicesDomain to be the domain used to discover Webex and set the VoiceServicesDomain to be the domain where DNS records are deployed. The voice services domain is configured as follows:

- The client uses the VoiceServicesDomain parameter in the configuration file. This option is available in clients that support the `jabber-config.xml` file.
- User clicks on a configuration URL that includes the VoiceServicesDomain. This option is available in the following clients:
  - Cisco Jabber for Android release 9.6 or later
  - Cisco Jabber for Mac release 9.6 or later
  - Cisco Jabber for iPhone and iPad release 9.6.1 or later
- The client uses the Voice_Services_Domain installation switch in the bootstrap files. This option is only available in the following version of the client:
  - Cisco Jabber for Windows release 9.6 or later

After Cisco Jabber gets the services domain, it queries the name server that is configured to the client computer or device.

Domain Name System Designs

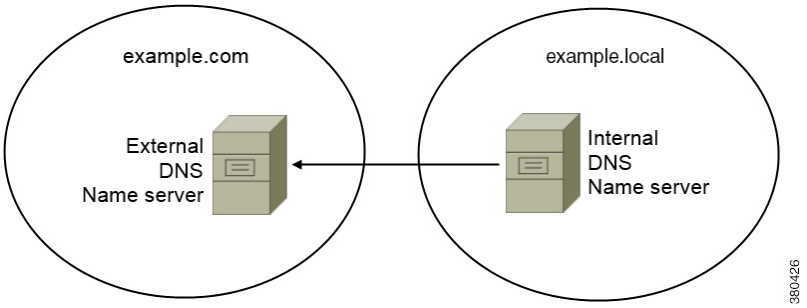
Where you deploy DNS service (SRV) records depends on the design of your DNS namespace. Typically there are two DNS designs:

- Separate domain names outside and inside the corporate network.
- Same domain name outside and inside the corporate network.

Separate Domain Design

The following figure shows a separate domain design:

Figure 10: Separate Domain Design



An example of a separate domain design is one where your organization registers the following external domain with an Internet name authority: `example.com`.

Your company also uses an internal domain that is one of the following:

- A subdomain of the external domain, for example, `example.local`.
- A different domain to the external domain, for example, `exampledomain.com`.

Separate domain designs have the following characteristics:

- The internal name server has zones that contain resource records for internal domains. The internal name server is authoritative for the internal domains.
- The internal name server forwards requests to the external name server when a DNS client queries for external domains.
- The external name server has a zone that contains resource records for your organization's external domain. The external name server is authoritative for that domain.
- The external name server can forward requests to other external name servers. However, the external name server cannot forward requests to the internal name server.

Deploy SRV Records in a Separate Domain Structure

In a separate name design there are two domains, an internal domain and an external domain. The client queries for SRV records in the services domain. The internal name server must serve records for the services domain. However in a separate name design, a zone for the services domain might not exist on the internal name server.

If the services domain is not currently served by the internal name server, you can:

- Deploy records within an internal zone for the services domain.
- Deploy records within a pinpoint subdomain zone on the internal name server.

Use an Internal Zone for a Services Domain

If you do not already have a zone for the services domain on the internal name server, you can create one. This method makes the internal name server authoritative for the services domain. Because it is authoritative, the internal name server does not forward queries to any other name server.

This method changes the forwarding relationship for the entire domain and has the potential to disrupt your internal DNS structure. If you cannot create an internal zone for the services domain, you can create a pinpoint subdomain zone on the internal name server.

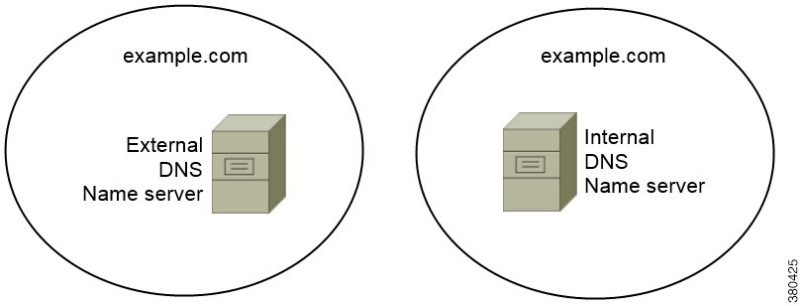
Same Domain Design

An example of a same domain design is one where your organization registers `example.com` as an external domain with an Internet name authority. Your organization also uses `example.com` as the name of the internal domain.

Single Domain, Split-Brain

The following figure shows a single domain with a split-brain domain design.

Figure 11: Single Domain, Split-Brain



Two DNS zones represent the single domain; one DNS zone in the internal name server and one DNS zone in the external name server.

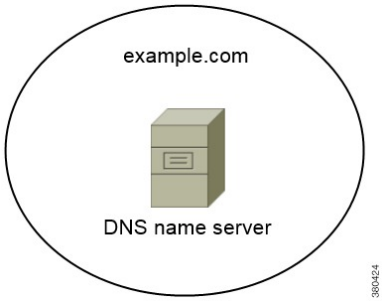
Both the internal name server and the external name server are authoritative for the single domain but serve different communities of hosts.

- Hosts inside the corporate network access only the internal name server.
- Hosts on the public Internet access only the external name server.
- Hosts that move between the corporate network and the public Internet access different name servers at different times.

Single Domain, Not Split-Brain

The following figure shows a single domain that does not have a split-brain domain design.

Figure 12: Single Domain, Not Split-Brain



In the single domain, not split-brain design, internal and external hosts are served by one set of name servers and can access the same DNS information.

Important This design is not common because it exposes more information about the internal network to potential attackers.

Method 2: Customization

You can customize service discovery by using installation parameters, URL configuration, or Enterprise Mobility Management.

Service Discovery Customization

Custom Installations for Cisco Jabber for Windows

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

- Use the Command Line—You can specify arguments in a command line window to set installation properties.

  Choose this option if you plan to install multiple instances.

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

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

- Create a Custom Installer—Open the default installation package, specify the required installation properties, and then save a custom installation package.

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

- Deploy with Group Policy—Install the client on multiple computers in the same domain.

Installer Switches

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

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

We recommend that you do not use a bootstrap file, and instead use service discovery for your Calling in Webex App (Unified CM) deployment.

Custom Installations for Cisco Jabber for Mac, iPhone and iPad, and Android

You can create customized installations of Cisco Jabber for Mac or mobile clients by using URL Configuration. For mobile clients you can also use Enterprise Mobility Management. These custom installations depend on installation parameters that enable services.

URL Configuration

To enable users launch Cisco Jabber without having to manually enter service discovery information, provide a configuration URL link to users to install the client.

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

Mobile Configuration Using Enterprise Mobility Management

You can configure Cisco Jabber using Enterprise Mobility Management (EMM) on Cisco Jabber for Android and Cisco Jabber for iPhone and iPad. For more information on setting up EMM, refer to the instructions for administrators provided by the EMM provider.

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

For more information about how to deploy EMM, see the section on *Deploy Cisco Jabber Applications* in the *On-Premises Deployment for Cisco Jabber* or in the *Cloud and Hybrid Deployments for Cisco Jabber*.

Method 3: Manual Installations

As an advanced option, users can manually connect to services at the sign in screen.

High Availability

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.

High availability is supported for LDAP. High availability is not supported when using UDS contact source.

Cisco Jabber supports high availability with the following servers:

Cisco Unified Communications Manager IM and Presence Service release 9.0 and higher

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

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

`High Availability Client Login Profiles`

`Troubleshooting High Availability`

Active Calls on Hold During Failover

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

High Availability in the Client

Client Behavior During Failover

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

Configure Login Parameters

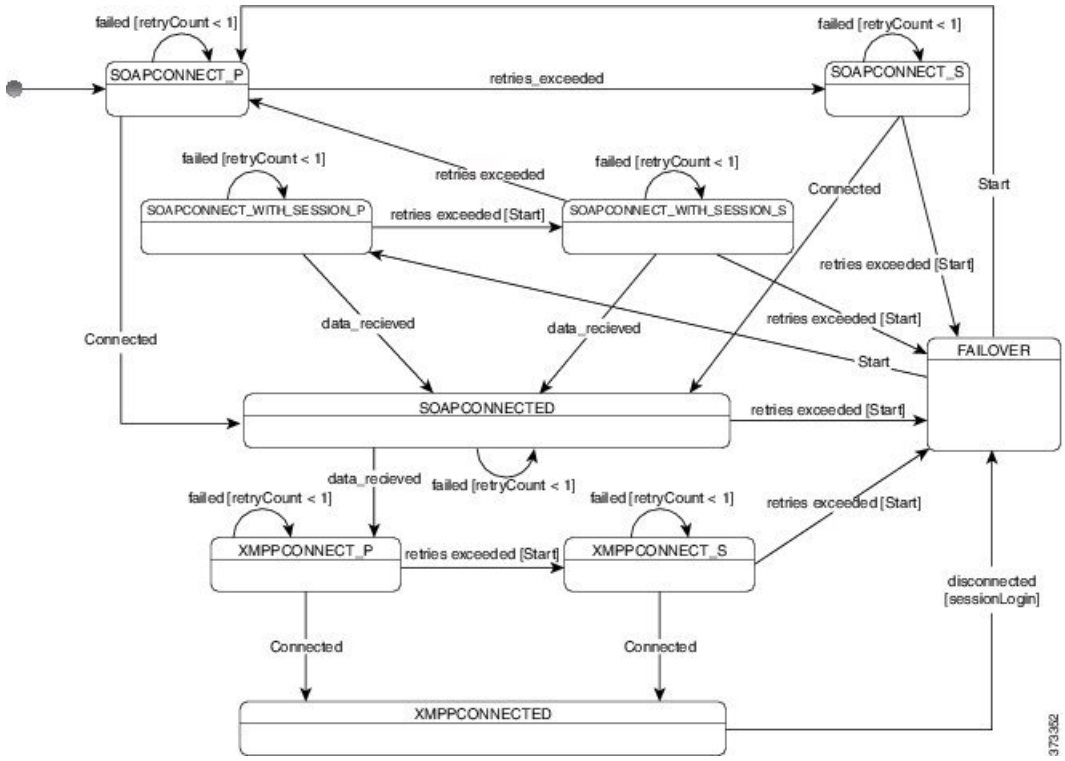
In Cisco Unified Communications Manager IM and Presence Service, you can configure the maximum and minimum number of seconds that Cisco Jabber waits before attempting to re-login to the server. On the server, you specify the re-login parameters in the following fields:

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

Client Behavior During a Failover

The following figure shows the client's behavior when the Cisco Unified Communications Manager IM and Presence service during a failover.

Figure 13: Client Behavior During a Failover



1. When the client is disconnected from its active server, the client goes from XMPPCONNECTED state to a FAILOVER state.
2. From a FAILOVER state, the client tries to attain a SOAPCONNECTED state by attempting SOAPCONNECT_SESSION_P (as the primary server), and if that fails, attempts SOAPCONNECT_SESSION_S (as the secondary server).
   - If it is unable to attain SOAPCONNECT_SESSION_P or SOAPCONNECT_SESSION_S, the client re-enters into the FAILOVER state.
   - From a FAILOVER state, the clients attempts to attain a SOAPCONNECT_P state, and if that fails, attempts to reach a SOAPCONNECT_S state.

- If the client cannot reach the SOAPCONNECT_P or SOAPCONNECT_S state, then the client does not attempt any more automatic connections to the IM&P server until a user initiates a login attempt.

3. From a SOAPCONNECT_SESSION_P, SOAPCONNECT_SESSION_S, SOAPCONNECT_P, or SOAPCONNECT_S state, the client retrieves its current primary secondary XMPP server address. This address changes during a failover.
4. From a SOAPCONNECTED state, the client tries to attain an XMPPCONNECTED state by attempting to connect to the XMPPCONNECT_P state, and if that fails, attempts XMPPCONNECT_S state.
   - If client cannot reach XMPPCONNECT_P or XMPPCONNECT_S state, then the client does not attempt any more automatic connections to the IM&P server until a user initiates a login attempt.
5. After the client is in an XMPPCONNECTED state, then the client has IM&P capability.

High Availability for Voice and Video

If one node in a subcluster becomes unavailable, voice and video failover to another node in the subcluster.

By default, it takes up to 120 seconds for a software phone device or desk phone to register with another node. If this timeout period is too long, adjust the value of the SIP Station KeepAlive Interval service parameter for your node. The SIP Station KeepAlive Interval service parameter modifies all phone devices on Cisco Unified Communications Manager. Before you adjust the interval, analyze the impact on the Cisco Unified Communications Manager servers.

To configure service parameters for the node, in Cisco Unified Communications Manager Administration, select **System** > **Service Parameters**.

For a phone mode deployment using the non-DNS SRV record method, failover isn't possible for Voice and Video, as there is only one Cisco Unified Communications Manager node specified.

High Availability for Persistent Chat

There is high availability support for persistent chat. During the failover window, users may be prompted that they can't send messages. When the node has failed over, users automatically rejoin the chat room and can send messages again.

High Availability for Contact Search and Contact Resolution

High availability is supported for contact search and contact resolution, which are provided by the Cisco Unified Communications Manager User Data Service (UDS). If the primary UDS server is unavailable, Jabber automatically fails over to a second UDS server, or to a third UDS server, if configured.

High Availability for Voicemail

If a secondary voicemail server is configured, then all clients automatically failover to the secondary voicemail server if the primary server becomes unavailable or unreachable.

Survivable Remote Site Telephony

Applies to Cisco Jabber for Windows and Cisco Jabber for Mac

When the Cisco Unified Communications Manager application is unreachable or the WAN is down, use Cisco Unified Survivable Remote Site Telephony (SRST) to retain basic telephony services for your remote users. When connectivity is lost, the client fails over to the local router at the remote site.

Note SRST versions 12.8 and later are supported.

SRST provides basic call control, when a system is in failover only start, end, hold, resume, mute, unmute, and dual-tone multifrequency signaling [DTMF]) are enabled.

The following services are not available during failover:

- Video
- Mid-call features (transfer, iDivert, call park, conferencing, send to mobile)
- Dial via Office (DvO)
- Ad hoc conferencing
- Binary Floor Control Protocol (BFCP) sharing

For detailed instructions about configuring SRST, see the relevant release of the *Cisco Unified Communication Manager Administration Guide.*

Configuration Priorities

When both a service profile and a configuration file are present, the following table describes which parameter value takes precedence.

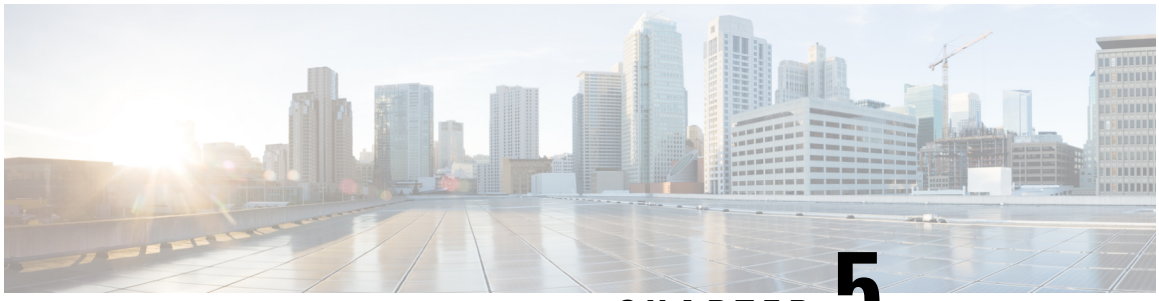
Service Profile	Configuration File	Which Parameter Value Takes Precedence?
Parameter value is set	Parameter value is set	Service profile
Parameter value is set	Parameter value is blank	Service profile
Parameter value is blank	Parameter value is set	Configuration file
Parameter value is blank	Parameter value is blank	Service profile blank (default) value

Group Configurations Using Cisco Support Field

Group configuration files apply to a subset of users. If you provision users with CSF devices, you can specify the group configuration file names in the **Cisco Support Field** field on the device configuration. If users do

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

Group configuration is supported on TCT and BOT with COP file later than 14122 version.



CHAPTER 5

Contact Source

What is a Contact Source?

A contact source is a collection of data for users. When users search for contacts or add contacts in the Cisco Jabber client, the contact information is read from a contact source.

Cisco Jabber retrieves the information from the contact source to populate contact lists, update contact cards in the client and other areas that display contact information. When the client receives any incoming communications, for example an instant message or a voice/video call, the contact source is used to resolve the contact information.

Contact Source Servers

Note All Jabber clients support the LDAPv3 standard for directory integration. Any directory server that supports this standard is compatible with these clients.

You can use the following contact source servers with Cisco Jabber:

- Active Directory Domain Services for Windows Server 2012 R2

- Active Directory Domain Services for Windows Server 2008 R2
- Cisco Unified Communications Manager User Data Server (UDS). Cisco Jabber supports UDS using Cisco Unified Communications Manager version 10.5 or higher.
- OpenLDAP
- Active Directory Lightweight Directory Service (AD LDS) or Active Directory Application Mode (ADAM)

Why Do I Need a Contact Source?

Cisco Jabber uses the contact source in the following ways:

- Users search for a contact—The client takes the information entered and searches in the contact source. Information is retrieved from the contact source and the client will display the available methods to interact with the contact.
- Client receives incoming notification—The client will take the information from the incoming notification and resolve the URI, number, JabberID with a contact from the contact source. The client will display the contact details in the alert.

When to Configure Contact Source Servers

Note Install Cisco Jabber on a workstation that is registered to an Active Directory domain. In this environment, you do not need to configure Cisco Jabber to connect to the directory. The client automatically discovers the directory and connects to a Global Catalog server in that domain.

Configure Cisco Jabber to connect to a directory service if you plan to use one of the following services as the contact source:

- Active Directory Service
- Cisco Unified Communications Manager User Data Service
- OpenLDAP
- Active Directory Lightweight Directory Service
- Active Directory Application Mode

You can optionally configure directory integration to:

- Change the default attribute mappings.
- Adjust directory query settings.
- Specify how the client retrieves contact photos.
- Perform intradomain federation.

Contact Source Options for Cisco Directory Integration

In on-premises deployments, the client requires one of the following contact sources to resolve directory look ups for user information:

- Lightweight Directory Access Protocol (LDAP)—If you have a corporate directory, you can use the following LDAP-based contact source options to configure your directory as the contact source:
  - Cisco Directory Integration (CDI)—Use this contact source option to deploy all clients.
- Cisco Unified Communications Manager User Data Service (UDS)—If you do not have a corporate directory or if your deployment includes users connecting with Expressway Mobile and Remote Access, you can use this option.

Lightweight Directory Access Protocol

How Cisco Directory Integration Works with LDAP

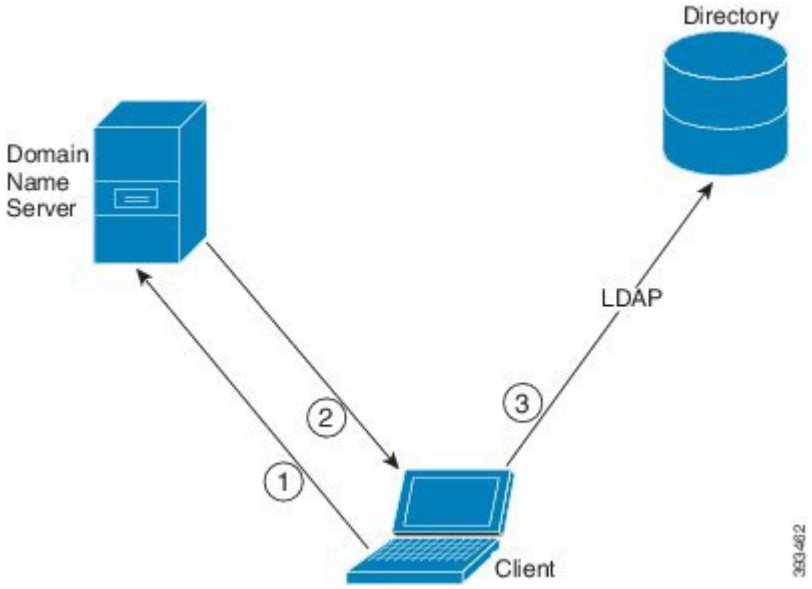
CDI uses service discovery to determine the LDAP server.

The following are the default settings for on-premises deployments with CDI:

- Cisco Jabber integrates with Active Directory as the contact source.
- Cisco Jabber automatically discovers and connects to a Global Catalog.

Automatic Service Discovery—Recommended

We recommend that you use service discovery to automatically connect and authenticate with the Global Catalog (GC) server or the LDAP server. If you want to customize your deployment, review the options for providing the LDAP server information and the authentication options that are available. Jabber first sends DNS queries to the GC domain to discover the GC servers. If it doesn't discover the GC servers, Jabber then send DNS queries to the LDAP domain to discover the LDAP servers.



When there is a GC available, the client does the following:

1. Gets the DNS domain from the workstation and looks up the SRV record for the GC.
2. Retrieves the address of the GC from the SRV record.
3. Connects to the GC with the signed-in user's credentials.

Discovery Using the Global Catalog Domain

Jabber attempts to discover GC servers with a DNS SRV query. First, Jabber gets the GC domain:

1. If available, Jabber uses the DNSFORESTNAME environment variable as the GC domain.
2. If DNSFORESTNAME is not available, Jabber checks the following for the GC domain:
   - On Windows, Jabber calls the Windows `DsGetDcName` API to get `DnsForestName`.
   - On non-Windows platforms, Jabber reads LdapDNSForestDomain from `jabber-config.xml`.

After Jabber gets the GC domain, it sends a DNS SRV query to get the GC server address:

- On Windows, Jabber checks if `SiteName` is available through Windows `DsGetSiteName` API:
  - If `SiteName` exists, Jabber sends out the DNS SRV query, `_gc._tcp.SiteName._sites.GCDomain`, to get the GC server address.
  - If `SiteName` doesn't exist or no SRV record is returned for `_gc._tcp.SiteName._sites.GCDomain`, Jabber sends out the DNS SRV query, `_gc._tcp.GCDomain`, to get the GC server address.
- On a non-Windows platform, Jabber sends out the DNS SRV query, `_gc._tcp.GCDomain`, to get the GC server address.

Discovery Using the LDAP Domain

If Jabber cannot discover a GC server, it then attempts to discover the LDAP domain:

1. If available, Jabber uses the USERDNSDOMAIN environment variable as the LDAP domain.
2. If USERDNSDOMAIN is not available, Jabber reads LdapUserDomain from `jabber-config.xml`.
3. If LdapUserDomain is not available, Jabber uses the email domain with which the user signed in as the LDAP domain.

After Jabber gets the LDAP Domain, it sends a DNS SRV query to get the LDAP server address:

- On Windows, Jabber checks if `SiteName` is available through Windows `DsGetSiteName` API.
  - If `SiteName` exists, Jabber sends out the DNS SRV query, `_ldap._tcp.SiteName.sites.LdapDomain`, to get the LDAP server address.
  - If `SiteName` doesn't exist or no SRV record is returned for `_ldap._tcp.SiteName.sites.LdapDomain`, Jabber sends out the DNS SRV query, `_ldap._tcp.LdapDomain`, to get the LDAP server address.
- On a non-Windows platform, Jabber sends out the DNS SRV query, `_ldap._tcp.LdapDomain`, to get the LDAP server address.

Once Jabber connects to the LDAP server, it reads the LDAP server's `SupportedSaslMechanisms` attribute that specifies a list and order of authentication mechanisms to use.

Manual Configuration for the LDAP Service

Manual Configuration for the LDAP Service

1. You can configure the PrimaryServerName parameter to define a specific LDAP server for Jabber to connect to.
2. You can configure the LdapSupportedMechanisms parameter in the `jabber-config.xml` file to override the list from the supportedSaslMechanisms attribute.

   The Contact Service and the LDAP server must support each of these mechanisms. Use a space to separate multiple values.

   - GSSAPI – Kerberos v5
   - EXTERNAL – SASL external
   - PLAIN (default) – Simple LDAP bind, anonymous is a subset of simple bind.

   Example:

   ```
   <LdapSupportedMechanisms>GSSAPI EXTERNAL PLAIN</LdapSupportedMechanisms>
   ```

3. If necessary, configure the LdapUserDomain parameter to set the domain that Jabber uses to authenticate with the LDAP server. For example:

   ```
   CUCMUsername@LdapUserDomain
   ```

LDAP Considerations

Cisco Directory Integration (CDI) parameters replace the Basic Directory Integration (BDI) and Enhanced Directory Integration (EDI) parameters. CDI parameters apply to all clients.

Cisco Jabber Deployment Scenarios

Scenario 1: If you are new to Jabber in 11.8

We recommend that you use service discovery to automatically connect and authenticate with the LDAP server. If you want to customize your deployment, review the options for providing the LDAP server information and the authentication options that are available.

Scenario 2: If you are upgrading to 11.8 from an EDI configuration

If your configuration only uses EDI parameters, then Jabber will read the EDI parameters and use those for your directory source integration. We still recommend that you upgrade your EDI parameters and replace them with the equivalent CDI parameters.

Scenario 3: If you are upgrading to 11.8 from a BDI configuration

If your configuration only uses BDI parameters, you must update the BDI parameters to the equivalent CDI parameters. For example, for the BDIPrimaryServerName you need to replace the parameter with PrimaryServerName. The BDIEnableTLS is replaced with the UseSSL parameter.

Scenario 4: If you are upgrading to 11.8 from a mixed EDI/BDI configuration

If your configuration uses both EDI and BDI, you must review your configuration for BDI as Jabber will use the EDI parameters when connecting to the LDAP server.

Directory Parameters

The following table lists the BDI and EDI parameters, indicating the CDI parameter name or if it doesn't apply to Jabber 11.8 or later.

BDI Parameters	EDI Parameters	CDI Parameters
-	DirectoryServerType	DirectoryServerType
-	ConnectionType	-
BDILDAPServerType	-	-
BDIPresenceDomain	PresenceDomain	PresenceDomain
BDIPrimaryServerName	PrimaryServerName	PrimaryServerName
-	SecondaryServerName	SecondaryServerName
BDIServerPort1	ServerPort1	ServerPort1
-	ServerPort2	ServerPort2
-	UseWindowCredentials	-
BDIUseJabberCredentials	-	-
BDIConnectionUsername	ConnectionUsername	ConnectionUsername

BDI Parameters	EDI Parameters	CDI Parameters
BDIConnectionPassword	ConnectionPassword	ConnectionPassword
BDIEnableTLS	UseSSL	UseSSL
-	UseSecureConnection	-
BDIUseANR	UseANR	UseANR
BDIBaseFilter	BaseFilter	BaseFilter
BDIGroupBaseFilter	GroupBaseFilter	GroupBaseFilter
BDIUseANR	-	-
BDIPredictiveSearchFilter	PredictiveSearchFilter	PredictiveSearchFilter
-	DisableSecondaryNumberLookups	DisableSecondaryNumberLookups
-	SearchTimeout	SearchTimeout
-	UseWildcards	UseWildcards
-	MinimumCharacterQuery	MinimumCharacterQuery
BDISearchBase1	SearchBase1, SearchBase2, SearchBase3, SearchBase4, SearchBase5	SearchBase1, SearchBase2, SearchBase3, SearchBase4, SearchBase5
BDIGroupSearchBase1	GroupSearchBase1, GroupSearchBase2, GroupSearchBase3, GroupSearchBase4, GroupSearchBase5	GroupSearchBase1, GroupSearchBase2, GroupSearchBase3, GroupSearchBase4, GroupSearchBase5
BDIUseSipUriToResolveContacts	UseSipUriToResolveContacts	UseSipUriToResolveContacts
BDIUriPrefix	UriPrefix	UriPrefix
BDISipUri	SipUri	SipUri
BDIPhotoUriSubstitutionEnab led	PhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled
BDIPhotoUriSubstitutionToken	PhotoUriSubstitutionToken	PhotoUriSubstitutionToken
BDIPhotoUriWithToken	PhotoUriWithToken	PhotoUriWithToken
BDIPhotoSource	PhotoSource	PhotoSource
LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom
LDAPUserDomain	LDAPUserDomain	LDAPUserDomain
-	-	LdapSupportedMechanisms

BDI Parameters	EDI Parameters	CDI Parameters
BDICommonName	CommonName	CommonName
BDIDisplayName	DisplayName	DisplayName
BDIFirstname	Firstname	Firstname
BDILastname	Lastname	Lastname
BDIEmailAddress	EmailAddress	EmailAddress
BDISipUri	SipUri	SipUri
BDIPhotoSource	PhotoSource	PhotoSource
BDIBusinessPhone	BusinessPhone	BusinessPhone
BDIMobilePhone	MobilePhone	MobilePhone
BDIHomePhone	HomePhone	HomePhone
BDIOtherPhone	OtherPhone	OtherPhone
BDIDirectoryUri	DirectoryUri	DirectoryUri
BDITitle	Title	Title
BDICompanyName	CompanyName	CompanyName
BDIUserAccountName	UserAccountName	UserAccountName
BDIDomainName	DomainName	DomainName
BDICountry	Country	Country
BDILocation	Location	Location
BDINickname	Nickname	Nickname
BDIPostalCode	PostalCode	PostalCode
BDICity	City	City
BDIState	State	State
BDIStreetAddress	StreetAddress	StreetAddress

Cisco Unified Communications Manager User Data Service

User Data Service (UDS) is a REST interface on Cisco Unified Communications Manager that provides contact resolution.

UDS is used for contact resolution in the following cases:

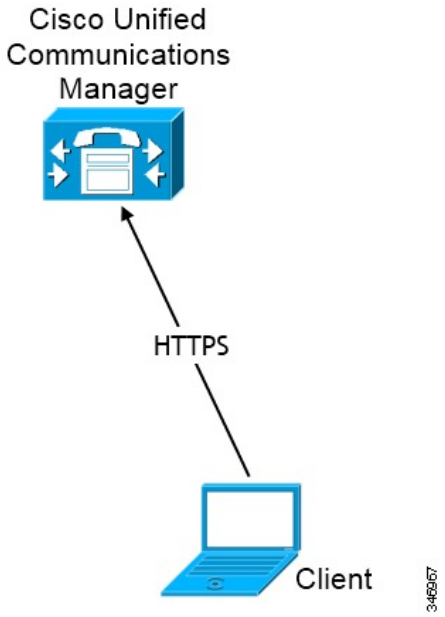
- If you set the DirectoryServerType parameter to use a value of UDS in the client configuration file.

With this configuration, the client uses UDS for contact resolution when it is inside or outside of the corporate firewall.

- If you deploy Expressway for Remote and Mobile Access.

  With this configuration, the client automatically uses UDS for contact resolution when it is outside of the corporate firewall.

You synchronize contact data into Cisco Unified Communications Manager from a directory server. Cisco Jabber then automatically retrieves that contact data from UDS.



Contact Resolution with Multiple Clusters

For contact resolution with multiple Cisco Unified Communications Manager clusters, synchronize all users on the corporate directory to each cluster. Provision a subset of those users on the appropriate cluster.

For example, your organization has 40,000 users. 20,000 users reside in North America. 20,000 users reside in Europe. Your organization has the following Cisco Unified Communications Manager clusters for each location:

- `cucm-cluster-na` for North America
- `cucm-cluster-eu` for Europe

In this example, synchronize all 40,000 users to both clusters. Provision the 20,000 users in North America on `cucm-cluster-na` and the 20,000 users in Europe on `cucm-cluster-eu`.

When users in Europe call users in North America, Cisco Jabber retrieves the contact details for the user in Europe from `cucm-cluster-na`.

When users in North America call users in Europe, Cisco Jabber retrieves the contact details for the user in North America from `cucm-cluster-eu`.

Extended UDS Contact Source

Extend the contact search from UDS to your LDAP server. In Cisco Unified Communications Manager 11.5(1) or later, you can configure if Jabber searches your LDAP server.

LDAP Prerequisites

Cisco Jabber searches the contact source using various attributes, not all of these attributes are indexed by default. To ensure efficient searches the attributes used by Cisco Jabber must be indexed.

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

- sAMAccountName
- displayName
- sn
- name
- proxyAddresses
- mail
- department
- givenName
- telephoneNumber
- otherTelephone
- mobile
- homePhone
- msRTCSIP-PrimaryUserAddress

LDAP Service Account

In Unified Communications Manager Release 12.5(1) SU2, Unified CM added support for securely passing encrypted LDAP credentials in the Service Profile. This update secures access to your directory by ensuring that the password is always stored and sent in an encrypted format. This change includes encryption during these processes:

- Directory access authentication
- Client configuration file downloads
- BAT imports/exports
- Upgrades

For more details, see the *Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1) SU2*.

In Jabber 12.8 with this Unified CM release or later, we take advantage of this capability by downloading the LDAP credentials as part of User Profile after end-user authentication.

To connect Jabber to an LDAP server, define how LDAP authenticates Jabber users:

- The default option is that Jabber automatically connects to the contact source server using Kerberos or client certificates (SASL External). We recommend this option as it's the most secure.
- If you define credentials in a service profile or in the `jabber-config.xml` file, they always take precedence over the default option.
- If you configure the LdapSupportedMechanisms parameter with the PLAIN value, but don't configure the directory profile username or password, then users can enter their directory credentials into the clients directly.
- Otherwise, if you connect to a secure port in the service profile, then you can define how Jabber connects to the contact source server. You define it by specifying the Cisco Unified Communications Manager credentials in the LDAP_UseCredentialsFrom parameter in the `jabber-config.xml` file.
- If the previous options aren't available, then use a well-known set of credentials provided by the Service Profile or the `jabber-config.xml` file. This option is the least secure. Jabber uses an account to authenticate with the contact source server. We recommend that this account has read-only access to the directory and is a commonly known public set of credentials. In this case, all Jabber users use these credentials for searches.

Note From Cisco Unified Communications Manager 12.0 version onwards, you can't configure username and password in the service profile. Jabber users get an option to authenticate themselves for using directory services. Users get a notification when they sign in to Jabber for the first time. If they don't authenticate themselves that first time, then they get an alert when they are trying to access contact list.

Jabber ID Attribute Mapping

The LDAP attribute for user ID is sAMAccountName. This is the default attribute.

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

The CDI parameter is UserAccountName. <UserAccountName>attribute-name</UserAccountName>

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

Search Jabber IDs

Cisco Jabber uses the Jabber ID to search for contact information in the directory. There are a few options to optimize searching in the directory:

- **Search base**—By default the client starts a search at the root of a directory tree. You can use search bases to specify a different search start or to restrict searches to specific 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**—Specify a directory subkey name only to retrieve objects other than user objects when you query the directory.
- **Predictive Search Filter**—You can define multiple, comma-separated values to filter search queries. The default value is ANR(Ambiguous name resolution.)

For more information on these options, see the chapter on directory integration in the *Parameters Reference Guide for Cisco Jabber*.

Local Contact Sources

Cisco Jabber has the ability to access and search local contact sources. These local contact sources include the following:

- Local contacts stored in Microsoft Outlook are accessed by Cisco Jabber for Windows.
- Local contacts stored in IBM Notes are accessed by Cisco Jabber for Windows (from release 11.1).
- Local address book contacts are accessed by Cisco Jabber for Mac, Cisco Jabber for Android and Cisco Jabber for iPhone and iPad.

Custom Contact Sources

Cisco Jabber for all clients provides users with the ability to import custom contacts into their client.

Contact Caching

Cisco Jabber creates a local cache. Among other things, the cache stores the user's contact list. When a user searches for somebody in their contact list, Jabber searches the local cache for a match before starting a directory search.

If a user searches for somebody who is not in their contact list, Jabber first searches the local cache and then searches the company directory. If the user then starts a chat or a call with this contact, Jabber adds the contact to the local cache.

The local cache information expires after 24 hours.

Resolving Duplicate Contacts

Contacts in Jabber can come from different sources. Jabber can find matches for the same contact in several contact sources. In that case, Jabber determines which records match the same person and combines all data for that person. To determine if a record in one of the contact sources matches the contact, Jabber looks for these fields in the following order:

1. **Jabber ID (JID)**—If the records have a JID, Jabber matches the records on that basis. Jabber does not further compare based on the mail or phone number fields.
2. **Mail**—If the records have a mail field, Jabber matched the records on that basis. Jabber does not further compare the records based on phone numbers.
3. **Phone Number**—If the records have a phone number, Jabber matches the records on that basis.

As Jabber compares the records and determines which match the same person, it merges the contact data to create one contact record.

Dial Plan Mapping

You configure dial plan mapping to ensure that dialing rules on Cisco Unified Communications Manager match dialing rules on your directory.

Application Dial Rules

Application dial rules automatically add or remove digits in phone numbers that users dial. Application dialing rules manipulate numbers that users dial from the client.

For example, you can configure a dial rule that automatically adds the digit 9 to the start of a 7 digit phone number to provide access to outside lines.

Directory Lookup Dial Rules

Directory lookup dial rules transform caller ID numbers into numbers that the client can lookup in the directory. Each directory lookup rule you define specifies which numbers to transform based on the initial digits and the length of the number.

For example, you can create a directory lookup rule that automatically removes the area code and two-digit prefix digits from 10-digit phone numbers. An example of this type of rule is to transform `4089023139` into `23139`.

Cisco Unified Communication Manager UDS for Mobile and Remote Access

Cisco Unified Communication Manager UDS is the contact source used when Cisco Jabber connects using Expressway for Mobile and Remote Access. If you deploy LDAP within the corporate firewall, we recommend 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.

Cloud Contact Source

Webex Contact Source

For Cloud deployments, contact data is configured in Webex Messenger Administration Tool or by user updates. The contact information can be imported using the Webex Messenger Administration Tool. For more information see the *User Management* section of the Webex Messenger Administration Guide.

Contact Photo Formats and Dimensions

To achieve the best result with Cisco Jabber, your contact photos should have specific formats and dimensions. Review supported formats and optimal dimensions. Learn about adjustments the client makes to contact photos.

Contact Photo Formats

Cisco Jabber supports the following formats for contact photos in your directory:

- JPG
- PNG
- BMP

Important Cisco Jabber does not apply any modifications to enhance rendering for contact photos in GIF format. As a result, contact photos in GIF format might render incorrectly or with less than optimal quality. To obtain the best quality, use PNG format for your contact photos.

Contact Photo Dimensions

Tip The optimum dimensions for contact photos are 128 pixels by 128 pixels with an aspect ratio of 1:1.

128 pixels by 128 pixels are the maximum dimensions for local contact photos in Microsoft Outlook.

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

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:

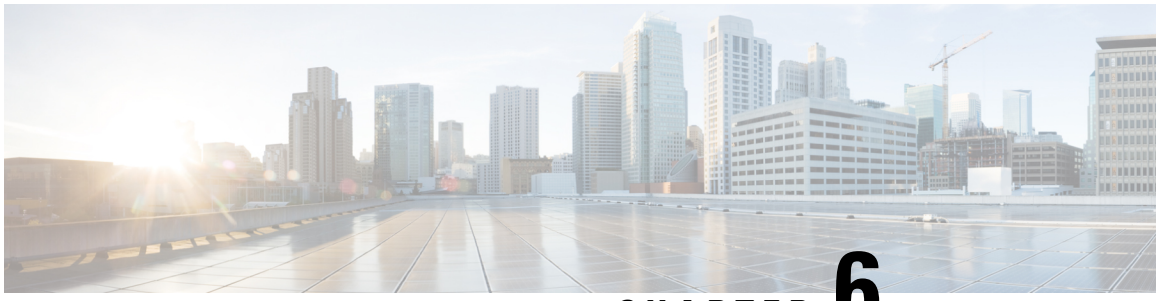
- Resizing—If contact photos in your directory are smaller or larger than 128 pixels by 128 pixels, the client automatically resizes the photos. For example, contact photos in your directory are 64 pixels by 64 pixels. When Cisco Jabber retrieves the contact photos from your directory, it resizes the photos to 128 pixels by 128 pixels.

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

- Cropping—Cisco Jabber automatically crops nonsquare contact photos to a square aspect ratio, or an aspect ratio of 1:1 where the width is the same as the height.
- Portrait orientation—If contact photos in your directory have portrait orientation, the client crops 30 percent from the top and 70 percent from the bottom.

  For example, if contact photos in your directory have a width of 100 pixels and a height of 200 pixels, Cisco Jabber needs to crop 100 pixels from the height to achieve an aspect ratio of 1:1. In this case, the client crops 30 pixels from the top of the photos and 70 pixels from the bottom of the photos.
- Landscape orientation—If contact photos in your directory have landscape orientation, the client crops 50 percent from each side.

  For example, if contact photos in your directory have a width of 200 pixels and a height of 100 pixels, Cisco Jabber needs to crop 100 pixels from the width to achieve an aspect ratio of 1:1. In this case, the client crops 50 pixels from the right side of the photos and 50 pixels from the left side of the photos.



CHAPTER 6

Security and Certificates

Encryption

Compliance and Policy Control for File Transfer and Screen Capture

If you send file transfers and screen captures using the Managed file transfer option on Cisco Unified Communications Manager IM and Presence 10.5(2) or later, you can send the files to a compliance server for audit and policy enforcement.

For more information about compliance, see the *Instant Messaging Compliance for IM and Presence Service on Cisco Unified Communications Manager* guide.

For more information about configuring file transfer and screen capture, see the *Cisco Unified Communications Manager IM and Presence Deployment and Installation Guide*.

Instant Message Encryption

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

On-Premises Encryption

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

Connection	Protocol	Negotiation Certificate	Expected Encryption Algorithm
Client to server	XMPP over TLS v1.2	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 Communications Manager IM and Presence
- Cisco Unified Communications Manager

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

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

Version	Key Length
Cisco Unified Communications Manager IM and Presence Service versions 9.0.1 and higher	2048 bit

XMPP Encryption

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

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

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

Instant Message Logging

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

See the following for more information about compliance:

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

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

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

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

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

Instant Message Logging

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

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

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

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

Client-to-Client Encryption

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

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

- **Support AES Encoding For IM**—Sending clients encrypt instant messages with the AES 256-bit algorithm. Receiving clients decrypt instant messages.
- **Support No Encoding For IM**—Clients can send and receive instant messages to and from other clients that do not support encryption.

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

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 *About Encryption Levels* in the Cisco WebEx documentation.

Encryption Icons

Review the icons that the client displays to indicate encryption levels.

Lock Icon for Client to Server Encryption

In both on-premises and cloud-based deployments, Cisco Jabber displays the following icon to indicate client to server encryption:

Lock Icon for Client to Client Encryption

In cloud-based deployments, Cisco Jabber displays the following icon to indicate client to client encryption:

Local Chat History

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

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

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

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

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

For mobile clients, the chat history files are not accessible.

Voice and Video Encryption

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

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

Authentication Methods for Secure Media

Use SIP oAuth to enable secure media in a token-based authentication. You can set up SIP oAuth instead of CAPF enrollment for your security authentication for on-premises, cloud, and hybrid deployments of Jabber.

SIP oAuth
Done once on your Cisco Unified Communications Manager set up. It ensures that your SIP traffic, including your RTP media, is secure.

CAPF Enrollment
Workflow for enabling CAPF enrolment is as follows:

- Create and Configure Jabber Devices
- Authentication Strings
- Configure Phone Security Profile

PIE ASLR Support

Cisco Jabber for Android, iPhone and iPad supports Position Independent Executable Address Space Layout Randomization (PIE ASLR).

Federal Information Processing Standards

The Federal Information Processing Standard (FIPS) 140 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. These cryptographic modules include the set of hardware, software, and firmware that implements approved security functions and is contained within the cryptographic boundary.

FIPS requires that all encryption, key exchange, digital signatures, and hash and random number generation functions used within the client are compliant with the FIPS 140.2 requirements for the security of cryptographic modules.

FIPS mode results in the client managing certificates more strictly. Users in FIPS mode may see certificate errors in the client if a certificate for a service expires and they haven't reentered their credentials. Users also see a FIPS icon in their hub window to indicate that the client is running in FIPS mode.

Enable FIPS for Cisco Jabber for Windows

Cisco Jabber for Windows supports two methods of enabling FIPS:

- Operating system enabled—The Windows operating system is in FIPS mode.
- Cisco Jabber bootstrap setting—Configure the FIPS_MODE installer switch. Cisco Jabber can be in FIPS mode on an operating system that is not FIPS enabled. In this scenario, only connections with non-Windows APIs are in FIPS mode.

Table 8: Cisco Jabber for Windows Setting for FIPS

Platform Mode	Bootstrap Setting	Cisco Jabber Client Setting
FIPS Enabled	FIPS Enabled	FIPS Enabled—Bootstrap setting.
FIPS Enabled	FIPS Disabled	FIPS Disabled—Bootstrap setting.
FIPS Enabled	No setting	FIPS Enabled—Platform setting.
FIPS Disabled	FIPS Enabled	FIPS Enabled—Bootstrap setting.
FIPS Disabled	FIPS Disabled	FIPS Disabled—Bootstrap setting.
FIPS Disabled	No setting	FIPS Disabled—Platform setting.

Note Jabber Voicemail service only accepts TLS Version TLS 1.2 for HTTPs request **https://164.62.224.15/vmrest/version with FIPS enabled** during an SSL connection.

Enable FIPS for Cisco Jabber for Mobile Clients

To enable FIPS for Cisco Jabber for mobile clients, set the FIPS_MODE parameter to TRUE in the Enterprise Mobility Management (EMM).

Important

- Enabling FIPS removes the users ability to accept untrusted certificates. In this case, some services may not be available to users. Certificate Trust List (CTL) or ITL file does not apply here. The servers' certificates must be properly signed, or the client must be made to trust the servers' certificates through side-loading.
- FIPS enforces TLS1.2, so the older protocols are disabled.
- Cisco Jabber for mobile clients don't support Platform Mode.

Common Criteria

The Common Criteria for Information Technology Security Evaluation comprise a set of international standards that are used to evaluate the security attributes of IT products. You can run Cisco Jabber in a mode that is compliant with the Common Criteria certification requirements. To do this, you must enable it for each of the clients.

To run Jabber in an environment that is enabled with Common Criteria:

- Jabber for Windows: Set the CC_MODE installation argument to TRUE.
- For Jabber for Android and Jabber for iPhone and iPad: Set the CC_MODE parameter to TRUE in your Enterprise Mobility Management (EMM).

- The RSA key length must be at least 2048 bits. To configure the RSA key length, read about how to *Create and Configure Cisco Jabber Devices* in the *On-Premises Deployment Guide for Cisco Jabber 12.5*.

For more information about how to set up Jabber to run in common criteria mode, read about how to *Deploy Cisco Jabber Applications* in the *On-Premises Deployment Guide for Cisco Jabber 12.5*.

Secure LDAP

Secure LDAP communication is LDAP over SSL/TLS

LDAPS initiates an LDAP connection over a SSL/TLS connection. It opens the SSL session then begins using the LDAP protocol. This requires a separate port, 636 or Global Catalog port 3269.

Authenticated UDS Contact Search

Enable authentication for UDS contact searches in Cisco Unified Communications Manager and Cisco Jabber provides credentials to authenticate with UDS for contact searches.

Certificates

Certificate Validation

The Certificate Validation Process

The operating system Cisco Jabber runs on validates server certificates when authenticating to services. When attempting to establish secure connections, the service presents Cisco Jabber with a certificate. The operating system validates the presented certificate against what is in the client device's local certificate store. If the certificate is not in the certificate store, the certificate is deemed untrusted and Cisco Jabber prompts the user to accept or decline the certificate.

If the user accepts the certificate, Cisco Jabber connects to the service and saves the certificate in the certificate store or keychain of the device . If the user declines the certificate, Cisco Jabber does not connect to the service and the certificate is not saved to the certificate store or keychain of the device.

If the certificate is in the local certificate store of the device, Cisco Jabber trusts the certificate. Cisco Jabber connects to the service without prompting the user to accept or decline the certificate.

Cisco Jabber can authenticate to several services, depending on what is deployed in the organization. A certificate signing request (CSR) must be generated for each service. Some public certificate authorities do not accept more than one CSR per fully qualified domain name (FQDN). Which means that the CSR for each service may need to be sent to separate public certificate authorities.

Ensure that you specify FQDN in the service profile for each service, instead of the IP address or hostname.

Signed Certificates

Certificates can be signed by the certificate authority (CA) or self-signed.

- CA-signed certificates (Recommended)—Users are not prompted because you are installing the certificate on the devices yourself. CA-signed certificates can be signed by a Private CA or a Public CA. Many certificates that are signed by a Public CA are stored in the certificate store or keychain of the device. Devicies using Android 7.0 or later recognize only CA-signed certificates.
- Self-signed certificates—Certificates are signed by the services that are presenting the certificates, and users are always prompted to accept or decline the certificate.

Certificate Validation Options

Before setting up certificate validation, you must decide how you want the certificates to be validated:

- Whether you are deploying certificates for on-premises or cloud-based deployments.
- What method you are using to sign the certificates.
- If are you deploying CA-signed certificates, whether you are going to use public CA or private CA.
- Which services you need to get certificates for.

Required Certificates for On-Premises Servers

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

Server	Certificate
Cisco Unified Communications Manager IM and Presence Service	HTTP (Tomcat) XMPP
Cisco Unified Communications Manager	HTTP (Tomcat) and CallManager certificate (secure SIP call signaling for secure phone)
Cisco Unity Connection	HTTP (Tomcat)
Webex Meetings Server	HTTP (Tomcat)
Cisco VCS Expressway Cisco Expressway-E	Server certificate (used for HTTP, XMPP, and SIP call signaling)

Important Notes

- Security Assertion Markup Language (SAML) single sign-on (SSO) and the Identity Provider (IdP) require an X.509 certificate.
- You should apply the most recent Service Update (SU) for Cisco Unified Communications Manager IM and Presence Service before you begin the certificate signing process.
- The required certificates apply to all server versions.
- Each cluster node, subscriber, and publisher, runs a Tomcat service and can present the client with an HTTP certificate.

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

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

Certificate Signing Request Formats and Requirements

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

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

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

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

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

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

Revocation Servers

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

Users are not notified of the following outcomes:

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

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

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

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

Server Identity in Certificates

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

- A trusted authority has issued the certificate.

- 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 or hostname, and the server certificate identifies the server with an FQDN, the client cannot identify the server as trusted and prompts the user.

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

Certificates for Multiserver SANs

If you use a multiserver SAN, you only need to upload a certificate to the service once per cluster per tomcat certificate and once per cluster per XMPP certificate. If you do not use a multiserver SAN, then you must upload the certificate to the service for every Cisco Unified Communications Manager node.

Certificate Validation for Cloud Deployments

Webex Messenger and Webex Meetings Center present the following certificates to the client by default:

- `CAS`
- `WAPI`

Note Webex certificates are signed by a public Certificate Authority (CA). Cisco Jabber validates these certificates to establish secure connections with cloud-based services.

Cisco Jabber validates the following XMPP certificates received from Webex Messenger. If these certificates are not included in your operating system, you must provide them.

- VeriSign Class 3 Public Primary Certification Authority - G5 — This certificate is stored in the Trusted Root Certificate Authority
- VeriSign Class 3 Secure Server CA - G3 —This certificate validates the Webex Messenger server identity and is stored in the Intermediate Certificate Authority.
- AddTrust External CA Root
- GoDaddy Class 2 Certification Authority Root Certificate

For more information about root certificates for Cisco Jabber for Windows, see https://www.identrust.co.uk/certificates/trustid/install-nes36.html.

For more information about root certificates for Cisco Jabber for Mac, see https://support.apple.com.

Server Name Indication Support for Multitenant Hosted Collaboration Solution

Cisco Jabber supports Server Name Indication (SNI) in a Mobile and Remote Access (MRA) deployment with a multitenant Hosted Collaboration Solution.

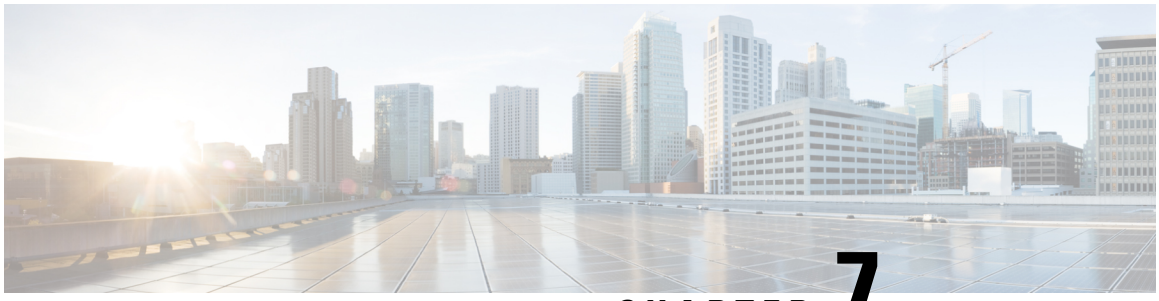
Cisco Jabber sends the domain information using SNI to Expressway. Expressway looks up the certificate storage to find the certificate that contains the domain information and returns the certificate to Cisco Jabber for validation.

For more information on multitenant deployment, see the sections *Endpoint Service Discovery with Domain Certificates* and *Jabber Service Discovery without Domain Certificates* from the Cisco Hosted Collaboration Solution, Release 11.5 Multitenant Expressway Configuration Guide.

Antivirus Exclusions

If you deploy antivirus software, include the following folder locations in the antivirus exclusion list:

- `C:\Users\<User>\AppData\Local\Cisco\Unified Communications\Jabber`
- `C:\Users\<User>\AppData\Roaming\Cisco\Unified Communications\Jabber`
- `C:\ProgramData\Cisco Systems\Cisco Jabber`



CHAPTER 7

Configuration Management

Fast Sign-in

This feature enables you to sign in to all Cisco Jabber services at the same time instead of the sequential sign-in process used earlier. Each service independently connects to its respective server and authenticates you based on cached data. This makes the sign-in process quick and dynamic. However, this feature is effective only from the second time you sign into Jabber.

You can configure the Fast Sign-in by using the STARTUP_AUTHENTICATION_REQUIRED parameter for all clients. However, for mobile clients you have to configure both STARTUP_AUTHENTICATION_REQUIRED and CachePasswordMobile parameters. For more information on configuring these parameters, see the latest *Parameters Reference Guide for Cisco Jabber*.

Configuration Refetch—Fast Sign-in does not retrieve server-side settings synchronously on every sign-in or sign-out. This happens only during the first sign-in as in previous Jabber releases.

For subsequent logins, a request is sent to fetch fresh configuration from the server at various points like within 1 to 5 minutes after sign-in, within 7 to 9 hours after sign-in, or whenever your users do a manual refresh for fetching the configuration.

You can configure ConfigRefetchInterval parameter to fetch configuration from the server every 7 or 8 hours. For more information on this parameter, see the latest *Parameters Reference Guide for Cisco Jabber*.

Action for Dynamic Configuration Changes

In Jabber 11.9, components and services react dynamically to configuration changes. You receive a notification prompt to Sign out or Reset Jabber depending on these scenarios:

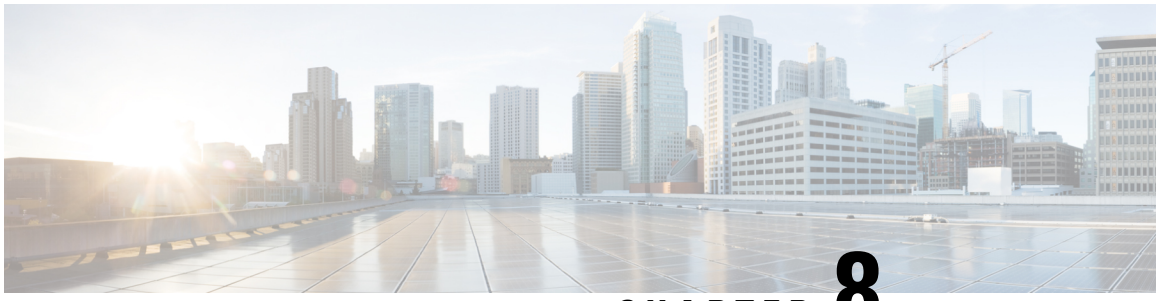
Reset Jabber—If a primary service is changed, you will receive a notification prompt to Reset Jabber. For example, if the IM&P and Telephony account changes to a Phone only account, Jabber will require a Reset.

Sign out from Jabber—If there are any changes in the configuration keys listed in the following table, Jabber will prompt the user to Sign out and Login to use the new configuration.

- **Windows**—You will receive a pop-up notification that configuration has changed. You can either ignore the notification or Sign out and Login to use the new configuration.

- **Mobile Clients**—Jabber signs out automatically. You then receive a pop-up notification indicating that the configuration has changed. Click **OK** to accept the configuration changes to sign in to Jabber automatically.

Key Name	Platform	Sign Out
RemoteAccess	All Clients	Sign out
Meetings_Enabled	All Clients	Sign out
DirectoryServerType	All Clients	Sign out
DirectoryUri	All Clients	Sign out
UseSipUriToResolveContacts	All Clients	Sign out
SipUri	All Clients	Sign out
UriPrefix	All Clients	Sign out
DirectoryUriPrefix	All Clients	Sign out
SwapDisplayNameOrder	All Clients	Sign out
PresenceDomain	All Clients	Sign out
Support_SSL_Encoding	All Clients	Sign out
Support_No_Encoding	All Clients	Sign out
IM_Logging_Enabled	All Clients	Sign out
IGS_CUP_ENABLESECURE	All Clients	Sign out
DISALLOW_FILE_TRANSFER_ON_MOBILE	All Clients	Sign out
Persistent_Chat_Enabled	Desktop Clients	Sign out
Persistent_Chat_Mobile_Enabled	Mobile Clients	Sign out
Disable_MultiDevice_Message	All Clients	Sign out
Location_Enabled/Location_Matching_Mode	All Clients	Sign out
IP_MODE	All Clients	Sign out
Telephony_Enabled	All Clients	Sign out
Voicemail_Enabled	All Clients	Sign out
EnableLoadAddressBook	Mobile Clients	Sign out
ShowRecentsTab	Jabber Windows only	Sign out
IM_Enabled	All Clients	Sign out
Disallow-jaibreak-device	Mobile Clients	Sign out
EnableChats	Jabber Windows only	Sign out



CHAPTER 8

Screen Share

Screen Share

There are four types of screen share:

- Cisco Webex share
- BFCP share
- IM Only share
- Escalate to a meeting and share

Webex Screen Share

Applies to Cisco Jabber for desktop clients in cloud deployments.

For cloud deployments, Webex Screen Share is selected automatically after choosing a contact, if BFCP and IM Only screen share options are not available.

You can start Webex Screen Share using one of the following methods:

- Right-click on a contact in the hub window and choose **Share screen..** from the menu options.
- Select a contact in the hub window and click on the **Settings** menu. Choose **Communicate** and select **Share screen...** from the menu options.
- When BFCP and IM Only screen share options are not available, then in a conversation window select **...** > **Share screen** from the menu options.

BFCP Screen Share

Applies to Cisco Jabber desktop clients, Cisco Jabber for mobile clients can only receive BFCP screen shares.

Binary Floor Control Protocol (BFCP) screen share is controlled by Cisco Unified Communications Manager. Cisco Unified Communications Manager handles the BFCP packets that users transmit when using video desktop sharing capabilities. When on a call select **...** > **Share screen** to start a BFCP screen share.

Remote screen control is not supported with this feature.

Video desktop sharing using BFCP is not supported if **Trusted Relay Point** or **Media Termination Point** are enabled on the software phone device.

Note In Jabber for Windows, the **Screen Share** button starts a BFCP screen share by default. If BFCP-based sharing is unavailable, the button starts an IM-only screen share if possible.

IM Only Screen Share

Applies to Cisco Jabber for Windows.

IM-only screen share is a one-to-one client-to-client screen share over Remote Desktop Protocol (RDP). The EnableP2PDesktopShare parameter controls whether IM-only screen shares are available. The PreferP2PDesktopShare parameter controls whether Jabber prefers video sharing or IM-only screen shares.

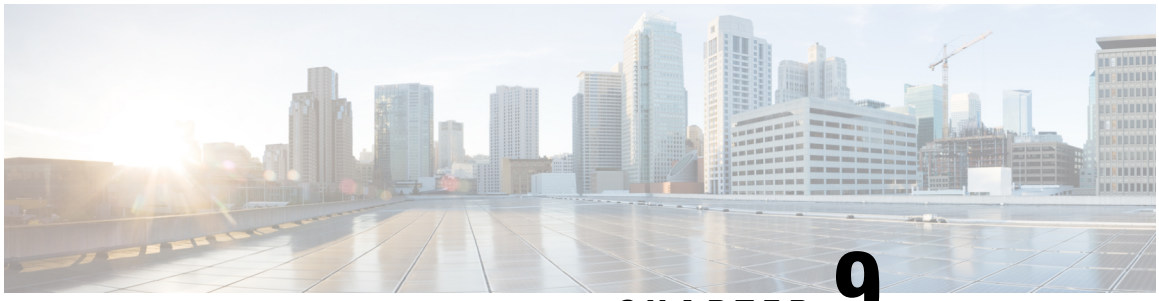
If your deployment allows IM-only screen share, select **...** > **Share screen** in the chat window to start a screen share.

RDP requires port 3389 by default. IM-only screen share default port range is 49152–65535 TCP and UDP. You can use the SharePortRangeStart and SharePortRangeSize parameters to restrict the port range.

Escalate to a Meeting and Share

Applies to all Cisco Jabber clients.

You can escalate to an instant Webex Meetings and share your screen using the Webex Meetings controls.



CHAPTER 9

Interdomain Federation

Interdomain federation enables Cisco Jabber users in an enterprise domain to share availability and send instant messages with users in another domain.

- Cisco Jabber users must manually enter contacts from another domain.
- Cisco Jabber supports federation with the following:
  - Microsoft Office Communications Server
  - Microsoft Lync
  - IBM Sametime
  - XMPP standard-based environments such as Google Talk

Note Expressway for Mobile and Remote Access doesn't enable XMPP Interdomain federation itself. Cisco Jabber clients connecting over Expressway for Mobile and Remote Access can use XMPP Interdomain federation if it has been enabled on Cisco Unified Communications Manager IM and Presence.

  - AOL Instant Messenger

You configure interdomain federation for Cisco Jabber on Cisco Unified Communications Manager IM and Presence Service. See the appropriate server documentation for more information.

- Intradomain Federation, on page 127
- User ID Planning for Federation, on page 128

Intradomain Federation

Intradomain federation enables users within the same domain to share availability and send instant messages between Cisco Unified Communications Manager IM and Presence Service and Microsoft Office Communications Server, Microsoft Live Communications Server, or another presence server.

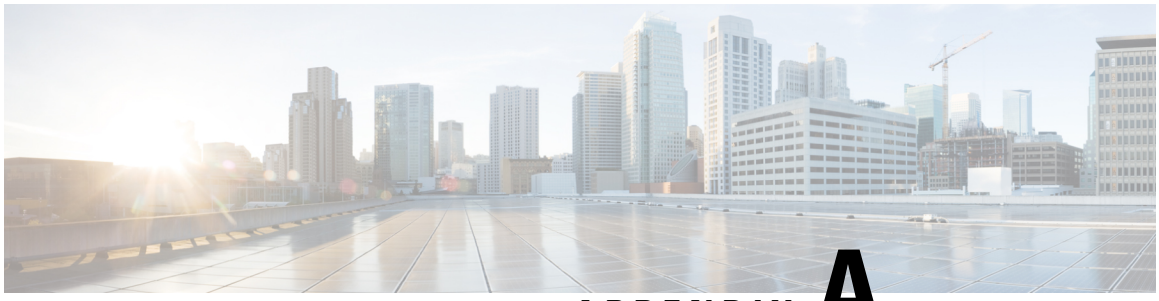
Intradomain federation allows you to migrate users to Cisco Unified Communications Manager IM and Presence Service from a different presence server. For this reason, you configure intradomain federation for Cisco Jabber on the presence server. See the following for more information:

- Cisco Unified Communications Manager IM and Presence Service: *Partitioned Intradomain Federation for IM and Presence Service on Cisco Unified Communications Manager*

User ID Planning for Federation

For federation, Cisco Jabber requires the contact ID or user ID for each user to resolve contacts during contact searches.

Set the attribute for the user ID in the SipUri parameter. The default value is `msRTCSIP-PrimaryUserAddress`. If there is a prefix to remove from your user ID you can set a value in the UriPrefix parameter, see the latest version of the *Parameters Reference Guide for Cisco Jabber*.



APPENDIX A

Jabber Supported Languages

Supported Languages

The following table lists the Locale Identifier (LCID) or Language Identifier (LangID) for the languages that the Cisco Jabber clients support.

Supported Languages	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android, Cisco Jabber for iPhone and iPad	LCID/LangID
Arabic - Saudi Arabia	X		X	1025
Bulgarian - Bulgaria	X	X		1026
Catalan - Spain	X	X		1027
Chinese (Simplified) - China	X	X	X	2052
Chinese (Traditional) - Taiwan	X	X	X	1028
Croatian - Croatia	X	X	X	1050
Czech - Czech Republic	X	X		1029
Danish - Denmark	X	X	X	1030
Dutch - Netherlands	X	X	X	1043
English - United States	X	X	X	1033
Finnish - Finland	X	X		1035

Supported Languages	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android, Cisco Jabber for iPhone and iPad	LCID/LangID
French - France	X	X	X	1036
German - Germany	X	X	X	1031
Greek - Greece	X	X		1032
Hebrew - Israel	X			1037
Hungarian - Hungary	X	X	X	1038
Italian - Italy	X	X	X	1040
Japanese - Japan	X	X	X	1041
Korean - Korea	X	X	X	1042
Norwegian - Norway	X	X		2068
Polish - Poland	X	X		1045
Portuguese - Brazil	X	X	X	1046
Portuguese - Portugal	X	X		2070
Romanian - Romania	X	X	X	1048
Russian - Russia	X	X	X	1049
Serbian	X	X		1050
Slovak - Slovakian	X	X	X	1051
Slovenian -Slovenia	X	X		1060
Spanish - Spain (Modern Sort)	X	X	X	3082
Swedish - Sweden	X	X	X	5149
Thai - Thailand	X	X		1054
Turkish	X	X	X	1055