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	9.x and later
	Webex Messenger	
Telephony	Cisco Unified Communications Manager	9.x and later
	Cisco Unified Survivable Remote Site Telephony	8.5 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	9.x and later

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	2.0 and later Cisco Jabber for Windows supports 1.5 and later
	Webex Meetings Center	WBS29 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	• For all Cisco Jabber clients, other than Cisco Jabber for Android, the recommended version is X8.10.1 and later. • For Cisco Jabber for Android, the minimum version is X8.1.1 or later and the recommended version is X8.10.1 and later.
	Cisco Expressway E	• For all Cisco Jabber clients, other than Cisco Jabber for Android, the minimum and recommended version is X8.10.1 and later. • For Cisco Jabber for Android, the minimum version is X8.1.1 or later and the recommended version is 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)
- Microsoft Windows 7

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)

Operating Systems for Cisco Jabber for Android

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

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.

Operating Systems for Cisco Jabber for iPhone and iPad

Cisco Jabber for iPhone and iPad supports the following operating systems:

- iOS 12 and later
- iOS 11 and later
- watchOS 5 and later
- watchOS 4 and later
- watchOS 3 and later

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
GPU	DirectX11 on Microsoft Windows 7	N/A
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 iPhone and iPad

The following Apple devices are supported for Cisco Jabber for iPhone and iPad on iOS 11.X . The devices that are not upgraded to these versions are not supported.

Apple Device	Generation
iPad	Third, fourth, fifth, sixth , 10.5 inch iPad Pro,
iPad Air	Air 1 and Air 2
iPad mini	Mini 2, mini 3, and mini 4
iPhone	5, 5c, 5s, 6, 6 Plus, , 6s, and 6s Plus, 7 and 7 Plus, 8 and 8 Plus, iPhone X, XS, and XS Max, and Apple Watch
iPod touch	5 and

The following Bluetooth headsets are supported on iPhone and iPad:

Jabra BIZ 2400	Jabra Supreme UC

Jabra Easygo	Jabra Wave +
Jabra Evolve 65 UC Stereo	Jawbone ICON for Cisco Bluetooth Headset
Jabra EXTREME 2	Plantronics Voyager Edge
Jabra Motion [1]	Plantronics Voyager Edge UC
Jabra PRO 9470	Plantronics Voyager Legend
Jabra Speak 450 for Cisco	Plantronics Voyager Legend UC
Jabra Speak 510	Sony Ericsson Bluetooth Headset BW600
Jabra Stealth	

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

Hardware Requirements for Cisco Jabber for Android 12.1

The minimum OS, CPU, and display requirements for the Android devices are:

- Android Operating System—4.4 or later.
- CPU—1.5 GHz dual-core, 1.2-GHz quad-core, or higher (quad-core recommended).
- Display—For two-way video, the minimum display resolution requirement is 480 x 800 or higher. For IM only, the minimum display resolution requirement is 320 x 480 or higher

Cisco Jabber for Android is not supported on Android devices that are based on an Intel chipset and Android devices with Tegra 2 chipset

Due to an Android kernel issue, Cisco Jabber cannot register to the Cisco Unified Communications Manager on some Android devices. If this problem occurs, see the troubleshooting articles.

Android Devices in Full UC Mode

Cisco Jabber for Android is tested with the Android devices listed here. Although other Android devices are not officially supported, you can use Cisco Jabber for Android on other Android devices.

Cisco Jabber for Android supports Full UC mode in all the Samsung devices that meet minimal hardware requirement.

Cisco Jabber for Android supports Full UC mode in the following devices with respective version of Operating System provided in the table:

Table 1: Supported Devices

Device	Device Model	Operating System	Notes
BlackBerry	Priv	Android OS 5.1 or later	Blackberry Priv device limitation: If Jabber is removed from the recently viewed apps list, and the device is kept idle for some time, then Jabber becomes inactive.
Fujitsu	Arrows M305	Android OS 4.4.2 or later	
	Arrows M357	Android OS 6.0.1 or later	
	Arrows M555	Android OS 4.4.2 or later	

Device	Device Model	Operating System	Notes
Google Nexus	4	Android OS 5.1.1 or later	
	5	Android OS 4.4 or later	
	5X	Android OS 6.0 or later	
	6	Android OS 5.0.2 or later	
	6P	Android OS 6.0 or later	If you have a Google Nexus 6P device with Android OS version 6.x or 7.0, then contact your administrator to set your Jabber phone service as a secure phone service. Otherwise, your device might not respond. However, if your Android OS version is 7.1 or later, no action is required.
	7	Android OS 4.4 or later	
	9	Android OS 5.0.2 or later	
	10	Android OS 4.4 or later	
	Pixel	Android OS 7.0 or later	
	Pixel C	Android OS 6.0 or later	
	Pixel XL	Android OS 7.0 or later	
	Pixel 2	Android OS 8.0 or later	During a Jabber call if the user switches audio from mobile device to a headset, then there might be some issues with the auido for few seconds.
	Pixel 2 XL	Android OS 8.0 or later	During a Jabber call if the user switches audio from mobile device to a headset, then there might be some issues with the auido for few seconds.
Honeywell Dolphin	CT50	Android OS 4.4.4 or later	

Device	Device Model	Operating System	Notes
HTC	10	Android 6.0 or later	
	A9	Android 6.0 or later	
	E9 PLUS	Android OS 5.0.2 or later	
	M7	Android OS 4.4.2 or later	
	M8	Android OS 4.4 or later	
	M9	Android OS 5.0 or later	
	One Max	Android OS 4.4 or later	
	X9	Android OS 6.0 and later	

Device	Device Model	Operating System	Notes
Huawei	G6	Android OS 4.4 or later	• There is a limitation that Jabber is made inactive due to the high power consumption on Huawei devices. • In Huawei devices with Android OS 7.x or later, enable app lock for Jabber so that it is not terminated by your device. And for devices with OS 8.x, "run in background" from app info must be enabled.
	Honor 7	Android OS 5.0 or later	
	M2	Android OS 5.0 or later	
	Mate 7	Android OS 4.4 or later	
	Mate 8	Android OS 6.0 or later	
	Mate 9	Android OS 6.0 or later	
	Nova	Android OS 7.0 or later	
	Mate 10	Android OS 8.0 or later	
	Mate 10 Pro	Android OS 8.0 or later	
	P8	Android OS 4.4.4 or later	
	P9	Android OS 6.0 and later	
	P10	Android OS 7.0 and later	
	P10 Plus	Android OS 7.0 and later	

Device	Device Model	Operating System	Notes
LG	G2	Android OS 4.4 or later	
	G3	Android OS 4.4 or later	
	G4	Android OS 5.1 or later	
	G5	Android OS 6.0 and later	
	G6	Android OS 7.0 and later	
	Optimus G Pro	Android OS 4.4 or later	
	V10	Android OS 5.0 or later	
Motorola	MC40	Android OS 4.4 or later	Cisco Jabber supports only audio mode with MC40 device. Cisco Jabber does not support launching Webex Meetings from MC40 device.
	Moto G	Android OS 4.4 or later	
	Moto X	Android OS 5.0 or later	
	Moto Z Droid	Android OS 6.0 or later	
OnePlus	One	Android OS 5.0 or later	
Panasonic	Toughpad FZ-X1	Android OS 4.4 or later	For Panasonic Toughpad FZ-X1 device, contact your administrator to set your Jabber phone service as a secure phone service. Also, in Panasonic Toughpad FZ-X1 device, Jabber plays ringback tone and busy tone at 24kHz.
Samsung	All	Android 4.4 and later	• In the Samsung devices with Android OS 5.x or later, the auto-run option for Jabber must be enabled. For Android OS 5.x, you can find the auto-run option under **Settings** and **Device Manager**. 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.

Device	Device Model	Operating System	Notes
Smartisan	M1L	Android 6.0.1 and later	
Sonim	XP7	Android OS 4.4.4	
Sony Xperia	M2	Android OS 4.4 or later	
	XZ	Android OS 7.0 or later	
	XZ1	Android OS 8.0 or later	
	Z1	Android OS 4.4 or later	
	Z2	Android OS 4.4.2 or later	
	Z2 tablet	Android OS 4.4.2 or later	
	Z3	Android OS 4.4.2 or later	Sony Xperia Z3 (Model SO-01G) with Android OS 5.0.2 has poor audio on Jabber calls.
	Z3 Tablet Compact	Android OS 4.4.4 or later	
	Z3+/Z4	Android OS 5.0.2 or later	Video call is unstable on Sony Z3+/Z4, you can disable your self-video for a video call or make a voice call only.
	Z4 TAB	Android OS 5.0 or later	
	Z5 Premium and Z5	Android OS 5.0.2 or later	
	ZR/A	Android OS 4.4 or later	There is a limitation that Sony devices with Android OS 6.0 cannot play voicemail in Jabber.

Device	Device Model	Operating System	Notes
Xiaomi	4C	Android OS 5.1 or later	
	MAX	Android OS 5.1 or later	
	Mi 4	Android OS 4.4 or later	
	Mi 5	Android OS 6.0 and later	
	Mi 5s	Android OS 7.0 and later	
	Mi 6	Android OS 7.0 and later	
	Mi Note	Android OS 4.4.4 or later	
	Mi Note 2	Android OS 7.0 or later	
	Mi Pad	Android OS 4.4.4 or later	
	Mi Pad 2	Android OS 5.1 or later	
	Mi MIX 2	Android OS 8.0 or later	
	Mi A1	Android OS 8.0 or later	
	Redmi 3	Android OS 5.1 or later	
	Redmi Note 3	Android OS 5.1 or later	
	Redmi Note 4X	Android OS 6.0.1 or later	
Zebra	MC67	Android OS 4.4.4 or later	MC67 did not meet the minimum hardware requirement for Jabber, but MC67 supports Jabber IM only mode and audio only mode. Video mode is not supported.
	TC70	Android OS 4.4.3 or later	TC70 device might sometimes have issues connecting to Wi-Fi network configured over DHCP. In TC70, the default value of **Keep wifi on during sleep** is **Off**, you must set it to **Always On** to use Jabber.

Jabber Supports Samsung Knox Version 2.6

Cisco Jabber for Android supports Samsung Knox Version 2.6 on these devices:

Samsung Galaxy Device Model	Operating System
Note 10.1 (2014 Edition)	Android OS 4.4.0 or later
Note 4	Android OS 4.4.0 or later
Note 5	Android OS 5.1.1 or later
Note Edge	Android OS 4.4.0 or later
S5	Android OS 4.4.0 or later
S6	Android OS 5.1.1 or later
S6 Edge	Android OS 5.1.1 or later
S6 Edge Plus	Android OS 5.1.1 or later
S7	Android OS 6.0.1 or later
S7 Edge	Android OS 6.0.1 or later
Tab S 8.4 and 10.5	Android OS 4.4.0 or later

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 cannot 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 M7	Android OS 4.4.2 or later
HTC M8	Android OS 4.4.2 or later
HTC M9	Android OS 5.0 or later
HTC One Max	Android OS 4.4.2 or later

Device Model	Operating System
Sony Xperia M2	Android OS 4.4 or later and kernel version earlier than 3.10.49. If a Sony device's android OS is 5.0.2 or later and kernel version is 3.10.49 or later, then the device can support non-secure mode.
Sony Xperia Z1	
Sony Xperia ZR/A	
Sony Xperia Z2	
Sony Xperia Z2 tablet	
Sony Xperia Z3	
Sony Xperia Z3 Tablet Compact	
Xiaomi Mi4	(Android OS 4.4 or later)
Xiaomi Mi Note	(Android OS 4.4.4 or later)
Xiaomi Mi Pad	(Android OS 4.4.4 or later)
Sonim XP7	(Android OS 4.4.4)
Honeywell Dolphin CT50	Android OS 4.4.4 or later

Supported Bluetooth Devices

Bluetooth Devices	Useful Information
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	

Bluetooth Devices	Useful Information
Jabra Easygo	
Jabra PRO 9470	
Jabra Speak 510	
Jabra Supreme UC	
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 cannot hear Audio. This limitation is applicable for Smartphones with versions earlier to Android 5.0 OS.
- In Sony Z4 / LG G4 /Devices with OS Android 6.0, when a user makes a Cisco Jabber call and connects the Bluetooth headset, then the users on that call might not hear audio. The workaround for this issue is to switch audio output device to speaker, then switch back to Bluetooth. Or connect Bluetooth headset before making a Cisco Jabber call.

Supported Android Wear

Cisco Jabber is supported on all Android wear devices with Android OS 5.0 or later and Google service 8.3 or later. Cisco Jabber is tested on these Android Wear devices:

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

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
- Samsung Chromebook Pro

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 the following ports are used based on 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.)
	30000 to 39999	FECC	UDP	Far end camera control (FECC).
	5070 to 6070	BFCP	UDP	Binary Floor Control Protocol (BFCP) for video screen sharing capabilities.
Voice or Video Media Exchange				
	16384 to 32766	RTP/SRTP	UDP	Cisco Unified Communications Manager media port range used for audio, video, and BFCP video desktop share.
	33434 to 33598	RTP/SRTP	UDP	Cisco Hybrid Services (Jabber to Jabber calling) media port range used for audio and video.
	49152 to 65535	RDP	TCP	IM-only desktop share. Applies to Cisco Jabber for Windows only.
	8000	RTP/SRTP	TCP	Used by Jabber Desk Phone Video Interface, allows users to receive video transmitted to their desk phone devices on their computers through the client.
Unity Connection				

	Port	Application Layer Protocol	Transport Layer Protocol	Description
	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).
	443	HTTPS	TCP	Connects to Cisco Unity Connection for voicemail.
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		Yes		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 Cisco Virtualization Experience Media Engine (VXME) . 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 9 version or iOS 10 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 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

The client captures and transmits video at 15 fps.

Resolution	Pixels	Bit Rate (kbits per second) with g.711 audio
w144p	256 x 144	290
w288p	512 x 288	340
w360p	640 x 360	415

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

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.

COP Files

Required COP Files for All Clients

- cmterm-bfcp-e.8-6-2.cop.sgn—To configure video screen sharing on Cisco Unified Communications Manager release 9.x and later.
- cmterm-bfcp-e.8-6-2.cop.sgn—To configure video screen sharing on Cisco Unified Communications Manager release 8.6.2 and later.
- cmterm-cupc-dialrule-wizard-0.1.cop.sgn—Deploy dial rules from Cisco Unified Communications Manager release 8.6.1 or earlier.
- cmterm-cucm-uds-912-5.cop.sgn—Cisco Unified Communications Manager 9.1(2).

Required COP Files for Cisco Jabber for Mobile Clients

This table describes about the COP files that are applicable for all Cisco Unified Communications Manager earlier than 11.5.1.

Cisco Jabber Mobile Clients	COP File
Android tablet	`cmterm-jabbertablet-install-151020.k3.cop.sgn`

Cisco Jabber Mobile Clients	COP File
Android phone	`cmterm-android-install-151020.k3.cop.sgn`
iPhone	`cmterm-iphone-install-151020.k3.cop.sgn`
iPad	`cmterm-jabbertablet-install-151020.k3.cop.sgn`

Note For Cisco Unified Communications Manager later than 11.5.1, you don't have to install COP file separately, because it is installed with the Cisco Unified Communications Manager software.

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
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.

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.