Release Notes for Cisco Jabber for Android 12.1

First Published: 2018-07-19

Last Modified: 2018-09-27

Introduction

Information for a maintenance release includes the features, requirements, restrictions, and bug fixes of the previous releases unless mentioned otherwise.

The article does not include updates for patches or hot fixes.

Before you install Cisco Jabber, we recommend that you review the release notes for information regarding issues that may affect your system.

Build Number

Release	Build Number
12.1(1)	12.1.1.269816
12.1	12.1.0.266498

What's New in Release 12.1(1)

Persistent Chat Rooms

Persistent chat rooms are now fully supported for mobile clients.

Android Pie

This release includes support for Android 9 Pie.

Resolved Caveats

This release provides fixes for several known defects.

What's New in Release 12.1

Telephony

- **TelephonyOnlyDiscovery**—This is a new parameter for Cisco Jabber operating in an on-premises and cloud deployment modes. This parameter specifies if your users have access to phone only mode or the default configuration that you have set up in your environment. For more information, see the *Parameter Reference Guide for Cisco Jabber 12.1*.

• **EnableSingleNumberReach**—This is a new parameter that specifies if users can access Single Number Reach from the user interface. For more information, see the *Parameter Reference Guide for Cisco Jabber 12.1.*

Administrator

• **Retain Secure Phone Certificate during a Cisco Jabber Reset**—Users must retain the secure phone certificate during a Cisco Jabber reset. If users have not retained the secure phone certificate, they have to contact you to configure the phone service.

• **Cisco Jabber for Android is Supported on Chromebook**—Your users can now use Cisco Jaber for Android on Chromebook, and use all the Cisco Jabber services. For complete details, see *Feature Configuration for Cisco Jabber 12.1*

Chat and Presence

• **Persistent Chat Room Support**—From this release onwards, Cisco Jabber introduces persistent chat room support for Cisco Jabber. Users can use chat rooms to collaborate with others and share ideas as a group. Persistent chat rooms allow users to perform the following tasks:

    • @Mention Notifications in Persistent Chat Rooms

    • Mute or Unmute Persistent Chat Rooms

    • Search and Find Persistent Chat Rooms

    • Leave from Persistent Chat Rooms

    • Add Participant in Persistent Chat Rooms

    • Join Persistent Chat Rooms

For more details about persistent chat rooms, see the *Persistent Chat Rooms* section from the *Feature Configuration for Cisco Jabber 12.1*.

• **Persistent_Chat_Mobile_Enabled**—This is a new parameter that specifies if persistent chat feature is available for Cisco Jabber for Android. For more information, see the *Parameter Reference Guide for Cisco Jabber 12.1.*

• **User name Displayed with an Animated Emoticon in Group Chat**—Cisco Jabber displays the user name when users send an animated emoticon to a group chat.

• **EnableConvertNumberToURI**—This is a new parameter that specifies if Cisco Jabber converts numbers into SIP URI when a user enters numbers in the chat window. For more information, see the *Parameter Reference Guide for Cisco Jabber 12.1.*

Settings

• **Refresh Cisco Jabber configuration**—When there are configuration updates, users can refresh Cisco Jabber for the updates to take effect. Users can refresh Cisco Jabber configuration from the **Settings**, **Configuration**, and **Refresh Configuration** anytime after they have signed in.

• **Cisco Jabber Diagnostics Check**—If users are unable to sign into Cisco Jabber or if Cisco Jabber services are not connected, they can use the **Diagnose Error** option from the **Sign In** page, or from the error notification message when connecting. Cisco Jabber then performs various checks to identify the

issue. If there is a issue, Cisco Jabber displays the error message with possible solution. If the problem still persists, users can send a problem report.

UI Enhancements

- **Contact Lookup Enhancement**—Support for base64-encoded thumbnail photos. Cisco Jabber contact lookup now supports base64-encoded contact photos when using LDAP or HTTP photo retrieval. Cisco Jabber will determine if the server response is a text URL (for LDAP only), an image, or a base64-encoded image, and displays it accordingly.

- **Help Link in the Cisco Jabber Sign-In Page**—We have added a **Help** link in the Cisco Jabber Sign-in page. This link takes users to the **Collaboration Help Portal** that contains articles about sign-in issues and troubleshooting tips.

- **Enter Your Company Mail Address**—Cisco Jabber displays a sign-in tip to use your company mail ID to sign into Cisco Jabber. For example, `username@company.com`.

- **Hide Contacts' Photo** —If your users don't want to see any of their contacts' photos, they can go to **Settings**, **Display**, and turn off **Show contact photo**. The contact's photo will not be displayed in contact list, chat, voicemail, recents, and call options

- **New Device Support**—See the *Device Requirements* section for all the new devices supported in this release.

Requirements

Software Requirements

Services

Install the COP file `cmterm-android-install-151020.k3.cop.sgn` for Android phones and the COP file `cmterm-jabbertablet-install-151020.k3.cop.sgn` for Android tablets, if you support the following services:

- Secure Phone (Mixed Mode Security)—On Cisco Unified Communications Manager Release 9.1(2) or later.

- Share Line and Graceful Registration under DvO—On Cisco Unified Communications Manager Release 10.5(1) or later.

- Group Configuration (Cisco Supported Field)—On Cisco Unified Communications Manager Release 10.5(2) or later.

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

Server Requirements

The following are the server requirements for Cisco Jabber for Android in this release:

Service	Software Requirement	Supported Version
IM and Presence	Cisco Unified Communications Manager IM and Presence Service	10.5(2) or later
	Cisco Webex Messenger	
Telephony	Cisco Unified Communications Manager	10.5(2) or later.
	Cisco Unified Survivable Remote Site Telephony	8.5 and later
Contact Search	Cisco Webex Messenger	
	Microsoft Active Directory	2008 R2 and later
	OpenLDAP	2.4 and later
	Cisco Unified Communications Manager User Data Service (UDS)	10.5(2) or later
Voicemail	Cisco Unity Connection	10.5 or later
Conferencing	Cisco Meeting Server (CMS)	2.2 or later
	Cisco TelePresence Server	3.1 and later
	Cisco TelePresence MCU	4.3 and later
	Cisco ISR PVDM3	Cisco Unified Communications Manager 9.1(2) and later
	Cloud CMR	Cisco Webex Meetings Server with Collaboration Meeting Room
	Cisco Webex Meetings Server	2.8 or later
	Cisco Webex Meetings	WBS31 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	Latest version on Play Store
	Cisco Expressway C	X8.1.1
	Cisco Expressway E	X8.1.1

Accessibility

Screen Readers and Assistive Touch

You can use Cisco Jabber for Android with a screen reader, and you can use assistive touch to help you navigate the app. Cisco Jabber for Android is compatible with the Google TalkBack screen reader app. With it, you can navigate Cisco Jabber for Android using Expore by Touch.

Device Requirements

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 later (quad-core is 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.

Supported Devices

Cisco Jabber for Android supports full UC mode in all the Samsung devices that meet minimal hardware requirement. For information on minimal hardware requirements, see *Device Requirements* section.

Cisco Jabber for Android supports the following devices with their respective version of OS:

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 Cisco Webex Meeting 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 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

Cisco supports the current Google Play version of Cisco Jabber for Android. Previous Google Play versions of Cisco Jabber become obsolete as new versions become available. Defects found in any Cisco Jabber release are evaluated against current versions.

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 One M7	Android OS 4.4.2 or later
HTC One M8	Android OS 4.4.2 or later
HTC One M9	Android OS 5.0.1 or later
HTC One Max	Android OS 4.4.2 or later
Sony Xperia M2	Android OS 4.4 or later and kernel version earlier than 3.10.49. If Sony device's android OS is 5.0.2 or higher and kernel version is 3.10.49 or higher, then it 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 or later
Honeywell Dolphin CT50	Android OS 4.4.4 or later
Panasonic Toughpad FZ-X1	Android OS 4.4 or later

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
S7	Android OS 6.0.1 or later
S7 Edge	Android OS 6.0.1 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
S5	Android OS 4.4.0 or later
Note 5	Android OS 5.1.1 or later
Note 4	Android OS 4.4.0 or later
Note 10.1 (2014 Edition)	Android OS 4.4.0 or later
Note Edge	Android OS 4.4.0 or later
Tab S 8.4 and 10.5	Android OS 4.4.0 or later

Note Samsung Galaxy A5 supports Samsung Knox version 2.8.

Android Wear Support

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

Bluetooth Device Support

We support Cisco Jabber for Android with tested Bluetooth devices. Although other Bluetooth devices are not officially supported, you may be able to use Cisco Jabber for Android with other devices.

The following Bluetooth devices are supported by Cisco Jabber for Android:

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	
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.

> ✎
>
> **Note** 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.

Network Requirements

- For optimal user experience when using Cisco Jabber over your corporate Wi-Fi network, we recommend that you:

    - 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 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.

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

    - Verify channel configurations do not overlap, 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:

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

- If you connect to the network remotely, the mobile device must be able to connect to the corporate network using a solid, high-bandwidth connection. Video and audio quality depends on connection quality and cannot be guaranteed.

> ✎
>
> **Note** For Jabber services and functions supported when connecting to Cisco Unified Communications Manager using Expressway for Mobile and Remote access, see the *Supported Services* section in the latest *Planning Guide for Cisco Jabber*.

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, you must 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 version 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 will be used based on LDAP configuration. **Note** from Cisco Jabber 11.7 if the LDAP ports are not configured, then LDAPS ports are used by default.				
	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 Cisco Webex Messenger service. The client sends XMPP through this port in cloud-based deployments only. If port 443 is blocked, the client falls back to port 5222.
	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 Premise 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	TCP	Far end camera control (FECC)
	5070 to 6070	BFCP	UDP	Binary Floor Control Protocol (BFCP) for video desktop sharing capabilities.
Voice/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.
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).
	443	HTTPS	TCP	Connects to Cisco Unity Connection for voicemail.
Cisco Webex Meetings				

Port	Application Layer Protocol	Transport Layer Protocol	Description
80	HTTP	TCP	Connects to Cisco Webex Meetings for meetings
443	HTTPS	TCP	Connects to Cisco Webex Meetings 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.

For information about port usage for Cisco Expressway for Mobile and Remote Access, see *Cisco Expressway IP Port Usage for Firewall Traversal*.

Supported Languages

Cisco Jabber for Android is localized for the following languages:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Croatian
- Danish
- Dutch
- English
- French
- German
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Portuguese (Brazil)
- Romanian
- Russian
- Slovak
- Spanish

- Swedish

- Turkish

Limitations and Restrictions

Limitations

The following limitations apply to all devices:

- 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.

- Jabber for Android can't start video calls from your Chromebook if another app is using the camera.

- Because of a limitation of Cisco Unity Connection, the voicemail server cannot display the URI for a missed call. This issue occurs if you decline an incoming Cisco Jabber call that was placed from a URI, and then that caller is diverted to voicemail. If the caller's contact information contains only a URI, the voicemail server displays the caller as Unknown. If the contact information contains a URI and a directory number, the voicemail server displays the directory number for that contact.

- If you play music with a third-party application in the background, and make or receive a Cisco Jabber for Android video call, the music does not pause or resume after the video call ends. To work around this issue, you can open the third-party application to pause or resume the music.

- If you make a Cisco Jabber for Android call using Expressway for Mobile and Remote Access over a 2G, 3G, or 4G network, you may experience audio quality issues.

- If you use Cisco AnyConnect Secure Mobility Client, MobilePASS one-time password generator from SafeNet, and Cisco Jabber for Android on the same device, you may experience problems due to compatibility issues between these applications. For example, during a Cisco Jabber for Android call, you may hear no audio or one-way audio, or you may experience delays if you transfer the call.

- Some users who have migrated to Common Identity server have an issue signing into Cisco Jabber. These users receive an "Incorrect username or password" error message when they enter their username and password. To resolve the issue, see this troubleshooting article.

- Notifications are not supported on Android Wear devices in Jabber team messaging mode.

- Contact Resolution for Enterprise Groups—Jabber resolves contacts in enterprise groups individually rather than all at once. As a result, when you add an enterprise group to your users' contact lists—or if they clear their local cache—they'll only see the username and domain for each person until they hover over or interact with them.

- Creating and Configuring Devices for Users in Cisco Unified Communications Manager 11.0—If you are creating devices for users in Cisco Unified Communications Manager 11.0, you can now specify a key order as RSA Only, EC Only, EC Preferred, or RSA Backup. However, the EC Only option is not currently supported by Cisco Jabber, and if you select it, the client fails to connect to the server.

- In a Mobile and Remote Access non-SSO environment, when Jabber loses its connection to the Cisco VCS Expressway server there is an interval of 120 seconds between sending connection requests. This is to prevent multiple requests to the server from multiple clients. During this 120-seconds interval, even if your network connection is active, Jabber remains inactive.

- There is 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

- In Samsung devices, when you install Jabber for the first time, Jabber is put in the unmonitored apps list automatically, which means it won't be put to sleep while running in the background. However, if you upgrade your Samsung OS from a version without unmonitored apps list, then you have to add Jabber to the unmonitored apps list manually.

- For Cisco TelePresence Video Communication Server Control (VCS) versions earlier than 8.10.X, you need to configure the editable inbound rules to enable the single number reach for users who are using Cisco Jabber over Mobile and Remote Access. For more information, see *Limitations* in *Enable Single Number Reach* section from the *Feature Configuration Guide for Cisco Jabber 12.0*.

- If your users have issues with signing into Cisco Jabber in SSO mode, they can upgrade Android System WebView and Chrome browser to resolve the issue. Users can upgrade Android System WebView and Chrome browser from Google Play Store.

Restrictions

The following restrictions apply to all devices:

- HTTP basic SAML SSO authentication—Sign in fails when switching users with the **Reset Jabber** option. Reset Cisco Jabber, quit the application fully in the Android OS, and try again.

- Because of the large number of third-party applications that support the tel:// URI feature, we cannot guarantee interoperability of this feature on all third-party applications. In some third-party applications, this feature allows you to click a tel:// link and select Cisco Jabber for Android to call.

- When transferring a file, the filename cannot exceed 168 characters (including extension). If you attempt to send a file with a longer name, you are notified that you have exceeded 168 characters.

- Security Survivable Remote Site Telephony (SRST) is not supported in Cisco Jabber for Android Release 10.6.

- If the Cisco Unified Communications Manager version is 11.0 and later, and you don't accept an invalid certificate when prompted within 10 seconds, for some HTTPS connections, the function of your application may be affected. You may have some issues such as, not being able to download some configuration from the server, or not being able to connect to the phone service or the voicemail.

- Only for users on SSO account Jabber stops working if the Android Webview is reset, upgraded, or restarted.

- During file transfer, only files with JPEG file format are compressed.

- Cisco WebEx Meetings—If the meeting siteType is "ORION", then Cisco Jabber for Android cannot start WebEx Meeting over Expressway for Mobile and Remote Access network.

Caveats

Caveats describe unexpected behavior. The following sections describe how to obtain the latest information.

Bug Severity Levels

Known defects, or bugs, have a severity level that indicates the priority of the defect. These release notes include the following bug types:

- All severity level 1 or 2 bugs
- Significant severity level 3 bugs
- All customer-found bugs except severity level 6 enhancement requests

Severity Level	Description
1 Catastrophic	Reasonably common circumstances cause the entire system to fail, or a major subsystem to stop working, or other devices on the network to be disrupted. No workarounds exist.
2 Severe	Important functions are unusable and workarounds do not exist. Other functions and the rest of the network is operating normally.
3 Moderate	Failures occur in unusual circumstances, or minor features do not work at all, or other failures occur but low-impact workarounds exist. This is the highest level for documentation bugs.
4 Minor	Failures occur under very unusual circumstances, but operation essentially recovers without intervention. Users do not need to install any workarounds and performance impact is tolerable.
5 Cosmetic	Defects do not cause any detrimental effect on system functionality.
6 Enhancement	Requests for new functionality or feature improvements.

Search for Bugs

To search for bugs not listed here, use the Bug Search Tool.

Procedure

Step 1 To access the Bug Search Tool, go to https://tools.cisco.com/bugsearch/search.

Step 2 Sign in with your Cisco.com user ID and password.

Step 3 To look for information about a specific problem, enter the bug ID number in the **Search for** field, then press **Enter**. Alternatively, you can search by product and release.

Open Caveats in Release 12.1(1)

Identifier	Severity	Headline
CSCvk58492	3	Jabber doesn't update call history after a call is transferred.

Resolved Caveats in Release 12.1(1)

Identifier	Severity	Headline
CSCvj91469	3	Jabber unexpectedly closes when moving from Wi-Fi to a mobile network.
CSCvm59210	3	One-way audio issue for Android devices.
CSCvm59284	3	Voice services won't reconnect after a network change for Jabber via MRA.
CSCvm59364	3	Jabber unexpectedly closes when the computer is locked or goes to sleep.
CSCvm59374	3	A user who has joined a persistent chat room is missing from the persistent chat room roster.
CSCvm59398	3	Jabber unexpectedly closes when a room invitation is received.

Open Caveats in Release 12.1

Identifier	Severity	Headline
CSCvj58886	3	Jabber keeps Rollover Counter and SSRC of SRTP stream after transfer
CSCvj58890	3	Jabber keeps Rollover Counter and SSRC of SRTP stream after hold/resume
CSCvj91469	4	Jabber stops working when moving from WiFi to Mobile network

Resolved Caveats in Release 12.1

Identifier	Severity	Headline
CSCvj73868	3	No group chat notification when Jabber is in the background
CSCvj85823	3	Jabber for Android: E911 Notification popup fails over MRA
CSCvj92828	2	Unable to sign into Jabber
CSCvk26965	4	Searched contact disappears on transfer when using UDS