

Release Notes for Cisco Jabber for Android 12.5

First Published: 2018-11-29

Last Modified: 2019-01-29

What's New in Cisco Jabber for Android 12.5(1)

Resolved Caveats

This release provides fixes for a number of known issues. See the Resolved Caveats 12.5(1) section for a list of caveats fixed in this release.

What's New in Cisco Jabber for Android 12.5

Preview Features are now Fully Supported

With the release with *Cisco Unified Communications Manager Release 12.5(1)* and *Cisco Expressway for Mobile and Remote Access X12.5*, the following features are now fully supported in Jabber:

- **UC Manager Configuration Tool**—Move your configuration from the `jabber-config.xml` file into the UC Manager, using our new configuration tool to simplify Jabber deployment. This feature requires Cisco UC Manager 12.5.

For more information about how it works and how to use it, see the *Parameters Reference Guide for Cisco Jabber 12.5*.

- **SIP OAuth Support**—Jabber now supports the OAuth protocol to authorize Jabber clients to use secure tokens for RTP and SIP traffic. We've built on the OAuth support from previous releases by now allowing SIP traffic to be encrypted. You set up SIP OAuth on the Cisco Unified Communications Manager. This feature requires UC Manager 12.5.

For more information, see the *Planning Guide for Cisco Jabber 12.5*. To set up SIP OAuth, see the [Feature Configuration Guide for Cisco Unified Communications Manager, Release 12.5\(1\)](#).

- **ICE Media Support**—Improve user experience when on the Expressway for Mobile and Remote Access. Clients that are outside the corporate network can use the ICE protocol to share media directly with each other. This feature requires Cisco Expressway X12.5.

To find out more about how ICE media works, see the *Planning Guide for Cisco Jabber 12.5*. To set up ICE media, see the [Mobile and Remote Access via Expressway Deployment Guide X12.5 and later](#).

Better Calling Experience

- **ActiveControl**—ActiveControl provides enhanced conferencing features to Cisco Jabber, like the ability to choose the video layout, record the call, mute and unmute yourself and others, and locking the conference call. You set up ActiveControl in Cisco Meeting Server (CMS) 2.3 or later and need Cisco

Unified Communications Manager 10.5 or later. We've put more information in the *Features Guide for Cisco Jabber 12.5* about how to set it up.

- **Disable Phone Services**—We've added a setting that lets you turn off Jabber's phone services without disabling chat or presence.

Easier Client Configuration

- **Common Criteria**—You can now run Jabber for Android in Common Criteria mode, which ensures that the environment is compliant with Common Criteria requirements. You turn on Common Criteria mode by using the `CC_mode=true` parameter in your EMM. For more information, see *Common Criteria* in the *Planning Guide for Cisco Jabber 12.5*.

Mobile Management and Headsets

- **New Android Device Support**—We've added new Android devices that you can use Jabber on.
- **Easier Sign In**—You can pre-define a user on a mobile device using the `LastLoadedUserProfile` parameter in your Enterprise Mobility Management, so that the user only needs to enter their password to sign in to the device. More information about this parameter is in the *On-Premises Deployment Guide for Cisco Jabber 12.5* or *Cloud Deployment Guide for Cisco Jabber 12.5*.

Enhancements

- **New User Experience**—Jabber looks even better now, with updated icons and a better layout.
- **Show Original Number**—We've improved how call forwarding works, so that when you've got it turned on, it will show both the number that's forwarding your call and the original caller's number.

Requirements

Cisco Jabber Requirements

Many Cisco Jabber requirements are common between client types. Client specific requirements are documented in the *Release Notes*, all other requirements are documented in the *Planning Guide for Cisco Jabber*.

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.

Hardware Requirements for Cisco Jabber for Android

Minimum requirements for Android devices

Android Operating System	CPU	Display
4.4 or later Important Minimum operating system version will be 5.0 in the next major Cisco Jabber release.	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 now supports Full UC mode in the following new devices with respective version of Operating System provided in the table:

Table 1: Supported Devices

Device	Device Model	Minimum Android Operating System version	Notes
BlackBerry	Priv	5.1	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	4.4.2	
	Arrows M357	6.0.1	
	Arrows M555	4.4.2	

Device	Device Model	Minimum Android Operating System version	Notes
Google Nexus	4	5.1.1	
	5	4.4	
	5X	6.0	
	6	5.0.2	
	6P	6.0	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	4.4	
	9	5.0.2	
	10	4.4	
	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 mobile device to a headset, then there might be some issues with the audio for few seconds.
	Pixel 2 XL	8.0	During a Jabber call if the user switches audio from mobile device to a headset, then there might be some issues with the audio for few seconds.
Honeywell Dolphin	CT50	4.4.4	

Device	Device Model	Minimum Android Operating System version	Notes
HTC	10	6.0	
	A9	6.0	
	E9 PLUS	5.0.2	
	M7	4.4.2	
	M8	4.4	
	M9	5.0	
	One Max	4.4	
	X9	6.0	

Device	Device Model	Minimum Android Operating System version	Notes
Huawei	G6	4.4	• 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	5.0	
	M2	5.0	
	Mate 7	4.4	
	Mate 8	6.0	
	Mate 9	6.0	
	Nova	7.0	
	Mate 10	8.0	
	Mate 10 Pro	8.0	
	P8	4.4.4	
	P9	6.0	
	P10	7.0	
	P10 Plus	7.0	
	P20	8.1	
	P20 Pro	8.1	

Device	Device Model	Minimum Android Operating System version	Notes
LG	G2	4.4	
	G3	4.4	
	G4	5.1	
	G5	6.0	
	G6	7.0	
	Optimus G Pro	4.4	
	V10	5.0	
	V30	8.0	
Motorola	MC40	4.4	Cisco Jabber supports only audio mode with MC40 device. Cisco Jabber does not support launching Webex Meetings from MC40 device.
	Moto G	4.4	
	Moto X	5.0	
	Moto Z Droid	6.0	
OnePlus	One	5.0	
	5	8.0	
	5T	8.0	
Panasonic	Toughpad FZ-X1	4.4	Contact your administrator to set your Jabber phone service to be secure. Jabber plays ringback tone and busy tone at 24kHz.

Device	Device Model	Minimum Android Operating System version	Notes
Samsung	All	4.4	- 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.
Smartisan	M1L	6.0.1	
Sonim	XP7	4.4.4	

Device	Device Model	Minimum Android Operating System version	Notes
Sony Xperia	M2	4.4	
	XZ	7.0	
	XZ1	8.0	
	XZ2	8.0	
	Z1	4.4	
	Z2	4.4.2	
	Z2 tablet	4.4.2	
	Z3	4.4.2	Sony Xperia Z3 (Model SO-01G) with Android OS 5.0.2 has poor audio on Jabber calls.
	Z3 Tablet Compact	4.4.4	
	Z3+/Z4	5.0.2	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	5.0	
	Z5 Premium and Z5	5.0.2	
	ZR/A	4.4	There is a limitation that Sony devices with Android OS 6.0 cannot play voicemail in Jabber.

Device	Device Model	Minimum Android Operating System version	Notes
Xiaomi	4C	5.1	
	MAX	5.1	
	Mi 4	4.4	
	Mi 5	6.0	
	Mi 5s	7.0	
	Mi 6	7.0	
	Mi Note	4.4.4	
	Mi Note 2	7.0	
	Mi Pad	4.4.4	
	Mi Pad 2	5.1	
	Mi MIX 2	8.0	
	Mi A1	8.0	
	Redmi 3	5.1	
	Redmi Note 3	5.1	
	Redmi Note 4X	6.0.1	
	Redmi Note 5	8.0	
Zebra	MC67	4.4.4	For Jabber IM-only mode, and audio-only mode. Video is not supported.
	TC70	4.4.3	TC70 devices 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.
	TC51	6.0	

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	Dependencies
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	Dependencies
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
- Fossil Gen 3 SmartWatch
- 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
- Google Pixelbook
- Asus C302

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](#).

Limitations and Restrictions

Limitations

- The following limitations apply to all devices:
 - Jabber will always display notifications for invalid certificates on Android 7.0 and later, even installed custom CA-signed certificates on the Android OS. This is because 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](#).
- 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.

Severity Level	Description
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.
-

Resolved Caveats in Release 12.5(1)

Identifier	Severity	Headline
CSCvo15426	2	Jabber on mobile 12.5 over MRA dropping calls randomly.
CSCvo04958	3	Jabber for Android imports native contact list inappropriately.
CSCvo12675	3	Jabber 12.5 DTMF RTP packets with incorrect timestamp.

Resolved Caveats in Release 12.5

Identifier	Severity	Headline
CSCvm92740	3	One way audio issue for Android device (SONY xz2, xz2 compact, xz3).
CSCvk58492	3	Jabber for Android doesn't update call history after transferring the call.
CSCvm83575	3	Jabber for Android fails to load the native contact list and eventually goes stuck on Jabber.
CSCvk48704	3	Jabber for Android user authentication with IM&P does not time out.
CSCvj91469	3	J4A crashing when moving from wifi to Mobile network.

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.

Open Caveats in Release 12.5

Identifier	Severity	Headline
CSCvn40864	3	J4A Regression ChromeBook Crash] crash when taking photo then answer a video call.

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

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

© 2019 Cisco Systems, Inc. All rights reserved.