Cisco Jabber for Android 11.0.x and 11.1.x Release Notes

First Published: June 24, 2015

Last Modified: July 28, 2015

Introduction

These release notes describe new features, requirements, restrictions, and caveats for all versions of Cisco Jabber for Android Release 11.0 and 11.1. These release notes are updated for every maintenance release but not for patches or hot fixes. Before you install Cisco Jabber for Android, we recommend that you review this document for information about issues that may affect your system.

New and Changed Features in Release 11.1

Calling Features

- **Jabber to Jabber Calling—**Jabber to Jabber calling provides basic voice and video calling feature between different Jabber clients without registering to Cisco Unified Communications Manager. Jabber to Jabber calling is supported to users who have access to the Cisco WebEx Messenger service. This calling feature supports calling only one contact at a time.

  Jabber to Jabber calling feature allows users to:

  - Make a Jabber to Jabber call
  - Answer a Jabber to Jabber call
  - End a Jabber to Jabber call
  - Mute or unmute the audio
  - Start or stop the video
  - Volume control
  - Open, close, or move the self-video
  - Switch to front or back camera

  Before you enable the Jabber to Jabber calling feature, contact the Cisco Customer Support team or your Cisco Customer Success Manager for the following:

  - ◦ To request that your organization be added to the Cisco Common Identity server. This process to add users to the Common Identity server takes some time to complete and it is necessary to access Jabber to Jabber calling capabilities.

    - For Single Sign On (SSO) users, there are additional steps to perform to ensure that SSO setup is completed successfully for your organization.

  For information on Jabber to Jabber call feature, see *Jabber to Jabber Call* section from the *Cisco Jabber 11.0 Deployment and Installation Guide*.

- **User can Set Android Device Default Ringtones for Incoming Cisco Jabber Calls—**Cisco Jabber allows user to use Cisco ringtone or Android device native ringtones for incoming calls.

  For more information, see *Cisco Jabber for Android 11.0 User Guide*.

Chat and Presence Features

More Emoticons Available for Chatting—Cisco Jabber provides more emoticons for users to use during the chat session.

Contact Features

Administrator can Configure to Swap the Display Name of the Contacts—Administrator can configure SwapDisplayNameOrder parameter in the `jabber-config.xml` file to set the display name of the contacts in either Lastname, Firstname or Firstname, Lastname format based on the locale configuration on the device. For more information, see *Client Parameter* section from the *Cisco Jabber 11.0 Parameters Reference Guide*.

Security Features

Encrypted Problem Report—Cisco Jabber supports encrypting and decrypting content in the problem reports for security. Administrator can configure the parameters EnablePRTEncription and PRTCertificateUrl to enable encrypting problem report. Administrator can define the HTTPS URL to download the certificate required for encrypting problem report.

For example, you can define a URL, `https://<web server address>/cert.pem`. For more information on configuring these parameters, see *Client Parameters* section in the *Cisco Jabber 11.0 Parameters Reference Guide*.

Note Once the Administrator encrypts the problem report with a specific certificate, the Cisco Customer Support team cannot receive the log from the problem report unless the Administrator decrypts the problem report.

User Experience Enhancement

- **Cisco Jabber Notifications on Android Wearable Devices—**Cisco Jabber allows users to view chat history and notifications like incoming instant messages, incoming calls, and voice messages from their Android wearable devices.
- **Reply through the Instant Messages from Android Wearable Devices—**Cisco Jabber allows users to reply through instant messages when there is an incoming call notification in Android wearable devices.

Documentation Improvements

- **Help Central knowledge base—**This knowledge base contains end-user documentation for Cisco Jabber for Android, which includes videos, getting started content, and new features. For more information, see knowledge base.

- **Cisco Jabber 11.0 Parameter Reference Guide—**This document is introduced in this release, which includes the list of group elements and parameters that are used to configure the features on Cisco Jabber client. For more information, see cisco.com.

New and Changed Features in Release 11.0.1

Calling Features

Silent Monitoring and Call Recording (Built-in Bridge) — In 11.0.1 Cisco Jabber for Android supports silent monitoring and call recording using Cisco Unified Communications Manager 10.5(2) su2 and later releases.

Stability Improvements

For the stability improvements in this release, see Resolved Caveats in Release 11.0.1, on page 23.

Required COP Files for Cisco Unified Communications Manager 11.0 and later

Required COP files for Cisco Unified Communications Manager 11.0 and later are:

- cmterm-android-install-141 122.k3.cop.sgn
- cmterm-jabbertablet-install-141 122.k3.cop.sgn

You can download these files from cisco.com

New and Changed Features in Release 11.0

New Features

Calling Features

- **Silent Monitoring and Call Recording (Built-in Bridge)** — Cisco Jabber for Android supports silent monitoring and call recording that can be used by company supervisors to monitor or record calls. This feature is only supported with Cisco Unified Communications Manager 11.0 or later releases.
- **Far End Camera Control** — You can direct cameras on the other end of video calls and control video display on participant screens using Cisco Jabber. A control panel is displayed on the video window that you can use to turn the far end camera to left, right, top, or down and to zoom in or zoom out. The FECC feature is supported on both smartphones and tablets. You can use FECC panel to change the layout for conference call.
- **G.722 Codec** — Support for the G.722 audio codec to enhance voice communication for VoIP calls. This wideband audio codec is a default codec for calls to Cisco IP deskphones and other portfolio endpoints, which delivers a superior call experience to the user.
- **Opus Codec** — Support for the Opus audio codec. You require Cisco Unified Communications Manager 11.0 to use Opus.

- **Click-to-Call: URI handler —** Support for a new call scheme, “Click-to-Call”. You can use the URI handler with clicktocall protocol followed by a contact's phone number or SIP URI address on a web browser or other applications to make a call. You can start a call by tapping on the URI link.
- **Flexible Differentiated Services Code Point (DSCP) —** Administrators can use flexible DSCP to set DSCP to assign different priorities to audio and video streams.
- **Define separate Port Range —** Administrators can set separate port ranges for audio and video on the SIP profile.
- **Collaboration Meeting Room (CMR) Conference —** Within a group chat you can escalate an IM conversation to audio and video conference using Cisco Cloud Collaboration Meeting Rooms (CMR).
- **WebEx Personal Room Conference —** Within a group chat you can escalate an IM conversation to audio and video conference using Cisco WebEx Personal Room.
- **Dual Tone Multi Frequency (DTMF) Digit Management—** The following enhancements are made for the DTMF digits:
    - When on a call, you can cut and paste DTMF digits such as a meeting PIN or phone number into the keypad. The valid DTMF digits are: 0123456789,*#ABCD.
    - You can enter a number with DTMF digits in the search bar or keypad, and make a call instead of typing the digits.
    - You can add DTMF digits with protocol handlers to create links that participants can use to access meetings.

Chat and Presence Features

- **Enterprise Groups (AD Groups) —** You can add a directory group to your Cisco Jabber for Android contacts from the Microsoft Active Directory (AD) groups in your enterprise. Since the group is maintained in your corporate directory, your client contact list is updated dynamically to synchronize with the enterprise group. Only first level contacts are added to the enterprise group. If a group contains more than 100 people, then no presence is displayed for those contacts. To add enterprise groups you require Cisco Unified Communications Manager IM & Presence Service 11.0.
- **Telephony and Chat URIs in Chat Window —** You can initiate chats and calls from a chat window by tapping on the telephony and chat URIs.
- **Publish Location Information —** You can add your location information on Cisco Jabber for Android for your contacts to see. To enable the location feature administrators must configure the Location_Enabled parameter.
- **Start Group Chat —** You can start a group chat with two or more contacts. You can invite participants for a group chat and add the topic for group chat.
- **Contact Group Management —** You can manage your contact groups by adding or removing the groups.
- **Administrative Control for Showing Offline Contacts —** Administrative control to show or hide the offline contacts on your contacts list is available. To show the offline contacts administrators must configure the ShowOfflineContacts parameter.

Security Features

Enhanced Security — Cisco Jabber provides a more secured solution for credentials and adds the administrative control to manage invalid certificate policies.

Deployment Features

- **Configuration Support with Android for Work —** Cisco Jabber for Android supports pre-configuring the application based on the "Android for Work" mechanism. With this feature, the company administrators can deploy and pre-configure Cisco Jabber for Android for an entire company through some of the Enterprise Mobility Management providers. This feature is only supported on Android mobile devices with Android OS version 5.0 or later. Cisco has tested the solution with Airwatch Mobile Device Management.
- **Customer Community Program (CCP) Community Based Wrapping Support for Cisco Mobile Application Management —** Cisco provides a private App Wrapping program for supported Enterprise Mobility Management providers through the CCP (previously known as Cisco User Group) community. If users want to wrap the Cisco Jabber and distribute it through the Mobile Device Management (MDM) or Mobile Application Management (MAM), they can get support from the CCP community.
- **Client Based Certificate Authentication for Single Sign On (SSO) —** Cisco Jabber supports the client based certificate authentication for SSO with WebEx Messenger Deployment. This feature is only supported on Android mobile devices with Android OS version 5.0 or later.
- **Auto-Proxy in DX phones using PAC file —** Support for connecting to Cisco WebEx Messenger server with auto-proxy settings using (Proxy Auto-Configuration) PAC file in DX650, DX70 and DX80 running on Cisco DX phone load 10.2.x.
- **Auto-Proxy in Android devices —** Support for auto-proxy settings using (Proxy Auto-Configuration) PAC file on smartphones and tablets with Android OS 5.0.

  > **Note** Cisco Jabber only supports proxy for HTTP requests using HTTP CONNECT, but does not support HTTPS CONNECT using proxy.

- **Availability on Google Play for Cisco DX phones —** Cisco Jabber for Android is available on Google Play for Cisco DX devices. Cisco Jabber for Android is preloaded in the phone load of the Cisco DX devices, users can still install or upgrade to the latest version of Cisco Jabber for Android on their Cisco DX devices from Google Play.
- **Force to register the Android device with TAB device —** Cisco Jabber for Android supports registering the Android device with TAB device in Cisco Unified Communication Manager manually. For example, you can register the Android tablet, which has the cellular call capability with TAB device to use the Android tablet and the Android smartphone at the same time. You can perform this operation using **Advanced Settings** option, which is available at the login page of Cisco Jabber.

User Experience Enhancement

Option to Display Cisco Jabber Availability in the Notification Center — You can control whether to display the availability of Cisco Jabber in the notification center or not by configuring the settings in Cisco Jabber.

Option to Mute or Stop Vibration during an Active Call — You can control whether to mute or stop vibration for the notifications during an active Cisco Jabber call.

Escalation Options when Selecting a Contact in the Contact List through Long Press — You have more escalation options when you press and hold on a contact or any group of contacts in the contact list. Some of the escalation options are starting an IM chat, a group chat, or a Cisco WebEx Meeting.

Indicator in the Chat tab for unsent message — Cisco Jabber displays a draft indicator for each IM session in the **Chat** tab, if there is an unsent chat message in the chat session. Cisco Jabber stores the unsent chat message for you until you send the message.

Hardware

- **Extended Device Support —** The supported device list includes 11 new devices. For the list of supported devices, refer to the Device Requirements section.

Requirements

Software Requirements

Services

Install the COP file `cmterm-android-install-141122.cop.sgn` for Android phones and the COP file `cmterm-jabbertablet-install-141122.cop.sgn` for Android tablet, if you support the following services:

- Secure Phone (Mixed Mode Security) — On Cisco Unified Communications Manager up to Release 9.1(2).
- Share Line and Graceful Registration under DvO — On Cisco Unified Communications Manager up to Release 10.5(1).
- Group Configuration (Cisco Supported Field) — On Cisco Unified Communications Manager up to Release 10.5(2).

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	8.6(2)* and later
	Cisco WebEx Messenger	
Telephony	Cisco Unified Communications Manager	8.6(2)* and later
	Cisco Unified Survivable Remote Site Telephony	8.5 and later

Service	Software Requirement	Supported Version
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)	9.1(2) and later For 9.1(2), use the following COP file: cmterm-cucm-uds-912-5.cop.sgn
Voicemail	Cisco Unity Connection	8.6(2)* and later
Conferencing	Cisco TelePresence Server	3.1 and later
	Cisco TelePresence MCU	4.3 and later
	Cisco ISR PVDM3	Cisco Unified Communications Manager 8.6(2)* and later
	Cloud CMR	Cisco WebEx Meetings Server with Collaboration Meeting Room
	Cisco WebEx Meetings Server	2.0 and later Cisco Jabber for Windows supports 1.5 and later
	Cisco WebEx Meeting Center	T28 and later
	Cisco WebEx Meetings Client	4.5 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	4.0.01287 and above For more information, refer to the Remote Access section.
	Cisco Expressway C	8.1.1
	Cisco Expressway E	8.1.1

For FIPS compliance, you can use version 8.6(1).

Accessibility

Screen Readers

Cisco Jabber for Android is compatible with the TalkBack screen reader.

Assistive Touch

You can navigate Cisco Jabber for Android using Explore by Touch.

Device Requirements

Cisco Jabber for Android supports Audio and Video Enabled mode in the following devices with respective version of Operating System provided in the table:

Device	Device Model	Operating System
Cisco DX	70	10.2.x version
	80	10.2.x version
	650	10.2.x version
HTC	One M7	Android OS 4.4.2 or later
	One M8	Android OS 4.4.2 or later
	One Max	Android OS 4.4.2 or later
Google Nexus	5	Android OS 4.4 or later
	6	Android OS 5.0.2 or later
	7	Android OS 4.4 or later
	9	Android OS 5.0.2 or later
	10	Android OS 4.4 or later
LG	G2	Android OS 4.2.2 or later
	G3	Android OS 4.4.2 or later
Motorola	Moto G	Android OS 4.4.2 or later
	Moto MC40	Android OS 4.1.1[1]

Device	Device Model	Operating System
Samsung Galaxy	Note II	Android OS 4.2 or later
	Note III	Android OS 4.3 or later
	Note IV	Android OS 4.4.4 or later
	Note Edge	Android OS 4.4.4 or later
	Note Pro 12.2	Android OS 4.4.2 or later
	Rugby Pro	Android OS 4.2.2 or later
	SII	Android OS 4.1.2 or later
	SIII	Android OS 4.2.2 or later
	S4	Android OS 4.2.2 or later
	S4 mini	Android OS 4.2.2 or later
	S5	Android OS 4.2.2 or later
	S5 mini	Android OS 4.2.2 or later
	Tab 3 8-inch	Android OS 4.4 or later
	S6	Android OS 5.0.2 or later
	S6 Edge	Android OS 5.0.2 or later
	Tab 4 7-inch, 8-inch, and 10.1-inch	Android OS 4.4.2 or later
	Tab PRO 8.4-inch and 10.1-inch	Android OS 4.4.2 or later
	Tab S 8.4-inch & 10.5-inch	Android OS 4.4.2 or later
	Note 10.1-inch 2014 Edition	Android OS 4.4.2 or later

Device	Device Model	Operating System
Sony Xperia	M2	Android OS 4.3 or later
	Z1	Android OS 4.2 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
	ZR/A	Android OS 4.1.2 or later
	Z3 Tablet Compact	Android OS 4.4.4 or later
Huawei Ascend	G6	Android OS 4.2.2 or later
	Mate 7	Android OS 4.4 or later
Sonim	XP7	Android OS 4.4.4
Xiaomi	4	Android OS 4.4 or later

[1] Cisco Jabber supports only audio mode with Moto MC40 device.

Note Cisco Jabber for Android is tested with the Android devices listed above. Although other Android devices are not officially supported, you might be able to use Cisco Jabber for Android on other Android devices.

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

- Chipset — Android devices that are based on an Intel chipset are not supported.
- 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.

Note

- Cisco Jabber for Android does not support the 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 chapter of the *Cisco Jabber for Android User Guide*.

Cisco Jabber for Android supports IM only mode on the Android devices that meet the following minimum specifications:

- Chipset — Android devices that are based on an Intel chipset are not supported.

- Android OS — 4.1.2 or higher
- CPU — 1.5 GHz dual-core, 1.2 GHz quad-core or higher (quad-core recommended).
- Display — 320 x 480 or higher

Bluetooth Device Support

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

- Plantronics Voyager Legend
- Plantronics Voyager Legend UC
- Plantronics Voyager edge UC
- Plantronics Voyager edge
- Jabra Motion
- Jawbone ICON for Cisco Bluetooth Headset

  If you use a Samsung Galaxy S4, you can experience problems due to compatibility issues between these devices.
- Plantronics BackBeat 903+

  If you use a Samsung Galaxy S4, you can experience problems due to compatibility issues between these devices.
- Jabra Wave+
- Jabra Biz 2400
- Jabra Easygo
- Jabra PRO 9470
- Jabra Speak 510
- Jabra Supreme UC
- Jabra Stealth
- Jabra Evolve 65 UC Stereo

Using a Bluetooth device for Samsung Galaxy SIII can cause distorted ringtone and call audio.

Remote Access

You can configure remote access using either a VPN or Expressway for Mobile and Remote Access. If you configure Expressway for Mobile and Remote Access, there is no need to configure VPN access. To connect with VPN, use the relevant version of Cisco AnyConnect, available from the Google Play Store.

- Cisco AnyConnect Secure Mobility Client
- Samsung AnyConnect — For Samsung devices running Android OS 4.4.x, use Samsung AnyConnect version 4.0.01128 or later.
- For Android OS version above 5.0, you must use ICS+ software version later than 4.0.01287.

Network Requirements

If you deploy Phone Services, the mobile device must be able to connect to the corporate network.

- 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.
- Bluetooth use can cause voice quality and connectivity issues.
- 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 is dependent on connection quality and cannot be guaranteed.

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.

Note There are no TCP/IP services enabled in the client.

Port	Application Layer Protocol	Transport Layer Protocol	Description
Inbound			
16384 to 32766	RTP	UDP	Receives Real-Time Transport Protocol (RTP) media streams for audio and video. You set these ports in Cisco Unified Communications Manager.
Outbound			
69	TFTP	UDP	Connects to the Trivial File Transfer Protocol (TFTP) server.
6970	HTTP	TCP	Connects to the TFTP server to download client configuration files.
80	HTTP	TCP	Connects to services such as Cisco WebEx Meeting Center for meetings or Cisco Unity Connection for voicemail.
389	LDAP	TCP (UDP)	Connects to an LDAP directory service.
3268	LDAP	TCP	Connects to a Global Catalog server for contact searches.
443	HTTPS	TCP	Connects to services such as Cisco WebEx Meeting Center for meetings or Cisco Unity Connection for voicemail.
636	LDAPS	TCP	Connects securely to an LDAP directory service.
3269	LDAPS	TCP	Connects securely to the Global Catalog server.
5060	SIP	TCP	Provides Session Initiation Protocol (SIP) call signaling.
5061	SIP over TLS	TCP	Provides secure SIP call signaling.
5222	XMPP	TCP	Connects to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service for instant messaging and presence.
5269	XMPP	TCP	XMPP federation.
8191	SOAP	TCP	Connects to the local port to provide Simple Object Access Protocol (SOAP) web services.

Port	Application Layer Protocol	Transport Layer Protocol	Description
8443	HTTPS	TCP	8443 is the port for 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.
16384 to 32766	RTP	UDP	Sends RTP media streams for audio and video.
53	DNS	UDP	Provides hostname resolution.
3804	CAPF	TCP	Issues Locally Significant Certificates (LSC) to IP phones. This is the listening port for Cisco Unified Communications Manager Certificate Authority Proxy Function (CAPF) enrollment.

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:
    - 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.
    - If you use Cisco Samsung AnyConnect Secure Mobility Client, use a version later than 4.0.01128. Earlier versions may cause connection problems.
    - If you want to use Cisco Jabber to initiate a Cisco WebEx meeting, you must install the Cisco Webex meeting client before installing Cisco Jabber for Android.
    - 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 knowledge base article.
- The following limitations apply to Android OS 4.0 and later:
    - Because of a limitation of Android OS 4.0 and later, Cisco Jabber cannot register to Cisco Unified Communications Manager on some devices. Cisco is working with select device manufacturers to resolve this issue at the Android OS level.

  - Because of a limitation with Android OS 4.1.2 and later on some devices, you may experience issues if you perform the following steps:

    1. Make a call from the native Android phone application.
    2. Select **Jabber** (or another voice application) from the dialog box.
    3. Select **Always** to indicate that you always want to use Cisco Jabber (or another voice application) to make calls.

    After you complete these steps, the native Android phone application no longer shows you the dialog box that allows you to select another voice application. Instead, you can only make calls through the native Android Phone application.

- Bluetooth limitations:

  - ◦ Because of a limitation with certain mobile carriers, if a user resumes an active Cisco Jabber VoIP call that was interrupted by an incoming mobile voice call to the device, and then the user tries to power on and use a Bluetooth audio device, the Bluetooth device cannot receive audio.
  - ◦ Switching between Bluetooth and other audio devices such as the device speaker, earphones, or a headset is supported only on Android OS 4.2.2 and above.
  - ◦ Because of a limitation of the Android OS, Cisco Jabber for Android does not support answering or ending calls with the **Talk** button on a Bluetooth headset. To work around this issue, answer and end your Cisco Jabber for Android calls using the Cisco Jabber user interface.
  - ◦ Because of a limitation of the Android OS, incoming call ringtone cannot be played to both the device speaker and a Bluetooth audio device.
  - ◦ If you use a Samsung Galaxy S4 with either Jawbone ICON for Cisco Bluetooth Headset or Plantronics BackBeat 903+, you may experience problems due to compatibility issues between these devices.
  - ◦ Using a Bluetooth device on a Samsung Galaxy SIII may cause distorted ringtone and distorted call audio.
  - ◦ 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.
  - ◦ 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.
  - ◦ Users using Nexus phones with Bluetooth Headset cannot listen to Voicemails.

- Phone Services mode users with more than 2,000 local contacts may experience performance issues when loading contacts from the native address book.
- If the administrator sets the parameter EnableLoadAddressBook to false, the native contacts are not loaded in the phone's address book.
- 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 Cisco DX Series Firmware Release 10.2(4)SR version, there are issues with sending files and problem report for the permission issue on Cisco DX device, it will be resolved in the next release.

Restrictions

The following restrictions apply to all devices:

- USE OF THE JABBER SOFTPHONE DURING AN EMERGENCY IS AT YOUR OWN RISK — The softphone technology may not provide sufficient voice quality or location data for emergency calls. Calls may be misdirected to the wrong emergency response center or the emergency response center may make errors when determining your location.
- If you are setting up Dial via Office - Reverse (DvO-R) on Cisco Unified Communications Manager consider the following:
  - The DvO-R feature only applies to Android phones.
  - The DVO-R feature requires Cisco Unified Communications Manager Release 8.6.2 SU4, 9.1.2, or 10.x.
  - DVO enabled devices may encounter issues registering with Cisco Unified Communications Manager. Resetting the device from the Cisco Unified Communications Manager administrative interface will fix this issue.
  - The DvO-R feature is not supported when users connect to the corporate network using Expressway for Mobile and Remote Access.
- When using Expressway for Mobile and Remote Access to connect to services from outside the corporate firewall, the client does not support:
  - LDAP for contact resolution — Instead, the client must use UDS for contact resolution.
  - Session persistency — The client cannot recover from disruptions caused by network transitions. For example, if you start a Cisco Jabber call inside the office and then walk outside the building and lose Wi-Fi connectivity, the call drops as the client switches to use Expressway for Mobile and Remote Access. Likewise, the call drops if the client switches from Expressway for Mobile and Remote Access to the office Wi-Fi network.
  - Cisco WebEx Meetings Server — When users use the Cisco WebEx Meetings Servers for meetings or the meeting siteType is “ORION”, the client cannot access the Cisco WebEx Meetings Server, and join or start on-premises Cisco WebEx meetings over Mobile and Remote Access (MRA).

    Note To use the WebEx meeting option in Cisco Jabber for Android, ensure that the meeting client is installed before installing Cisco Jabber for Android.

  - CAPF enrollment.
  - End-to-end media encryption — Media is not encrypted on the call path between the Cisco Expressway-C and devices that are registered locally to Cisco Unified Communications Manager.

    The **Device Security Mode** must be set to **Authenticated**. The client does not support media encryption with Expressway for Mobile and Remote Access when you set the **Device Security Mode** to **Encrypted**.

- In most cases, you can sign in to the client for the first time using Expressway for Mobile and Remote Access to connect to services from outside the corporate firewall. In the following cases, however, you must perform initial sign in while on the corporate network:
    - If the voice services domain is different from the services domain. In this case, you must be inside the corporate network to get the correct voice services domain from the jabber-config.xml file.
    - If Cisco Jabber needs to complete the CAPF enrollment process, which is required when using a secure or mixed mode cluster.
- Expressway for Mobile and Remote Access+SSO feature support is only for Cisco Unified Communications Manager 10.5(2)and VCS C/E version 8.5 and higher.
- HTTP basic SAML SSO authentication — Login 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 on a tel:// link and select Cisco Jabber for Android to place the call.
- Cisco Jabber for Android does not support downloading the app from Google Play with the following devices:
    - Android phones with Intel chipsets.
    - Android phones with screen resolution that is lower than 320 x 480.
- Cisco Jabber for Android supports graceful registration over Expressway for Mobile and Remote Access from Cisco Unified Communications Manager Release 10.5.(2) 10000-1.
- Advanced Encryption Standard (AES) 256 and TLS1.2 are only supported over corporate Wi-Fi, these are not supported over Expressway for Mobile and Remote Access.
- When transferring a file, the filename can not 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.
- We do not support first time login on a public network if using a secure phone via an Expressway for Mobile and Remote Access environment.

  If the configuration is for a secure profile with encrypted TFTP, then the first time login must be on-premises to allow CAPF enrolment to occur. This is not supported, and it cannot be supported without Cisco Unified Communications Manager, Expressway for Mobile and Remote Access, and Cisco Jabber enhancements.

  However we do support:
    - Encrypted TFTP, with first time login on-premises.
    - Unencrypted TFTP, with first time login via Expressway for Mobile and Remote Access or on-premises.
- If the Cisco Unified Communications Manager version is higher than 11.0, and you do not accept the certification when prompted within 10 seconds (if the server has an invalid certificate), 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.

Android Version Support Policy for Cisco Jabber for Android

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:
    - HTC One M8 (Android OS 4.4.2 or later)
    - HTC One M7 (Android OS 4.4.2 or later)
    - HTC One Max (Android OS 4.4.2 or later)
    - Sony Xperia M2 (Android OS 4.3 or later)
    - Sony Xperia Z1 (Android OS 4.2 or later)
    - Sony Xperia ZR/A (Android OS 4.1.2 or later)
    - Sony Xperia Z2 (Android OS 4.4.2 or later)
    - Sony Xperia Z2 tablet (Android OS 4.4.2 or later)
    - Sony Xperia Z3 (Android OS 4.4.2 or later)
    - Sony Xperia Z3 Tablet Compact (Android OS 4.4.4 or later)
    - Huawei Ascend G6 (Android OS 4.2.2 or later)
    - Huawei Ascend Mate 7 (Android OS 4.4 or later)
    - Sonim XP7 (Android OS 4.4.4)
    - Xiaomi 4 (Android OS 4.4 or later)

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.

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 11.1

Identifier	Severity	Headline
CSCuw08191	3	Cisco Jabber cannot end the audio call even after disconnecting the call.
CSCuw21062	3	The file that is transferred in the AFT mode is deleted when the user switches the network in the phone.

Identifier	Severity	Headline
CSCuw08630	3	There is only one-way video displayed under 4G hotspot Wi-Fi through Expressway for Mobile and Remote Access.
CSCuw21243	4	Jabber to Jabber call displays work number in call view.
CSCuw21266	3	Cannot enable Multi-device Messaging (MDM) through provisioned URL
CSCuw23307	3	Jabber Call option is not available sometimes with Expressway for Mobile and Remote Access.

Closed Caveats in Release 11.1

There are no closed caveats in this release.

Resolved Caveats in Release 11.1

Identifier	Severity	Headline
CSCuv32470	3	Unable to access audio or video call after the Cisco Jabber is idle for 20 minutes.
CSCuv32575	2	Unable to see instant messages if the user has enabled Advanced Encryption Standard (AES) and Mobile Device Management (MDM).
CSCuv37167	3	Unable to make Jabber to Jabber call if the secure phone user reconnects VM account.
CSCuv54669	3	Cisco Jabber for Android 11.0.1 stops working while answering a call.
CSCuv37251	3	Unable to make Jabber to Jabber call after switching the network.
CSCuv32917	3	Cisco Jabber for Android stops working when a user tries to join the group chat.
CSCuv74866	3	Cisco Jabber for Android cannot connect over Mobile and Remote Access (MRA) when there are multiple non-clustered Cisco VCS setup.
CSCuu82286	3	Chat and search buddy status is not updated if a group has more than hundred members.
CSCuv78778	3	If a user has Cisco Jabber installed on Windows and Android device, and if the user makes a call from the Windows device, the Cisco Jabber for Android which is inactive will become active.
CSCuv36672	3	Cisco Jabber for Android missed call Information is incorrect.
CSCuv78781	3	Unable to connect to voicemail service.

Identifier	Severity	Headline
CSCuv39348	3	Cisco Jabber for Android video call stops working.
CSCuv39341	3	Cisco Jabber for Android does a service discovery even after the user accepts the certificates, and then deletes those accepted certificates, which is resulting in the certificate warning message.
CSCuv13114	3	During a Jabber to Jabber video call the user is not able to view the self-video.
CSCuw13570	3	Cannot join Cisco WebEx meeting invitation from Cisco DX80 on Cisco Jabber 11.0.
CSCuw02541	3	Self-view during a Cisco Jabber video call keeps flashing hide/show several times, and then Cisco Jabber does not respond.
CSCuv84669	3	Remote media parameters are not set properly.
CSCuv78822	3	Presence status of contacts does not update unless Cisco Jabber is active.
CSCuw11046	3	UDS Search with "ß" character is not possible for Cisco Unified Communications Manager (CUCM) 10.5.2.
CSCuw08239	3	Cisco Jabber cannot send video after disconnecting a Jabber to Jabber call and then resuming a Cisco Unified Communications Manager (CUCM) call.
CSCuw08738	3	Unable to make a Jabber to Jabber call using Cisco Jabber for Android.
CSCuw13682	3	Jabber to Jabber feature is not available after reconnecting on Expressway for Mobile and Remote Access.
CSCuw08378	3	Cisco Jabber sends video even when the mobile data network is disabled.
CSCuw25441	3	*Cisco Jabber 11.0 Planning Guide* and *Cisco Jabber 11.0 Deployment and Installation Guide* are updated with file transfer mechanism for mobile clients.

Open Caveats in Release 11.0.1

There are no open caveats in this release.

Closed Caveats in Release 11.0.1

There are no closed caveats in this release.

Resolved Caveats in Release 11.0.1

Identifier	Severity	Headline
CSCuu98444	3	Video call via alphashn fails after 10 minutes, and then Cisco Jabber restarts.
CSCuu83433	2	Issue with the evaluation of umc-android for OpenSSL June 2015.
CSCuv09248	3	Cisco Jabber does not display the incoming call when the device is on Restrict background data option or Sleep mode.
CSCuv14897	3	Cisco Jabber does not hide show token information.
CSCuv21045	3	Unable to access contact list in Cisco Jabber.
CSCuu69149	3	Voicemail stops working after starting a new session.
CSCuv21055	3	Cisco Jabber stops working when you enter the email address in login page.
CSCuv16758	3	The quality of the video sent over Cisco Jabber is low in new Android devices.
CSCuv21052	3	Cisco Jabber stops working.
CSCuv36697	3	Cisco Jabber saves user password after the user logs out.
CSCuv23785	3	Jabber stops working while switching network between Non-Corporate Wi-Fi and Mobile Data.
CSCuv41653	3	Voicemail does not reconnect automatically.
CSCuv45316	3	Cisco Jabber 11.0 cannot handle server redirection.

Open Caveats in Release 11.0

The following bugs have not yet been resolved.

Identifier	Severity	Headline
CSCuu69149	3	VM account token expired and displays new session but does not respond when tapped
CSCuu69150	3	Cisco Jabber does not reconnect to phone service after roaming from MRA
CSCuu92271	3	Phone service cannot connect when log in using SSO via Edge

Closed Caveats in Release 11.0

There are no plans to resolve the following bugs.

Identifier	Severity	Headline
CSCus07600	3	Self-video stops after switching from background to foreground
CSCus35847	3	IM reconnection caused by TP Error
CSCus54818	3	[DQ] 11.0 cannot start meeting on Sony Z3 Tablet
CSCut13520	3	Far End Camera Control not working under conference hosted by TP unit
CSCuu06041	3	Delay in ring back in Cisco Jabber for Android
CSCuu09599	3	JPN: Sony Xperia Z2 Z3 Tablet: cached files wrapped in three lines
CSCuu50375	4	Availability in a meeting is not updated when launching meeting client

Resolved Caveats in Release 11.0

Identifier	Severity	Headline
CSCus64062	3	Bluetooth audio stream is redirected when Cisco Jabber for Android is launched on a Motorola device
CSCut22048	3	Sometimes phone services do not connect even if the network is connected
CSCut52460	3	Only the calling name, no calling number or call type, appears in incoming calls
CSCut62403	3	Contacts are duplicated in Favorites when a contact is added to different groups
CSCut86602	3	Call information is not changed in incoming call during call transfer
CSCuu27976	3	Cisco Jabber stops working during video calls
CSCuu54460	3	If the first call is cancelled, the second one is also cancelled

Documentation Resources

The following documents are available for Cisco Jabber for Android:

- *Cisco Jabber for Android Release Notes* - Provide administrators with a summary of information about the release, which include feature enhancements, requirements, limitations and restrictions of the software, and caveats overview.
- *Cisco Jabber Deployment and Installation Guide* - Provides administrators with task-based information for all Cisco Jabber clients. It contains end-to-end client deployment procedures, deployment scenarios, workflows, infrastructure configuration of services, and client configuration and installation.
- *Cisco Jabber Planning Guide* - Provides administrators with background and reference material to plan the deployment and installation of all Cisco Jabber clients. This guide contains information that helps you make decisions about how you are going to deploy the product, such as a product overview, planning considerations, deployment information, and requirements.
- *Cisco Jabber for Android Licensing Information* - This Licensing information document provides information on the open source libraries used by the application.
- *Cisco Jabber for Android Quick Start Guide* - Instructions to help end users navigate around Cisco Jabber for Android for the first time and use a few key features.
- *Cisco Jabber for Android User Guide* - Provides an overview of task-based information about end user operation of the client, including accessibility information.
- *Cisco Jabber Parameter Reference Guide* - Provides list of group elements and parameters that are used to configure the features on Cisco Jabber client.

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.