Release Notes for Cisco Jabber for Android 12.7

First Published: 2019-09-09

Last Modified: 2021-01-21

What's New in Release 12.7(2)

Android 10 Support

We added support for Android 10.

Resolved Caveats

This release provides fixes for a number of known issues. See the Resolved Caveats 12.7(2) section for a list of caveats fixed in this release.

What's New in Release 12.7(1)

We created this maintenance release to meet a technical requirement in Google's upgrade policy. The build number is 12.7.1.300418.

This release makes no changes to the features or caveats that we delivered in Release 12.7(0).

What's New in Release 12.7

Improved User Experience

64-Bit Android Support

Cisco Jabber for Android now comes as a 32-bit app and a 64-bit app. If your Android device has a 64-bit OS, you get a faster and richer experience by running the 64-bit Jabber client. If you install or update Jabber from Google Play Store, you will automatically get the version that is best suited for your device.

Start Cellular Calls with Video

Administrators can control the default value of whether Jabber calls over cellular networks start with video with the new StartCallsWithVideoOverCellular parameter. When set to `false` (the default), calls over a cellular network start without video. When set to `true`, the calls start with video. For details, see the Parameters Reference Guide for Cisco Jabber.

Users may change this setting in **Settings** > **Call options** > **Call capability over cellular network**.

Application Rating Behavior

If they install the Jabber wrapped apk file, users won't get notifications asking them to rate the application after they make calls in Jabber.

Single Number Reach Settings

It's now easier for you to set up Single Number Reach, which allows calls that are made to different devices to all reach you at a single number. You can find the Single Number Reach option directly in **Settings**.

Chromebook Notification Support

Jabber for Android 12.7 with Webex Messenger or Cisco Unified Communications Manager IM and Presence Service now supports incoming chat notifications on Chromebook. The IM notification window appears in the bottom-right corner of the Chromebook screen and offers several default reply buttons that you can tap. You can also tap **Reply** to open a chat window with the sender.

Modern Input Box Style

We improved how you send messages on your mobile devices. The options to add files, videos, or photos have moved to the bottom of the screen, beside the emoticons.

Updated Navigation

We moved the navigation options to the bottom of the screen.

Save PRT Logs Locally

If your organization does not allow users to send emails from their mobile phone, you need another method to capture PRT logs. You can allow users to save the logs locally with EnableSaveLogsToLocal. The parameter defaults to allowing users to save PRT logs in local storage.

Jabber Team Messaging Mode

Configure Clients Through Cisco Webex Control Hub

You can run Jabber Team Messaging Mode in IM-Only Mode which doesn't need Cisco Unified Communications Manager and its calling capabilities. To replace Unified CM as the deployment site for the Jabber configuration file, you can upload your Jabber configuration file to the Control Hub. You can upload one configuration file for each organization.

Go to **Services**, then select the **Message** card, and choose **Settings**. Then, select **Upload Configuration File**. The file must be in .xml format.

If you have Jabber configuration files in both the Control Hub and Unified CM, the value of a parameter from the Unified CM takes precedence.

People Insights

People Insights provides Jabber Team Message Mode users with professional profiles of their contacts. Anywhere a contact card appears, user can access People Insights: contact lists, in conversations, from the call history, and voicemail history.

The feature only displays publicly available information in profiles, and internal company directory information to users in the same company. This internal directory information is not visible to users outside the company. Users can edit their own profiles to add more data. For more information, see What Is People Insights.

To enable People Insights, go to the Control Hub, and select **Settings** > **Directory Synchronization and People Insights** and turn on the **Show People Insights** toggle.

Do Not Disturb Setting

We changed the intervals in the **Do Not Disturb** setting to 30 minutes, 1 hour, 2 hours, 4 hours, 8 hours, and 24 hours.

Messaging Service Status

You can check your connection to the messaging service from the **Settings** > **Messaging** menu. A **Service Impacted** label appears when some messaging services in the Webex platform are not working.

Enterprise Content Management (ECM) Support

You can view, send, and receive ECM files. Upload ECM files from OneDrive or SharePoint Online, and send them via chat to other Jabber users who are authorized to view them. When users send attachments, they can choose to upload files from their computer or ECM account. Users can choose to send the files to other people in their organization, or to specific people who have access to the file. When the recipient gets the message with the ECM attachment, they'll need to be logged in to that ECM service before they can view or open the file.

For more information, see https://help.webex.com/en-us/nfia8at/ Configure-Enterprise-Content-Management-Settings-in-Cisco-Webex-Control-Hub and https://help.webex.com/ en-us/nuvy9lb/Enterprise-Content-Management-in-Cisco-Webex-Control-Hub.

Quote Message

You can add context to a message by quoting another message in the same space. To quote a message, touch and hold the message that you want to quote and choose **Quote message** from the list that appears. After you send the message, the quoted message appears above your message in the space.

BOT Support

BOTs now appear in your search results, and you can add them to spaces and to an existing conversation, and create a new conversion with a BOT . To find a BOT, go to the search bar and type the first few letters of its name. BOTs appear in their own category underneath results from your contacts and directory.

Jabber Team Messaging Mode users can search for and use BOTs that are deployed as part of the Webex Platform Service. You can find these BOTs on the Cisco Webex App Hub or develop your own for your users. BOTs from the Cisco Jabber BOT SDK work only for on-premises and Webex Messenger deployments.

Space Details

In users' spaces in team messaging mode, we replaced the information icon with a drop-down arrow. It expands to show options for the space, such as adding participants, adding the space to your favorites, muting notifications, and other details about the space.

Meetings

Updates to Collaboration Meeting Room Controls

Users on Jabber mobile clients can now use several meeting room controls that were previously only available to desktop users.

Hosts can make another participant the host. The new host is moved to the top of the participant list. They can also mute/unmute everyone; and pause and resume the meeting recording.

A host can choose to either end a meeting or leave it after selecting another participant to host.

Auto-Login to Meetings

If SSO is enabled using the same IDP on Cisco Unified Communications Manager and Webex meeting, Jabber automatically connects.

Calling

Call Pickup

Users can now use Call Pickup on their mobile devices. Call Pickup allows users to pick up others' incoming calls in various answer groups. You configure answer groups on the server side. You configure this feature in Jabber using the following existing parameters: EnableCallPickup (default: false), EnableOtherGroupPickup (default: false), and EnableGroupCallPickup (default: false). For more information about how call pickup works, see the Feature Configuration for Cisco Jabber guide.

Security

Updated Sign-Out Behavior

If users sign out of Jabber, they must now re-authenticate when they next sign in.

Users do not have to re-authenticate in these cases:

- A configuration change requires them to sign out.
- They kill the Jabber app and restart it. (For desktop users, this includes when you choose **Exit Jabber**.)
- Mobile Jabber users with touch, fingerprint, or face ID enabled.

OAuth Handling of Refresh Tokens

If you have OAuth enabled in your deployment, Jabber now checks, by default, for expired refresh tokens when users sign in. If a refresh token has expired, the user must re-authenticate. If the refresh token expires while a user is signed in, Jabber signs them out with a message that their session expired.

The LegacyOAuthLogout parameter controls this behavior. The default value of **false** checks for expired refresh tokens. If you set the value to **true**, Jabber never checks for expired refresh tokens. For details, see the Parameters Reference Guide for Cisco Jabber.

Samsung Knox Support

Samsung Knox consists of a highly secure platform that is built into Samsung devices and provides a set of solutions that leverage this platform. For more information about Knox, see www.samsungknox.com

Support for Customized Certificate Authority

Starting with Release 12.7, you can use a customized certificate authority (CA) on Android devices.

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

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
5.0 or later	1.5 GHz dual-core Recommended: 1.2-GHz quad-core or higher	For two-way video: 480p x 800p or higher. For IM only: 320p x 480p or higher.

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

Table 1: Supported Android Devices

Device	Model	Minimum Android OS Version	Notes
BlackBerry	Priv	5.1	If you remove Jabber from the recently viewed apps list and you keep the device idle for some time, then Jabber becomes inactive.
Fujitsu	Arrows M357	6.0.1	

Device	Model	Minimum Android OS Version	Notes
Google	Nexus 4	5.1.1	
	Nexus 5	5.0	
	Nexus 5X	6.0	
	Nexus 6	5.0.2	
	Nexus 6P	6.0	For Google Nexus 6P with Android OS version 6.x or 7.0, your administrator must set your Jabber phone service as a secure phone service. Otherwise, your device might not respond. No action is required for Android OS version 7.1 or later.
	Nexus 7	5.0	
	Nexus 9	5.0.2	
	Nexus 10	5.0	
	Pixel	7.0	
	Pixel C	6.0	
	Pixel XL	7.0	
	Pixel 2	8.0	During a Jabber call, if the user switches audio from the mobile device to a headset, momentary audio issues are possible.
	Pixel 2 XL	8.0	During a Jabber call, if the user switches audio from the mobile device to a headset, momentary audio issues are possible.
	Pixel 3	8.0	If you use the attached headset with the phone, then there might be some issues with the audio for few seconds.
	Pixel 3 XL	8.0	If you use the attached headset with the phone, then there might be some issues with the audio for few seconds.
Honeywell Dolphin	CT50	5.0	
	CT40	7.1.1	
	CT60	7.1.1	

Device	Model	Minimum Android OS Version	Notes
HTC	10	6.0	
	A9	6.0	
	E9 PLUS	5.0.2	
	M7	5.0	
	M8	5.0	
	M9	5.0	
	One Max	5.0	
	X9	6.0	
Huawei	Honor 7	5.0	
	M2	5.0	
	Mate 7	5.0	
	Mate 8	6.0	
	Mate 9	6.0	
	Nova	7.0	
	Mate 10	8.0	
	Mate 10 Pro	8.0	
	P8	5.0	
	P9	6.0	
	P10	7.0	
	P10 Plus	7.0	
	P20	8.0	
	P20 Pro	8.0	
	Mate20	8.0	
	Mate20 Pro	8.0	
	P30	9.0	
	P30 Pro	9.0	

Device	Model	Minimum Android OS Version	Notes
LG	G2	5.0	
	G3	5.0	
	G4	5.1	
	G5	6.0	
	G6	7.0	
	V10	5.0	
	V30	8.0	
Motorola	MC40	5.0	Cisco Jabber supports only audio mode with an MC40 device. Jabber doesn't support launching Webex Meetings from an MC40 device.
	Moto Z Droid	6.0	
Nokia	6.1	8.0	
OnePlus	One	5.0	
	5	8.0	
	5T	8.0	
	6	9.0	
	6T	9.0	
Panasonic	Toughpad FZ-X1	5.0	Contact your administrator to set your Jabber phone service to be secure. Jabber plays ringback tone and busy tone at 24 kHz.
Samsung	All	5.0	• In the Samsung devices with Android OS 5.x or later, enable the auto-run option for Jabber. 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	Model	Minimum Android OS Version	Notes
Smartisan	M1L	6.0.1	
Sonim	XP8	7.1.1	
Sony Xperia	M2	5.0	
	XZ	7.0	
	XZ1	8.0	
	XZ2	8.0	
	XZ3	9.0	
	Z1	5.0	
	Z2	5.0	
	Z2 tablet	5.0	
	Z3	5.0	Sony Xperia Z3 (Model SO-01G) with Android OS 5.0.2 has poor audio on Jabber calls.
	Z3 Tablet Compact	5.0	
	Z3+/Z4	5.0.2	Video call is unstable on Sony Z3+/Z4. Try disabling your self-video for a video call. Otherwise, make a voice call only.
	Z4 TAB	5.0	
	Z5 Premium and Z5	5.0.2	
	ZR/A	5.0	Sony devices with Android OS 6.0 can't play voicemail in Jabber.

Device	Model	Minimum Android OS Version	Notes
Xiaomi	4C	5.1	Only the 32-bit version runs on these devices.
	MAX	5.1	
	Mi 4	5.0	
	Mi 5	6.0	
	Mi 5s	7.0	
	Mi 6	7.0	
	Mi 8	8.0	
	Mi 9	9.0	
	Pocophone	8.0	
	Mi Note	5.0	Only the 32-bit version runs on these devices.
	Mi Note 2	7.0	
	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	TC70	5.0	TC70 devices might sometimes have issues connecting to a Wi-Fi network configured over DHCP. In TC70, the default value of **Keep wifi on during sleep** is **Off**, set it to **Always On** for use with Jabber.
	TC75X	6.0	
	TC51	6.0	

Jabber Support for Samsung Knox

Cisco Jabber for Android supports Samsung Knox as follows:

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

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

Jabber Supports Samsung Dex

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

Support Policy on Earlier Android Versions for Cisco Jabber

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

Upgrade the Android kernel to 3.10 or later version.

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

Device Model	Operating System
HTC M7	Android OS 5.0 or later
HTC M8	Android OS 5.0 or later

Device Model	Operating System
HTC M9	Android OS 5.0 or later
HTC One Max	Android OS 5.0 or later
Sony Xperia M2	Android OS 5.0 or later and kernel version earlier than 3.10.49.
Sony Xperia Z1	If the device's Android OS is 5.0.2 or later and kernel version is 3.10.49 or later, then the device can support nonsecure mode.
Sony Xperia ZR/A	
Sony Xperia Z2	
Sony Xperia Z2 tablet	
Sony Xperia Z3	
Sony Xperia Z3 Tablet Compact	
Xiaomi Mi4	Android OS 5.0 or later
Xiaomi Mi Note	Android OS 5.0 or later
Xiaomi Mi Pad	Android OS 5.0 or later
Sonim XP7	Android OS 5.0 or later
Honeywell Dolphin CT50	Android OS 5.0 or later

Supported Bluetooth Devices

Bluetooth Devices	Dependencies
Cisco 561	
Cisco 562	
Plantronics Voyager Legend	
Plantronics Voyager Legend UC	
Plantronics Voyager edge UC	
Plantronics Voyager edge	
Plantronics PLT focus	
Plantronics BackBeat 903+	If you use a Samsung Galaxy S4, you can experience problems due to compatibility issues between these devices.

Bluetooth Devices	Dependencies
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.

Bluetooth limitations:

- Using a Bluetooth device on a Samsung Galaxy SIII may cause distorted ringtone and distorted call audio.

- If a user disconnects and reconnects the Bluetooth Headset during a Jabber call, then the user can't hear the audio. This limitation applies to Smartphones with versions earlier to Android 5.0 OS.

- In Sony Z4 / LG G4 /Devices with OS Android 6.0, users can experience audio loss when switching to a Bluetooth headset after starting a Jabber call. As a workaround, switch the audio output to a speaker and then switch back to Bluetooth. Or connect the Bluetooth headset before making a Cisco Jabber call.

Supported Android Wear

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

- Fossil Gen 3 SmartWatch

- Huawei watch

- LG G Watch R

- LG Watch Urbane

- Moto 360

- Moto 360 (2nd Gen)

- Samsung Gear Live

- Sony SmartWatch 3

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

Supported Chromebook Models

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

- HP Chromebook 13 G1 Notebook PC

- Google Chromebook Pixel

- Google Chromebook Pixelbook

- Samsung Chromebook Pro

- Asus C302

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:

- As of Release 12.7, Jabber for Android doesn't support automatically starting with the OS.

- Webex site disclaimers don't appear when you join Webex meetings from Jabber. This limitation applies whether joining from the meeting reminder popup, or by selecting **Join in Webex** in Jabber.

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

- Because of a limitation of Cisco Unity Connection, the voicemail server can't display the URI for a missed call. This issue occurs when you decline an incoming Cisco Jabber call from a URI and the call diverts to voicemail. If the contact information for the caller 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.

- When you play music with a third-party application, the music doesn't automatically pause when you make or receive a Cisco Jabber for Android video call. To work around this issue, you can open the third-party application to pause and 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 from network instability.

- 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.

- Jabber team messaging mode doesn't support notifications on Android Wear devices.

- 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 see only 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're creating devices for users in Cisco Unified Communications Manager 11.0, you can specify a key order:

  - RSA Only

  - EC Only

  - EC Preferred

  - RSA Backup

  However, Jabber doesn't support the EC Only option, 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's an interval of 120 seconds between sending connection requests. This interval prevents multiple requests to the server from multiple clients. During this 120-seconds interval, even if your network connection is active, Jabber remains inactive.

- There's an audio quality issue in Samsung devices with chipset Exynos 7580. The audio becomes unclear when the device screen is off. Here is the device list:

  - Samsung Galaxy A3 2016

  - Samsung Galaxy A5 2016

  - Samsung Galaxy A7 2016

  - Samsung Galaxy S5 Neo

  - Samsung Galaxy J7

  - Samsung Galaxy View

- When you install Jabber for the first time, Samsung devices automatically put Jabber in the unmonitored apps list. The device doesn't put unmonitored apps to sleep while they run in the background. However, if you upgrade your Samsung OS from a version without unmonitored apps list, 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, 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.

- Auto authentication at startup is no longer supported.

- Jabber turns off Wi-Fi when you answer a call on cellular network to avoid call drops.

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.

Resolved Caveats in Release 12.7(2)

Identifier	Severity	Headline
CSCvr62048	2	On Jabber 12.7 users cannot login after CUCM cluster migration

Open Caveats in Release 12.7

Identifier	Severity	Headline
CSCvq36013	2	Jabber for Android loses incoming call in background
CSCvr12533	3	Jabber for Android does not refresh access token in failover scenario over MRA

Resolved Caveats in Release 12.7

Identifier	Severity	Headline
CSCvp45073	3	DTMF digits not transferred in time (within 50ms)
CSCvq17036	3	SQLite3 rtreenode() Function Heap Out-of-Bounds Read Vulnerability
CSCvq92136	3	Jabber for Android 911 Notification Fails over MRA
CSCvr05064	3	Change in DNS/proxy behaviour results in user failing to login in 12.6 sync with windows
CSCvr05071	3	Jabber does not show hunt pilot information
CSCvm79502	6	Certificate warning in jabber for android when certificates are signed using private CA