Release Notes for Cisco Jabber for iPhone and iPad 12.7

First Published: 2019-09-09

Last Modified: 2020-04-07

What's New in Release 12.7(1)

Resolved Caveats

This release provides fixes for a number of known issues. See the Resolved Caveats 12.7(1) section for a list of caveats fixed in this release.

What's New in Release 12.7

Improved User Experience

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 users install the Jabber wrapped ipa file, they 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**.

Parameter to Suppress Unread Message Deletion Notifications

When you enable IM push notifications, some users receive notifications about impending deletions of unread messages from the server. The notifications can appear when the message queue is too large or when session suspensions last too long.

The UnreadMessageDeleteAlert parameter suppresses these notifications. The default value of `true` shows the notifications. If you set the value to `false`, these notifications do not appear.

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.

Jabber Team Messaging Mode

Safari View Support for Teams Messaging Mode

In deployments with Single Sign-On (SSO), Jabber authenticates first with the Webex platform and then with Unified Communications Manager. By default, Jabber uses the Web view to sign in users to SSO.

To enable users to do SSO authentication with the Webex platform through the Safari browser view, set the AllowTeamsUseEmbeddedSafari parameter.

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.

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.

Safari SSO Token Improvement

You can define Safari as the browser for users to do the SSO authentication for Webex Meetings. In earlier releases, joining a Webex Meeting through the Safari browser sometimes forced users to sign in again. In Release 12.7, the Safari session can access an existing SSO token to avoid signing in again.

Auto-Login to Meetings

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

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.

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 iPhone and iPad

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

☞

Important Cisco supports only the current App Store version of Cisco Jabber for iPhone and iPad. Defects found in any Cisco Jabber for iPhone and iPad release are evaluated against current versions.

Hardware Requirements for Cisco Jabber for iPhone and iPad

The following Apple devices are supported for Cisco Jabber for iPhone and iPad on iOS 11.X, iOS 12.X, and iOS 13.X. The devices that are not upgraded to these versions are not supported.

Apple Device	Version
iPad	5th and 6th generation
iPad Air	Air 1, Air 2, and Air 3
iPad Pro	9.7 and 10.5 inch 12.9 inch, 1st, 2nd and 3rd generation
iPad mini	Mini 2, mini 3, mini 4, and mini 5
iPhone	5s, 6, 6 Plus, 6s, 6s Plus, 7, 7 Plus , 8, 8 Plus, X, Xs, Xs Max, XR and SE
iPod touch	6th generation

Apple Device	Version
Apple Watch	WatchOS 5 running on Apple Watch and Apple Watch 2, 3 and 4.

The following Bluetooth headsets are supported on iPhone and iPad:

Table 1:

Manufacturer	Model(s)
Cisco	561, 562
Jabra	BIZ 2400, Easygo, Evolve 65 UC Stereo, EXTREME 2, Motion[1], PRO 9470, Speak 450 for Cisco, Speak 510, Stealth Supreme UC, Wave +
Jawbone	ICON for Cisco Bluetooth Headset
Plantronics	Voyager Edge, Voyager Edge UC, Voyager Legend, Voyager Legend UC
Sony Eriksson	MW-600

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

Accessibility

Screen Readers

Cisco Jabber for iPhone and iPad is compatible with the VoiceOver screen reader. Users who require screen readers should always use the most recent version to ensure the best possible user experience.

Assistive Touch

You can navigate Cisco Jabber for iPhone and iPad using Explore by Touch.

Limitations and Restrictions

- Apple has new requirements for trusted certificates in iOS 13 (see https://support.apple.com/en-us/ HT210176). Ensure that the certificates on the Unified Communications Mananger, IM & Presence, and Expressway servers meet these requirements. If your certificates don't meet these requirements, Jabber prompts users to accept the certificates for each session.

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

- Applies to Cisco TelePresence Video Communication Server Control (VCS) versions earlier than 8.10.X.

Configure the editable inbound rules to enable single number reach for those who use 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*.

- Cisco Jabber for mobile clients don't show the **Favorite** icon for users with Phone Only account.

- Without Apple Push Notifications (APNs), when Cisco Jabber receives an incoming call or chat, the iOS doesn't wake Cisco Jabber. The call or instant message appears on the device after several minutes or when you bring Cisco Jabber the foreground. As a workaround, reset the network settings for your iOS device by going to **Settings** > **General** > **Reset** > **Reset Network Settings**.

- Users can no longer edit their Phone Services servers manually, except when they are in hybrid cloud mode. In hybrid deployments, administrators can configure the Phone Services servers to be editable.

- The first usage of Secure Phone functionality must be on the corporate network or VPN to ensure proper certificate installation.

- Voice recognition for voicemail PIN is highly sensitive to background noise. The system may interpret background noise as user input, even when the user doesn't input anything. See *System Administration Guide for Cisco Unity Connection* to disable this function.
  https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

- Certificate validation windows pop up when the certificate on Cisco Unified Communications Manager is issued by an intermediate certificate authority. Use a certificate that is signing with the root rather than an intermediate certificate authority.

- From Release 10.5 onward, all the Cisco Jabber account related files, including Configuration, Contacts, Credentials, History, Logs, Photo and so on, aren't backed up on the iCloud and iTunes due to privacy reasons.

- 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.

- With Jabber running in the background, if users try moving between networks; for example, from WiFi to 3G, the client disconnects from the servers. It can take up to 11 minutes to reconnect and can lead to missed calls. To avoid missed calls, it is recommended to enable Apple Push Notification service.

- There is a known issue with signing into Cisco Jabber for some users who have migrated to Common Identity. If users receive an Incorrect user name or password error message when entering their username and password, see the following knowledge base article,
  https://cisco-support.webex.com/guest/articles/en_US/Troubleshooting/WBX000019555/myr=false.

- CallKit functionality is deactivated in China due to government regulations.

iPhone

- Due to some limitations when Cisco Jabber for iPhone and iPad is running on iOS, Configure the Single Number Reach (SNR) feature within Cisco Unified Communications Manager for users that require 100% reliability in call notifications. The limitations include:

  - iOS may shut down Cisco Jabber and other applications that are running in the background to preserve resources. While the client attempts to relaunch, there is a possibility that calls may be missed. To minimize the impact, it is recommended to enable Apple Push Notification service.

- Without Apple Push Notifications (APNs), the device sometimes switches connection from the Wi-Fi data network to the mobile voice network while the device is in Sleep mode. Incoming calls may be missed due to this issue. To prevent this issue, go to the iPhone Settings and turn off **Cellular Data** or alternatively turn on **SNR**.

- The VPN can disconnect when Connect-On-Demand is enabled and the user changes networks. Cisco Jabber for iPhone and iPad may take up to 11 minutes to reconnect through the VPN. This issue can lead to missing incoming calls. This occurs when the Wi-Fi signal is not stable or sometimes the mobile network takes priority and it switches between Wi-Fi and mobile network, while Jabber is unable to quickly connect to phone services during the handover. After Cisco Jabber for iPhone and iPad reconnects, users who have voicemail enabled in their account receive voicemail notifications for any missed calls that went to voicemail. To minimize the time to reconnect, users can bring the app to the foreground after changing connection environments. It is also recommended to enable Apple Push Notification service.

- **Cisco Webex Meetings**— If the meeting siteType is ORION, then Cisco Jabber for iPhone and iPad cannot start Webex Meetings over Expressway for Mobile and Remote Access network.

- If Cisco Jabber on iPhone is unable to reach the primary subscriber due to packet loss, it does not failover to secondary CM node. For more information, see CSCux83785.

- If you are setting up Dial via Office - Reverse (DVO-R) on Cisco Unified Communications Manager consider the following:

  - The feature only applies to iPhone; it is not supported on iPad or iPod Touch devices because it requires that the device can access a mobile network.

  - You can make DvO-R calls over Expressway for Mobile and Remote Access when you are outside corporate network. DVO-R is supported over Cisco Expressway X8.7 and Cisco Unified Communications Manager 11.0(1a)SU1.

  - DVO enabled devices may encounter issues registering with Cisco Unified Communications Manager 8.6 and above. Resetting the device from the Cisco Unified Communications Manager administrative interface fixes this issue.

  - The feature requires Cisco Unified Communications Manager Release 8.6.2 SU4, 9.1.2, or 10.x.

  - The feature cannot be used in conjunction with the Secure Call feature. Secure calls cannot be established if DVO-R is enabled.

  - Due to a limitation with Cisco Unified Communications Manager, if the user places a DVO-R call to an invalid phone number over a SIP trunk, the user hears several seconds of silence instead of an audio message stating the number was invalid.

- If the user is on a Cisco Unified Communications Manager call and receives an incoming mobile call, iPhone starts ringing and prompts the user to answer or decline the mobile call. At the same time, the Cisco Unified Communications Manager call on Cisco Jabber goes on hold automatically.

- To ensure that you do not miss incoming Cisco Jabber chats and calls, go to **iOS Settings** > **Notification Center** and check that the Cisco Jabber sound setting is turned on.

- If you receive a Cisco Unified Communication Manager call, while placing a VoIP call, Cisco Jabber for iPhone and iPad sends the incoming call to voicemail. If you do not have voicemail, Cisco Jabber for iPhone and iPad ignores the call.

- The maximum number of participants for ad-hoc conferences is limited to three; this is the maximum number of calls for TCT devices. The maximum participants for ad-hoc conference is configured on Cisco Unified Communication Manager in **Service Parameter Configuration** > **Clusterwide Parameters** > **Maximum Ad Hoc Conference Required**.

- Voice and video quality over non-corporate Wi-Fi or mobile data networks cannot be guaranteed.

- The quality of video calls varies depending on the network connection. Cisco Technical Assistance Center (TAC) cannot troubleshoot video quality when you use 3G or 4G networks to connect Cisco Jabber for iPhone and iPad with Cisco AnyConnect Secure Mobility Client or another VPN client.

- If you receive an incoming call on your iPhone, the iPhone automatically disables the microphone for all other applications, and there is no time to inform your current caller that you need to take another call. If you accept the new incoming call, your Cisco Jabber for iPhone and iPad Cisco Unified Communications Manager call is automatically placed on hold, and you cannot return to it until you end the iPhone call. To work around this issue, decline the call and then tap Resume so that your current caller can hear you again. If your device is locked, quickly press the On/Off Sleep/Wake button twice to decline the call, and then tap Resume.

- SIP Digest Authentication is not supported.

- Cisco Unified Communications Manager as a directory source is capable of scaling to 50% of the device capacity that a Cisco Unified Communications Manager node can handle.

- When the device is in Do Not Disturb (DND) mode and locked, then it vibrates upon receiving a Cisco Jabber call.

- With iOS versions 10 and 11 with Cisco Jabber 12.0, you cannot receive call notifications on Apple Watch because CallKit can't work with Apple Watch. This is an Apple iOS limitation.

- When in the background for a few hours, Jabber relaunches without notification.

iPad

- When users transition between networks, their availability status may not be accurate.

- Cisco Jabber for iPhone and iPad supports interoperability and optimal video quality with Cisco TelePresence System (CTS) devices if you use a TelePresence or video bridge to connect the devices. The number of devices that you can use for joining a video call will be determined by the Multipoint Control Unit (MCU) and settings defined for the conference bridge.

Required versions and settings for CTS interoperability
VCS call control environment: All CTS devices must be using 1.9.1(68) or a later firmware version.
Cisco Unified Communications Manager call control environment: • All CTS devices must be using 1.9.1(68) or a later firmware version.   • Create Media Regions for iPad and CTS by following these steps: 1. Provision two media regions with the first region for CTS using a maximum video call bit rate of 32000 Kbps and second region for iPad using a maximum video call bit rate of 768 Kbps.   2. Create a region relationship from the CTS region to the iPad region, described in step 1, using a maximum video call bit rate of 512 Kbps.

Required versions and settings for CTS interoperability
To verify your VCS firmware and hardware codec versions, check the Device information screen in the Cisco TelePresence System Administration.

Consult the Cisco Unified Communications Manager Administration documentation for details about setup.

• You cannot block contacts who are within your own organization.

• If you delete a group of contacts on another device other than an iPad, they may still appear in Cisco Jabber for iPhone and iPad. Sign out and then sign in again for the changes to take effect.

• If you start an action, such as signing in or tapping **Webex Meeting** to start a meeting, and then bring Cisco Jabber for iPhone and iPad to the background before the action completes, you can't successfully complete the action.

• If you tap **Webex Meeting** to start a meeting, the system sends a meeting invitation when either the meeting starts or 60 seconds has elapsed.

• When on a Cisco Jabber call and you put Cisco Jabber to the background, sometimes the call indicator shows Cisco Jabber recording, depending on the iOS versions.

Apple Watch

Notifications aren't supported on Apple Watch in Jabber team messaging mode.

Performance and Behavior Notes

Multiple Resource Login

When a user signs in to multiple instances of the client at the same time, the chat feature behaves as follows:

• The first incoming chat message is sent to all the clients.

• The first client to reply to the incoming chat message gets all the subsequent messages. The other clients do not get these subsequent incoming messages.

• If the client does not use the chat feature for 5 minutes, the next incoming message is sent to all the clients again.

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.

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(1)

Identifier	Severity	Headline
CSCvr55497	2	On Jabber 12.7 users cannot login after CUCM cluster migration
CSCvr40957	3	MFT does not work on J4I when connected via mobile network
CSCvr66108	3	Jabber iOS 12.6 not authenticating with CWMS

Identifier	Severity	Headline
CSCvr61388	3	Jabber Search Result via UDS Proxy Switches to Wrong User

Open Caveats in Release 12.7

Identifier	Severity	Headline
CSCvr12542	3	Jabber does not refresh access token in failover scenario over MRA

Resolved Caveats in Release 12.7

Identifier	Severity	Headline
CSCvp25135	3	Intermittent no audio issue after "Hold & Accept" operation for 2nd call
CSCvq70474	3	iPhone showing presence offline when away
CSCvq95562	4	Jabber does not prompt for session about to expire when in background and call comes in