Release Notes for Cisco Jabber for iPhone and iPad 12.1

First Published: 2018-07-19

Last Modified: 2018-09-27

Introduction

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

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

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

Build Number

Release	Build Number
12.1(2)	12.1.2.269866
12.1(1)	12.1.1.268230
12.1	12.1.0.266556

What's New in Release 12.1(2)

Persistent Chat Rooms

Persistent chat rooms are now fully supported for mobile clients.

iOS 12

This release includes support for iOS 12.

Resolved Caveats

This release provides fixes for several known defects.

What's New in Release 12.1(1)

This release provides a fix for a known issue relating to presence in Japanese localizations. See the *Resolved Caveats in Release 12.1(1)* section for more information about the caveat fixed in this release.

What's New in Release 12.1

Telephony

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

Administrator

- **Retain Secure Phone Certificate during a Cisco Jabber Reset**—Users can retain the secure phone certificate during a Cisco Jabber reset. If users choose to remove the certificate, they cannot use the phone services on Cisco Jabber until you reconfigure it for them.

Security

- **Push Notification Support for end to end encrypted Message**—Cisco Jabber provides push notification support for end to end encrypted instant messages, even if Jabber is terminated, inactive, or is available in the background. For more details, see the *Push Notification Service for IM* section from the *Feature Configuration for Cisco Jabber 12.1.*
- **Push Notification Support for Jabber to Jabber call**—Cisco Jabber provides push notification support for all Jabber to Jabber calls even if Jabber is terminated, inactive, or is available in the background. For more details, see the *Push Notification Service for IM* section from the *Feature Configuration for Cisco Jabber 12.1.*

Chat and Presence

- **Persistent Chat Room Support**—From this release onwards, Cisco Jabber introduces persistent chat room support for mobile clients. Users can use chat rooms to collaborate with others and share ideas as a group. Persistent chat rooms allow users to perform the following tasks:
  - @Mention Notifications in Persistent Chat Rooms
  - Mute or Unmute Persistent Chat Rooms
  - Search and Find Persistent Chat Rooms
  - Leave from Persistent Chat Rooms
  - Add Participant in Persistent Chat Rooms
  - Join Persistent Chat Rooms

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

- **Persistent_Chat_Mobile_Enabled**—This is a new parameter that specifies if persistent chat feature is available for Cisco Jabber for iPhone and iPad. For more information, see the *Parameter Reference Guide for Cisco Jabber 12.1.*
- **EnableConvertNumberToURI**—This is a new parameter that specifies if Cisco Jabber converts numbers into SIP URI when a user enters numbers in the chat window. For more information, see the *Parameter Reference Guide for Cisco Jabber 12.1.*
- **User name Displayed with an Animated Emoticon in Group Chat**—Cisco Jabber displays the user name when users send an animated emoticon to a group chat.

Settings

- **Refresh Cisco Jabber configuration**—When there are configuration updates, users can refresh Cisco Jabber for the updates to take effect. Users can refresh Cisco Jabber configuration from the **Settings**, **Configuration**, and **Refresh Configuration** anytime after they have signed in.
- **Cisco Jabber Diagnostics Check**—If users are unable to sign into Cisco Jabber or if Cisco Jabber services are not connected due to network issues, they can use the **Diagnose Error** option from the **Sign In** page, or from **Settings** > **Accounts** > **Instant Messaging** or **Phone Services** page. Cisco Jabber then performs various checks to identify the issue. If there is an issue, Cisco Jabber displays the error message with possible solution. If the problem still persists, users can send a problem report.

UI Enhancements

- **Custom Tab Display Webpages Icon**—When users create custom tab of any webpage, the default icon of the webpage is displayed on the custom tab.
- **Contact Lookup Enhancement**—Support for base64-encoded thumbnail photos. Cisco Jabber contact lookup now supports base64-encoded contact photos when using LDAP or HTTP photo retrieval. Cisco Jabber will determine if the server response is a text URL (for LDAP only), an image, or a base64-encoded image, and displays it accordingly.
- **Help Link in the Cisco Jabber Sign-In Page**—We have added a Help link in the Cisco Jabber Sign-in page. This link takes users to the Collaboration Help Portal that contains articles about sign-in issues and troubleshooting tips.
- **Enter Your Company E-Mail Address**—Cisco Jabber displays a sign-in tip to use your company email ID to sign into Cisco Jabber. For example, `username@company.com`.
- **Added Labels to the Contact Numbers**—When users tap the call icon of a contact from the chats window the contact numbers are listed indicating a work phone or mobile phone.
- **Operating System Support**—Cisco Jabber for iPhone and iPad Release 12.1 supports only iOS version 11 or later.
- **New Device Support**—We have provided support to the latest iPad 9.7 inch (2018) device. For more details, see the *Device Requirements* section.

Requirements

Services

Service Requirements

Install the COP file cmterm-iphone-install-151020.k3.cop.sgn for iPhone and the COP file cmterm-jabbertablet-install-151020.k3.cop.sgn for iPad to 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).

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.

Server Requirements

The following are the server requirements for Cisco Jabber for iPhone and iPad in this release:

Service	Software Requirement	Supported Version
IM and Presence	Cisco Unified Communications Manager IM and Presence Service	10.5(2) or later 11.5(1) SU2 or later (Recommended)
	Cisco Webex Messenger	
Telephony	Cisco Unified Communications Manager	10.5(2) or later 11.5(1) SU3 or later (Recommended)
	Cisco Unified Survivable Remote Site Telephony	8.5 and later
Contact Search	Cisco Webex Messenger	
	Microsoft Active Directory	2008 R2 and later
	OpenLDAP	2.4 and later
	Cisco Unified Communications Manager User Data Service (UDS)	10.5 (2) and later
Voicemail	Cisco Unity Connection	10.5 or later

Service	Software Requirement	Supported Version
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	2.8 and later
	Cisco Webex Meetings Center	WBS31 and later
	Cisco Meeting Server (CMS)	2.2 and later
Remote Access	Cisco AnyConnect Secure Mobility Client	Latest version on App Store
	Cisco Expressway C	X8.10.1 or later
	Cisco Expressway E	X8.10.1 or later

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

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.

Supported Codecs

Audio Codecs

Modes	Supported Audio Codec
Low-bandwidth	G.729a
Normal	G.711, G.711 mu-law, G.711 a-law, G.722, G.722.1, Opus, and G.729a

Note Users can turn Low-bandwidth mode ON or OFF in the client settings, if they experience voice quality issues.

Video Codecs

H.264/AVC

Voicemail Codecs

- PCM linear
- G.711 mu-law (default)
- G.711 a-law
- GSM 6.10

Note Cisco Jabber for iPhone and iPad does not support visual voicemail with G.729. However, users can access their voice messages using G.729 and the **Call Voicemail** feature.

Hardware Requirements

Device Requirements

The device and operating system requirements are:

- **Devices**
  - iPhone 5s, iPhone 6, iPhone 6 Plus, iPhone 6s, iPhone 6s Plus, iPhone SE, iPhone 7 iPhone 7 Plus, iPhone 8, iPhone 8 Plus, iPhone X, iPhone XS, and iPhone XS Max.
  - iPad with Retina display (4th generation), iPad Air, iPad Air 2, iPad mini2, iPad mini 3, iPad mini 4, iPad 5th and 6th generation, 9.7 inch iPad Pro, 10.5-inch iPad Pro, 12.9 inch iPad Pro (1st and 2nd generation),iPad 9.7 inch 2017 and 2018.
  - iPod touch 6th generation
  - Apple Watch
- **Operating Systems**
  - iOS 12 or later
  - iOS 11 or later
  - watchOS 5 or later
  - watchOS 4 or later
  - watchOS 3 or later

Cisco supports only the current App Store version of Cisco Jabber for iPhone and iPad. Previous App Store versions of Cisco Jabber for iPhone and iPad become obsolete once the new version is available. Defects found in any Cisco Jabber release are evaluated against current versions.

Apple iOS Version Support Policy

Cisco supports Cisco Jabber releases only on the latest major iOS release. To help enterprise customers transition to new major iOS updates, Cisco supports the last OS release of the previous major release for three months after a new release is introduced.

Bluetooth Headset Support

The following Bluetooth headsets are supported on iPhone and iPad:

- Jabra Easygo
- Jabra EXTREME 2
- Jabra Speak 450 for Cisco
- Jabra Supreme UC
- Jabra Wave +
- Jabra Motion
- Sony Ericsson Bluetooth Headset BW600
- Jabra PRO 9470
- Jabra BIZ 2400
- Jabra Speak 510
- Jawbone ICON for Cisco Bluetooth Headset
- Jabra Stealth
- Jabra Evolve 65 UC Stereo
- Plantronics Voyager Legend
- Plantronics Voyager Legend UC
- Plantronics Voyager Edge
- Plantronics Voyager Edge UC

The Jabra Motion Bluetooth headsets with firmware version 3.72 or above support call control.

Bluetooth and Network Interference

Bluetooth headsets use the same 2.4 GHz frequency as 802.11b, 802.11g, and 802.11n wireless networks. Interference from other devices can impact Bluetooth transmissions and Bluetooth headsets may interfere with wireless connections to the iPhone, iPad, or iPod Touch. This issue is not specific to Cisco Jabber for iPhone and iPad but can result in dropped or interrupted calls and voice quality issues.

Minimize interference to wireless networks from Bluetooth headsets by ensuring a strong wireless network signal is available throughout the coverage area.

The following Apple support articles contain useful information on these issues:

- AirPort and Bluetooth: Potential sources of wireless interference
- Bluetooth: Static heard on Bluetooth headset

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. Cisco recommends that you:

- Verify nonoverlapping channel configurations, 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:

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

If users 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.

	Port	Application Layer Protocol	Transport Layer Protocol	Description
Configuration				

	Port	Application Layer Protocol	Transport Layer Protocol	Description
	6970	HTTP	TCP	Connect to the TFTP server to download client configuration files.
	6972	HTTPS	TCP	Connects to the TFTP server to download client configuration files securely for Cisco Unified Communications Manager version 11.0 and later.
	53	DNS	UDP	Hostname resolution
	3804	CAPF	TCP	Issues Locally Significant Certificates (LSC) to IP phones. This port is the listening port for Cisco Unified Communications Manager Certificate Authority Proxy Function (CAPF) enrollment.
	8443	HTTPS		Traffic to Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service.
	8191	SOAP	TCP	Connects to local port to provide Simple Object Access Protocol (SOAP) web services
Directory Integration-For LDAP contact resolution one of the following ports will be used based on LDAP configuration. **Note** from Cisco Jabber 11.7 if the LDAP ports are not configured, then LDAPS ports are used by default.				
	389	LDAP	TCP	LDAP TCP (UDP) Connects to an LDAP directory service
	3268	LDAP	TCP	Connects to a Global Catalog server for contact searches.
	636	LDAPS	TCP	LDAPS TCP Connects securely to an LDAP directory service.
	3269	LDAPS	TCP	LDAPS TCP Connects securely to the Global Catalog server.
Instant Messaging and Presence				

	Port	Application Layer Protocol	Transport Layer Protocol	Description
	443	XMPP	TCP	XMPP traffic to the WebEx Messenger service. The client sends XMPP through this port in cloud-based deployments only. If port 443 is blocked, the client falls back to port 5222.
		Apple Push Notification Service	TCP	Used on Wi-Fi network. It is also used when the devices are unable to communicate with Apple Push Notification server on port 5223
	5222	XMPP	TCP	Connects to Cisco Unified Communications Manager IM and Presence Service for instant messaging and presence.
	5223	Apple Push Notification Service	TCP	Sends messages from Apple Push Notification server to iPhone and iPad.
	37200	SOCKS5 Bytestream	TCP	Peer to Peer file transfer, In on-premises deployments, the client also uses this port to send screen captures.
	7336	HTTPS	TCP	MFT File transfer (On Premise only)
Communication Manager Signaling				
	2748	CTI	TCP	Computer Telephony Interface (CTI) used for desk phone control.
	5060	SIP	TCP	Provides Session Initiation Protocol (SIP) call signaling.
	5061	SIP over TLS	TCP	SIP over TCP Provides secure SIP call signaling. (Used if Secure SIP is enabled for device)
	30000 to 39999	FECC	TCP	Far end camera control (FECC)
	5070 to 6070	BFCP	UDP	Binary Floor Control Protocol (BFCP) for video desktop sharing capabilities.
Voice/Video Media Exchange				
	16384 to 32766	RTP/SRTP	UDP	Cisco Unified Communications Manager media port range used for audio, video and BFCP video desktop share.
	33434 to 33598	RTP/SRTP	UDP	Cisco Hybrid Services (Jabber to Jabber calling) media port range used for audio and video.
	49152 to 65535	RDP	TCP	IM-only desktop share. Applies to Cisco Jabber for Windows only.
Unity Connection				

	Port	Application Layer Protocol	Transport Layer Protocol	Description
	7080	HTTP	TCP	Used for Cisco Unity Connection to receive notifications of voice messages (new message, message update, and message deleted).
	7443	HTTPS	TCP	Used for Cisco Unity Connection to securely receive notifications of voice messages (new message, message update, and message deleted).
	443	HTTPS	TCP	Connects to Cisco Unity Connection for voicemail.
Cisco WebEx Meetings				
	80	HTTP	TCP	Connects to Cisco WebEx Meeting Center for meetings
	443	HTTPS	TCP	Connects to Cisco WebEx Meeting Center for meetings
	8443	HTTPS	TCP	Web access to Cisco Unified Communications Manager and includes connections for the following: • Cisco Unified Communications Manager IP Phone (CCMCIP) server for assigned devices. • User Data Service (UDS) for contact resolution.

Ports and Protocols

The client uses the ports and protocols listed in the following table. If you plan to deploy a firewall between the client and a server, you must configure the firewall to allow these ports and protocols.

	Port	Application Layer Protocol	Transport Layer Protocol	Description
Configuration				
	6970	HTTP	TCP	Connect to the TFTP server to download client configuration files.
	6972	HTTPS	TCP	Connects to the TFTP server to download client configuration files securely for Cisco Unified Communications Manager version 11.0 and later.
	53	DNS	UDP	Hostname resolution
	3804	CAPF	TCP	Issues Locally Significant Certificates (LSC) to IP phones. This port is the listening port for Cisco Unified Communications Manager Certificate Authority Proxy Function (CAPF) enrollment.
	8443	HTTPS		Traffic to Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service.
	8191	SOAP	TCP	Connects to local port to provide Simple Object Access Protocol (SOAP) web services

	Port	Application Layer Protocol	Transport Layer Protocol	Description
Directory Integration-For LDAP contact resolution one of the following ports will be used based on LDAP configuration. **Note** from Cisco Jabber 11.7 if the LDAP ports are not configured, then LDAPS ports are used by default.				
	389	LDAP	TCP	LDAP TCP (UDP) Connects to an LDAP directory service
	3268	LDAP	TCP	Connects to a Global Catalog server for contact searches.
	636	LDAPS	TCP	LDAPS TCP Connects securely to an LDAP directory service.
	3269	LDAPS	TCP	LDAPS TCP Connects securely to the Global Catalog server.
Instant Messaging and Presence				
	443	XMPP	TCP	XMPP traffic to the Webex Messenger service. The client sends XMPP through this port in cloud-based deployments only. If port 443 is blocked, the client falls back to port 5222.
		Apple Push Notification Service	TCP	Used on Wi-Fi network. It is also used when the devices are unable to communicate with Apple Push Notification server on port 5223
	5222	XMPP	TCP	Connects to Cisco Unified Communications Manager IM and Presence Service for instant messaging and presence.
	5223	Apple Push Notification Service	TCP	Sends messages from Apple Push Notification server to iPhone and iPad.
	37200	SOCKS5 Bytestream	TCP	Peer to Peer file transfer, In on-premises deployments, the client also uses this port to send screen captures.
	7336	HTTPS	TCP	MFT File transfer (On Premise only)
Communication Manager Signaling				

	Port	Application Layer Protocol	Transport Layer Protocol	Description
	2748	CTI	TCP	Computer Telephony Interface (CTI) used for desk phone control.
	5060	SIP	TCP	Provides Session Initiation Protocol (SIP) call signaling.
	5061	SIP over TLS	TCP	SIP over TCP Provides secure SIP call signaling. (Used if Secure SIP is enabled for device)
	30000 to 39999	FECC	TCP	Far end camera control (FECC)
	5070 to 6070	BFCP	UDP	Binary Floor Control Protocol (BFCP) for video desktop sharing capabilities.
Voice/Video Media Exchange				
	16384 to 32766	RTP/SRTP	UDP	Cisco Unified Communications Manager media port range used for audio, video and BFCP video desktop share.
	33434 to 33598	RTP/SRTP	UDP	Cisco Hybrid Services (Jabber to Jabber calling) media port range used for audio and video.
	49152 to 65535	RDP	TCP	IM-only desktop share. Applies to Cisco Jabber for Windows only.
Unity Connection				
	7080	HTTP	TCP	Used for Cisco Unity Connection to receive notifications of voice messages (new message, message update, and message deleted).
	7443	HTTPS	TCP	Used for Cisco Unity Connection to securely receive notifications of voice messages (new message, message update, and message deleted).
	443	HTTPS	TCP	Connects to Cisco Unity Connection for voicemail.
Cisco Webex Meetings				
	80	HTTP	TCP	Connects to Cisco Webex Meeting Center for meetings
	443	HTTPS	TCP	Connects to Cisco Webex Meeting Center for meetings
	8443	HTTPS	TCP	Web access to Cisco Unified Communications Manager and includes connections for the following: • Cisco Unified Communications Manager IP Phone (CCMCIP) server for assigned devices. • User Data Service (UDS) for contact resolution.

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

Supported Languages

Language	Application	User Guides
Arabic	Yes	—
Chinese (Simplified)	Yes	Yes
Chinese (Traditional)	Yes	Yes
Croatian	Yes	—
Danish	Yes	Yes
Dutch	Yes	Yes
English	Yes	Yes
French	Yes	Yes
German	Yes	Yes
Hungarian	Yes	—
Italian	Yes	Yes
Japanese	Yes	Yes
Korean	Yes	Yes
Polish	Yes	Yes
Portuguese	Yes	Yes
Romanian	Yes	—
Russian	Yes	Yes
Slovak	Yes	—
Spanish	Yes	Yes
Swedish	Yes	Yes
Turkish	Yes	—

Limitations and Restrictions

- For Cisco TelePresence Video Communication Server Control (VCS) versions earlier than 8.10.X, you have to configure the editable inbound rules to enable the single number reach for users who are using Cisco Jabber over Mobile and Remote Access. For more information, see *Limitations* in *Enable Single Number Reach* section from the *Feature Configuration Guide for Cisco Jabber 12.0*.
- Due to a defect in Apple iOS version 9.3.x, in some versions of iPhone, the Cisco Jabber client doesn't ring for an incoming call sometimes when the device is locked.
- Cisco Jabber for mobile clients do not show Favorite icon for users with Phone Only account.
- When Cisco Jabber is suspended and receives an incoming call or chat, the iOS does not wake up Cisco Jabber. The call or instant message appears on the device after several minutes or when Cisco Jabber is

taken to the foreground. As a workaround, reset the network settings using **Settings** > **General** > **Reset** > **Reset Network Settings** in the iOS device.

- 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 the background noise and may interpret background noise as user input when the user doesn't input anything. Refer to *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 10.5 release onwards, all the Cisco Jabber account related files, including Configuration, Contacts, Credentials, History, Logs, Photo and so on, are not 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.
  - 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.
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. You will need to sign out and sign in 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 is completed, you cannot successfully complete the action.
- If you tap **Webex Meeting** to start a meeting, a meeting invitation is sent 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 will show Cisco Jabber recording, depending on the iOS versions.

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.

Severity Level	Description
3 Moderate	Failures occur in unusual circumstances, or minor features do not work at all, or other failures occur but low-impact workarounds exist. This is the highest level for documentation bugs.
4 Minor	Failures occur under very unusual circumstances, but operation essentially recovers without intervention. Users do not need to install any workarounds and performance impact is tolerable.
5 Cosmetic	Defects do not cause any detrimental effect on system functionality.
6 Enhancement	Requests for new functionality or feature improvements.

Search for Bugs

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

Procedure

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

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

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

Open Caveats in Release 12.1(2)

Identifier	Severity	Headline
CSCvm67800	3	Jabber sometimes doesn't receive messages or calls after iOS12 has been installed.

Resolved Caveats in Release 12.1(2)

Identifier	Severity	Headline
CSCvm17626	2	Jabber prompts sign-out because of `EnableVoipSocket` parameter.
CSCvm33760	3	Jabber generates several UDS requests, which may degrade Call Manager performance.
CSCvm52895	3	Search results do not display immediately when response for first query is received.

Resolved Caveats in Release 12.1(1)

Identifier	Severity	Headline
CSCvk53979	3	Japanese "Available" presence on Jabber for iPhone and iPad 12.1 displays wrong meaning.

Open Caveats in Release 12.1

Identifier	Severity	Headline
CSCvj58867	3	Jabber keeps Rollover Counter and SSRC of SRTP stream after hold/resume.
CSCvj58876	3	Jabber keeps Rollover Counter and SSRC of SRTP stream after transfer.

Resolved Caveats in Release 12.1

Identifier	Severity	Headline
CSCvj71504	3	Cisco Jabber displays the `jabberAllConfig.xml` file as `jabber-config.xml` in the Problem Report.
CSCvj72793	3	Presence between Jabber for Windows and Jabber for iPhone and iPad does not sync after the app is brought to foreground.
CSCvj53337	3	The cache results of the initial Domain Name System (DNS) is re-used for each connection in a session.
CSCvj95723	3	Cisco Jabber crashes during launch because of the configurationparse error in the Telephony.