Release Notes for Cisco Jabber for Mac 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(1)	12.1.1.269866
12.1	12.1.0.266498

The DownloadURL file element in the XML file for automatic updates is:

Release	File Name
12.1(1)	Install_Cisco-Jabber-Mac-12.1.1.269866-76849656-MCwCFGTVpWwR0U2yaAR5Z6MT5T3sdE0HAhQ8uMs_vRUfZajT_h_0Q1ksjqzQ!!.zip
12.1	Install_Cisco-Jabber-Mac-12.1.0.266498-76830696-MCwCFA99MQpwOPMebIZAv7iAf_xOaglzAhRa5AGtnBfKKxeHqFmpuEfRDRkOw!!.zip

DownloadURL

The DownloadURL file element refers to the Cisco Jabber for Mac installation file. The installation file on the update server must be renamed to match this DownloadURL file element name.

You can also download the manual installation file, if your users install the client manually.

Note To ensure the DSA signature succeeds, configure Web servers to escape special characters. For example, on Microsoft IIS the option is: **Allow double spacing**.

What's New in Release 12.1(1)

New Values for Saving Chat History

The parameter `SaveChatHistoryToExchangeOperationMode` has additional values that affect how you can save Cisco Jabber chats to a folder in Microsoft Outlook. For more information, see the *Parameters Reference Guide for Cisco Jabber 12.1*.

macOS Mojave

This release includes support for macOS Mojave 10.14.

Resolved Caveats

This release provides fixes for several known defects.

What's New in Release 12.1

Telephony

- **Multiline Support for All Lines Over MRA**—Multiline is supported on all lines (primary and secondary) when using Cisco Jabber for desktop in Mobile and Remote Access (MRA) mode.

  For more information on configuring this feature, see the *Feature Configuration Guide for Cisco Jabber 12.1*.

- **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 have not retained the secure phone certificate, they have to contact you to configure the phone service.

- **DomainsForOutlookPresence**—Cisco Jabber for Mac now supports the parameter DomainsForOutlookPresence.

- **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.

Chat and Presence

- **Send Call Icon to Contacts**—Users can send a call icon to contacts by typing **:callme** in the chat window so that they can simply click on it to call back. To use this feature, you must enable URI dialing.

- **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.

- **Prevent Contact Duplication for Custom Contacts**—Cisco Jabber displays a notification if the custom contact details you're trying to add already exists. You can however add a duplicate contact if the user is already a directory contact.

Meetings

- **MacCalendarIntegrationType**—You can now integrate Google calendar with Cisco Jabber for Mac using the existing MacCalendarIntegrationType parameter. You can use this parameter to integrate Google Calendar with the Meetings tab.

- **Set Up Google Calendar**— You can now integrate Google calendar with Cisco Jabber for Mac.

UI Enhancements

- **Mobile Icon Added**—Cisco Jabber displays the mobile icon alongside the contact name in several areas of Jabber like contact list, search bar, profile, group chat participants list, and conference list. This icon indicates that the contact is signed into Cisco Jabber on a mobile device.

- **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.

- **Mute Individual Chat Rooms**—Users can disable notifications from specific chat rooms by muting them in the client.

Requirements

Software Requirements

Server	Software
Operating systems	• macOS Mojave 10.14 or later • macOS High Sierra 10.13 or later • macOS Sierra 10.12 or later • OS X El Capitan 10.11 or later

Server	Software

On-premises servers	• Cisco Unified Communications Manager version 10.5(2) or later (Minimum)
	
	Cisco Unified Communications Manager version 11.5(1) SU3 or later (Recommended)
	
	• Cisco Unified Communications Manager IM & Presence version 10.5(2) or later
	
	• Cisco Unity Connection version 10.5 or later
	
	• Cisco WebEx Meetings Server version 2.0 or later
	
	• Cisco Expressway Series for Cisco Unified Communications Manager
	
	    • Cisco Expressway-E:
	
	        • X8.10.1 or later (Recommended)
	
	    • Cisco Expressway-C:
	
	        • X8.10.1 or later (Recommended)
	
	• Cisco TelePresence Video Communication Server 8.1.1 or later
	
	• Cisco Meeting Server (CMS) 2.2 or later

Cloud-based servers	• Cisco WebEx Messenger service • Cisco WebEx Meeting Center, minimum supported version WBS31 or later
Directory servers	• Active Directory Domain Services for Windows Server 2012 R2 • 2.2 or later • Cisco Unified Communications Manager User Data Service (UDS) with Cisco Unified Communications Manager 10.5(2) or later • OpenLDAP 2.4 and later

Hardware Requirements

Hardware	Requirement
Installed RAM	2 GB RAM
Free Physical Memory	1GB
Free Disk Space	300 MB

Hardware	Requirement
CPU Speed and Type	Intel Core 2 Duo or later processors in any of the following Apple hardware: • Mac Pro • MacBook Pro (including Retina Display model) • MacBook • MacBook Air • iMac • Mac Mini
I/O Ports	USB 2.0 for USB camera and audio devices.

Network Requirements

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, 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 release 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 are used based on LDAP configuration.				

	Port	Application Layer Protocol	Transport Layer Protocol	Description
	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.
	5222	XMPP	TCP	Connects to Cisco Unified Communications Manager IM and Presence Service for instant messaging and presence.
	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-Premises 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	UDP	Far end camera control (FECC).
	5070 to 6070	BFCP	UDP	Binary Floor Control Protocol (BFCP) for video screen sharing capabilities.
Voice or 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.
	8000	RTP/SRTP	TCP	Used by Jabber Desk Phone Video Interface, allows users to receive video transmitted to their desk phone devices on their computers through the client.

	Port	Application Layer Protocol	Transport Layer Protocol	Description
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 Meetings Center for meetings.
	443	HTTPS	TCP	Connects to Cisco Webex Meetings 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.
Accessories Manager				
	8001		TCP	In Cisco Jabber for Windows and Mac, Sennheiser plugin uses this port for Localhost traffic for call controls.

Ports for Other Services and Protocols

In addition to the ports listed in this section, review the required ports for all protocols and services in your deployment. You can find the port and protocol requirements for different servers in the following documents:

• For Cisco Unified Communications Manager, Cisco Unified Communications Manager IM and Presence Service, see the *TCP and UDP Port Usage Guide*.

• For Cisco Unity Connection, see the *System Administration Guide*.

• For Cisco Webex Meetings Server, see the *Administration Guide*.

• For Cisco Webex services, see the *Administrator's Guide*.

• For Expressway for Mobile and Remote Access, refer to *Cisco Expressway IP Port Usage for Firewall Traversal*.

• For file transfer port usage, see the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

Limitations and Restrictions

Single Number Reach

For Cisco TelePresence Video Communication Server Control (VCS) versions earlier than 8.10.X, you need to configure the editable inbound rules to enable the single number reach for users who are using Cisco Jabber over Mobile and Remote Access. For more information, see *Limitations* in *Enable Single Number Reach* section from the *Feature Configuration Guide for Cisco Jabber 12.0*.

SIMPLE BIND LDAP Mechanism

Jabber for Mac only supports SIMPLE BIND LDAP mechanism.

Save Chats to Outlook

When you use Outlook 2016, all images sent in chats are not saved in Outlook, however any emoji sent in chats are saved in Outlook.

Audio Device Setting After Upgrade

When users upgrade the client, intermittently this results in a reset of their selected audio devices. To resolve this issue, set the audio devices in the **Audio/Video Preferences** window. This limitation is documented in CSCva48136.

Antivirus

When the client connects to Cisco Unity Connection on a device that has antivirus software, users can have issues with voicemail connections. To resolve this issue, add the Cisco Unity Connection server information to the exceptions list for the antivirus software.

Users in Common Identity

There is a known issue 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.

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** or **EC Preferred, RSA Backup**. However, the **EC Only** option is not supported by Cisco Jabber, and if you select it, the client fails to connect to the server.

Certificate Validation for CTI Connections

Cisco Jabber uses certificate validation for CTI connections. We recommend using either Public CA or Private CA to sign certificates.

Connecting to Cisco Unified Communications Manager using a self-signed certificate, results in a certificate validation failure, to resolve this issue do one of the following:

- The user accepts the invalid Cisco Unified Communications Manager self-signed certificate on first certificate validation failure and Cisco Jabber saves this certificate to the trust store.

• Deploy the certificates using a certificate deployment management application.

Expressway for Mobile and Remote Access Deployment

For an Expressway for Mobile and Remote Access deployment, when using an online certificate status protocol (OCSP) or online certificate revocation lists (CRL) to obtain the revocation status of the certificates, the Cisco Jabber client expects a response time of less than 5 seconds. Connections will fail if the response time is greater than the expected 5 seconds.

Network Disconnection When Using Cisco Jabber on Audio or Video Call

There is a known issue in the Mac OS where network interfaces drop intermittently when DSCP is enabled.

If you encounter this issue, do the following:

1. Select **Preferences > Calls > Advanced**.
2. Uncheck **Enable Differentiated Service for Calls**.

Standard CTI Secure Connection User Group

Cisco Jabber for Mac does not currently support CTI connections over transport layer security (TLS). As a result, Cisco Jabber for Mac users cannot switch from using a CSF device to using a desk phone device if they belong to the Standard CTI Secure Connection user group.

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(1)

Identifier	Severity	Headline
CSCvm47906	3	Jabber tries to reconnect to server even when LDAP bind fails because of invalid credentials.

Resolved Caveats in 12.1(1)

Idendifier	Severity	Headline
CSCvm44563	2	Contacts Directory under Account Preferences UI should not be available to edit.
CSCvj47601	3	Jabber generates several UDS requests, which may degrade Call Manager performance.
CSCvm49327	3	Search results do not display immediately when response for first query is received.

Open Caveats in Release 12.1

Identifier	Severity	Headline
CSCvj58903	3	Jabber keeps Rollover Counter and SSRC of SRTP stream after transfer.
CSCvj58906	3	Jabber keeps Rollover Counter and SSRC of SRTP stream after hold/resume.

Resolved Caveats in Release 12.1

Identifier	Severity	Headline
CSCvj47601	3	Jabber should not fall back on non-batch UDS search after batch API or bulk UDS search fails.
CSCvj85070	3	Broadcast Message option not available when a contact without an IM address is present.
CSCvj95503	3	Outlook presence feature can cause high CPU usage on CUCM/LDAP Server.
CSCvj62636	3	Unable to take screen captures.
CSCvj53345	3	Cache initial DNS results and reuse results for every connection in a session.
CSCvf88433	4	Jabber 11.9 voicemail menu calls Voicemail directly.
CSCvf92476	6	No chat sounds received in IM Only account.