Release Notes for Cisco Jabber for Mac 12.7

First Published: 2019-09-09

Last Modified: 2020-04-07

Build Number

Version	Build Number
12.7(1)	12.7.1.300628
12.7	12.7.0.288631

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

Release	File Name
12.7(1)	Install_Cisco-Jabber-Mac-12.7.1.300628-104904515-MC0CFQCYaddr1zsE2jCHTVW0yOYX9vT0kgIUC9VQJ8gByHM2jqVV4HXQVD1U5rE!.zip
12.7	Install_Cisco-Jabber-Mac-12.7.0.288631-104883351-MCwCFH0RoLLSfqAE5WPykrhxmMLECwXDAhRx0Uipg4aNaanhyMQBFUWEZKvHuQ!!.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 12.7(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

Apple Notarization Impact

We have completed Apple's notarization process for Cisco Jabber for Mac 12.7 on macOS 10.15.

However, these third-party Sennheiser headset plug-in is not yet notarized.

Because of the notarization requirements, Cisco Jabber for Mac 12.7 cannot support call controls (answer, decline, hold, and resume) on these headsets.

Refer to Sennheiser for more information on this issue.

Improved User Experience

Modern Design

We improved the user experience in this release with a new Modern Design. The Modern Design features a single-window UI. Jabber defaults to the Modern Design in all deployments. Users in on-premises and Webex Messenger deployments can choose to use the Classic Design.

Jabber Team Messaging Mode only supports the Modern Design view. Users cannot choose the Classic Design in Jabber Team Messaging Mode.

If you want your on-premises or Webex Messenger deployment to default to the Classic Design, you can set the default with the UXModel parameter. The allowed values are **Modern** (the default) and **Classic**. Each user's preference takes precedence over this parameter. For details, see the Parameters Reference Guide for Cisco Jabber.

Users can also customize their app by choosing their preferred design in **Preferences** > **Appearances**.

Themes

We have added themes for the Jabber app. The available themes are:

- Default

- Dark

- High Contrast

- System Settings

Users can switch between the available themes through **Preferences** > **Appearances**.

Improved Prompts for Office 365 Migration

After administrators migrate user accounts to Office 365, users that use Save Chats to Outlook, will receive a message that the account has been migrated and prompted to resubmit their credentials in order to continue using this feature.

Accessibility Improvements

We made accessibility improvements throughout the client, including the following:

- Improved accessibility text for screen readers.

- Added a high contrast theme which improves the color contrast and supports larger font sizes.

- Added a shortcut key, Ctrl + Cmd + M, to place focus on the screen share button. You can then choose to stop the share or share a different application.

Chat Rooms Maintains Participant List Visibility

We changed participant list behavior for group chats and chat rooms in on-premises and Webex Messenger deployments. Now, when you switch from one chat room to another chat room, it maintains the visibility of the participant list. If you open the participant list in Chat A and then switch to Chat B, the participant list is visible when you return to Chat A.

Person-to-person chats do not behave this way.

Display Tab Labels

By default in Release 12.6, the client didn't display tab labels in the hub window. Users can enable tab labels through their preferences.

If you want to change the default behavior for displaying tabs, use the new ShowTabLabel parameter. Each user's preference takes precedence over this parameter. For details, see the Parameters Reference Guide for Cisco Jabber.

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.

Presence Based on Non-Jabber Activity

In previous releases, Jabber team messaging mode reported users presence based only on their activity in the Jabber app. Jabber now reports your presence based on activity across your computer.

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, hover the cursor over the message you want to quote and select **Quote message**. 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.

Proxy Authentication Support

Earlier releases do not support proxy authentication. Jabber now supports proxy authentication as outlined in this table:

Product	Supported Authentication Types	Supported Proxy Configuration Methods
Cisco Jabber for Windows	No Auth, Basic, NTLM, Negotiate	Manual, PAC
Cisco Jabber for Mac	No Auth, Basic, NTLM	Manual, PAC
Cisco Jabber Softphone for VDI	No Auth, Basic, NTLM, Negotiate	Manual, PAC
For NTLM authentication on Mac, users are prompted for a password if the computer is not signed in to the domain. For Windows or Jabber Softphone for VDI, the computer must be signed in to the domain. For *No Auth* authentication types, you can set up the computer with a proxy address, but no authentication is used.		

For information on Proxy Auto-Config (PAC) files, see https://www.cisco.com/c/en/us/td/docs/security/web_
security/connector/connector2972/PACAP.html.

Proxy Authentication and Certificates

If you deploy a TLS-inspecting proxy, install a CA certificate into the OS of the device with a trust chain that allows a successful certificate validation.

Jabber validates the certificates of the systems with which it communicates. Jabber validates the certificates for a TLS session against the list of trusted root certificate authorities in the other system's OS. Jabber also checks the certificates against known malicious or compromised certificate authorities.

Meetings

On-Demand Recording

In previous releases, you could only enable or disable recording for all calls in Jabber. On-demand recording gives you the option to enable users to selectively record calls over Jabber's Built-In Bridge (BiB). When you enable this feature, the call control menu includes a **Record** option for the user to start and stop recording at any time.

You need Cisco Unified Communications Manager Release 12.5(1) to support this feature.

For information on using on-demand recording, see the Feature Configuration for Cisco Jabber guide.

You can force all recording to occur on the Jabber BiB with the Prefer_BIB_recorder parameter. For details, see the Parameters Reference Guide for Cisco Jabber.

Application Sharing

When you share your screen during a call, CMR meeting call, or CMS meeting call, you can limit what you share to a specific application, instead of sharing the entire screen. Now, from the Share Screen, you have the option of choosing which application to share.

Update to Collaboration Meeting Room Controls

This release gives the host the ability to mute or unmute all participants.

Calling

Voicemail Improvements

We improved the voicemail capabilities in the desktop clients.

Users can create voicemails without making a call and then send the voicemail to one or more contacts. The voicemail server's administrator can also create distribution lists to which users can send voicemails. Users can select recipients from the voicemail server's catalog.

Users can directly reply to the sender of a voicemail or to all recipients of that message. Users can also forward voicemails to new recipients.

Display Directory Number or Label for Single Lines

In multiline operation, users choose between their configured lines in a selection list. The selection list displays the directory number or the label for each line. In earlier releases, the selection list does not appear for users who only have a single line.

Now, for Phone-Only Mode and Phone Mode with Contacts deployments, the single line's number or label appears by default. For Full UC Mode deployments, the single line's number or label is hidden by default.

You can override the default behavior for single-line operation with the new SingleLinePhoneLabel parameter. For details, see the Parameters Reference Guide for Cisco Jabber.

Multiline Improvements

In earlier releases, Jabber has these multiline limitations:

- CTI-enabled users can only control the primary line on their desk phone.

- You couldn't configure two lines with the same number that are associated with different partitions.

As of Release 12.7, users can control all lines on their desk phone. You can also configure two lines with the same number that are associated with different partitions.

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.

Global Shortcut Keys

For security, we now disable global shortcut keys by default.

To enable global shortcut keys, first update your system security settings. Go to **System Preferences** > **Security & Privacy** > **Privacy** > **Input Monitoring** and enable Cisco Jabber. You can then set global shortcut keys in Jabber through **Preferences** > **General** > **Global Shortcuts**.

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 System for Cisco Jabber for Mac

You can install Cisco Jabber for Mac on the following operating systems:

- macOS Catalina 10.15 (or later)

- macOS Mojave 10.14 (or later)

- macOS High Sierra 10.13 (or later)

- macOS Sierra 10.12 (or later)

Hardware Requirements for Desktop Clients

Requirement	Cisco Jabber for Windows	Cisco Jabber for Mac
Installed RAM	2-GB RAM	2-GB RAM
Free physical memory	128 MB	1 GB
Free disk space	256 MB	300 MB
CPU speed and type	AMD Mobile Sempron Processor 3600+ 2 GHz Intel Core 2 Duo Processor T7400 @ 2.16 GHz	Intel Core 2 Duo or later processors in any of the following Apple hardware: • iMac Pro • MacBook Pro (including Retina Display model) • MacBook • MacBook Air • iMac • Mac Mini
GPU	DirectX11 on Microsoft Windows 7	N/A
I/O ports	USB 2.0 for USB camera and audio devices.	USB 2.0 for USB camera and audio devices

CTI Supported Devices

To view the list of Computer Telephony Integration (CTI) supported devices for your Unified Communications Manager:

1. From the **Cisco Unified Reporting** page, select **Unified CM Phone Feature List** from the **System Reports** menu.

2. After opening the report, select **CTI controlled** from the **Feature** drop-down list.

Limitations and Restrictions

Single Number Reach

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*.

Save Chats to Outlook

When you use Outlook 2016, Outlook won't save images that are sent in chats. However, Outlook does save any emoji in the chats.

Audio Device Setting After Upgrade

When users upgrade the client, it can intermittently result in a reset of their selected audio devices. To resolve this issue, set the audio devices in the **Audio/Video Preferences** window. CSCva48136 documents this limitation.

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's a known issue signing into Cisco Jabber for some users who have migrated to Common Identity. If users receive an *Incorrect username 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're creating devices for users in Cisco Unified Communications Manager 11.0, you can now specify a key order as either:

- **RSA Only**

- **EC Only**

- **EC Preferred, RSA Backup**

However, Cisco Jabber doesn't support the **EC Only** option. 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 verify certificate status, Cisco Jabber expects a response time of less than 5 seconds. Connections fail if the response time is greater than the 5 seconds.

Network Disconnection When Using Cisco Jabber on Audio or Video Call

There's 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 doesn't currently support CTI connections over transport layer security (TLS). As a result, Cisco Jabber for Mac users can't 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. When you add an enterprise group to your users' contact lists or they clear their local cache, they originally only see each person's username and domain. More information appears when they next hover over or interact with a person.

Caveats

Caveats describe unexpected behavior. The following sections describe how to obtain the latest information.

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.

For more information, select **Help** at the top right of the Bug Search page.

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.

Open Caveats in Release 12.7(1)

Identifier	Severity	Headline
CSCvr43256	3	Jabber Mac screen sharing immediately causes Jabber to crash

Resolved Caveats in Release 12.7(1)

Identifier	Severity	Headline
CSCvr39510	2	Jabber needs to mask the option to start a conversation when IM is disabled
CSCvr58963	2	Jabber login message "The Telephony configuration settings are invalid."

Open Caveats in Release 12.7

Identifier	Severity	Headline
CSCvr12551	3	Jabber does not refresh access token in failover scenario over MRA

Resolved Caveats in Release 12.7

Identifier	Severity	Headline
CSCvq46893	2	Jabber 12.6.1 crashes on opening for MAC

Identifier	Severity	Headline
CSCvp61058	3	Voice over screen feature on Jabber MAC does not enunciate the searched contacts return
CSCvq03999	3	Meeting host discrepancy between Jabber and Mac Calendar Integration
CSCvq10625	3	German translation error in Jabber, the button "Zeitplan" should normally be "geplante Konferenz"
CSCvq28009	3	Jabber bot: typing in HTML <textarea> moves focus to client's message input window
CSCvq66901	3	Jabber for Mac 12.6.1 Unable to see Participant list when calling into Webex
CSCvq97047	3	Jabber MAC strips country code when dialling out from call history.