Release Notes for Cisco Jabber for Mac 11.6

First Published: April 21, 2016

Introduction

These release notes describe new features, requirements, restrictions, and caveats for all versions of Cisco Jabber for Mac Release 11.6. These release notes are updated for every maintenance release but not for patches or hot fixes. Note that each maintenance release includes the features, requirements, restrictions, and bug fixes of the previous releases unless mentioned otherwise. Before you install Cisco Jabber for Mac, we recommend that you review this document for information about issues that may affect your system.

Build Number

Release 11.6

The build number for this release is:

`11.6.0.235520`

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

`Cisco-Jabber-Mac-11.6.0.235520-64245738-MC0CFEjxQKnTvq+20k0D+QxjUd_L1pcxAhUAmdDxKIBlPn0_hpuNVTHR7Q8tcg8!.zip`

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.

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 11.6

Presence Updates

- **Custom Status—**Users can quickly create their custom status on the Cisco Jabber hub window. For further information, see the *User Guide for Cisco Jabber for Mac*..
- **Visual Design—**Presence icons and contact avatars have been updated, for further information see the *User Guide for Cisco Jabber for Mac*.

Accessibility

- **Shortcuts—**Updates to shortcuts to improve accessibility, for further information see the *User Guide for Cisco Jabber for Mac*.
- **Visual Design—**Accessibility icons are updated, for further information see the *User Guide for Cisco Jabber for Mac*.

Select Screen to Share

When users decide to share their screen and they have more than one screen, they are provided with a list of screens to select which one to share.

Note This applies to BFCP screen share.

Smart Card Authentication Support

Cisco Jabber supports Smart Card authentication using the X.509 certificate. When more than one certificate is present, the client presents the user with a list to choose the appropriate certificate.

Note This is only supported when the Identity Provider (IdP) uses X.509 authentication as a single method for authentication.

Chats

When your users are enabled for logging instant message history, they can do the following:

- Users can choose if the chats are stored locally and also where the chats are stored. This is configured using the EnableAutosave parameter, for more information see the *Parameters Reference Guide for Cisco Jabber 11.6*.
- Users can save chats to file. This is configured using the EnableSaveChatToFile parameter, for more information see the *Parameters Reference Guide for Cisco Jabber 11.6*

For more information on allowing clients to log instant message history, see the *Feature Configuration for Cisco Jabber 11.6* guide.

IPv6

Cisco Jabber 11.6 is fully IPv6 ready, it works as normal in pure IPv6 and hybrid networks with the limitations listed in the Requirements chapter of the *Planning Guide for Cisco Jabber 11.6*. Cisco Collaboration solutions does not currently fully support IPv6. For example, Cisco VCS Expressway for Mobile and Remote Access has limitations in pure IPv6 networks that require NAT64/DNS64 to be deployed in mobile carrier networks. Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence don't currently support HTTPS in pure IPv6 networks.

This feature is configured in Jabber using the IP_Mode parameter to set the protocol to IPv4, IPv6, or dual stack. Dual stack is the default setting. The IP_Mode parameter can be included in the jabber-config.xml file, the bootstrap for Windows, and the URL configuration for Mac and Mobile clients. For more information, see the *Parameters Reference Guide for Cisco Jabber 11.6*.

The network IP protocol used by Jabber when connecting to services is determined by the following factors:

- The jabber-config.xml IP_Mode parameter.
- The client operating system IP capabilities.
- The server operating system IP capabilities.
- The availability of a DNS record for IPv4 and IPv6.
- Cisco Unified Communications Manager SIP setting for softphone devices configuration for IPv4, IPv6, or both. The SIP connection setting for softphone devices must match the Jabber IP_Mode parameter setting to make a successful connection.
- Underlying network IP capabilities.

On Cisco Unified Communications Manager, the IP capability is determined by generic server settings and device-specific settings. The following table lists the expected Jabber connections given the various settings, this list assumes that the DNS records for IPv4 and IPv6 are both configured.

When you use Jabber in IPv6_only mode, NAT64/DNS64 is required to connect to an IPv4 infrastructure. For example, when connecting to Cisco WebEx Messenger service, Cisco VCS Expressway for Mobile and Remote Access, and Cisco Spark.

Documentation Updates

The document *Features and Options for Cisco Jabber* has been renamed to *Feature Configuration for Cisco Jabber*. This document has been restructured so that features are grouped in functional sections and listed alphabetically.

Requirements

Software Requirements

Server	Software
Operating systems	• Apple OS X El Capitan 10.11 (or later) • Apple OS X Yosemite 10.10 (or later) • Apple OS X Mavericks 10.9 (or later)

Server	Software
On-premises servers	• Cisco Unified Communications Manager version 9.x or later • Cisco Unified Communications Manager IM & Presence version 9.x or later • Cisco Unity Connection version 8.6(2) or later • Cisco WebEx Meetings Server version 2.0 or later • Cisco Expressway Series for Cisco Unified Communications Manager ◦ Cisco Expressway-E Version 8.1.1 or later ◦ Cisco Expressway-C Version 8.1.1 or later • Cisco TelePresence Video Communication Server ◦ Cisco VCS Expressway Version 8.1.1 or later ◦ Cisco VCS Control Version 8.1.1 or later
Cloud-based servers	• Cisco WebEx Messenger service • Cisco WebEx Meeting Center, minimum supported versions T28 or later
Directory servers	• Active Directory Domain Services for Windows Server 2012 R2 • Active Directory Domain Services for Windows Server 2008 R2 • Cisco Unified Communications Manager User Data Service (UDS) Cisco Jabber supports UDS with Cisco Unified Communications Manager version 9.1(2) with the COP file cmterm-cucm-uds-912-3.cop.sgn. • 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.

	Port	Application Layer Protocol	Transport Layer Protocol	Description
Directory Integration—For LDAP contact resolution one of the following ports are used based on LDAP configuration.				
	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	TCP	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	UDP	Sends RTP media streams for audio or video.
	49152 to 65535	RDP	TCP	IM-only screen share. Applies to Cisco Jabber for Windows only.

	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 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 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

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.

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.

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 11.6

Identifier	Severity	Headline
CSCuy67512	Severe	Frequent crash in meetings
CSCuy64393	Moderate	No record in recents list, when call is answered on a shared line
CSCuv11787	Moderate	Jabber for mac does not send all digits when pasted into current call
CSCuy37533	Minor	Jabber for Mac recreates contact list group "Contacts" at each login
CSCux38739	Moderate	Jabber getting hang after sleep and resume
CSCux87795	Moderate	J4M- antivirus blocking voicemail connectivity after upgrade to 11.5

Closed Caveats in Release 11.6

Identifier	Severity	Headline
cscuw99634	Moderate	Remote side see presentation continuously refresh and or go blank.

© 2016 Cisco Systems, Inc. All rights reserved.