



Cisco Jabber for Windows 10.6.x Release Notes

Release Notes	2
Introduction	2
Requirements	7
Limitations and Restrictions	11
Performance and Behavior Notes	17
Caveats	19
Documentation Resources	29

Revised: June 9, 2016,

Release Notes

Introduction

These release notes describe new features, requirements, restrictions, and caveats for all versions of Cisco Jabber for Windows Release 10.6.x. 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 Windows, we recommend that you review this document for information about issues that may affect your system.

Build Number

Release	Build Number
Release 10.6(7)	10.6.7.29576
Release 10.6(6)	10.6.6.18021
Release 10.6(5)	10.6.5.16138
Release 10.6(4)	10.6.4.63238
Release 10.6(3)	10.6.3.61622
Release 10.6(2)	10.6.2.59142
Release 10.6(1)	10.6.1.55781
Release 10.6	10.6.0.52330

New and Changed Features in Release 10.6(7)

Resolved Caveats

This release provides fixes for a number of known issues. See the *Resolved Caveats in Release 10.6(7)* section for a list of caveats fixed in this release.

New and Changed Features in Release 10.6(6)

Resolved Caveats

This release provides fixes for a number of known issues. See the *Resolved Caveats in Release 10.6(6)* section for a list of caveats fixed in this release.

New and Changed Features in Release 10.6(5)

Changes to Call History for Transferred Calls

In previous releases, when a call was transferred to a user, the call history showed the call from the user who transferred the call. For example, User A calls User B and User B transfers the call to User C. The call history showed the call from User B.

In 10.6(5), the call shows as coming from the originator. For example, User A calls User B and User B transfers the call to User C. The call history shows the call from User A.

Set Automatic Refreshes for IBM Lotus Notes or Google Calendar

You can now define an automatic refresh time for IBM Lotus Notes or Google calendars using the `CalendarAutoRefreshTime` parameter. The default value is zero, meaning that the calendars do not automatically refresh. The value for the parameter defines the number of minutes after which the calendar refreshes.

Note that a high frequency refresh may affect performance of the IBM Lotus Notes server.

New and Changed Features in Release 10.6(4)

Disable Print Chat Feature

You can disable the ability for users to print conversations from the chat window using the `printchat_enabled` parameter. This parameter is true by default, where users can print chats. For more information about configuring this parameter, see the section on *Client Parameters* in the *Cisco Jabber 10.6 Deployment and Installation Guide*.

New and Changed Features in Release 10.6(3)

Disable Screen Savers During Calls

Specify whether you want the screen saver or computer lock function to be able to activate during a Cisco Jabber call. The new behavior is applied if the screen save or computer lock function is enabled on users' Windows computers and the user is inactive for a period of time. This parameter does not control any behavior for incoming calls when the screen is already locked or the screen saver is already on. After you finish the call or accept or reject the incoming call alert, then the screen saver or computer lock is enabled again.

The parameter is `SystemIdleDuringCalls`. The default behavior is that the parameter is false, and the screen saver or computer lock is not activated during active Cisco Jabber calls. For more information about configuring this parameter, see the *Client Parameters* section of the *Cisco Jabber 10.6 Deployment and Installation Guide*.

Show Recents Tab on Hub Window

Specify whether you want to show or hide users' call history from the **Recents** tab on the Cisco Jabber hub window. Configure this behavior with the `ShowRecentsTab` parameter. The default value is `true`, which shows the tab.

For more information about configuring this parameter, see the *Client Parameters* section of the *Cisco Jabber 10.6 Deployment and Installation Guide*

Enable Telemetry for Cloud IM-Only Users

You can now enable the collection of telemetry data in the Cisco WebEx Connect Administration Tool for IM-Only users in cloud deployments. If you have Telemetry settings defined in both the `jabberconfig.xml` file and in WebEx, then the setting in WebEx takes priority.

Show Display Names as Lastname, Firstname Format in Contacts List

For some locales, you can use the *Lastname, Firstname* format to display names in Cisco Jabber if the **displayname** directory field is empty or not available. This feature is only available for the following locales: Chinese (Hong Kong), Chinese (People's Republic of China), Chinese (Taiwan), Japanese, and Korean.

This display name format is configured by the `SwapDisplayNameOrder` parameter and is `true` by default, meaning that for the relevant system locales, when the **displayname** directory field is empty or not available, users' own display names and the display names of their contacts are displayed in the *Lastname, Firstname* format.

For more information about configuring this parameter, see the *Client Parameters* section of the *Cisco Jabber 10.6 Deployment and Installation Guide*

New and Changed Features in Release 10.6(2)

Call Forward Number Remembered in Client

In previous releases, when the user forwarded calls to another number, the number was removed from the client after call forward was turned off by the user. In 10.6(2), the last call forward number is saved in the call forward menu. Any time the user selects to forward calls to a new number, the previous call forward number is replaced.

Changes to IM Alert

When you receive a new IM, the alert that you hear is louder and slightly different to help ensure you don't miss new messages.

New and Changed Features in Release 10.6(1)

Certificate Validation for CTI Connections

Cisco Jabber for Windows no longer uses CTI server certificate validation.

Call with Edit

A new **Call with Edit** menu option is available from the hub window by right-clicking over a contact's name. Users can edit the number they are calling prior to making the call. When users select a number from this menu option, the call number is copied into the **Search or Call** field with the cursor automatically placed at the front of the number. Users can edit the call number prior to making the call.

No configuration is required to enable this feature.

Show Contact Pictures in Hub

The Cisco Jabber client has renamed the **Show Contact Pictures** option as **Show Contact Pictures in Hub**. This option is available in the client under the **Options > View** menu.

Only the name of the option has changed, the behavior has not; selecting it displays users' contact photos in the hub window on the **Contacts**, **Recents**, and **Voice Messages** tabs.

Prioritize Screen Share over Video Share

You can use a new configuration parameter, `PreferP2PDesktopShare`, to prioritize person to person screen sharing over video sharing in the Jabber configuration file. The default value is `false`, meaning that there is no change to the behavior in previous releases. For more information on this parameter, see the *Common Policies* section of the chapter to *Configure the Clients* in the *Cisco Jabber 10.6 Deployment and installation Guide*.

How you configure this new parameter does not affect the priority of video share during a conference call. Sharing your screen during a conference call will continue to use BFCP video share.

New and Changed Features in Release 10.6

Chat and Presence

- **Alert When Available** - Set your client to notify you when a contact becomes available. Right-click over the user's name to select the **Alert When Available** option. You are notified the first time the user next becomes available. A message notification is displayed on the top-right corner of your screen to alert you that the user is available.
- **Locations** - Create, define, and display your location in your client for your contacts to see. Configure the Locations feature using the `Location_Enabled` parameter, and users can define their settings in the **Options** menu.
- **Spell Check** - For Windows 7 and Windows 8, you can define a default language from the **Options** menu. From the chat window with another user, you can personalize the language for chats with that user that is different from the default language in your client.
- **Print Chat** - You can print a conversation with a right-click from a chat window with another user or by pressing CTRL + P. You can also highlight a portion of the text to print it.
- **AutoSave Chat** - From the **Options** menu, you can automatically save chats to your computer when you close a chat window. Once the chats are saved to your computer, search the chat files or use your Windows file search capability to search the chat files. You can save peer-to-peer and group chat conversations. This feature is off by default.
- **Client Behavior at Start Up** - By default, the client opens in a minimized state. However, you can configure the client to open in the same state that it was in when you last closed it. For example, if you last exited the client with the Jabber window open, then the next time you start Jabber, the window is opened. You set the `HonourLastWindowState` parameter to `true`. The option to **Start Cisco Jabber when my computer starts** must be enabled by the user for the parameter to take effect.
- **Remove Group Chat Participants** - The person who starts a group chat can now also remove group chat participants. Removed chat participants can be re-invited to the chat room at any time.
- **Conversation Tab Reordering** - You can drag and drop any kind of tab in your conversation window to put them in your preferred order. You can drag and drop tabs from person to person chat, group chat, and persistent chat room conversations. You can also drag and drop tabs from persistent chat room searches and filters, and all types of call tabs for audio and video.
- **Conversation Tab Switching Shortcut** - You can move between chat tabs by using CTRL+TAB keyboard navigation, or use CTRL+SHIFT+TAB to move up and down between tabs for each conversation.
- **Chat Security Labels** - Label chats with security labels are now available, such as "secret" or "top secret", or your company can create its own labels. Compliant with the XEP-256 standard.

- Passwords for Persistent Chat Rooms (on-premises deployments only) - Persistent chat room administrators can restrict access to rooms by adding passwords to them.
- Save Chat History to Outlook Folder - Enable saving chat history automatically in a Microsoft Outlook folder. This feature is off by default. Prerequisites: Microsoft Exchange 2010 or 2013.

Sharing

- Share Menu - A new menu is available from chat windows to share your screen and start instant WebEx meetings. To access these options, select the **More** button from the conversation window.
- Size Limit for File Transfers - Define a file size limit for Cisco Jabber users when transferring files.
- File Transfer enhancements (on-premises deployments only, prerequisite: Cisco Unified Communications Manager 10.5(2)) - In addition to standard file transfer between peers, you can now transfer files in group chats or persistent chat rooms. You can also use this feature to enable file transfer compliance, where you can manage screen captures and file transfers to restrict who can send and receive files, and keep a history of the file transfer and screen captures for auditing purposes.

Voice and Video

- Do Not Disturb - Call alerts and ringers are suppressed when your presence is Do Not Disturb, or in any red presence state. If you receive a call while in Do Not Disturb, you still see a missed call notification on your client. However, if you are using a headset with its own ringer, then the call rings is not suppressed on the headset. Both administrators and users can change settings for this feature.
- Call Notifications on Other Device - For users who do not want to interrupt their work to answer the phone, you can now disable incoming call alerts, which requires the call to be answered from a desk phone or a headset.
- Mute Before Answer - When you are joining a call, you can now mute your phone before you connect to the call.
- Audio Device Selection - You can select your preferred headset or other audio device directly from chat windows. A new option allows you to open audio options in the Jabber client, and select your microphone, headset, and ringer preferences.
- Ring on All Devices - You can hear incoming Jabber calls and alerts on your computer speakers and all connected devices. Even if your headphones are plugged in, when you receive a Jabber phone call or IM alert, the sound is played in both your headset and through your computer speakers. This feature is enabled by default, but users can change their ringer and alert preferences in the **Audio** tab of the Options menu.
- Call Stats - When on a call, users can now view information about the active call from their **File** menu, under **View > Show call statistics**.

Japanese Language

- This release includes improved Japanese localization.

User Management

- Single Sign On for Expressway for Mobile and Remote Access - You can now use SAML Single Sign On when connecting to the client from outside the corporate firewall on the Expressway for Mobile and Remote Access. Prerequisite: Cisco Expressway VCS-C or VCS-E 8.5(2).
- Mandatory Upgrade Support - You can now enable the client to require users to upgrade their client. To set mandatory upgrades for on-premises deployments, you set the Mandatory parameter in the upgrade .xml file to true. If you do not define mandatory

upgrades, or you set it to false, then users can choose to install the update. If you set the mandatory parameter to true, then users can only select to install the update or exit the client. This feature is supported in Cisco Jabber for Windows 10.5(2) and later.

- Flexible Jabber ID - When setting up Jabber, the Jabber ID (which identifies the Jabber user) can be mapped to the **Directory URI** field on Cisco Unified Communications Manager. This ID allows Jabber to identify the Jabber user by their AD mail attribute or their AD msRTCSIP-primaryuseraddress attribute. A user can log into Jabber with their sAMAccountName attribute, while the Jabber ID is mapped to the **Directory URI** field. For more information, see the ID Address Scheme section in the *Cisco Jabber 10.6 Deployment and Installation Guide*.
- Multiple Presence Domains - Also known as Multiple IM Address Domains, Jabber can be deployed into an infrastructure where users are organized into more than one domain, or into domains with subdomains.

US Federal Government Requirements

- FIPS 140-2 - You can use Cisco Jabber for Windows in compliance with FIPS (*Federal Information Processing Standard, Publication 140-2*) to ensure compliance with the standards for information security and encryption. When you set your Operating System to run in FIPS mode, Jabber detects FIPS mode and also runs in it. For more information, see the Security chapter in the *Cisco Jabber 10.6 Planning Guide*.

Changes to Documentation

Administrator Documentation - The administrator documentation set includes a *Planning Guide* and a *Deployment and Installation Guide*. The *Planning Guide* contains content from the previous release of the *Deployment and Installation Guide* and is intended to be used as a planning reference prior to installation. The *Deployment and Installation Guide* has several structural improvements which follows the installation process more closely, and has been rewritten to be more task-focused.

End User Documentation - The end-user documentation set includes a *Quick Start Guide* and a *User Guide*. The *User Guide* includes advanced topics, accessibility information, and troubleshooting information. It replaces the *Advanced Features Guide* and *Accessibility Guide* from the previous release.

Requirements

Software Requirements

Operating Systems

- Microsoft Windows 7 SP1 or later, 32 and 64 bit
- Microsoft Windows 8.x, 32 and 64 bit

On-Premises Servers

- Cisco Unified Communications Manager version 8.6(2) or later
- Cisco Unified Presence version 8.6(2) or later
- Cisco Unity Connection version 8.6(2) or later
- Cisco WebEx Meetings Server version 1.5 or later
- Cisco Expressway Series for Cisco Unified Communications Manager 8.1.1 or later

- Cisco TelePresence Video Communication Server 8.1.1 or later

Cloud-Based Servers

- Cisco WebEx Messenger service
- Cisco WebEx Meeting Center, version WBS28 or later

Directory Servers

- Active Directory Domain Services for Windows Server 2012 R2
- Active Directory Domain Services for Windows Server 2008 R2
- OpenLDAP
- Active Directory Lightweight Directory Service (AD LDS) or Active Directory Application Mode (ADAM)
- Cisco Unified Communications Manager User Data Service (UDS)

Cisco Jabber supports UDS using the following Cisco Unified Communications Manager versions:

- Cisco Unified Communications Manager version 9.1(2) with the following COP file: `cmterm-cucm-uds-912-5.cop.sgn`.
- Cisco Unified Communications Manager version 10.0(1). No COP file is required.

Hardware Requirements

Installed RAM

2 GB RAM on Microsoft Windows 7 and Windows 8

Free Physical Memory

128 MB

Free Disk Space

256 MB

CPU Speed and Type

- Mobile AMD Sempron Processor 3600+ 2 GHz
- Intel Core2 CPU T7400 @ 2.16 GHz

GPU

DirectX11 on Microsoft Windows 7

I/O Ports

USB 2.0 for USB camera and audio devices.

Network Requirements

Ports and Protocols

Port	Protocol	Description
443	TCP (Extensible Messaging and Presence Protocol [XMPP] and HTTPS)	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. Note Cisco Jabber can also use this port for: <ul style="list-style-type: none"> • HTTPS traffic to Cisco Unity Connection and Cisco WebEx Meetings Server. • Saving chats to the Microsoft Exchange server.
30000 to 39999	FECC	The client uses this port for far end camera control.
389	UDP/TCP	Lightweight Directory Access Protocol (LDAP) directory server.
636	LDAPS	LDAP directory server (secure).
2748	TCP	Computer Telephony Interface (CTI) used for desk phone control.
3268	TCP	Global Catalog server.
3269	LDAPS	Global Catalog server (secure).
5070 to 6070	UDP	Binary Floor Control Protocol (BFCP) for video desktop sharing capabilities.
5222	TCP (XMPP)	XMPP traffic to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.
8443	TCP (HTTPS)	Traffic to Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service.
7080	TCP (HTTPS)	Cisco Unity Connection for notifications of voice messages (new message, message update, and message deletion).
53	UDP/TCP	Domain Name System (DNS) traffic.
80	HTTP	Saving chats to Microsoft Exchange server. Depending on your server configuration on Microsoft Exchange, use either port 80 or 443, but not both.

Port	Protocol	Description
37200	SOCKS5 Bytestreams	Peer-to-peer file transfers. In on-premises deployments, the client also uses this port to send screen captures.
5060	UDP/TCP	Session Initiation Protocol (SIP) call signaling.
5061	TCP	Secure SIP call signaling.
49152 to 65535	TCP	IM-only screen share. The client randomly selects a port from the range. The actual range may vary. To find the real range, enter the netsh interface ipv4 show dynamicportrange tcp command. You can use the <code>SharePortRangeStart</code> and <code>SharePortRangeSize</code> parameters to narrow the range used for IM screen share. For more information on these parameters, see the section on Common Policies parameters in the <i>Deployment and Installation Guide</i> .

Third-party Requirements

Microsoft Internet Explorer

- Microsoft Internet Explorer 8 or later

Microsoft Office

- Microsoft Office 2013, 32 and 64 bit
- Microsoft Office 2010, 32 and 64 bit



Note Microsoft Exchange integrates directly with Cisco Unified Communications Manager. For more information, see the *Configuration Guides* for the appropriate version of Cisco Unified Communications Manager.

Microsoft SharePoint

- Microsoft SharePoint 2013
- Microsoft SharePoint 2010

Microsoft 365

Cisco Jabber for Windows supports client-side integration with Microsoft Office 365 with the following applications using an on-premises Active Directory (AD) deployment:

- Microsoft Office 2013
- Microsoft Office 2010
- Microsoft SharePoint 2010

Third-Party Calendars

- Microsoft Outlook 2013, 32 and 64 bit
- Microsoft Outlook 2010, 32 and 64 bit
- IBM Lotus Notes 9 32 bit
- IBM Lotus Notes 8.5.3 32 bit
- IBM Lotus Notes 8.5.2 32 bit
- IBM Lotus Notes 8.5.1 32 bit
- Google Calendar

Antivirus Exclusions

If you deploy antivirus software, include the following folder locations in the antivirus exclusion list:

- C:\Users\- C:\Users\- C:\ProgramData\Cisco Systems\Cisco Jabber

Limitations and Restrictions

Common Deployment Scenarios (Applicable to On-Premises and Cloud)

Authenticated Proxies

Hosted photos cannot be displayed in Cisco Jabber for Windows due to an issue supporting authenticated proxies, even if the server is listed in the Bypass setting. For more information on this item, see CSCul02706.

Blank Screen Share over VXME

If you are connecting to the client and meet all criteria below, the person you are sharing your screen with does not see the video content inside the share window. The user only sees a black rectangle.

- Connecting to your client in virtual environment
- Using VXME for softphone calls
- On a video call
- Sharing your screen

Call History Limit

The client can store up to 250 entries in your call history.

Call Pickup

The Call Pickup feature contains the following limitations:

- If the options for **Calling Party Information** and **Called Party Information** are disabled in Cisco Unified Communications Manager, then users logged into Call Pickup in softphone mode do not see either calling party or called party information displayed in the call alert notification. However, if those options are disabled and users log into Call Pickup in deskphone mode, then calling party or called party information is still displayed in the alert.
- If you select the **Audio only** notification on Cisco Unified Communications Manager and the user is on a call, then the user does not hear any sound indicating that there is a call to pick up.
- If users select **Pickup** on their deskphone when in Deskphone Mode, a conversation window is displayed momentarily.
- The pickup notification alert only displays a maximum of 23 characters.

Check Point VPN

Cisco Jabber for Windows does not currently support Check Point VPN.

Cisco Medianet Metadata Support

Cisco Medianet Metadata is no longer supported in Cisco Jabber for Windows.

Cisco Unity Connection Dispatch Messages

In Cisco Unity Connection, a dispatch message is sent to a distribution list with the message configured in such a way that only one user responds to that message. A user can accept, decline, or postpone the dispatch message. Cisco Jabber for Windows does not support Cisco Unity Connection dispatch messages.

Configuration Parameters for Photo Retrieval

You must include the configuration parameters for photo retrieval in the global configuration XML file (jabber-config.xml). If you include them in the group configuration XML file, photo retrieval might fail.

Declining Calls in Hunt Group

If you enable the **Legacy Immediate Divert** option in Cisco Unified Communications Manager, users cannot decline calls when they are logged into Hunt Group in softphone mode, but can decline calls in deskphone mode. To disable users to decline Hunt Group calls in both softphone and deskphone mode, you must enable the parameter `preventdeclineonhuntcall` in the configuration file.

Descriptions for Multiple Devices

You must enter descriptions for each device if Cisco Jabber for Windows users have multiple deskphone devices of the same model. Cisco Jabber for Windows displays these descriptions to users so that they can distinguish between multiple deskphone devices. If you do not enter descriptions, the client displays the model name of the device and users cannot distinguish between various devices of the same model.

Emails to a Group of Contacts

There is a limit of 2083 characters in the To field when sending an email to a group of contacts. Depending on the length of the email addresses and the number of contacts, not all contacts may be added to the email. For more information about the 2083 character limitation, see <https://support.microsoft.com/en-ie/kb/208427>. This limitation is documented in CSCuz80198.

Emoticons Not Displayed in IM Notifications

When you receive an IM notification that contains an emoticon, the IM notification only displays the description of the emoticon and not the actual emoticon. The emoticon is displayed normally in the actual IM conversation.

Expressway for Mobile and Remote Access Unsupported Features

When using Expressway Mobile and Remote Access to connect to services from outside the corporate firewall, the client does not support the following capabilities:

- Some High Availability Services—Voicemail services and audio and video services are not supported for high availability when you are connected to the client using the Expressway for Mobile and Remote Access. High availability for instant messaging and presence is supported.
- LDAP for contact resolution—Instead, the client must use UDS for contact resolution.
- Desk phone control mode (CTI), including extension mobility.
- Remote desktop control.
- Extend and Connect—You cannot use the Jabber client to make and receive calls on a non-Cisco IP Phone in the office; to control a non-Cisco IP Phone in the office, such as hold/resume; or control a home or hotel phone when connecting with Expressway Mobile and Remote Access.
- Session persistency—The client cannot recover from disruptions caused by network transitions. For example, if a users start a Cisco Jabber call inside their office and then they walk outside their building and lose Wi-Fi connectivity, the call drops as the client switches to use Expressway Mobile and Remote Access.
- Cisco WebEx Meetings Server—The client cannot access Cisco WebEx Meetings Server, or join or start Cisco WebEx meetings.
- Sending problem reports—To work around this issue, users can save the report locally and send the report in another manner.
- CAPF enrollment.
- Early Media—Early Media allows the client to exchange data between endpoints before a connection is established. For example, if a user makes a call to a party that is not part of the same organization, and the other party declines or does not answer the call, Early Media ensures that the user hears the busy tone or is sent to voicemail. When using Expressway Mobile and Remote Access, the user does not hear a busy tone if the other party declines or does not answer the call. Instead, the user hears approximately one minute of silence before the call is terminated.
- Self Care Portal—Users cannot access the Cisco Unified Communications Manager Self Care Portal when outside the firewall. The Cisco Unified Communications Manager user page cannot be accessed externally. The Cisco VCS Expressway or Cisco Expressway-E proxies all communications between the client and unified communications services inside the firewall. However, The Cisco VCS Expressway or Cisco Expressway-E does not proxy services that are accessed from a browser that is not part of the Cisco Jabber client.
- End-to-end media encryption— Media is not encrypted on the call path between the Cisco VCS Control or Cisco Expressway-C and devices that are registered locally to Cisco Unified Communications Manager. The media path outside of the enterprise is encrypted.

Extension Mobility Cross Cluster

Cisco Jabber for Windows does not currently support extension mobility cross cluster (EMCC).

Microsoft Outlook Local Contacts and Presence

Users' presence is unknown when the contact is manually added to contacts in Microsoft Outlook 2010 and 2013, when the contact is added to local (custom) contacts with an email address type of SMTP. To resolve this issue, delete the contact and add it again manually, ensuring the email address type is Exchange (EX). This item is documented in CSCu057172.

Multiple Resource Login

When a user signs in to multiple instances of the client at the same time, the chat feature behaves as follows in common deployment scenarios (more on multiple resource login in On-Premises Deployment Scenarios):

- Availability states change to 'Available' on all clients when users resume from hibernate on one client.
- Resuming from idle overrides custom availability states.
- Users who are signed in to multiple Cisco Jabber for Windows clients can join group chats from only one client.
- Cisco Jabber for Windows does not always reformat incoming text correctly when the sender is signed in to a client other than Cisco Jabber for Windows.

Plantronics Accessories and Software

If you use Plantronics accessories for Cisco Jabber call management, and if you have Plantronics Hub installed, ensure that at least version 3.5 is installed. Download Plantronics Hub 3.5 from the Plantronics website.

SAML Single Sign-On Limitations

When configuring SAML SSO on Cisco Unified Communications Manager and Unity Connection servers, you must use a fully qualified domain name (FQDN) instead of an IP Address to define the server name. If you use an IP Address, the client displays a warning message that the certificate is not valid. The requirement to use an FQDN is because the embedded Internet Explorer browser is not able to validate IP addresses in the **Subject Alternate Name** (SAN) certificate.

Software Phone Not Supported in Virtual Environments (VDI mode)

Software phones (CSF devices) are not supported in virtual environments. Use Cisco Virtualization Experience Media Engine (VXME) for Cisco Jabber for Windows call capabilities in a virtual environment.

Space Characters in Credentials

The following rules apply to space characters and credentials:

- Usernames can contain spaces in on-premises deployments.
- Usernames cannot contain spaces in cloud-based deployments.
- Passwords cannot contain spaces in any deployment scenario.
- The first and last characters of usernames in on-premises deployments must not be spaces. This is also true for usernames synchronized from a directory source.

Special Characters in Usernames or Passwords

Users with upper ACSII characters in their usernames or passwords is supported in Cisco Unified Communications Manager 9.1(2) or later, or users must use lower ASCII characters for their username and passwords for earlier versions. The Cisco Jabber for Windows softphone fails to register with Cisco Unified Communications Manager when users enter some special characters such as ü, ä, or ö in the username or password. The user receives the following error message: "Invalid username or password entered. Go to Phone Services in the Options window and enter the correct username and password".

Standard CTI Secure Connection User Group

Cisco Jabber for Windows does not currently support CTI connections over transport layer security (TLS). As a result, Cisco Jabber for Windows 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.

Third-Party Unified Communications Applications

Installing Cisco Jabber for Windows and third-party unified communications applications on the same machine may result in broken presence integration with Microsoft Office. This behavior is a result of both applications attempting to use the same Microsoft Office API. To resolve the issue, you can disable the Click2X command line installation switch in Cisco Jabber, or remove the third-party application. For more information, see *Common Installation Arguments* in the *Cisco Jabber Deployment and Installation Guide*.

Using Click-To-X feature with Contacts in Microsoft Outlook

If you are using UDS as a directory source, users can only use Click-To-X capabilities, such as Click-To-Call and Click-To-IM, to contact Microsoft Outlook users if they are already in the cache file. A cache file is created for someone if they are in the users' Cisco Jabber contacts list, or have a Cisco Jabber history created by the user previously searching, IMing, or calling them, or by leaving a voice message.

Using Hunt Group on Desk Phones

If users select **Use my phone for calls** in their client to enable deskphone mode, then they must log in or logout of their hunt groups using the deskphone. If users are in deskphone mode, then the **Log Into Hunt Groups** option in the Cisco Jabber client becomes disabled.

Video Resolution of Lifesize Endpoint after Hold/Resume

Users may experience resolution issues when using Jabber to make a call with a Lifesize Express 220 endpoint. If the user puts the call on hold, then after resuming the call the send and receive video resolutions on the Jabber end is greatly reduced.

Voice Messages

The client cannot play broadcast voice messages.

On-Premises Deployment Scenarios

Adding Federated Contacts

When adding federated contacts, Cisco recommends that users add the federated contacts as company contacts (**File > New > Company Contact**), rather than as custom contacts. Adding federated contacts as custom contacts can cause intermittent presence issues. This issue is documented in CSCuz59060.

Expressway for Mobile and Remote Access Unsupported Features

When using Expressway Mobile and Remote Access to connect to services from outside the corporate firewall, the client does not support the following on-premises deployment scenarios (more information in Common Deployment Scenarios):

- Cisco WebEx Meetings Server. The client cannot access Cisco WebEx Meetings Server, or join or start on-premises Cisco WebEx meetings.
- Sending problem reports. To work around this issue, users can save the report locally and send the report in another manner.

Disabling File Transfers and Screen Captures

You can disable file transfers and screen captures on Cisco Unified Communications IM and Presence with the **Enable file transfer** parameter.

If you disable the setting on the server, you must also disable file transfers and screen captures in the client configuration. Set the following parameters to false in your configuration file:

- Screen_Capture_Enabled
- File_Transfer_Enabled

Multiple Resource Login

When a user signs in to multiple instances of the client at the same time, the chat feature behaves as follows in on-premises deployments (more on multiple resource login in Common Deployment Scenarios):

- Signing in on one client changes custom availability states to 'Available' on other clients.
- If you set the availability state from 'On a call' to another state while on a call, the availability state does not automatically change to 'On a call' for subsequent calls.

Space Characters in Credentials

The following rules apply to space characters and credentials in on-premises deployment scenarios:

- Usernames can contain spaces in on-premises deployments.
- Passwords cannot contain spaces in any deployment scenario.
- The first and last characters of usernames in on-premises deployments must not be spaces. This is also true for usernames synchronized from a directory source.

Server Presence Issue in Client

If you are using Cisco Unified Presence 8.6.5 SU2 or earlier, or Cisco Unified Communications Manager IM and Presence 9.1.1 SU1 or earlier, the client might display users' presence as offline when the user is actually online and has a network connection. This presence issue is fixed in Cisco Unified Presence 8.6.5 SU3 and Cisco Unified Communications Manager IM and Presence 9.1.1 SU1 and 10.0.1. This item is documented in CSCui29999.

Contacting Federated Users After Changing Privacy Policies

Users may experience issues contacting federated users in the scenario below when the privacy policy is changed:

- 1 Users add federated contact to their contact lists.

- 2 Users change the policy for contacts outside the domain from **Prompt me every time** to **Block everyone** on the **Privacy** tab of the **Options** window.

As a result, the federated contacts remain in the contact list but do not display availability. Likewise, users cannot send or receive instant messages from those federated contacts.

- 3 Users change that policy from **Block everyone** to **Prompt me every time**.
As a result, Cisco Unified Presence removed the federated contacts from the contact lists. Cisco Unified Presence does not repopulate the federated contacts.

Because Cisco Unified Presence removed the federated contacts from the contact lists, users must add the federated contacts to their contact lists again to send instant messages or display availability status to those federated contacts. However, the federated contacts can send instant messages to the users, even if they are not in the contact list.

Cloud Deployment Scenarios

Blocking Users in Enterprise Groups

Blocking users does not prevent a blocked user's status from being displayed if the blocked users are in a contact list as part of an enterprise group. For example, User A blocks User B. However, User A is in User B's contact list as part of an enterprise group. As a result, User B can view User A's availability status.

Space Characters in Credentials

The following rules apply to space characters and credentials in cloud-only deployment scenarios:

- Usernames cannot contain spaces in cloud-based deployments.
- Passwords cannot contain spaces in any deployment scenario.

Photo Display

In late 2011, the WebEx server made changes to how photos are stored and formatted on the server. Due to this change, any photo uploaded before January 1, 2012 is not displayed in the client. To resolve the issue, users must re-upload the photo. For more information on this item, see CSCui05676.

Performance and Behavior Notes

Certificate Validation for CTI Connections

For Cisco Jabber Windows 10.6 connecting to Cisco Unified Communications Manager using a self-signed certificate results in a certificate validation failure. In this release, Cisco Jabber uses certificate validation for CTI connections.

To avoid certificate validation errors, we recommend the following:

- Use either Public CA or Private CA to sign certificates; don't use self-signed certificates.
- Deploy the certificates using a certificate deployment management application to ensure the certificates are in users' certificate store or keychain.
- Use fully-qualified domain names (FQDNs) instead of IP Addresses or Host Names in the service profile for each service.

If you use a self-signed certificate, users can accept the invalid Cisco Unified Communications Manager self-signed certificate when they receive the first certificate validation failure. Then Cisco Jabber saves this certificate to the trust store to prevent future certificate validation failures.

For more information on certificate validation in Cisco Jabber, see the chapter on *Certificates* in the *Cisco Jabber Planning Guide* and the chapter on how to *Set Up Certificate Validation* in the *Cisco Jabber Deployment and Installation Guide*.

Changes to IM-Only Telephony Configuration

If you are upgrading to this release, and your client is enabled for IM-only mode, then you must set the `Telephony_Enabled` parameter to `false`. If you do not set this parameter in IM-only mode deployments, then users may see disabled telephony capabilities on their user interface.

Conversation Window Behavior During Conference Calls

The settings to define the behavior of conversation windows are sometimes bypassed during conference calls. For example, a user configures the behavior of conversation windows to never come to the front. Then, during a conference call, the conversation window is brought to the front to add users to the conference call.

There are some situations where the conversation window does not behave as expected to benefit the user experience. These items are documented in CSCuo83446, CSCuo83415, CSCuo83452, CSCuo83387.

Credentials Prompt for SAML SSO Users

When users first sign-in using SAML SSO, they may be prompted to enter their user credentials outside of the Identity Provider (IdP). On subsequent logins, they are prompted by the IDP for credentials. This is because the user's email address is required to confirm whether they are enabled for SSO, and when the user supplies credentials, they are used to the email address associated with their username to confirm this information to determine whether the user is enabled for SSO.

To avoid initially prompting the user twice for their credentials upon initial sign-in to SAML SSO, you can set the `ServicesDomainSsoEmailPrompt` parameter that requires the user to sign in using their email address, which immediately confirms their status as being SSO-enabled and does not prompt them a second time to provide credentials.

For more information about this parameter, see the parameters description in the *Cisco Jabber Deployment and Installation Guide*.

Users may also be prompted to provide credentials to the client on a first log in attempt, before getting the IdP credentials page on a second log in. This occurs in the following circumstance:

- Users are homed on 10.5 SAML SSO-enabled cluster using 9.1 or 10.1 Central UDS
- Users sign in with clean cache and reset Jabber

Display Name Changes in Corporate Directory

When a user's first name or last name is changed either in LDAP or UDS directories, Cisco Jabber does not automatically update this information in the contact list for all watchers of this user. Users must manually update their contact lists using the following procedure:

- 1 Remove the contact from their contact list.
- 2 Sign out of Cisco Jabber.
- 3 Reset Cisco Jabber.
Click the gear icon and select **File > Reset Cisco Jabber**.
- 4 Sign in to Cisco Jabber again.
- 5 Add the contact again.

Incorrect Contact Name shown for Incoming Call

When the client receives an incoming call, an incorrect contact name can display. This can occur when you have a contact in Microsoft Outlook that has the same phone number as a contact in your company directory.

Meeting Reminders

Cisco Jabber displays pop-up reminders for Cisco WebEx meetings only. Reminders for non-Cisco WebEx meetings are not displayed.

Two meeting reminders are displayed for a meeting. One reminder displays the **Time to join** message. The other reminder includes a **Meeting details** link. Both reminders are sent automatically by the meeting host at the meeting start time. This behavior is documented in CSCuz06684.

If the URL for a WebEx meeting is changed (for example, by URL filter software), attempts to join the meeting from the meeting reminder or from the Meetings tab fail.

Phone-only Mode after Cisco Unified Communications Manager IM and Presence Service Upgrade

For on-premise deployments, if Cisco Unified Communications Manager IM and Presence Service is upgraded from release 9.1(1) to release 10.5(2) and clients appear in phone-only mode after the upgrade, then all clients must be reset.

Removing Participants During Conference Calls

Users can only remove participants from a conference call when using the softphone(CSF) device for calls. Users can't remove participants from conference calls in desk phone control mode or using extend and connect.

Text for Icons in Hub Window of Localized Clients

In localized versions of the client, the icons on the hub window contain descriptive text, such as Contacts, Recents, Voice Messages, and Meetings. When this text is localized into other languages, if the translation of the text for even one icon is too long to be displayed on the user interface, then no text is displayed for any of the icons.

Caveats

Search for Bugs

Bug Classification

Known defects, or bugs, have a severity level that indicates the priority of the defect. Development managers usually define bug severity. Severity helps the product team focus on bug fixes for future releases and prioritize fixes.

The following table describes bug severity levels:

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.

Severity level		Description
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

Use the **Bug Search** page to obtain more information about a bug.

- 1 Go to <https://tools.cisco.com/bugsearch>.
- 2 Sign in with your Cisco.com user ID and password.
- 3 Enter a bug ID or specify search parameters.

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

Open Caveats in Release 10.6(7)

There are no changes to the open caveats since Release 10.6(6). See the *Open Caveats in Release 10.6(6)* section for a list of open caveats in this release.

Resolved Caveats in Release 10.6(7)

Identifier	Severity	Headline
CSCux88529	2	Jabber client does not allow to enforce STARTTLS as required
CSCux41461	2	Evaluation of jabber-windows for OpenSSL December 2015 vulnerabilities
CSCux44307	2	libxml2 December 2015 parsing vulnerabilities
CSCuw61575	2	Edge Server Cert validation not checking Server Cert for a domain
CSCux50088	3	Jabber for Windows - Unable to load file sourced embedded tab icons
CSCux30543	3	Displaying 'Unable to load custom contact(s)' in phone only mode
CSCux39992	3	Jabber crash in enhanced_callcontrol_MD
CSCuw79394	6	Jabber retries SOAP login too aggressively on TCP_TIMEOUT

Open Caveats in Release 10.6(6)

Identifier	Severity	Headline
CSCuu41838	3	Transfer fails from CAD when used with Jabber on Agent Desktop.
CSCuu48040	3	Jabber custom tab does not load when registered through Expressway/MRA.
CSCuu78526	3	Calls on Windows 7 lang En to German can hear delay of voice.
CSCuu88517	3	Turkish translation issue with Outlook chat history.
CSCuu94669	3	Jabber 10.6.X IM/BFCP screen share between MS Surface Pros.
CSCuu94851	3	Jabber SSO webpage does not login when pressing enter.
CSCuu98714	3	Intermittent random hang in csfnetutil.

Resolved Caveats in Release 10.6(6)

Identifier	Severity	Headline
CSCuu81060	3	Unable to join meeting.
CSCuv43351	2	Jabber cannot start a WebEx Share with MS Patch KB3069392.
CSCuv32877	3	Jabber can't login by proxy with Webex Meeting Manager registry setting.

Open Caveats in Release 10.6(5)

Identifier	Severity	Headline
CSCuu41797	3	No alert given to users to re-login after downloading group config file.
CSCuu41838	3	Transfer fails from CAD when used with Jabber on Agent Desktop.
CSCuu48040	3	Jabber custom tab does not load when registered through Expressway/MRA.
CSCuu72531	3	Auto-Away overwrites "On a call" status in Jabber for Windows 10.6.4.
CSCuu78526	3	Calls on Windows 7 lang En to German can hear delay of voice.
CSCuu88517	3	Turkish translation issue with Outlook chat history.
CSCuu92387	3	Intermittent random Jabber Windows hang.

Identifier	Severity	Headline
CSCuu94669	3	Jabber 10.6.X IM/BFCP screen share between MS Surface Pros.
CSCuu94851	3	Jabber SSO webpage does not login when pressing enter.
CSCuu98714	3	Intermittent random hang in csfnutil.

Resolved Caveats in Release 10.6(5)

Identifier	Severity	Headline
CSCuu81136	2	Jabber Meeting integration causes a performance issue on Lotus Notes.
CSCuu01267	2	Directory search stops working after AD account lockout.
CSCuu15104	3	Jabber for Windows 10.6 login fails with non-ASCII characters in password.
CSCuu13788	3	Jabber for Windows 10.6.2 with SSO not starting minimized.
CSCuu40258	3	Jabber should do case insensitive comparison of username.
CSCuu09901	3	Jabber for Windows not using UDS Batch API under Phone only mode.
CSCuu94246	3	In one case EdgeRefreshTimer did not fire when expected.
CSCuu40662	3	Jabber for Windows missing IM log after pipe character in Outlook chat history.
CSCuu52975	3	Custom tab in group config file requires a restart.
CSCuu57551	3	Jabber unable to connect to Lotus Notes.
CSCuu63031	3	Plantronics headset issue with Jabber 10.6.3 and 10.6.4.
CSCut78172	3	Jabber 10.6 - Visual Voicemail stops updating/arriving in client.
CSCut73020	3	Custom script integration with Jabber 10.6.1(Custom Tab) does not work.
CSCut70830	3	Jabber for Windows unable to switch to softphone when primary CCM service is down.
CSCut83959	3	Jabber for Windows + A24 showing multiple devices for phone control.
CSCus56839	3	Transferred call history log is not the same as deskphone's.
CSCuu59562	6	Outlook 2013 Calendaring requires reg key to be installed by installer.

Open Caveats in Release 10.6(4)

Identifier	Severity	Headline
CSCuu01267	2	Jabber for Windows directory search stops working.
CSCut27108	3	Jabber hangs in ContactService!csf::Thread::join.
CSCut70830	3	Client won't failover to the secondary CUCM when primary is down.
CSCut77337	3	Jabber BFCP needs to keep ports open when traversing a firewall.
CSCut78172	3	Visual Voicemail stops updating/arriving in client.
CSCut83959	3	Jabber for Windows showing multiple devices for phone control.
CSCut95237	3	Persistent Chat error on maximum number of participants on PC boot.
CSCut95325	3	Jabber Expressway for Mobile and Remote Access failover - failing to set X-auth tag based on cached cookies.
CSCut99017	3	" File transfer cancelled" message appears two times in chat window.

Resolved Caveats in Release 10.6(4)

Identifier	Severity	Headline
CSCuu02593	3	Jabber 10.x getting delay and slow response due to Microsoft KB3038314.
CSCuu13833	3	Jabber Chat Records saved in Outlook have wrong date.
CSCuu30838	3	Jabber IM client Error: It was not a new session started, they try again.

Open Caveats in Release 10.6(3)

Identifier	Severity	Headline
CSCuu01267	2	Jabber for Windows directory search stops working.
CSCut27108	3	Jabber hangs in ContactService!csf::Thread::join.
CSCut64674	3	Directory connection fails on Jabber Windows with FIPS.
CSCut70830	3	Client won't failover to the secondary CUCM when primary is down.

Identifier	Severity	Headline
CSCut77337	3	Jabber BFCP needs to keep ports open when traversing a firewall.
CSCut78172	3	Visual Voicemail stops updating/arriving in client.
CSCut83959	3	Jabber for Windows showing multiple devices for phone control.
CSCut95237	3	Persistent Chat error on maximum number of participants on PC boot.
CSCut95325	3	Jabber Expressway for Mobile and Remote Access failover - failing to set X-auth tag based on cached cookies.
CSCut99017	3	" File transfer cancelled" message appears two times in chat window.
CSCuu02593	3	Jabber 10.x getting delay and slow response after Microsoft KB3038314.

Resolved Caveats in Release 10.6(3)

Identifier	Severity	Headline
CSCup13053	3	Text on some buttons doesn't fit in all languages.
CSCut07506	3	Jabber for Windows 10.6 unable to hear audio after hold/resume in SRST.
CSCut20185	3	Group Pickup fails when group pickup number starts with a *.
CSCut28286	3	Jabber for Windows unable to switch to Softphone when primary CCM service is down.
CSCut43021	3	Slow login when IM is disabled in IM&P server.
CSCut47808	3	Jabber audio alert stops working.
CSCut53747	3	Jabber over UDS - Name resolution doesn't work for E.164 numbers.
CSCut54481	3	After CTI failover the "Phone setting" message doesn't disappear.
CSCut62868	3	Jabber can't re-connect to Google calendar after network loss.
CSCut68738	3	Jabber for Windows unable to control Extension Mobility phone if Jabber logs in first.
CSCut76202	3	Disable location feature before first launch.
CSCut99760	3	Unable to re-connect to Jabber over Edge.
CSCuu03869	3	Jabber MRA failover - UDS directory search fails when VCSe goes down.
CSCuu08599	3	Edit contact, then rename group: there is a duplicate group on sign in/sign out.

Open Caveats in Release 10.6(2)

Identifier	Severity	Headline
CSCus90391	2	Jabber for Windows user failed to pass WebEx account authentication using Option > Meeting menu.
CSCur52815	3	SSO Web window may appear minimized when using Plantronics plugin.
CSCus95252	3	Silent installation of Jabber for Windows 10.6 with MediaNet 4.1.2 fails.
CSCut07506	3	Jabber for Windows 10.6 unable to hear audio after hold/resume in SRST.
CSCut20185	3	Jabber for Windows 10.6: Group Pickup fails when group pickup number starts with a "*".
CSCut27108	3	Jabber hangs in ContactService!csf::Thread::join.
CSCut42854	3	Jabber for Windows displays meetings that have been cancelled.
CSCut43021	3	Slow login when IM is disabled in IM&P server.
CSCut53747	3	Name resolution doesn't work for E.164 numbers- Jabber over UDS.
CSCut54481	3	After CTI failover, the "Phone setting..." message doesn't disappear.
CSCut27447	3	Refresh icon associated with Meetings tab does not act like a button.
CSCut28286	3	Jabber for Windows unable to switch to Softphone when primary CCM service is down.
CSCut47808	3	Jabber audio alert stops working.

Resolved Caveats in Release 10.6(2)

Identifier	Severity	Headline
CSCut16425	3	Incorrect display of "Time To Join" meeting pop-up in Norwegian.
CSCut17074	3	Jabber cannot control desktop until top of chat window toolbar goes away.
CSCut10632	3	Jabber iDivert for a second incoming call continues to ring.
CSCut04262	3	Jabber Photo URL will not work if it contains a space or %20.
CSCut02686	3	Duplicate participant list when starting group chat from a conference call.
CSCus50618	3	Voicemail playback quality can be choppy through Citrix.

Identifier	Severity	Headline
CSCus70832	3	Call made from deskphone shown as unknown in Jabber call log .db file.
CSCus90239	3	Jabber for Windows on Expressway for Mobile and Remote Access fails to connect when VPN is up.
CSCus52796	3	Call history change after call transfer.
CSCut29988	3	Auto upgrade fails to download installer via proxy.
CSCut57979	3	Contacts cache is corrupted when there are multiple lines in an AD field.
CSCut53424	3	Issue after upgrade from Jabber for Windows 10.5.1 to 10.6.1 CAPF Hash value.

Open Caveats in Release 10.6(1)

Identifier	Severity	Headline
CSCus90391	2	Jabber for Windows user failed to pass WebEx account authentication in Option >Meeting.
CSCuq85758	3	Jabber for Windows calendar integration in Lotus Notes.
CSCur52815	3	SSO Web window may appear minimized when using Plantronics plugin.
CSCus52796	3	Call history change after call transfer.
CSCus70832	3	Call made from deskphone shown as unknown in Jabber call log .db file.
CSCus90239	3	Jabber for Windows on MRA fails to connect when VPN is up.
CSCus95252	3	Silent installation of Jabber for Windows 10.6 with MediaNet 4.1.2 fails.
CSCut02686	3	Duplicate participant list on starting group chat from a conference call.
CSCut04136	3	Incorrect display name for Jabber users when phone numbers match.
CSCut04262	3	Jabber Photo URL will not work if it contains a space or %20.
CSCus42063	3	WebEx: Presence for contact remains offline until added to contact list.
CSCut07506	3	Jabber for Windows 10.6 unable to hear audio after hold/resume in SRST.
CSCut08284	3	File Transfer fails when users logged into both desktop and mobile clients.

Resolved Caveats in Release 10.6(1)

Identifier	Severity	Headline
CSCus64434 CSCus77103	3	Invalid certificate prompt when a CTI Connection is made.
CSCuq91678	3	For incoming calls, if no calling number is sent, then calling name is not shown.
CSCus77302	3	Jabber doesn't attempt the TFTP servers in the order returned by UDS API.
CSCus12594	3	After network disconnect & end call, presence always returns to Available.
CSCus50013	3	Deskphone not restoring when Jabber reconnected to network.
CSCus49913	3	When clicking chat rooms, all rooms change user to offline status.
CSCus50618	3	Voicemail playback quality can be choppy through Citrix.
CSCus91525	3	Jabber phone mode does not retain launch on startup setting.
CSCus56024	3	If userid != email, Jabber fails to connect to Exchange server.
CSCus80883	3	Jabber Excluding CUCM service still results in SRV query/login.
CSCut03774	3	Crash in csfnetutils from telemetry data.
CSCus90420	3	Incorrect user shown in group chat when user is removed/re-added.
CSCut04480	3	Jabber crashes intermittently in Contact Service after 10.6 upgrade.
CSCus38943	3	Remove "Check for Updates" from Help menu if no UpdateUrl is specified.

Open Caveats in Release 10.6

Identifier	Severity	Headline
CSCus49580	3	Jabber send traffic to Exchange even though calendar integration is OFF.
CSCuh67006	3	If LDAP not indexed, searches can be delayed and time out.
CSCuq91678	3	For incoming calls, if no calling number sent then the calling name not shown.
CSCun86894	3	HTML Tab - Unexpected behavior using CTreeNode.
CSCus18018	3	DTMF Fails if SIP Incoming/Contact Header port configured differently.

Identifier	Severity	Headline
CSCus48171	3	A small blank Jabber Panel pops up in front of Jabber's main panel.
CSCus32121	3	Unexpected failure when unable to render self view.
CSCus40093	3	CUP Service Discovery lookup not triggered on every signing.
CSCus50141	3	Custom contact photo lost on exit/sign out when adding the photo on edit.
CSCus42063	3	WebEx: Presence for contact remains offline until added to contact list.
CSCus45668	3	Installation issues upgrading from 9.* -> 10.*
CSCus49819	3	Call Forward number is not saved in Jabber Windows.
CSCus49913	3	Clicking Chat Rooms > All Rooms changing user to offline status.
CSCus12594	3	After network disconnect and call ends, presence always returns to Available.
CSCus50618	3	Voicemail playback quality can be choppy through Citrix.
CSCus52469	3	Jabber for Windows Unable to Desktop Share with Polycom MCU.
CSCuj40988	3	Client may show incorrect called number when in deskphone mode.
CSCus64434 CSCus77103	3	Invalid certificate prompt when a CTI Connection is made.

Resolved Caveats in Release 10.6

Identifier	Severity	Headline
CSCus03304	3	Chat Reply button not present on incoming call toast.
CSCur68119	3	Photo not displayed when png files are used.
CSCur43586	3	Clients try to authenticate multiple times when using MRA.
CSCuq49103	3	Issues joining instant WebEx meeting in Jabber.
CSCuq38365	3	Client adds route to CUCM to the Windows Routing table.
CSCur92836	3	IM History setting on CUP being ignored in Jabber client.
CSCuq65359	3	Click2X: When user is non-admin user on OS, there's an error in Jabber.
CSCur52815	3	SSO Web window may appear minimized when using Plantronics plugin.

Identifier	Severity	Headline
CSCus03203	3	OpenSSL 1.0.1h: SSLv3 CBC Padding Information Disclosure Vulnerability.

Documentation Resources

The following documents are available for Cisco Jabber for Windows.

- *Cisco Jabber for Windows Release Notes* - Provide administrators with a summary of information about the release, which include feature enhancements, requirements, limitations and restrictions of the software, and caveats overview.
- *Cisco Jabber Deployment and Installation Guide* - Provides administrators with task-based information for all Jabber clients. It contains end-to-end client deployment procedures, deployment scenarios and workflows, infrastructure configuration of services, and client configuration and installation.
- *Cisco Jabber Planning Guide* - Provides administrators with background and reference material to plan the deployment and installation of all Cisco Jabber clients. This guide contains information that helps you make decisions about how you are going to deploy the product, such as a product overview, planning considerations, deployment information, and requirements.
- *Cisco Jabber for Windows Licensing Information* - This Licensing Information document provides information on the open source libraries used by the application.
- *Cisco Jabber for Windows Quick Start Guide* - Instructions to help navigate end users around Cisco Jabber for Windows for the first time and use a few key features.
- *Cisco Jabber for Windows User Guide* - Provides an overview of task-based information about end user operation of the client, including accessibility information.

Related Topics

[Cisco Jabber for Windows Documentation Home Page](#)

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.