



Release Notes for Cisco Jabber for Windows 12.0

First Published: 2018-03-29

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

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

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

Build Number

Release	Build Number
Release 12.0	12.0.0.61695

What's New in Cisco Jabber for Windows 12.0

Telephony

- **Multiline Support**—Cisco Jabber introduces Multiline support for desktop clients. Multiline allows your users to perform various tasks using more than one configured line or phone number. You can configure up to 8 lines in softphone mode. When you enable multiline and your users access Cisco Jabber using a Mobile and Remote Access (MRA) deployment, only the primary line is supported. .
Cisco Jabber for Windows 12.0 supports Cisco Hosted Collaboration Solution (HCS), Cisco Packaged Contact Center Enterprise (PCCE), Cisco Contact Center Enterprise (CCE), and Cisco Unified Contact Center Express (CCX) 11.6 (up to 4 lines). For information on features and configuring Multiline, see the *Feature Configuration Guide for Cisco Jabber 12.0*.
- **Phone Mode with Contacts Deployment**—You can now deploy Cisco Jabber in phone-only mode with contacts, with the option of enabling presence for users. For more information, see the *Deployment Scenarios* chapter in the *Planning Guide for Cisco Jabber 12.0*.
- **Turn On or Turn Off Single Number Reach Destinations**—Your users can choose numbers from the available single number reach destinations in Cisco Jabber from the **Phone Controls** menu. For more information, see *Single Number Reach* section from the *Feature Configuration Guide for Cisco Jabber 12.0*.

- **Mute Cisco Jabber Calls**—You can configure your users microphone to be automatically muted for their Jabber calls. Use the **MuteAudioByDefault** parameter. Your users can change this setting in Cisco Jabber. For information, see the *Parameters Reference Guide for Cisco Jabber 12.0*.
- **Ignore Incoming Calls**—Users who don't have voicemail set up for them can now choose to ignore an incoming call. For more information, see the *Let Users Without Voicemail Ignore Calls* section from the *Feature Configuration Guide for Cisco Jabber 12.0*.
- **Enhanced Dual-Tone Multi-Frequency (DTMF) Support**—If a user enters a DTMF signal that is not supported by the system that Jabber is calling, then Jabber ignores the DTMF input from the user. Cisco Jabber supports the DTMF signals 0-9, *, #, +, A-D. For more information, see the *DTMF Support* section from the *On-Premises Deployment for Cisco Jabber 12.0*.
- **Cisco Headset Support**—Cisco Jabber supports Cisco headset models 531 and 532.

Administrator

- **Cisco Jabber Bots**—You can use the Cisco Devnet to get the Cisco Jabber Bot SDK to create an XMPP Chat Bot for your users. Configure the **AdminConfiguredBot** parameter to automatically add bots to users' contact lists and the **WhitelistBot** parameter to create a trusted Bot list. For more information, see the *Bots* section from the *Feature Configuration Guide for Cisco Jabber 12.0*.
- **Define Mobile and Remote Access Policies for User Profiles**—You can add MRA access policies in Cisco Unified Communications Manager for users working outside the corporate network, and control what services in Cisco Jabber they can access. You can allocate different MRA access policies to users in your organization. For more information, see the *Define Mobile and Remote Access Policies for User Profiles* section from the *On-Premises Deployment for Cisco Jabber 12.0*.
- **Access Web Pages through Custom Tabs**—You can configure your users web page as an internal or an external page to your network using the *internal* attribute using true or false values. For more information, see *Custom Embedded Tab Definitions* section from the *Feature configuration Guide for Cisco Jabber 12.0* and *Supported Services* section from the *Planning Guide for Cisco Jabber 12.0*.
- **Search by JID**—You can now set up Cisco Jabber to use the JID or email address of a user to resolve their presence in Microsoft Outlook. For more information, see *Microsoft Outlook Presence Integration* in the *Feature Configuration Guide for Cisco Jabber 12.0*.

Security

- **Wireless Location Monitoring**—It allows you to determine the physical location where your Cisco Jabber users are accessing the corporate network. This information is stored in Cisco Unified Communications Manager, and it helps integrated applications such as Cisco Emergency Responder to determine the physical location of a Cisco Jabber user who makes an emergency call. For more information, see *Wireless Location Monitoring* section from the *Feature configuration Guide for Cisco Jabber 12.0*.
- **Server Name Indication (SNI)**—Cisco Jabber supports SNI in an MRA deployment with a multitenant Hosted Collaboration Solution. For more information, see *Server Name Indication Support for Multitenant Hosted Collaboration Solution* section from the *Planning Guide for Cisco Jabber 12.0*.

Meetings

- **Schedule Meetings from Cisco Jabber**—Your users can leverage the capability of Outlook (must be installed) to schedule a meeting during a chat in Jabber. They can also add WebEx meeting links (via WebEx Productivity Tool T32.11 or later) to the meeting for users who are joining remotely.
- **Personal Meeting Room (PMR) Support for IBM Notes and Google Calendar**—Cisco Jabber now displays **Join in Jabber** and **Join in WebEx** buttons for WebEx PMR meetings when integrated with IBM Notes and Google Calendar.

Chat and Presence

- **New Animated Emoticons**—We've added 12 new animated emoticons.
- **Reset Password for Cisco Jabber**—If your organization is using fast sign-in, users now have a way to reset their password. We've updated the `Forgot_Password_URL` parameter so that you can configure it for all clients, which adds a **Forgot Password** link to their **Instant Messaging** account to let them change their passwords. For more information, see *Parameters Reference Guide for Cisco Jabber 12.0*.
- **Choose Front Camera for Video Calls**—If your users have Windows devices with front and rear cameras, Cisco Jabber will detect both cameras and offer users the ability to choose a camera in their **Video** tab. By default, their front camera will be used for video calls.

UI Enhancements

- **Voicemail**—We've renamed **Voice Messages** to **Voicemail**, and we've moved it under **Meetings**.
- **Meet Now** —When users right-click over someone's name in their contact list, the **Meet Now** option is now called **Start Meeting**.
- **Chat Rooms** —We've renamed the **Chat Rooms** tab to **Rooms**.

Requirements

Software Requirements

Server	Software
Operating systems	<ul style="list-style-type: none"> • Microsoft Windows 10, 32 and 64 bit (Desktop OS x86) • Microsoft Windows 8.x, 32 and 64 bit • Microsoft Windows 7 SP1 or later, 32 and 64 bit

Server	Software
On-premises servers	<ul style="list-style-type: none"> • Cisco Unified Communications Manager version 10.5(2) or later (Minimum) Cisco Unified Communications Manager version 11.5(1) SU3 or later (Recommended) • Cisco Unified Communications Manager IM & Presence version 10.5(2) or later • Cisco Unity Connection version 10.5 or later • Cisco WebEx Meetings Server version 2.6 MR1 or later • Cisco Expressway Series for Cisco Unified Communications Manager <ul style="list-style-type: none"> ◦ Cisco Expressway-E Version 8.10.1 or later ◦ Cisco Expressway-C Version 8.10.1 or later • Cisco TelePresence Video Communication Server 8.1.1 or later • Cisco Meeting Server (CMS) 2.0 or later
Virtual servers	<ul style="list-style-type: none"> • Citrix XenDesktop 6.5, 7.5, and later 7.x versions • Citrix XenApp 6.5, 7.5, and later 7.x versions for published apps and desktop • VMware Horizon 6.0 (with View) • VMware Horizon 6 version 6.1.0, 6.2.0, 7.0, and later 7.x versions
Cloud-based servers	<ul style="list-style-type: none"> • Cisco WebEx Messenger service • Cisco WebEx Meeting Center, version WBS31 or later • Cisco WebEx Meetings Server 1.5 and later
Directory servers	<ul style="list-style-type: none"> • Active Directory Domain Services for Windows Server 2016 • Active Directory Domain Services for Windows Server 2012 R2 • Active Directory Domain Services for Windows Server 2008 R2 • Any server that supports the LDAPv3 protocol • Active Directory Lightweight Directory Service (AD LDS) or Active Directory Application Mode (ADAM)
User Data Service	Cisco Unified Communications Manager User Data Service (UDS) with Cisco Unified Communications Manager 10.5(2) or later
Instant Messaging	Microsoft Internet Explorer 9 or later

Hardware Requirements

Hardware	Requirement
Installed RAM	2 GB RAM
Free Physical Memory	128 MB
Free Disk Space	256 MB
CPU Speed and Type	<ul style="list-style-type: none"> • Mobile AMD Sempron Processor 3600+ 2 GHz • Intel Core2 CPU T7400 at 2.16 GHz • Intel Atom
GPU	DirectX11 on Microsoft Windows 7
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				

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

	Port	Application Layer Protocol	Transport Layer Protocol	Description
	2748	CTI	TCP	Computer Telephony Interface (CTI) used for desk phone control.
	5060	SIP	TCP	Provides Session Initiation Protocol (SIP) call signaling.
	5061	SIP over TLS	TCP	SIP over TCP Provides secure SIP call signaling. (Used if Secure SIP is enabled for device.)
	30000 to 39999	FECC	UDP	Far end camera control (FECC).
	5070 to 6070	BFCP	UDP	Binary Floor Control Protocol (BFCP) for video screen sharing capabilities.
Voice or Video Media Exchange				
	16384 to 32766	RTP/SRTP	UDP	Cisco Unified Communications Manager media port range used for audio, video, and BFCP video desktop share.
	33434 to 33598	RTP/SRTP	UDP	Cisco Hybrid Services (Jabber to Jabber calling) media port range used for audio and video.
	49152 to 65535	RDP	TCP	IM-only desktop share. Applies to Cisco Jabber for Windows only.
	8000	RTP/SRTP	TCP	Used by Jabber Desk Phone Video Interface, allows users to receive video transmitted to their desk phone devices on their computers through the client.
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				

	Port	Application Layer Protocol	Transport Layer Protocol	Description
	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: <ul style="list-style-type: none"> • Cisco Unified Communications Manager IP Phone (CCMCIP) server for assigned devices. • User Data Service (UDS) for contact resolution.
Accessories Manager				
	8001		TCP	In Cisco Jabber for Windows and Mac, Sennheiser plugin uses this port for Localhost traffic for call controls.

Ports for Other Services and Protocols

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

- For Cisco Unified Communications Manager, Cisco Unified Communications Manager IM and Presence Service, see the *TCP and UDP Port Usage Guide*.
- For Cisco Unity Connection, see the *System Administration Guide*.
- For Cisco WebEx Meetings Server, see the *Administration Guide*.
- For Cisco WebEx services, see the *Administrator's Guide*.
- For Expressway for Mobile and Remote Access, refer to *Cisco Expressway IP Port Usage for Firewall Traversal*.
- For file transfer port usage, see the *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*.

Third-Party Requirements

Third-Party Software	Requirement
Microsoft Internet Explorer	Microsoft Internet Explorer 9 or later Note Browser Click to Call is not supported on Microsoft Edge.

Third-Party Software	Requirement
Microsoft Office	<ul style="list-style-type: none"> • Microsoft Office 2016 Desktop OS Version, 32 and 64 bit • Microsoft Office 2013, 32 and 64 bit • Microsoft Office 2010, 32 and 64 bit <p>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.</p>
Microsoft SharePoint	<ul style="list-style-type: none"> • Microsoft SharePoint 2013 • Microsoft SharePoint 2010
Microsoft 365	<p>Cisco Jabber for Windows supports client-side integration with Microsoft Office 365 with the following applications using an on-premises Active Directory (AD) deployment:</p> <ul style="list-style-type: none"> • Microsoft Office 2016 Desktop OS Version, 32 and 64 bit • Microsoft Office 2013 • Microsoft Office 2010
Third-party calendars	<ul style="list-style-type: none"> • Microsoft Outlook 2016, 32 and 64 bit • 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\\AppData\Local\Cisco\Unified Communications\Jabber
- C:\Users\\AppData\Roaming\Cisco\Unified Communications\Jabber
- C:\ProgramData\Cisco Systems\Cisco Jabber

Limitations and Restrictions

Limitations and Restrictions All Deployments

Single Number Reach

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

Voicemail Credential Popup during Sign in

In a hybrid deployment, if Webex messenger, Call Manager and Unity connection are all SSO enabled, and voicemail credentials have been previously saved to cloud, users may see the **Update Credentials** popup for voicemail during the sign-in process. The workaround is to not configure voicemail server address on the cloud server but only configure it in the service profile or the `jabber-config.xml` file.

IBM Notes Contact Search

When searching for an IBM Notes contact, entering either " or \ as the first character in the search string won't find the correct contact.

Real-Time Transport Control Protocol (RTCP)

Jabber will continue to send RTCP packets even when disabled. RTCP is an integral component of Jabber Telephony services.

Outlook Save Chat feature with Office 365

Applies to: Cisco Jabber for desktop clients.

To use the Outlook **Save Chat** feature with Office 365, the user must enter credentials manually in Jabber with a single sign-on (SSO) deployment.

Cannot Copy Image

You cannot right-click over an image in a conversation in Jabber and select copy. You must highlight the image and then right-click to copy it.

Microsoft Outlook OST File

Intermittently Cisco Jabber for Windows is unable to access the Microsoft Outlook OST file. To resolve this issue, restart Jabber and restart Outlook.

Automatic Detection of Proxy Settings (WPAD)

Cisco Jabber does not support Web Proxy Auto-Discovery (WPAD) proxy discovery. For information about how to configure proxy settings for Cisco Jabber, see *Configure Proxy Settings* in the *On-Premises Deployment for Cisco Jabber* guide.

Call Transfers

When you are transferring a call to a third party, the third party must respond to the call before you can complete the transfer. You cannot currently dial the third party and connect the first party while waiting for the call to connect (also known as a blind transfer).

Chat Reply and No Voicemail Profile

The chat reply feature does not work if the user has no voicemail profile configured. If the user selects **Chat reply** in an incoming call, the call continues to ring and the **Chat reply** and **Answer** options are greyed out. This limitation is documented in CSCux75667.

Check Point VPN

Cisco Jabber for Windows does not currently support Check Point VPN. This limitation is documented in CSCuy34099.

Cisco AnyConnect Secure Mobility Client

Cisco Jabber for Windows supports Cisco AnyConnect Secure Mobility Client version 4.0 and later. This limitation is documented in CSCuy14721.

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. This limitation is documented in CSCuw31908.

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>.

Location Feature and Multiple Domain Support

Consider the following deployment scenario:

When you deployed your Cisco Unified Communications Manager IM and Presence Service node, all users were imported with single domain support. You later changed the address scheme to Directory URI (multiple domain support).

The location feature will now not work for newly added domain users. Users in the initial domain are unaffected. This limitation is documented in CSCuu63734.

Logitech Keyboard Display Changes

The built-in display for Logitech UC keyboard K725-C does not display caller or device information on incoming calls. Instead, the Cisco logo is displayed.

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 CSCuo57172.

Phone Mode Deployments with Microsoft Lync

Click-to-x functionality must be disabled if you want to deploy Cisco Jabber for Windows in phone mode on the same computer as Microsoft Lync. See the *Common Installation Arguments* section of the *Deployment Guide* for more information about the CLICK2X installer switch.

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.

Remote Desktop Control over Mobile and Remote Access

Remote desktop control over Mobile and Remote Access is not supported. This limitation is documented in CSCuz19139.

SAML Single Sign-On Limitations

When configuring SAML SSO on Cisco Unified Communications Manager and Cisco Unity Connection servers, 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.

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 rule is also true for usernames synchronized from a directory source.

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. This limitation is documented in CSCux83786.

.TIFF Images Not Supported

In this release, if users have a .tiff image as their avatar, then Jabber will display the default icon image instead. To use a personal avatar, users must upload an image in a supported format, such as jpg, bmp or png.

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

If you use 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.

Supported Characters in a Cisco Jabber User ID/E-mail Address

The following characters are supported in a Cisco Jabber user ID/E-mail Address:

- Uppercase characters (A to Z)
- Lowercase characters (a to z)
- Numbers (0-9)
- Period (.)
- Hyphen (-)
- Underscore (_)
- Tilde (~)

Limitations and Restrictions for On-Premises Deployments

Adding Federated Contacts

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

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 currently supported by Cisco Jabber, and if you select it, the client will fail to connect to the server.

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.

SIP Trunk for Phone Presence

From Release 11.5(3), you must configure a SIP trunk between Cisco Unified Communications Manager and IM and Presence Service if you want Cisco Jabber users to see phone presence. In previous releases, a SIP trunk was not required for phone presence. This limitation is documented in CSCuz85578.

Limitations and Restrictions for Cloud Deployments

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.

Invitees to Instant WebEx Meetings

Invitees to instant WebEx meetings must be provisioned with WebEx accounts before they can join an instant WebEx meeting. For example, User A has a WebEx account and starts an instant WebEx meeting from Cisco Jabber. User A then invites User B, who does not have a WebEx account, to the meeting. When User B clicks on the meeting link in Cisco Jabber, an error message is displayed and the user can't join the meeting. User B must be provisioned with a WebEx account before attempting to join any instant WebEx meetings. This limitation is documented in CSCux52068.

Jabber to Jabber Calls

We recommend running Internet Explorer 10 or greater while using the Jabber to Jabber calling feature. Using this feature with previous versions of Internet Explorer or with Internet Explorer in Compatibility Mode can cause issues with Cisco Jabber client login (non-SSO setup) or Jabber to Jabber calling capability (SSO setup).

Users in Common Identity

There is a known issue with signing into Cisco Jabber for some users who have migrated to Common Identity. If users receive an *Incorrect user name or password* error message when entering their username and password, see the following knowledge base article https://cisco-support.webex.com/guest/articles/en_US/Troubleshooting/WBX000019555/myr=false

Performance and Behavior Notes

Presence indicators on Sharepoint 2016

When you sign-out of Jabber, the presence indicator bubbles are grayed out and do not refresh after signing back into Jabber.

You can resolve this behavior by refreshing the webpage. This will ensure that accurate presence information is displayed.

Do Not Disturb (DND)

If Jabber is controlling the Deskphone and if Do Not Disturb (DND) is set on the Deskphone, the presence status of the Jabber client does not change.

This behavior indicates that the Jabber client is functioning as designed. No action is required from the user.

Mobile Presence Icon

The icon that shows other users that you are in a mobile location is not displayed in this release.

Jabber to Jabber Calls and Symantec Host IDS (HIDS)

Jabber to Jabber calls can trigger errors in Symantec HIDS.

Symantec HIDS has a rule that disables connections from internet-based servers if it receives 5 connection requests from the same internet-based server within 200 seconds. For example, 3 Jabber to Jabber calls within 200 seconds will trigger Symantec HIDS. When this happens, ongoing Jabber to Jabber calls are dropped and Jabber to Jabber calls are disabled for 600 seconds.

To avoid this scenario, you must add Cisco Jabber to the Symantec exception list. This behavior is documented in CSCuw32007.

HTML Sanitization Code

The Jabber HTML sanitization code has been modified to disallow 'masked' links in XMPP message payloads due to its potential abuse in phishing attacks. These links are no longer allowed for security reasons.

It is recommended that Jabber Administrators educate potential users who may be affected by this feature enhancement.

Meeting Reminders

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

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. This behavior is documented in CSCux03658.

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.

Video Calls

The **Start My Video** button doesn't work immediately after a call connects. Users must wait approximately 6 seconds after the call starts before clicking the **Start My Video** button. This behavior is documented in CSCuz06415.

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.
-

Open Caveats

Identifier	Severity	Headline
CSCvi34495	2	Jabber unable to merge UDS servers in cache config during fast login.
CSCvi72433	2	Unable to complete consult conference, seen on finesse agent 1's desktop - CTI error.
CSCvi12423	3	Jabber shows a default avatar instead of user's photo on the login screen.
CSCvi15038	3	Jabber desk phone control menu shows CIPC, although it's not supported.
CSCve68106	3	Conference failing with Jabber in MRA mode.

Identifier	Severity	Headline
CSCvi49056	3	Jabber should not attempt to resolve contact by numbers when the numbers are from Outlook source.
CSCvi46984	3	Chinese Simplified & Traditional characters appear bold.
CSCvi25845	3	Jabber quits unexpectedly at TextInputFramework!KeyStateTracker::InitializeAsyncKeyStateReader()
CSCvi25348	3	Jabber uses proxy IP address for LDAP directory integration.
CSCvi17064	3	Skype for Business initiated group chat cannot be joined by Jabber from Jabber 11.8.4.
CSCvh97506	3	Jabber screen share disable button not visible.
CSCvh29610	3	Memory leak detected while switching from front to rear camera on Microsoft Surface.
CSCvh15607	3	Title bar display not clear in multiple monitors with high dpi.

Resolved Caveats

Identifier	Severity	Headline
CSCve71017	2	Enhancement request : Jabber to perform GC/LDAP DNS SRV on domain name.
CSCvf51026	2	Jabber login fails when username contains # symbol.
CSCvf32185	3	Jabber incorrectly sends DTMF flash event even when peer doesn't support it.
CSCvg00193	3	Jabber unable to share a presentation during a secure call.
CSCvg01290	3	Jabber may crash during Outlook contact search.
CSCvg22265	3	Jabber for Windows 11.9.1 crashes in DesktopShareNotificationInfo::ConnectBindings.
CSCvi60638	3	Jabber freezes and forces a restart when making or receiving calls.
CSCvg25718	3	Surface Pro 4 & Surface Book - Unable to search UDS directory.
CSCvg48175	3	Jabber for Windows contact search delay with an invalid LDAP server configuration.

Identifier	Severity	Headline
CSCvg72905	3	Jabber for Windows 11.9.1 SSO cookie refresh failure, request too long.
CSCvg84104	3	Directory connection fails with OpenLDAP for Anonymous Binding.
CSCvg86464	3	SSO cookie needs to be cleared upon sign out if Fast Login is disabled.
CSCvg92408	3	Jabber for Windows unable to retain CTIRD directory information after a reset.
CSCvg96504	3	Jabber for Windows fails to transform URL when trying to connect over MRA.
CSCvh05723	3	Jabber does not correctly handle 302 redirect during an SSO session.
CSCvh44061	3	Jabber for Windows in Citrix environment produces echoes when receiving IM.
CSCvh53260	3	Display Jabber "Mobile Phone" icon on contact list for iOS/Android users.
CSCvh61653	3	Local web-server hostname included in IE exception list not bypassed by Jabber if format is < local >.
CSCvh75441	3	Jabber client displays garbled description on desk phone.
CSCvi19867	3	Jabber does not show Caller ID on transfer calls in the call window.
CSCvi24548	3	Chats history tab not updating presence info for users not in contact list.
CSCvi30936	3	When using call pickup with hunt pilot, no call window appears for Jabber for Windows 11.9.3.
CSCvi31585	3	Jabber for Windows displays blank IM messages.
CSCvi36313	3	Jabber for Windows 11.9 does not use usesystemlanguage parameter for the client language.
CSCuw75539	4	Jabber for Windows call statistics shows incorrect channel rate.
CSCvh13730	4	Windows repair of Jabber Desk Phone Video Services Interface 4.1.7 for Windows 10 causes failures.
CSCvf31969	6	Enhancement: Persistent chat window should be resizable.
CSCvi21206	6	Enhancement: Add scroll button to option "Add to:" for 'Status Request' pop-up

