Cisco Jabber for Windows 10.6 Release Notes

Revised: January 26, 2015,

Release Notes

Introduction

Build Number

The build number for this release is 10.6.52330.

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.

Features and Enhancements

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 T28 or later
- Cisco WebEx Meetings (Wbx 11, High Touch only)

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) or later 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 (XMPP and HTTPS)	XMPP traffic to the Cisco 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 HTTPS traffic to Cisco Unity Connection and Cisco WebEx Meetings Server.
389	UDP / TCP	LDAP directory server
636	LDAPS	LDAP directory server (secure)
3268	TCP	Global Catalog server
3269	LDAPS	Global Catalog server (secure)
5222	TCP (XMPP)	XMPP traffic to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.

Port	Protocol	Description
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
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 signalling
5061	TCP	Secure SIP call signalling

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

Limitations and Restrictions

Limitations and Restrictions

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

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`".

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.

Cisco Medianet Metadata Support

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

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.

Call History Limit

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

Plantronics Accessories and Software

If you are using Plantronics accessories for Cisco Jabber call control, ensure that Plantronics Spokes or Plantronics Hub software is not installed on any deployments of Cisco Jabber as it causes issues with the user experience. Consult with Plantronics on the recommended software that can be used with Cisco Jabber.

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.

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.

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.

Voice Messages

The client cannot play broadcast voice messages.

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.

Extension Mobility Cross Cluster

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

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.

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.

Check Point VPN

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

Third-Party Unified Communications Applications

Installing Cisco Jabber for Windows and third-party unified communications applications on the same machine may result in unexpected behavior in the client and is not recommended.

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.
- 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.

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.

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.

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.

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.

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.

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

On-Premises Deployment Scenarios:

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

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 a 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.

ServicesDomainSsoEmailPrompt

ON

OFF (default)

For more information on 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

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.

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.

Certificate Validation for CTI Connections

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*.

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.
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.

Severity level		Description
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.

Opened in this Release

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.
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.

Identifier	Severity	Headline
CSCuj40988	3	Client may show incorrect called number when in deskphone mode.
CSCus64434	3	Invalid certificate prompt when a CTI Connection is made.

Fixed in this Release

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.

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