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 NONINFRINGEMENT 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)

© 2015 Cisco Systems, Inc. All rights reserved.
CONTENTS

CHAPTER 1

Introduction 1

Build Number 1

Documentation Resources 1

New Features and Enhancements 2

CHAPTER 2

Requirements 7

Software Requirements 7

Hardware Requirements 8

Network Requirements 9

Third-party Requirements 10

CHAPTER 3

Limitations and Restrictions 13

Limitations and Restrictions 13

Performance and Behavior Notes 22

CHAPTER 4

Caveats 25

Bug Severity Levels 25

Search for Bugs 26

Open Caveats 26

Resolved Caveats 27
CHAPTER 1

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, page 1
- Documentation Resources, page 1
- New Features and Enhancements, page 2

Build Number

The build number for this release is 10.5.37889.

Documentation Resources

The following documents are available for 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.

Deployment and Installation Guide

Provides administrators with information for all Jabber clients in one guide. It contains end-to-end client deployment procedures, comprising requirements, deployment scenarios and workflows, infrastructure configuration of services, and client configuration and installation.

Licensing Information

This Licensing Information document provides information on the open source libraries used by the application.
Quick Start Guide
Instructions to help navigate end users around Cisco Jabber for Windows for the first time and use a few key features.

Advanced Features Guide
Provides an overview of task-based information about end user operation of the client.

Accessibility Guide
Provides information on navigating the client, including shortcut keys, keyboard navigation, and other accessibility features.

New Features and Enhancements

User Management

Single Sign On
Security Assertion Markup Language (SAML) is an XML-based open standard data format that enables you to access a defined set of Cisco services seamlessly after verifying credentials with an Identity Provider. You enable SAML SSO in Cisco WebEx Messenger Services, Cisco Unified Communications Manager, or Cisco Unity Connection. It is deployed in the Jabber client using service discovery.

For more information about SAML SSO, see the chapter on Single Sign-On (SSO) Deployments in the Cisco Jabber Deployment and Installation Guide.

Reset Jabber
Resetting Jabber gives users the ability to reset Jabber to the originally-installed state.

Telemetrics
In this release, the client is enabled to help improve your Cisco Jabber experience by sending anonymous data to Cisco on elements such as call analytics and call quality.

Calling Features

Personal Ringtone
Users can select a ringtone for incoming calls from a menu of distinctive ringtones for their client in the Options menu, under Sounds and Alerts.
Hunt Groups

Hunt Groups enable incoming calls to be directed to a group of users. The call route is based on a number of factors, including first available, longest Idle, broadcast hunting and circular hunting. You can use Cisco Jabber and deskphones to answer hunt group calls.

A hunt group works in conjunction with route filters and hunt lists to direct calls to specific devices. If a phone or device is ringing and not being answered, then another available number is searched for until the call is answered.

A hunt list contains a set of line groups in a specific order. A single line group can appear in multiple hunt lists. A line group comprises a group of directory numbers in a specific order. The order controls the progress of the search for available directory numbers for incoming calls.

Call Pickup

Call Pickup allows users to pick up incoming calls from their own group. Group Call Pickup and Directed Call Pickup allows users to pick up incoming calls to another group or individual, respectively. You can use Cisco Jabber and deskphones to answer call pickup calls.

Directory numbers are assigned to call pickup groups and Cisco Unified Communications Manager automatically dials the appropriate call pickup group number. Users select Pickup to answer the call.

There are four kinds of call pickup that allow users to ensure incoming phone calls are not missed.

- **Call pickup**: Allows users to pick up incoming calls from their own group.
- **Group call pickup**: Allows users to pick up incoming calls from another group.
- **Other group pickup**: Allows users to pick up incoming calls from a group that is associated with their group. You cannot use this option with the hunt group feature.
- **Directed call pickup**: Allows users to pick up an incoming call on a directory number. You cannot use this option with the hunt group feature.

Video Call Quality

Improvements in video image edge interpolation deliver smoother and sharper video calling for users in call scenarios.

Using the available graphics processing hardware, if it is available on the client machines, also reduces the CPU load for Cisco Jabber video calling and ensures faster bandwidth adaptation.

Audio Call Quality

The G.722 wideband audio codec is now introduced as the default codec for calls to Cisco IP deskphones and other portfolio endpoints, which delivers a superior call experience to the user. You can provision other audio codec selection preferences in Cisco Unified Communications Manager, if required.

Plantronics Call Control

In addition to Jabra and Logitech headsets, users can now use Plantronics accessories to control their calls on Cisco Jabber to adjust call volume, answer and end phone calls, and mute.

Self-view

Users can move and resize the self-view window on video calls.
IM & Presence

IM Only Screen Sharing

In addition to the video screen share (BFCP) feature that is available to video-enabled clients when on a call, users can now screen share directly from an IM conversation when video share is not provisioned or available. IM screen sharing uses Microsoft RDP, which is a secure connection. When using IM only screen sharing, the screen share resolution and bandwidth allocations are directly managed by the underlying Windows OS.

Users can share their screens from IM with up to five other Cisco Jabber for Windows 10.5 users in a group chat.

Unlike BFCP, users do not need to be in a call to share their screen. Screen sharing is not currently supported while on the Expressway for Mobile and Remote Access.

Remote Desktop Control

When screen sharing from an IM, a user can request permission to remotely control the desktop of the user who is sharing the screen. Either user can revoke the remote desktop control at anytime. Remote desktop control is not currently supported while on the Expressway for Mobile and Remote Access.

IM Notifications

This release offers new incoming chat message alerts, new chat alert sound and IM badges in the Windows taskbar. In addition to your Cisco Jabber client icon flashing on your Windows taskbar, users also receive notifications that pop up on their screens when they have a new message. IM notifications are displayed for chats, group chats, and in persistent chat rooms.

IM Do Not Disturb

The client now offers Do Not Disturb in the client to suppress IM notifications. Only notifications are suppressed and not the messages. Users can configure whether they receive the notifications from the Options menu.

Spellcheck (Windows 8)

Spellcheck is available for instant messaging chats on Cisco Jabber clients running on Windows 8 operating system. Language support is dependent on those supported by Windows 8. Spellcheck is active only for the language defined for your operating system, not the language defined for your Jabber client.

New Emoticons

The selection of emoticons has been increased for users in their chat conversations. The existing emoticons have also been redesigned for improved user experience.

Persistent Chat Rooms

Persistent Chat Rooms are applicable to on-premises deployments only.

Persistent Chat Room Administration and Moderation

Administrators can now create and delete rooms, manage membership, and moderate rooms. You can define up to 30 room moderators who can create or remove rooms, add or remove members, and define room types and descriptions.
Persistent Chat Room Message Search

Users can search for messages in their chat room histories.

Persistent Chat Room Notifications

Users get notifications for new chat room messages and filter matches.

Telephony

Conversation Window Control in Deskphone Control Mode

The user can control whether the conversation window comes into focus for different types of call when in deskphone control mode.

Users can now configure when to bring their conversation window to the front when in deskphone control mode (CTI mode). When users pick up their phone, a conversation window is displayed on the user's screen. Users can configure the conversation window to open for all calls, video calls only, or never. Users configure this window behavior in the Options menu. The default behavior is to have the conversation window come into focus for calls, as it was in previous releases.

Administrators can define a new default behavior by defining the following configuration key: ctiwindowbehaviour.

Table 1: Configuration for ctiwindowbehaviour parameter

<table>
<thead>
<tr>
<th>Option</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>OnCall</td>
<td>Conversation window is displayed automatically when the deskphone is picked up or there is an incoming call.</td>
</tr>
<tr>
<td>OnVideo</td>
<td>Conversation window is displayed only when there is an incoming video call.</td>
</tr>
<tr>
<td>Never</td>
<td>Conversation window is not displayed for a call. Instead, it is automatically minimized in the Windows task bar with the Cisco Jabber icon.</td>
</tr>
</tbody>
</table>

Call Statistics

You can now view real-time statistics when on a call. Use Ctrl + Shift + S to open call statistics. You can view audio, video, and screen share statistics, and copy the statistics into the clipboard to send to others.

IM Protocol Handler Enhancement

You can now configure the IM protocol handlers that are supported by Cisco Jabber for Windows to pre-populate the conversation window with a subject line and body text when users click on the link text for both peer-to-peer and group messages.
Changes to Cisco Jabber for Windows Documentation

In Cisco Jabber for Windows 10.5, the documentation resources contain the following changes since the previous release:

**New: Cisco Jabber Deployment and Installation Guide**

This new guide comprises deployment, configuration, and installation information for all Jabber clients: Cisco Jabber for Windows, Cisco Jabber for Mac, Cisco Jabber for iPhone and iPad, and Cisco Jabber for Android.

It contains procedures in one guide that were previously published in the *Installation and Configuration Guide, Server Setup Guide,* and *DNS Configuration Guide.*

**Required Upgrade for Cisco WebEx Meeting Center Compliance**

You must upgrade to one of the follow Cisco Jabber for Windows releases to continue using Cisco WebEx Meeting Center:

- Cisco Jabber for Windows 10.5 or later
- Cisco Jabber for Windows 9.7.4 or later
- Cisco Jabber for Windows 9.6.3 or later

These releases are compliant with changes in Cisco WebEx Meeting Center, versions T28 and T29.


To receive further details on the dates of the required Cisco WebEx Meeting Center upgrade, contact us at the following email address and include your WebEx Meetings domain(s):

mailto:webexserverupgrade@cisco.com
Requirements

Software Requirements

Depreciated Support
Support for the following software has been depreciated in this release:

- Microsoft Office 2007
- Microsoft SharePoint 2007
- Active Directory Windows Server 2003

Operating Systems

- Microsoft Windows 7, 8, and 8.1, 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, minimum supported versions Version T27 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) 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.

Media

Cisco Medianet MSI 4.1.2 for deskphone video.

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>(XMPP)</td>
<td></td>
</tr>
<tr>
<td>30000 to 39999</td>
<td>FECC</td>
<td>The client uses this port for far end camera control.</td>
</tr>
<tr>
<td>636</td>
<td>LDAPS</td>
<td>LDAP directory server (secure).</td>
</tr>
<tr>
<td>2748</td>
<td>TCP</td>
<td>Computer Telephony Interface (CTI) used for desk phone control.</td>
</tr>
<tr>
<td>3268</td>
<td>TCP</td>
<td>Global Catalog server.</td>
</tr>
<tr>
<td>3269</td>
<td>LDAPS</td>
<td>Global Catalog server (secure).</td>
</tr>
<tr>
<td>5222</td>
<td>TCP</td>
<td>XMPP traffic to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.</td>
</tr>
<tr>
<td></td>
<td>(XMPP)</td>
<td></td>
</tr>
<tr>
<td>8443</td>
<td>TCP</td>
<td>Traffic to Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service.</td>
</tr>
<tr>
<td></td>
<td>(HTTPS)</td>
<td></td>
</tr>
<tr>
<td>7080</td>
<td>TCP</td>
<td>Cisco Unity Connection for notifications of voice messages (new message, message update, and message deletion).</td>
</tr>
<tr>
<td></td>
<td>(HTTPS)</td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>UDP/TCP</td>
<td>Domain Name System (DNS) traffic.</td>
</tr>
<tr>
<td>37200</td>
<td>SOCKS5 Bytestreams</td>
<td>Peer-to-peer file transfers. In on-premises deployments, the client also uses this port to send screen captures.</td>
</tr>
</tbody>
</table>
### Third-party Requirements

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5060</td>
<td>UDP/TCP</td>
<td>Session Initiation Protocol (SIP) call signaling.</td>
</tr>
<tr>
<td>5061</td>
<td>TCP</td>
<td>Secure SIP call signaling.</td>
</tr>
<tr>
<td>49152 to 65535</td>
<td>TCP</td>
<td>IM-only screen share. The client randomly selects a port from the range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The actual range may vary. To find the real range, enter the netsh interface ipv4 show dynamicportrange tcp command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can use the SharePortRangeStart and SharePortRangeSize 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 Deployment and Installation Guide.</td>
</tr>
</tbody>
</table>

**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

**Microsoft Exchange**
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

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

Special German Characters in Usernames or Passwords

The Cisco Jabber for Windows softphone fails to register with Cisco Unified Communications Manager when users enter some German 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". To resolve the issue, upgrade to Cisco Unified Communications Manager 9.1(2) or users should use lower ASCII characters for their username and passwords.

Cisco Medianet Metadata Support

As of this release, Cisco Medianet Metadata is no longer supported.

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.
SAML Single Sign-On Limitations

In this release, deploying SAML single sign-on is not supported if Expressway for Mobile and Remote Access is also deployed. If the Jabber client detects that Expressway for Mobile and Remote Access is deployed, it will never detect SAML SSO, even if you are not using it at the time.

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. This item is documented in CSCun44797.

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.

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.

Cached Contacts in Microsoft Exchange

Microsoft Exchange 2013 has changed the way it handles cached contacts. This change may result in some cached contacts being stored in hidden folders in Microsoft Outlook that are not viewable or customizable by the end user.

As a result, the Cisco Jabber client may return duplicate and incorrect contacts when searching Microsoft Outlook. If the incorrect contacts are stored as a contact in a user's client, it may lead to other side-effects such as incorrect presence in both the client and Microsoft Outlook. This item is documented in CSCup78097.

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 they have a Cisco Jabber history created by the user previously searching, IMing, or calling them, or by leaving a voice message. This item is documented in CSCuo88534.
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.

Diverting Calls in Do Not Disturb State

Setting your status to "Do Not Disturb" in the client does not divert or block incoming calls.

Extension Mobility Cross Cluster

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

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 user names in on-premises deployments must not be spaces. This 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.
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:

- **SAML Single Sign-On**
  In this release, single sign-on is not supported when users are providing their credentials from outside the corporate firewall using Expressway Mobile and Remote Access.

- **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.

- **File transfer, including screen capture, is not supported with on-premises deployments.** File transfer using Expressway for Mobile and Remote Access is only supported using WebEx Cloud deployments.

- **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 user starts 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 the Cisco WebEx Meetings Server server, or join or start s Cisco WebEx meetings.

- **Scheduling 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.

- The person receiving a call also receives a call pickup notification when they are URI dialed. This issue is documented in CSCuo75418.

**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 CSCu02706.

**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. For more information, see CSCur02498.
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):

• File transfer, including screen capture, is not supported with on-premises deployments.
• 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

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.

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.

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.

**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.

**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.
Caveats

• Bug Severity Levels, page 25
• Search for Bugs, page 26
• Open Caveats, page 26
• Resolved Caveats, page 27

Bug Severity Levels

Known problems (bugs) are graded according to severity level. The following table describes bug severity levels:

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Catastrophic</td>
</tr>
<tr>
<td>2</td>
<td>Severe</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
</tr>
<tr>
<td>4</td>
<td>Minor</td>
</tr>
<tr>
<td>5</td>
<td>Cosmetic</td>
</tr>
<tr>
<td>6</td>
<td>Enhancement</td>
</tr>
</tbody>
</table>
Search for Bugs

To search for bugs, do the following:

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Go to <a href="https://tools.cisco.com/bugsearch/search">https://tools.cisco.com/bugsearch/search</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Sign in with your Cisco.com user ID and password.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the bug ID or specify search parameters.</td>
</tr>
</tbody>
</table>

What to Do Next

For more information, select Help on the Bug Search page.

Open Caveats

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Severity</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCuq34958</td>
<td>2</td>
<td>CTI Manager Service crashes when user ID exceeds 10 characters.</td>
</tr>
<tr>
<td>CSCuo58251</td>
<td>2</td>
<td>UDS returning IP Address to Jabber, Cert validation browser pop-ups.</td>
</tr>
<tr>
<td>CSCup56878</td>
<td>3</td>
<td>HTML Tab: Unexpected behavior when calling CTooltip::Show().</td>
</tr>
<tr>
<td>CSCup82846</td>
<td>3</td>
<td>Wrong user may be selected on Jabber search.</td>
</tr>
<tr>
<td>CSCuq06441</td>
<td>3</td>
<td>After network disconnect and end call, presence return to Available instead of Custom Available.</td>
</tr>
<tr>
<td>CSCuq16548</td>
<td>3</td>
<td>Jabber Edge XMPP reconnect timer too long when VCS-c fails over.</td>
</tr>
<tr>
<td>CSCup29889</td>
<td>3</td>
<td>Phone, company and photo intermittently are missing on Windows 8 (Japanese).</td>
</tr>
<tr>
<td>CSCuq23747</td>
<td>3</td>
<td>Jabber for Windows can't add more than 7 custom contact in one login session.</td>
</tr>
<tr>
<td>CSCuo75418</td>
<td>3</td>
<td>Called party also receives call pickup notification when URI dialled.</td>
</tr>
<tr>
<td>CSCuo88572</td>
<td>3</td>
<td>Show-unavailable not working after joining as hidden.</td>
</tr>
<tr>
<td>CSCuq39413</td>
<td>3</td>
<td>Screen capture corrupted when AES enabled.</td>
</tr>
<tr>
<td>CSCup78097</td>
<td>3</td>
<td>Jabber search on a user is returning multiple Outlook contacts for users.</td>
</tr>
<tr>
<td>CSCuq08775</td>
<td>3</td>
<td>No presence in Outlook after upgrading Jabber with Outlook running.</td>
</tr>
</tbody>
</table>
## Resolved Caveats

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Severity</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCun55968</td>
<td>2</td>
<td>Intermittent SSO Login Failure - XML displayed in login window.</td>
</tr>
<tr>
<td>CSCun84531</td>
<td>2</td>
<td>Jabber IMs lost due to interop with Webex Social.</td>
</tr>
<tr>
<td>CSCun84550</td>
<td>2</td>
<td>Jabber IMs lost due to mismatch with Connect Encryption.</td>
</tr>
<tr>
<td>CSCuo58290</td>
<td>2</td>
<td>Jabber for Windows crashes intermittently.</td>
</tr>
<tr>
<td>CSCuo82526</td>
<td>2</td>
<td>MRA Jabber does not send cookie x-auth token with login request.</td>
</tr>
<tr>
<td>CSCup23913</td>
<td>2</td>
<td>Multiple Vulnerabilities in OpenSSL.</td>
</tr>
<tr>
<td>CSCup49887</td>
<td>2</td>
<td>Unexpected behavior in Telephony plugin</td>
</tr>
<tr>
<td>CSCug96646</td>
<td>3</td>
<td>Jabber for Windows Photo Retrieval fails if PC username is non-English.</td>
</tr>
<tr>
<td>CSCuj91246</td>
<td>3</td>
<td>Different IM/Email Outlook local contacts</td>
</tr>
<tr>
<td>CSCuj93682</td>
<td>3</td>
<td>J4W emoticons are garbled after some UTF-8 Characters.</td>
</tr>
<tr>
<td>CSCun95601</td>
<td>3</td>
<td>Jabber Windows call window becomes active after 15 minutes.</td>
</tr>
<tr>
<td>CSCun70392</td>
<td>3</td>
<td>Unexpected exit while idle over Edge.</td>
</tr>
<tr>
<td>CSCun71221</td>
<td>3</td>
<td>Caller information (ID,Photo) does not update on call toast and window.</td>
</tr>
<tr>
<td>CSCun79048</td>
<td>3</td>
<td>Importing Contact in Jabber Windows Phone-only mode.</td>
</tr>
<tr>
<td>CSCun81773</td>
<td>3</td>
<td>Jabber automatic roll out not possible - missing signature for VBScript.</td>
</tr>
<tr>
<td>CSCun83632</td>
<td>3</td>
<td>Jabber shows groups incorrectly for non-ASCII characters and CUPC.</td>
</tr>
<tr>
<td>CSCun84091</td>
<td>3</td>
<td>Search clearing is inconsistent.</td>
</tr>
<tr>
<td>CSCuo09358</td>
<td>3</td>
<td>Users' self-presence shows offline.</td>
</tr>
<tr>
<td>CSCuo11530</td>
<td>3</td>
<td>Intermittent crash on searching for contacts.</td>
</tr>
<tr>
<td>CSCuo60610</td>
<td>3</td>
<td>Cisco Jabber for Windows does not honor Jabber-config file.</td>
</tr>
<tr>
<td>CSCuo62929</td>
<td>3</td>
<td>Failing to update in-memory dialing rules.</td>
</tr>
<tr>
<td>CSCuo73272</td>
<td>3</td>
<td>Crash in Person Manager.</td>
</tr>
<tr>
<td>CSCuo83479</td>
<td>3</td>
<td>Can't view contact's profile although permission is on.</td>
</tr>
<tr>
<td>CSCuo90291</td>
<td>3</td>
<td>Jabber screen sharing quality varies due to cached low bandwidth level.</td>
</tr>
<tr>
<td>CSCuo95351</td>
<td>3</td>
<td>Presence shows offline while chatting with user on my contact list.</td>
</tr>
<tr>
<td>CSCuo98047</td>
<td>3</td>
<td>Need UDS details of how to configure Jabber for Expressway MRA.</td>
</tr>
<tr>
<td>CSCup02217</td>
<td>3</td>
<td>J4W: Quality of screen sharing degrades upon offered max-fs by Windows.</td>
</tr>
<tr>
<td>CSCup14715</td>
<td>3</td>
<td>Private number is not stored in call history of Jabber for Windows.</td>
</tr>
<tr>
<td>CSCup16016</td>
<td>3</td>
<td>Contact Name becomes IM address after reboot.</td>
</tr>
</tbody>
</table>
### Resolved Caveats

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Severity</th>
<th>Headline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCup28751</td>
<td>3</td>
<td>Czech characters in name not displayed correctly when used through UDS.</td>
</tr>
<tr>
<td>CSCup39611</td>
<td>3</td>
<td>Jabber requires Voicemail server config on IMP.</td>
</tr>
<tr>
<td>CSCup45076</td>
<td>3</td>
<td>Jabber Windows exits unexpectedly immediately after login while parsing VCard.</td>
</tr>
<tr>
<td>CSCup54435</td>
<td>3</td>
<td>Enabling VVM in OrgAdmin, enables it for all users.</td>
</tr>
<tr>
<td>CSCup70296</td>
<td>3</td>
<td>Jabber incorrectly modifying nickname field.</td>
</tr>
<tr>
<td>CSCup82773</td>
<td>3</td>
<td>Call drops after a temporary network loss.</td>
</tr>
<tr>
<td>CSCup84971</td>
<td>3</td>
<td>AllowUserCustomTabs=false doesn't work if you have a custom tab created.</td>
</tr>
</tbody>
</table>