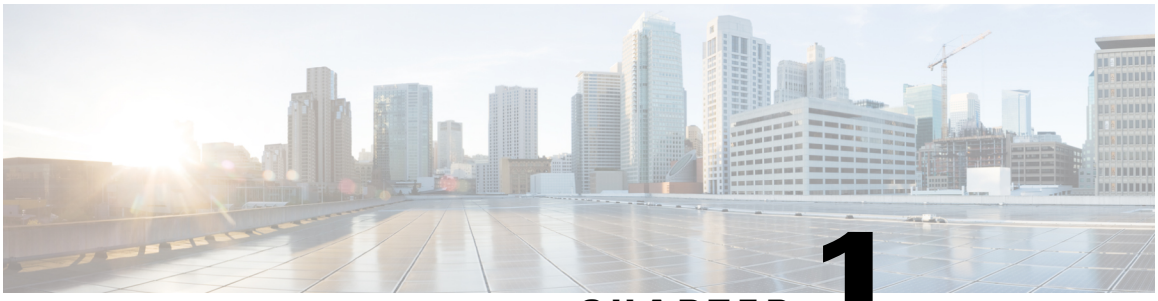
Cisco Jabber for Windows 9.7(7) Release Notes

First Published: March 03, 2016

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Release Information

Build Number

The build number for this release is 9.7.7.19443.

Documentation Resources

The following documents are available for Cisco Jabber for Windows.

Installation and Configuration Guide

The Installation and Configuration Guide provides administrators with information on software, hardware, system, and network requirements; deployment planning; installation; and client configuration.

Server Setup Guide

The Server Setup Guide provides administrators with task-based information to help configure client services such as directory integration, instant messaging and presence, audio and video calling, voicemail, and conferencing.

DNS SRV Configuration Guide

The Cisco Jabber DNS Configuration Guide provides administrators with information on how to set up a domain name server for Cisco Jabber clients. Cisco Jabber uses domain name servers to do the following:

- Automatically discover on-premises servers inside the corporate network.
- Determine whether the client is inside or outside the corporate network.

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.

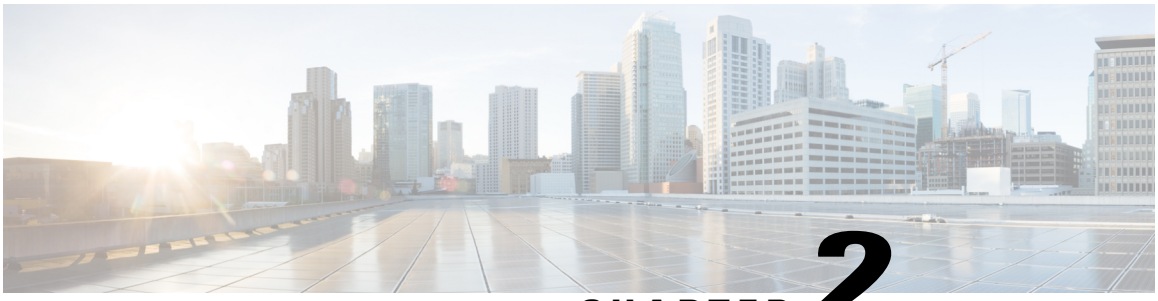
Advanced Features Guide

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

Features and Enhancements

Resolved Caveats

This release includes a number of resolved caveats. For more information, see the *Fixed in this Release* section.



CHAPTER 2

Known Issues, Limitations, and Important Notes

Known Issues

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.

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 SU2 and 10.0.1. This item is documented in CSCui29999.

Performance and Behavior Notes

Review the content in this topic to understand client performance and behavior in certain cases.

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 last four digits in the phone number as a contact in your company directory.

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

Due to a limitation with UDS, 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 voicemail. 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:

- Availability states change to 'Available' on all clients when users resume from hibernate on one client.
- Resuming from idle overrides custom availability states.
- In on-premise deployments, signing in on one client changes custom availability states to 'Available' on other clients.
- In on-premise deployments, 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.
- 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.

Voicemail Messages

The following restrictions currently apply to voicemail messages:

- The client cannot play broadcast voicemail messages.

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

Blocking Users in Enterprise Groups

This issue applies to Cisco Jabber for Windows in cloud-based deployments only.

Blocking users does not deny availability status if the blocked users exist 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.

Contacting Federated Users After Changing Privacy Policies

In on-premise deployments, the following can occur:

1. Users add federated contacts 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 then change that policy from **Block everyone** to **Prompt me every time**.

   As a result, Cisco Unified Presence removes the federated contacts from the contact lists. Cisco Unified Presence does not repopulate the federated contacts.

Because Cisco Unified Presence removes 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.

Descriptions for Multiple Devices

If Cisco Jabber for Windows users have multiple desk phone devices of the same model, you should enter descriptions for each device. Cisco Jabber for Windows displays these descriptions to users so that they can tell the difference between multiple desk phone devices. If you do not enter descriptions, Cisco Jabber for Windows displays the model name of the device. As a result, users cannot tell the difference between their devices if they have multiple 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 usernames 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 are not supported in virtual environments. Use Cisco Virtualization Experience Media Engine (VXME) for Cisco Jabber for Windows call capabilities in a virtual environment.

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:

- LDAP for contact resolution. Instead, the client must use UDS for contact resolution.
- File transfer, including screen capture, is not supported with on-premise 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 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 the Cisco WebEx Meetings Server 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.
- 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.

Call History Limit

The client can store up to 250 entries in your call history. This item is documented in CSCun44797.

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.

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.

Important Notes

This topic describes issues with interoperability with other clients, devices, and third party software, along with server-side issues or defects that impact client functionality. In addition, this topic includes some best practice information to prevent issues with the client.

Audio Issues with Cisco Security Agent

In some cases audio calls hang and users cannot end active calls if you run the Cisco Security Agent (CSA) while using Cisco Jabber.

This issue:

- Affects users with USB microphones or USB cameras that include microphones, but might not be limited to USB devices.
- Is most likely to occur when the computer's battery is running low.

Phone Mode Deployments with the Microsoft Lync Client

Click-to-x functionality must be disabled to deploy Cisco Jabber for Windows in phone mode on the same computer as the Microsoft Lync client. Refer to the section on Command Line Arguments in the *Installation and Configuration Guide* for an explanation of the `CLICK2X` installer switch usage.

Upgrade Cisco WebEx Connect Client

If you use the Cisco WebEx Connect client, you can upgrade to Cisco Jabber for Windows 9.7 from Cisco WebEx Connect version 7.2.2 only.

You can upgrade from Cisco WebEx Connect version 7.x to any Cisco Jabber for Windows version up to 9.2(0). You can then upgrade the Cisco Jabber for Windows client to version 9.2(1) or higher.

Cisco Jabber for Windows and the Cisco WebEx Connect Client

You should not install and run Cisco Jabber for Windows on the same computer as the Cisco WebEx Connect client. If you do run both the Cisco WebEx Connect client and Cisco Jabber for Windows on the same computer, unexpected behavior is likely to occur.

In the event that you do install Cisco Jabber for Windows on the same computer as the Cisco WebEx Connect client, the following error message displays when you launch the Cisco WebEx Connect client:

```
Can't load webxcOIEx.exe, error code[], please check whether the executable is in your
install directory.
```

To resolve this error, you must reinstall the Cisco WebEx Connect client.

Cloud-Based SSO with Microsoft Internet Explorer 9

In cloud-based deployments that use single sign-on (SSO), an issue exists with Internet Explorer 9. Users with Internet Explorer 9 get security alerts when they sign in to Cisco Jabber for Windows. To resolve this issue, add `webexconnect.com` to the list of websites in the **Compatibility View Settings** window.

BFCP Desktop Share with PVDM3

Packet Voice Digital Signal Processor Module (PVDM3) enabled routers do not support BFCP video desktop sharing capabilities.

Presence States After Loss of Network Connection

In cloud-based deployments, it can take several minutes for the Cisco WebEx Messenger service to detect when clients lose network connections or become abruptly disconnected. For example, the Cisco WebEx Messenger service might take up to 5 minutes to detect when a client loses a network connection by pulling the network cable or walking out of range of a wireless network. This behavior is due to normal operation of the network stack to provide a robust connection.

As a result of the delay in the server detecting the loss of connection with the client, the server does not immediately publish the presence state of users who have lost their network connection. For this reason, there is a period of time during which users can see an online presence state even when remote contacts are offline.

Calls on Hold Dropped During Failover

If a user puts a call on hold, the call drops if Cisco Unified Communications Manager failover occurs. An example of this behavior is as follows:

1. User A and user B are connected to the primary instance of Cisco Unified Communications Manager.
2. User A calls user B.
3. User A puts the call on hold.
4. Failover occurs from the primary instance of Cisco Unified Communications Manager to the secondary instance.

As a result, user A's call drops. User B's call remains available in preservation mode.

Hold Active Calls During Failover

You cannot place an active call on hold if failover occurs from the primary instance of Cisco Unified Communications Manager to the secondary instance.

MAPI Server Requests for Local Outlook Contacts

Cisco Jabber for Windows attempts to retrieve local Microsoft Outlook contacts from the Outlook PST file. If Outlook does not cache local contacts in the PST file, Cisco Jabber for Windows sends contact resolution requests to the MAPI server. As a result, the MAPI server can experience an impact to performance. Cisco recommends that you configure Outlook to cache local contacts in the PST file. Otherwise, you must ensure that your MAPI server is capable of managing the requests from Cisco Jabber for Windows.

Upgrading with Microsoft Group Policy

Microsoft Group Policy does not detect existing installations of Cisco Jabber for Windows. As a result, if you upgrade Cisco Jabber for Windows with Microsoft Group Policy, Group Policy does not uninstall the existing version before installing the upgrade version.

Calls Drop Intermittently on Network Profile Change

A known bug exists with Microsoft Windows 7 and Microsoft Windows Server 2008 R2 that causes the network profile to change unexpectedly. This change in the network profile closes network ports that Cisco Jabber for Windows requires for calls. As a result, if you are on a call when the network profile changes, that call automatically terminates.

To resolve this issue, apply the fix available from the Microsoft support site at: http://support.microsoft.com/kb/2524478/en-us

Voicemail Prompt Truncated

The start of the audio that prompts users to leave voicemail messages can be truncated in some instances. The result of the truncation is that users do not hear the first second or two of the voicemail prompt.

To resolve this issue, set a value for the **Delay After Answer** field in the Cisco Unity Connection advanced telephony integration settings. See the Cisco Unity Connection documentation at: http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/gui_reference/guide/8xcucgrg120.html#wp1056978

Loss of Video on Calls with CTS Devices

Cisco TelePresence System (CTS) devices do not allow users to send video only.

For this reason, when users place calls from their software phones (CSF devices) to CTS devices, loss of incoming video and video desktop sharing occurs if users de-escalate from a video call to an audio only call.

Removing Participants from Conference Calls

The functionality to remove participants from conference calls while using software phone devices is available on Cisco Unified Communications Manager version 8.6.2 and higher.

Custom Contacts from Microsoft Outlook

Bi-directional synching of contacts to Microsoft Outlook is not supported. If contacts are imported from Microsoft Outlook and added to your Jabber contact list and then edited in the Jabber client, the changes are not reflected in Microsoft Outlook.

To import Outlook contacts, the contact must have a valid Jabber ID (JID).

Clients That Do Not Support Graceful Registration

You should exit clients that do not implement graceful registration before you start Cisco Jabber for Windows if both clients use the same CSF device.

For example, Cisco Unified Personal Communicator does not support graceful registration. Cisco Unified Personal Communicator takes over registration of the CSF device if:

- You are signed in to both Cisco Unified Personal Communicator and Cisco Jabber for Windows at the same time.
- Both clients register to the same CSF device.

Call History and Roaming Profiles

Call history is lost when the application is running in a Roaming Profile environment. Roaming Profile environments include those running Virtual Desktop Infrastructure such as VMware View or Citrix Xen or hot desks. For more information, go to the section on Deployment in a Virtual Environment in the *Installation and Configuration Guide*.

Service Discovery Steps in New Installations

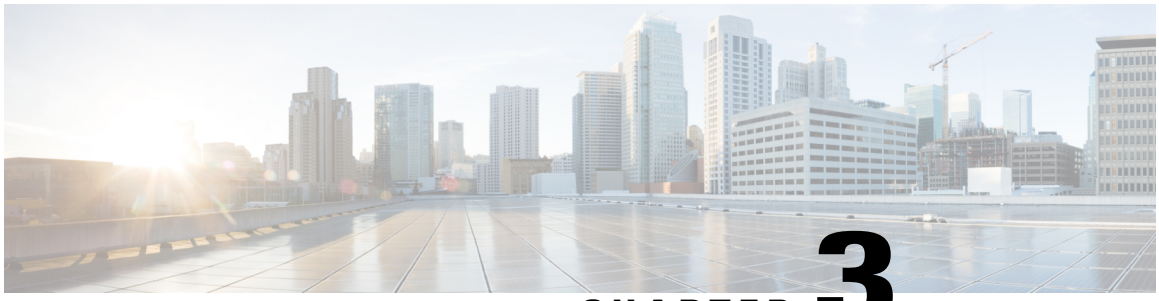
Service Discovery information is retrieved by the client in new installations using the following steps:

1. The client looks for a services domain value in the `SERVICES_DOMAIN` installer switch. The services domain represents the domain where the client discovers available services. These services are:
   - Cisco WebEx Messenger
   - Cisco Unified Communications Manager
   - Cisco Unified Communications Manager IM & Presence
   - Cisco Expressway for Mobile and Remote Access

   In hybrid environments, the WebEx Messenger domain may not be the same domain as for on-premises services, such as Unified Communications Manager, Unified Communications Manager IM & Presence, and Expressway for Mobile and Remote Access. In such environments, `SERVICES_DOMAIN` specifies the domain to perform a CAS lookup for WebEx Messenger. Another installer switch, `VOICE_SERVICES_DOMAIN`, specifies the domain to perform DNS SRV lookups for Unified Communications Manager, Unified Communications Manager IM & Presence, and Expressway for Mobile and Remote Access.
2. If neither `SERVICES_DOMAIN` or `VOICE_SERVICES_DOMAIN` are specified, the client reads the`AUTHENTICATOR` installer switch. The `AUTHENTICATOR` switch specifies to Jabber what service to connect to. The `AUTHENTICATOR` switch must be used with another switch to specify the service location, for example, `AUTHENTICATOR`=CUP, CUP_ADDRESS=cup1.domain.com or AUTHENTICATOR=CUCM, TFTP=cucm1.domain.com, CCMCIP=cucm1.domain.com.
3. If none of the above switches are specified, the client prompts the user to enter services domain information at initial sign in.

Cisco MediaSense

When a Cisco Jabber client calls another Cisco Jabber client, Cisco MediaSense call recording is currently not supported. The G.722.1 codec is used by default. This media protocol is not supported by Cisco MediaSense, which impacts Built-in Bridge (BiB) and silent record.



CHAPTER 3

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.
6	Enhancement	Requests for new functionality or feature improvements.

Search for Bugs

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

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

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

Open in this Release

There are no new open caveats in this release.

Fixed in this Release

Identifier	Severity	Headline
CSCux88529	2	Jabber client does not allow to enforce STARTTLS as required.
CSCuu70858	2	Jabber sends Authorization Header over unencrypted connection.