Cisco Jabber for Windows 10.5(4) Release Notes

First Published: January 16, 2015

CONTENTS

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

The build number for this release is 10.5.4.51578.

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.

Features and Enhancements

Resolved Caveats

This release provides fixes for a number of known issues. See the Fixed Caveats section for a list of resolved caveats.

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 WBS27 or later

Directory Servers

- Active Directory Domain Services for Windows Server 2012 R2

- Active Directory Domain Services for Windows Server 2008 R2

- OpenLDAP

- Active Directory Lightweight Directory Service (AD LDS) or Active Directory Application Mode (ADAM)

- Cisco Unified Communications Manager User Data Service (UDS)

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

- Cisco Unified Communications Manager version 9.1(2) with the following COP file:`cmterm-cucm-uds-912-5.cop.sgn.`

- Cisco Unified Communications Manager version 10.0(1). No COP file is required.

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

Port	Protocol	Description

443	TCP
	
	(Extensible Messaging and Presence Protocol [XMPP] and HTTPS)
		XMPP traffic to the WebEx Messenger service.
		
		The client sends XMPP through this port in cloud-based deployments only. If port 443 is blocked, the client falls back to port 5222.
		
		Note Cisco Jabber can also use this port for:
		
		    • HTTPS traffic to Cisco Unity Connection and Cisco WebEx Meetings Server.
		
		    • Saving chats to the Microsoft Exchange server.

30000 to 39999	FECC	The client uses this port for far end camera control.
389	UDP/TCP	Lightweight Directory Access Protocol (LDAP) directory server.
636	LDAPS	LDAP directory server (secure).
2748	TCP	Computer Telephony Interface (CTI) used for desk phone control.
3268	TCP	Global Catalog server.
3269	LDAPS	Global Catalog server (secure).
5222	TCP (XMPP)	XMPP traffic to Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.
8443	TCP (HTTPS)	Traffic to Cisco Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service.
7080	TCP (HTTPS)	Cisco Unity Connection for notifications of voice messages (new message, message update, and message deletion).
53	UDP/TCP	Domain Name System (DNS) traffic.

Port	Protocol	Description
80	HTTP	Saving chats to Microsoft Exchange server. Depending on your server configuration on Microsoft Exchange, use either port 80 or 443, but not both.
37200	SOCKS5 Bytestreams	Peer-to-peer file transfers. In on-premises deployments, the client also uses this port to send screen captures.
5060	UDP/TCP	Session Initiation Protocol (SIP) call signaling.
5061	TCP	Secure SIP call signaling.

Third-party Requirements

Microsoft Internet Explorer

- Microsoft Internet Explorer 8 or later

Microsoft Office

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

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

Microsoft SharePoint

- Microsoft SharePoint 2013
- Microsoft SharePoint 2010

Microsoft 365

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

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

Third-Party Calendars

- Microsoft Outlook 2013, 32 and 64 bit

- Microsoft Outlook 2010, 32 and 64 bit

- IBM Lotus Notes 9 32 bit

- IBM Lotus Notes 8.5.3 32 bit

- IBM Lotus Notes 8.5.2 32 bit

- IBM Lotus Notes 8.5.1 32 bit

- Google Calendar

Antivirus Exclusions

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

- C:\Users\<User>\AppData\Local\Cisco\Unified Communications\Jabber

- C:\Users\<User>\AppData\Roaming\Cisco\Unified Communications\Jabber

- C:\ProgramData\Cisco Systems\Cisco Jabber

Limitations and Restrictions

- Limitations and Restrictions, page 9
- Performance and Behavior Notes, page 17

Limitations and Restrictions

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

Authenticated Proxies

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

Blank Screen Share over VXME

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

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

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.

Call History Limit

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

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.

Check Point VPN

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

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.

Declining Calls in Hunt Group

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

Descriptions for Multiple Devices

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

Diverting Calls in Do Not Disturb State

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

Emails to a Group of Contacts

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

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 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, or join or start Cisco WebEx meetings.

- Sending problem reports—To work around this issue, users can save the report locally and send the report in another manner.

- CAPF enrollment.

- Early Media—Early Media allows the client to exchange data between endpoints before a connection is established. For example, if a user makes a call to a party that is not part of the same organization, and the other party declines or does not answer the call, Early Media ensures that the user hears the busy tone or is sent to voicemail. When using Expressway Mobile and Remote Access, the user does not hear a busy tone if the other party declines or does not answer the call. Instead, the user hears approximately one minute of silence before the call is terminated.

- Self Care Portal—Users cannot access the Cisco Unified Communications Manager Self Care Portal when outside the firewall. The Cisco Unified Communications Manager user page cannot be accessed externally. The Cisco VCS Expressway or Cisco Expressway-E proxies all communications between the client and unified communications services inside the firewall. However, The Cisco VCS Expressway or Cisco Expressway-E does not proxy services that are accessed from a browser that is not part of the Cisco Jabber client.

- End-to-end media encryption—Media is not encrypted on the call path between the Cisco VCS Control or Cisco Expressway-C and devices that are registered locally to Cisco Unified Communications Manager. The media path outside of the enterprise is encrypted.

Extension Mobility Cross Cluster

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

Microsoft Outlook Local Contacts and Presence

Users' presence is unknown when the contact is manually added to contacts in Microsoft Outlook 2010 and 2013, when the contact is added to local (custom) contacts with an email address type of SMTP. To resolve this issue, delete the contact and add it again manually, ensuring the email address type is Exchange (EX). This item is documented in CSCuo57172.

Multiple Resource Login

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

- Availability states change to 'Available' on all clients when users resume from hibernate on one client.

- Resuming from idle overrides custom availability states.

- Users who are signed in to multiple Cisco Jabber for Windows clients can join group chats from only one client.

- Cisco Jabber for Windows does not always reformat incoming text correctly when the sender is signed in to a client other than Cisco Jabber for Windows.

Plantronics Accessories and Software

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

SAML Single Sign-On Limitations

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.

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.

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.

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.

Standard CTI Secure Connection User Group

Cisco Jabber for Windows does not currently support CTI connections over transport layer security (TLS). As a result, Cisco Jabber for Windows users cannot switch from using a CSF device to using a desk phone device if they belong to the Standard CTI Secure Connection user group.

Third-Party Unified Communications Applications

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

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. This item is documented in CSCuo88534.

Using Hunt Group on Desk Phones

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

Video Resolution of Lifesize Endpoint after Hold/Resume

Users may experience resolution issues when using Jabber to make a call with a Lifesize Express 220 endpoint. If the user puts the call on hold, then after resuming the call the send and receive video resolutions on the Jabber end is greatly reduced. For more information, see CSCur02498.

Voice Messages

The client cannot play broadcast voice messages.

On-Premises Deployment Scenarios:

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

Meeting Reminders

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

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

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 Caveats

Identifier	Severity	Headline
CSCus18018	2	Jabber Windows DTMF Fails - Incoming/Contact Header port different.
CSCuq91678	3	Jabber for Windows does not show calling name if no calling number is sent.
CSCuq40557	3	Waiting to Join shows up one after another for video conference call.
CSCus18564	3	Unable to type certain Polish characters.
CSCus20007	3	Jabber uses JID to send reminder instead of email.

Fixed Caveats

Identifier	Severity	Headline
CSCus23601	3	File transfer failing: Jabberwerx unable to handle writeError.
CSCus40093	3	The _cuplogin SRV lookup not done on each sign in.
CSCus40139	3	Microsoft Office error after installing Jabber 10.5.