



# General Troubleshooting

---

- [Problem Reporting Tool, on page 1](#)
- [Virtual Channel Problem, on page 2](#)
- [Configuration Files, on page 2](#)
- [Verify That Cisco JVDI Agent Is Installed, on page 2](#)
- [Verify Device Registration with Cisco Unified Communications Manager, on page 3](#)
- [Verify the Connection Status in Cisco Jabber, on page 3](#)
- [Jabber VDI Fallback Mode, on page 3](#)
- [Disable BFCP desktop share, on page 4](#)

## Problem Reporting Tool

The Problem Reporting Tool (PRT) is a small program that automatically runs if Cisco Jabber encounters an unrecoverable error, unhandled exception, or crash. The tool collects logs from the thin client and hosted virtual desktop and then creates a problem report. The report is a zip file that you can send to the Cisco Technical Assistance Center (TAC), to provide the necessary information to solve the problem. The tool saves the file to the user's desktop. Users must accept the privacy agreement to run the PRT.



---

**Tip** Advise users to include a memory dump with the problem report if Cisco Jabber crashes. We also recommend that users provide a description of the circumstances that lead up to the error.

---

If a user experiences an error that does not crash the software, the user can run the PRT from the Cisco Jabber menu: **Help > Report a problem**.

If Cisco Jabber is not running, users can generate a problem report from the Windows **Start** menu. To access the tool from outside the application, choose **Start > All Programs > Cisco Jabber > Cisco Jabber Problem Report**.



---

**Important** Problem reports include logs from the thin client, the hosted virtual desktop, and any detailed information that users enter. You can use this information to help troubleshoot the issue.

---

If there is a problem with the virtual channel, or if Cisco Jabber is not running, the problem report does not include logs from the thin client. For more information, see [Virtual Channel Problem, on page 2](#).

---

## Virtual Channel Problem

If a problem exists with the virtual channel, the problem-reporting tool cannot collect the logs from the thin client. A problem with the virtual channel can cause the Device Selector to not start or to not populate with devices.

Cisco Technical Assistance Center (TAC) personnel may ask you to gather the logs manually by running one of the following executables:

- **Windows OS 32-bit:** `C:\Program Files (x86)\Cisco Systems\Cisco JVDI\CollectCiscoJVDIClientLogs.exe`
- **Windows OS 64-bit:** `C:\Program Files\Cisco Systems\Cisco JVDI\CollectCiscoJVDIClientLogs.exe`
- **Linux-based OS:** `/usr/bin/collect-files`

The executable gathers the logs from the thin client and saves them to the desktop as a `CiscoJVDIClient-logs[timestamp].7z` file. You can still use the PRT to gather the logs from the hosted virtual desktop. Submit all logs gathered to TAC.

## Configuration Files

For each Cisco Unified Client Services Framework (CSF) device that you add to the system, Cisco Unified Communications Manager creates a configuration (CNF.xml) file. The CNF file contains the device specifications for the associated user.

When users sign in to Cisco Jabber, Cisco Jabber Softphone for VDI starts the download of the associated CNF file to the thin client. To ensure the successful transfer of the file, open the relevant ports in all firewall applications to allow the thin client to access the ports. For more information about how to open ports, see the documentation for the firewall software.



---

**Important**

Download of the CNF.xml file follows the system setting for HTTP proxy. Ensure that the proxy does not route the HTTP request from the thin client outside of the corporate network.

---

## Verify That Cisco JVDI Agent Is Installed

You can use the Windows Control Panel to verify that Cisco JVDI Agent is installed. You can also verify the version.

---

**Step 1** From Control Panel, open **Programs and Features** (Windows 7) or **Programs** (Windows 8 and later).

**Step 2** Scroll through the list of installed programs to locate Cisco JVDI Agent.

The Cisco JVDI Agent version appears in the **Versions** column.


---

# Verify Device Registration with Cisco Unified Communications Manager

After device registration, verify that the CSF device registered to the Cisco Unified Communications Manager from the thin client IP address. For more information, see the documentation for your version of Cisco Unified Communications Manager.

## Verify the Connection Status in Cisco Jabber

After you sign in to Cisco Jabber for Windows, you can check the connection status for Jabber and for Cisco Softphone for VDI. You can also confirm the versions for the JVDI Agent and the JVDI Client.

**Step 1** Click  to open the **Settings Menu**.

**Step 2** Go to **Help > Show connection status**

**Step 3** In the **Connection Status** window, click **JVDI Details**.

You can see the following information:

- **JVDI Client version**

**Tip** If the JVDI Client version is 12.5 or 12.1, the client version doesn't appear until after the softphone connects.

- **JVDI Agent version**

- **Virtual Channel status** indicates whether communication between the JVDI Client and Cisco Jabber is successful.

- **SIP status** indicates whether SIP communication with Cisco Unified Communications Manager is successful.

- **Softphone CTI status** indicates whether CTI communication is successful.

**Tip** If the **SIP status** is **Connected**, but the **Softphone CTI status** is **Not connected**, check the CTI configuration in CUCM.

**Step 4** To see detailed diagnostic information for Cisco Jabber, press **Ctrl +Shift +D**.

## Jabber VDI Fallback Mode

Jabber VDI fallback mode offers short-term support for basic audio and video calls when VDI can't establish the virtual channel. Fallback mode supports standard calls and call recording. The full feature set isn't supported. For example, you can't forward a call that you're recording in fallback mode. Call quality is lower because of the server or network issues that cause the switch to fallback mode.

## Disable BFCP desktop share

The Jabber parameter `EnableBFCPVideoDesktopShare` might not work properly in JVDI environments.

In Jabber Softphone for VDI Release 14.0.3, we added a JVDI configuration parameter to force the proper behavior if necessary.

**ENABLE\_BFCP\_DESKTOP\_SHARE**—Applies to JVDI Client for Windows and Linux

Added to fix [CSCwa33411](#). This parameter helps disable BFCP screen sharing if necessary.

You configure this parameter in the `cisco.conf` of JVDI Client. On Windows, `cisco.conf` is in `C:\Program Files\Cisco Systems\Cisco VXME` or `C:\Program Files (x86)\Cisco Systems\Cisco VXME`. On Linux, `cisco.conf` is in `/etc/`

- `true` (default)—Enables BFCP screen sharing
- `false`—Disables BFCP screen sharing