Deployment and Installation Guide for Cisco Jabber Softphone for VDI—Unicon eLux Release 12.6

First Published: 2019-04-10

Last Modified: 2019-11-26

CONTENTS

Cisco Jabber Softphone for VDI

Purpose of this Guide

This guide provides information about the following topics:

- Installing and configuring Cisco Jabber Softphone for VDI—Unicon eLux

- Installing and configuring Cisco AnyConnect Secure Mobility Client in a Cisco Jabber Softphone for VDI—Unicon eLux deployment

- Upgrading Cisco Jabber Softphone for VDI—Unicon eLux

About Cisco Jabber Softphone for VDI

Cisco Jabber Softphone for VDI extends the Cisco collaboration experience to virtual deployments. With a supported version of Cisco Jabber for Windows, users can send and receive phone calls on their hosted virtual desktops (HVD). The Cisco Jabber Softphone for VDI software detects the virtual environment and routes all audio and video streams directly from one endpoint to another, without going through the HVD.

The applications in the Cisco Jabber Softphone for VDI family of products are:

- Cisco Jabber Softphone for VDI—HP Thin Pro and Ubuntu

- Cisco Jabber Softphone for VDI—Unicon eLux

- Cisco Jabber Softphone for VDI—Windows

Virtual Deployments

With Cisco Jabber Softphone for VDI, thin client users can place and receive calls with their Cisco Unified Communications application (Cisco Jabber). Cisco Jabber Softphone for VDI consists of the Cisco JVDI

Agent and the Cisco JVDI Client. To reduce latency and to enhance media quality, Cisco Jabber Softphone for VDI streams media between the endpoints without going through the hosted virtual desktops.

Figure 1: Cisco Jabber Softphone for VDI—Data Flow
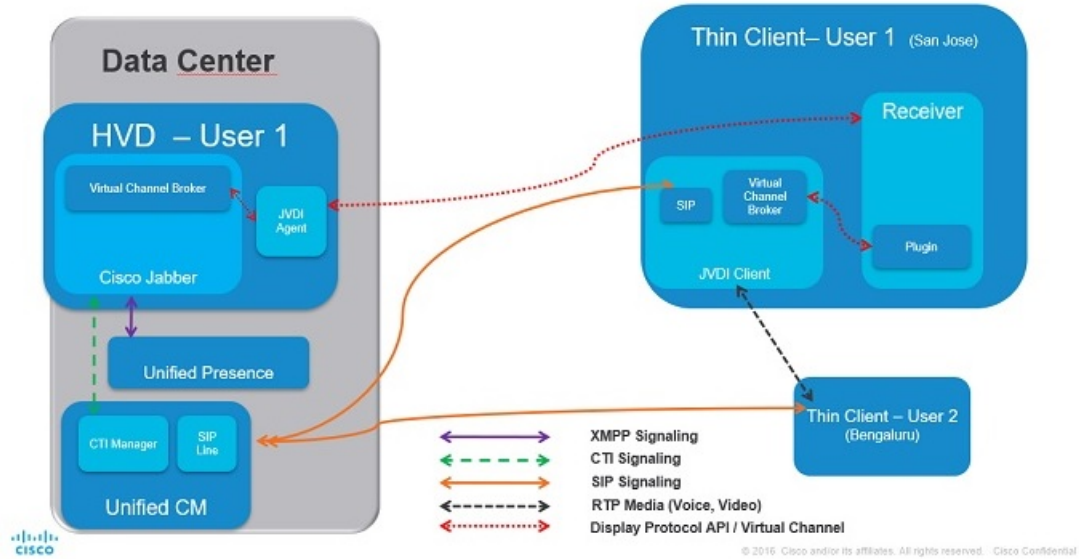
Cisco Jabber Softphone for VDI supports some audio and video accessories. For a complete listing of supported audio and video accessories, see *Unified Communications Endpoint and Client Accessories*, at http://www.cisco.com/c/en/us/products/unified-communications/uc_endpoints_accessories.html.

Use the following flowchart to determine whether you require Cisco Jabber Softphone for VDI.

Figure 2: Do You Need Cisco Jabber Softphone for VDI?
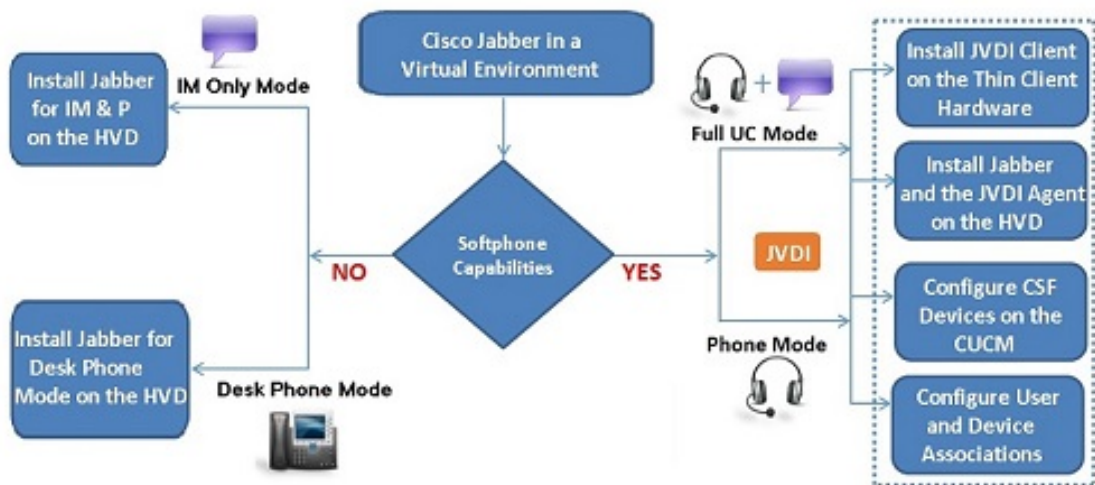
A Cisco Jabber Softphone for VDI deployment consists of the following components:

- Supported Unicon eLux thin clients.

For more information about supported thin clients, see *Release Notes for Cisco Jabber Softphone for VDI for Unicon eLux*.

- Cisco JVDI Client installed on the thin client.

- Windows hosted virtual desktops (HVD), in a data center.

  The Virtual Machines for the HVDs can be either Citrix-, or VMware-provisioned. Citrix-provisioned virtual machines can be dedicated, or have multiple users connected over multiple remote sessions. To support multiple remote sessions, the virtual machine must be running a supported Microsoft Windows Server operating system.

- Cisco Jabber installed on the HVD.

- Cisco JVDI Agent installed on the HVD.

- Cisco Unified Communications Manager.

Differences in the Virtual Environment

The user experience, with Cisco Jabber Softphone for VDI and a supported Cisco Unified Communications client, is similar to the experience provided by a standard installation. However, in a virtual environment there are some differences:

- The Cisco Unified Communications client detects the virtual environment at run time and starts in virtualization mode.

- Cisco Jabber can control a Cisco IP Phone or use the computer to make and receive calls. The default phone selection is **Use my computer for calls**. After device selection, the Cisco Jabber Softphone for VDI application starts the transfer of the phone configuration data for that user. For more information, see Configuration Files, on page 21.

- Use the **Device Selector**, which is located in the Windows notification area, to manage camera and audio devices. Device management is also available from within the Cisco Unified Communications client.

- By default, all calls send and receive video if both parties have video capability. The available options are:

  - **Always start calls with video:** Starts all calls as video calls, which send local video

  - **Never start calls with video:** Starts all calls as audio-only calls

  This setting applies to all calls placed and received. The default setting is **Always start calls with video**.

  > **Note** You can disable video globally or on a per-device basis on the Cisco Unified Communications Manager. Navigate to **System** > **Enterprise Phone Configuration** and set **Video Calling** to **Disabled**.

- Some menus and options are different in a virtual deployment. For example, Video Desktop Share (Binary Floor Control Protocol) is not available from the call window. Video Desktop Share is supported only from the IM-chat window (Remote Desktop Protocol).

☞

Important   If Cisco Jabber is also installed on the thin clients, ensure that everyone exits Jabber before signing in to their HVD. If Cisco Jabber is running on the local desktop, and one tries to sign in to Jabber on their HVD, the Cisco JVDI Client cannot register. Problems with accessories can also occur.

C H A P T E R 2

Requirements

Requirements

☞

Important   Each of the components listed in the following table must meet the requirements. Use of unsupported components can result in a nonfunctional deployment.

Only the components, versions, and minimum hardware requirements listed in the table are supported.

Component	Requirements
Unicon eLux thin clients—Hardware	The minimum hardware requirements for thin clients are: • 1.6-GHz dual-core processor • 2-GB RAM The following client hardware was tested with eLux RP 5.7.0: • HP T620 Dual Core / Quad Core • HP T630 Dual Core / Quad Core • HP T730 • Cisco VXC 6215 • Dell Wyse Z50D

Component	Requirements
Hosted virtual desktop OS (server-side)	• Microsoft Windows 7 32 bit • Microsoft Windows 7 64 bit • Microsoft Windows 8 32 bit • Microsoft Windows 8 64 bit • Microsoft Windows 8.1 32 bit • Microsoft Windows 8.1 64 bit • Microsoft Windows 10 32 bit • Microsoft Windows 10 64 bit
Connection broker for the hosted virtual desktop [1]	• Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop) versions 6.x, 7.x–7 1811, and 7.15 LTSR—Published desktops only • VMware Horizon 6.0 (with View)—Published desktops only • VMware Horizon 6 versions 6.x–7.7—Published desktops only Published Application is not supported with Cisco Jabber Softphone for VDI for Unicon eLux.
Citrix Workspace app or VMware Horizon Client [2] (Installed on the thin client)	**Unicon eLux 5.7 (eLuxRP-5.7.2000_AllPackages-1)** Unicon eLux contains the required Citrix and VMware versions. The eLux package is available from Unicon eLux. For assistance locating the download, contact eLux support.
Cisco Unified Communications client on the hosted virtual desktop: Cisco Jabber for Windows.	Cisco Jabber for Windows 12.5 running on the hosted virtual desktop (HVD). Cisco Jabber Softphone for VDI is compatible with all future 12.6(x) Cisco Jabber for Windows versions. For complete information about virtual environment compatibility, see the Cisco Jabber documentation for your release.
Cisco Unified Communications Manager	• Recommended CUCM Release 11.5(1)SU3 or later • Minimum CUCM Release 10.5
Cisco AnyConnect (Optional)	vpnsystem V4.5-1

Component	Requirements
Accessories	For a complete listing of supported audio and video accessories, see *Unified Communications Endpoint and Client Accessories*, at http://www.cisco.com/c/en/us/products/unified-communications/uc_endpoints_accessories.html.
	Important Ensure that all Jabra devices are running the latest firmware. You can use Jabra Direct to update the firmware. For more information visit: http://www.jabra.com.

[1] A connection broker is software that creates connections to hosted virtual desktops. A connection broker performs a number of tasks including the following:

- Validating the username and providing a connection for the user.

- Allowing the user to connect to a specific virtual desktop.

[2] The Citrix Workspace app or VMware Horizon Client provides a user interface for the corresponding connection broker.

Considerations for Thin Clients

Unicon eLux thin clients must meet all system requirements. For more information, see *Release Notes for Cisco Jabber Softphone for VDI—Unicon eLux* for your release.

Unicon Scout Enterprise is the recommended deployment tool to deploy Cisco Jabber Softphone for VDI to Unicon eLux-based thin clients.

☞

Important Cisco does not support any management administrative method to deploy Cisco Jabber Softphone for VDI to Unicon eLux-based thin clients. Support for adding and enabling add-ons is provided by Unicon, using Unicon Scout Enterprise or other methods supported by Unicon.

Port Requirements

The following table lists the ports and port ranges used by Cisco Jabber Softphone for VDI.

Table 1: Port Usage

Port	Description
69 and Ephemeral	UDP Outbound traffic for TFTP
	Note An ephemeral port is a short-lived transport protocol port for IP communications. IP software can allocate ephemeral ports automatically from a predefined range. The following protocols can use an ephemeral port assignment for the client end of a communication, to a well-known port on a server.
	• Stream Control Transmission Protocol (SCTP)
	• Transmission Control Protocol (TCP)
	• User Datagram Protocol (UDP)
	A well-known port is a port reserved by the Internet Corporation for Assigned Names and Numbers (ICANN) for assignment for specific applications.
5060	TCP (default) or UDP Outbound traffic for Session Initiation Protocol (SIP) call signaling
5061	TCP Outbound traffic for Secure SIP call signaling
6970	TCP Outbound traffic for HTTP
16384–32767	UDP Inbound and outbound traffic for RTP (audio and video streams)
	You can configure the Cisco Unified Communications Manager to reduce this port range. Change the **Start/Stop Media Port** setting in the SIP Profile, which is associated with the CSF device.

Supported Codecs

Table 2: Supported Audio and Video Codecs

Audio Codec	Video Codec
G.722	H.264/AVC
G.722.1 (24 and 32k) G.722.1 is supported on Cisco Unified Communications Manager 8.6.1 or later.	

Audio Codec	Video Codec
G.711 A-law	
G.711 u-law	
G.729a	
Opus Opus is supported on Cisco Unified Communications Manager 11.0 or later.	

Installation and Deployment

Deployment and Installation Workflow

👉

Important The Cisco Jabber for Windows and Cisco JVDI Agent versions must always match. The Cisco JVDI Client version can be the same, or up to two releases earlier. The available feature set is determined by the earlier software version.

You must install both Cisco JVDI Agent and Cisco JVDI Client; otherwise, the softphone fails to register.

We recommend that you read the *Release Notes for Cisco Jabber Softphone for VDI—Unicon eLux* for your release. Review the requirements to confirm that all required hardware and software meet them. Failure to meet all requirements can result in a nonfunctional deployment.

Procedure

Step 1 Follow the instructions to deploy Cisco Jabber for Windows, up to the installation of the Jabber client.

Important You must create CSF devices for Cisco Jabber Softphone for VDI users, and add each user to the following Access Control Groups:

- Standard CCM End Users

- Standard CTI Enabled

See *On-Premises Deployment for Cisco Jabber* for your release.

For hybrid deployments, see *Cloud and Hybrid Deployments for Cisco Jabber* for your release.

Jabber deployment guides are available from: https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html.

Step 2 Create and set up the hosted virtual desktops in the data center.

Ensure that the hosted virtual desktops (HVD) are ready for you to install Cisco Jabber Softphone for VDI.

Step 3 Set up and configure the thin clients. Documentation for Unicon eLux thin clients is available from the individual hardware vendors. Documentation for Unicon eLux is available from www.unicon-software.com/udocs.

Step 4 Configure the network. See Port Requirements, on page 8.

Step 5 Install the Cisco Jabber Softphone for VDI components on the thin clients and the hosted virtual desktop. See Install the Components Workflow, on page 13.

After you install Cisco JVDI Agent and other required software on the HVD, you can clone the HVD.

Use the Elias tool to create an image that contains Cisco JVDI Client. Deploy the image to the thin clients. For more information about how to create an image or how to update the thin client, see the Elias documentation available from the Unicon website.

Set up the Hosted Virtual Desktops Workflow

Procedure

Step 1 Log in to the Microsoft Windows HVD as the new user, with administration rights.

Step 2 Join the HVD to the corporate domain.

You must have domain administration rights.

Step 3 Set up Citrix or VMware access to the HVDs.

Step 4 Install Cisco JVDI Agent on the HVD.

Step 5 Install Cisco Jabber on the HVD.

See the installation guide for your release: http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

Step 6 Clone the HVD image.

For best practices for cloning Microsoft Windows HVD images, consult the documentation for your Citrix or VMware product.

Install the Components Workflow

☞

Important   The Cisco Jabber for Windows and Cisco JVDI Agent versions must always match. The Cisco JVDI Client version can be the same, or up to two releases earlier. The available feature set is determined by the earlier software version.

Procedure

Step 1   Download the Cisco JVDI Client, on page 13

Step 2   Download the Cisco JVDI Agent, on page 14

Step 3   (Optional) Download Cisco AnyConnect, on page 14

Perform this step only if users require VPN connectivity.

Step 4   Have all users log out of the hosted virtual desktops.

Step 5   On the thin client, install the Cisco JVDI Client. If users require VPN connectivity, deploy Cisco AnyConnect at the same time.

Step 6   On the HVD, uninstall any previously installed version of Cisco VXME Agent or Cisco JVDI Agent.

Step 7   On the HVD, uninstall any previously installed Cisco Unified Communications clients such as Cisco Jabber.

Step 8   On the HVD, install Cisco JVDI Agent.

Double-click the MSI file and follow the installation wizard steps.

Step 9   On the HVD, install Cisco Jabber for Windows.

Double-click CiscoJabberSetup.msi and follow the installation wizard steps. For detailed information about how to install Jabber for Windows, see *On-Premises Deployment for Cisco Jabber* for your release.

For hybrid deployments, see *Cloud and Hybrid Deployments for Cisco Jabber* for your release.

Jabber deployment guides are available from: https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html.

Download the Cisco JVDI Client

Procedure

Step 1   Visit the following URL:

http://www.cisco.com/cisco/software/navigator.html

Step 2   Go to **Products** > **Unified Communications** > **Unified Communications Applications** > **Messaging** > **Cisco Jabber Softphone for VDI for Unicon eLux**.

Step 3 From the list, choose the file for your release.

Step 4 Click **Download** or **Add to cart** and follow the prompts.

Download the Cisco JVDI Agent

Install Cisco JVDI Agent on the hosted virtual desktops (HVD), before you install Cisco Jabber for Windows.

Procedure

Step 1 Visit the following URL:

http://www.cisco.com/cisco/software/navigator.html

Step 2 Go to **Products** > **Unified Communications** > **Unified Communications Applications** > **Messaging** > **Cisco Jabber Softphone for VDI for Unicon eLux**.

Step 3 From the list, choose the file for your release.

Step 4 Click **Download** or **Add to cart** and follow the prompts.

Download Cisco AnyConnect

The supported **vpnsystem** package is available from Unicon.

Procedure

Step 1 Visit the Unicon web site: http://www.myelux.com.

Step 2 Locate and download the package.

Upgrade

Upgrade Notes

The following upgrade paths are supported:

- Cisco Jabber Softphone for VDI for Unicon eLux Release 12.0 to Cisco Jabber Softphone for VDI for Unicon eLux Release 12.6.

- Cisco Jabber Softphone for VDI for Unicon eLux Release 12.1 to Cisco Jabber Softphone for VDI for Unicon eLux Release 12.6.

- Cisco Jabber Softphone for VDI for Unicon eLux Release 12.5 to Cisco Jabber Softphone for VDI for Unicon eLux Release 12.6.

The Cisco Jabber for Windows and Cisco JVDI Agent versions must always match. However, the JVDI Client version can be the same, or up to two releases earlier (N-2 support). For example, the following version combinations are supported:

- Cisco Jabber for Windows Release 12.6, Cisco JVDI Agent Release 12.6, and Cisco JVDI Client Release 12.6

- Cisco Jabber for Windows Release 12.6, Cisco JVDI Agent Release 12.6, and Cisco JVDI Client Release 12.5

- Cisco Jabber for Windows Release 12.6, Cisco JVDI Agent Release 12.6, and Cisco JVDI Client Release 12.1

Important   The limitations and restrictions for the earlier JVDI Client release apply. The available features are limited to those available for the earlier release. For more information, see the *Release Notes for Cisco Jabber Softphone—Unicon eLux*, for the earlier release. For example, if your JVDI Client Release is 12.1, see the release notes document for Release 12.1.

Upgrade Workflow

☞

Important	To enable the Unified Communications features, upgrade all the following components:

> • The platform image on the thin client
>
> • Cisco Jabber Softphone for VDI—Cisco JVDI Client (thin client) and Cisco JVDI Agent (HVD)
>
> • Cisco Unified Communications software on the hosted virtual desktop (HVD)

Procedure

Step 1 Read the Release Notes document for your release of Cisco Jabber Softphone for VDI, available from http://www.cisco.com/c/en/us/support/collaboration-endpoints/virtualization-experience-media-edition/products-release-notes-list.html.

Review the important notes for information about limitations or restrictions that may affect your deployment.

Step 2 See Requirements, on page 5.

Review the system requirements to confirm that all required hardware and software meet them. Failure to meet all requirements can result in a nonfunctional deployment.

Step 3 Have all users log out of the hosted virtual desktops.

Step 4 Install the Cisco Jabber Softphone for VDI components on the thin clients and hosted virtual desktops.

See Install the Components Workflow, on page 13.

If your users do not require VPN access, you can skip the optional steps to install Cisco AnyConnect.

Upgrade Cisco Jabber for Windows

Use this procedure to upgrade to a supported maintenance release of Cisco Jabber for Windows. For supported Cisco Jabber versions, see the "System Requirements" section in the *Release Notes for Cisco Jabber Softphone for Unicon eLux* for your release.

Procedure

Step 1 Close Cisco Jabber and ensure that it is not running on the HVD.

Important If Cisco Jabber is running during the installation, exit and restart Cisco Jabber to enable virtualization.

Step 2 Install Cisco Jabber.

Troubleshooting

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 Platform Base Image Version

Procedure

Step 1 On the **Start** menu, select **Control Panel**.

Step 2 Select the **Setup** tab.

Step 3 Select the **General** tab and look for the OS line.

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.

Procedure

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 andCisco 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**.

Verify That Cisco JVDI Client Is Installed

Use this procedure to verify that Cisco JVDI Client is installed, and to confirm the Cisco JVDI Client version.

Procedure

Step 1   On the **Start** menu, select **Control Panel**.

Step 2   Select the **Setup** tab.

Step 3   Select the **General** tab.

Step 4   Scroll down the list of packages and look for **Cisco JVDI Client**.

The add-on versions appear in the same line.

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.

Procedure

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

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 That VXC Is Running on the Thin Client

Cisco Jabber Softphone for VDI requires that the `vxc` process be running.

Procedure

Step 1   Use Secure Shell (SSH) to connect to the thin client.

Step 2   Search the running programs for `vxc`.

ps -ef | grep -r vxc

You should see the following lines:

```
 admin@LWT44d3ca76ba19:~> ps -ef |grep -r vxc

thinuser 6536 1 0 Mar14 ? 00:07:43 /bin/bash /usr/bin/pidrun.sh -c run_vxc.sh -a -m -o
/var/log/cisco/vxcConsole.log -e /var/log/cisco/vxcError.log

thinuser 6538 6536 0 Mar14 ? 00:00:00 /bin/bash /usr/bin/run_vxc.sh -m

thinuser 6547 6538 8 Mar14 ? 13:02:16 vxc -m

admin 31576 31303 0 11:05 pts/0 00:00:00 grep -r vxc

admin@LWT44d3ca76ba19:~>
```

Call Control Is Lost After a Network Failure

Users see a prompt to reconnect to their hosted virtual desktops (HVDs). After the users reconnect, Cisco Jabber call control features do not work.

This problem can occur if the thin client loses network connectivity.

To resolve this issue, have the users exit Cisco Jabber and disconnect from their HVDs. Next they can log back in to their HVDs and sign back in to Cisco Jabber to restore call control.

Call Is Lost After HVD Disconnection

Users receive a prompt to log back in to their hosted virtual desktops (HVD) during an active call, and the call drops. The other party to the call has no indication that the call has ended, except the line is silent.

This issue can occur if the connection between the thin client and the HVD drops, causing a temporary loss of registration and call control.

To work around this issue, users can call the other party back. If the other party is not available, users can send an instant message (IM).

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 21.

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.