



## **Deployment and Installation Guide for Cisco Jabber Softphone for VDI—Windows Release 12.1**

**First Published:** 2018-06-18

**Last Modified:** 2020-01-24

### **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

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 NON-INFRINGEMENT 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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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: [www.cisco.com go trademarks](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. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

<b>CHAPTER 1</b>	<b>Cisco Jabber Softphone for VDI</b>	<b>1</b>
	Purpose of this Guide	1
	About Cisco Jabber Softphone for VDI	1
	Virtual Deployments	1
	Differences in the Virtual Environment	3

---

<b>CHAPTER 2</b>	<b>Requirements</b>	<b>5</b>
	System Requirements	5
	Considerations for Thin Clients	8
	Port Requirements	9
	Supported Codecs	10

---

<b>CHAPTER 3</b>	<b>Installation and Deployment</b>	<b>11</b>
	Deployment and Installation Workflow	11
	Install the Components Workflow	12
	Set up the Hosted Virtual Desktops Workflow	13
	VMware Installation—Required Setting	13
	Download the Cisco JVDI Client	16
	Download the Cisco JVDI Agent	16
	Cisco JVDI Client Installation	16
	Run the Microsoft Installer	17
	Use the Command Line	17
	Use the Group Policy Editor	18
	Set the Language Code	19

---

<b>CHAPTER 4</b>	<b>Configuration</b>	<b>21</b>
------------------	----------------------	-----------

- Configuration Files 21
- Set up Users on the Cisco Unified Communications Manager Workflow 21
  - Create a CSF Device and a Directory Number for Each User 22
  - Associate New Devices with a User 24
  - Enable the CTI Protocol for Users 24
  - Configure Cisco Unified Communications Features for Users 25
  - Change a User Password 25

---

**CHAPTER 5**

**Upgrade 27**

- Upgrade Workflow 27
- Upgrade Cisco Jabber for Windows 28
- Upgrade the Citrix Receiver or the VMware Client 28
- Change the Hosted Virtual Desktop Connection Type 29

---

**CHAPTER 6**

**Troubleshooting 31**

- Registry Keys 31
- Verify That Cisco JVDI Client Is Running 31
- Verify That Cisco JVDI Agent Is Installed 32
- Confirm the Version of Cisco JVDI Client 32
- Call Control Is Lost After a Network Failure 32
- Call Is Lost After HVD Disconnection 33
- Problem Reporting Tool 33
  - Virtual Channel Problem 33



## CHAPTER 1

# Cisco Jabber Softphone for VDI

---

- [Purpose of this Guide, on page 1](#)
- [About Cisco Jabber Softphone for VDI, on page 1](#)
- [Virtual Deployments, on page 1](#)
- [Differences in the Virtual Environment, on page 3](#)

## Purpose of this Guide

This guide provides information about the following topics:

- Installing and configuring Cisco Jabber Softphone for VDI for Windows
- Installing and configuring Cisco AnyConnect Secure Mobility Client in a Cisco Jabber Softphone for VDI for Windows deployment
- Upgrading Cisco Jabber Softphone for VDI for Windows

## 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:

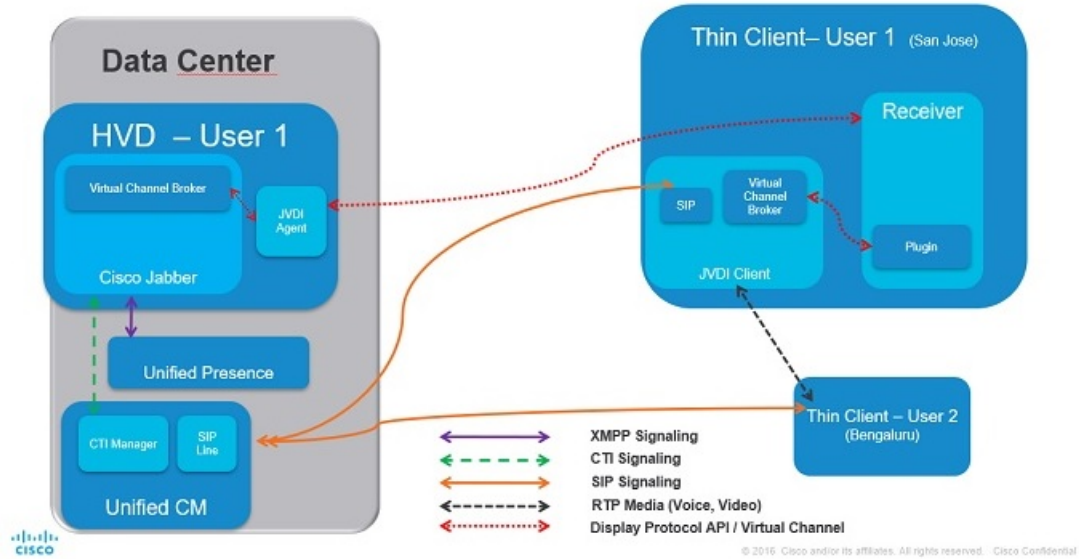
- Cisco Jabber Softphone for VDI—HP Thin Pro and Ubuntu
- Cisco Jabber Softphone for VDI—Unicon eLux
- Cisco Jabber Softphone for VDI—Windows

## 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.

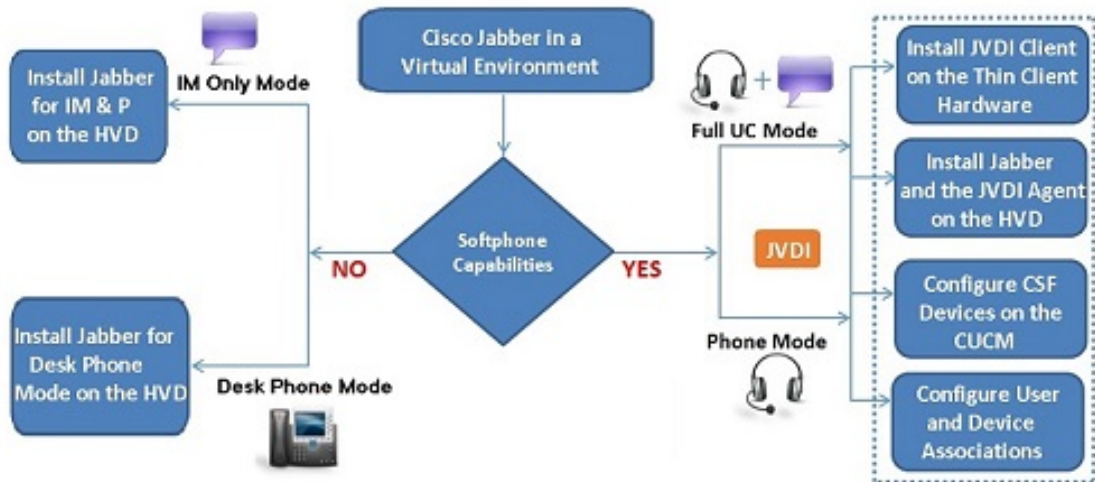
Figure 1: Cisco Jabber Softphone for VDI—Data Flow



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](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 Windows thin clients.

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

- 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).







## CHAPTER 2

# Requirements

- [System Requirements](#), on page 5
- [Considerations for Thin Clients](#), on page 8
- [Port Requirements](#), on page 9
- [Supported Codecs](#), on page 10

## System 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
Microsoft Windows-based thin client hardware	<ul style="list-style-type: none"><li>• Installed RAM 2 GB</li><li>• Free Physical Memory 128 MB</li><li>• Free Disk Space 256 MB</li><li>• CPU Mobile AMD Sempron Processor 3600+, 2-GHz Intel Core 2 CPU, or T7400 2.16 GHz</li><li>• DirectX 11 compatible GPU</li><li>• USB 2.0 for USB camera and audio devices</li></ul> <p><b>Note</b> Cisco Jabber Softphone for VDI for Windows does not require the Microsoft .NET Framework or any Java modules.</p>

Component	Requirements
Microsoft Windows-based thin client OS	<ul style="list-style-type: none"> <li>• Microsoft Windows 7 32 bit</li> <li>• Microsoft Windows 7 64 bit</li> <li>• Microsoft Windows 8 32 bit</li> <li>• Microsoft Windows 8 64 bit</li> <li>• Microsoft Windows 8.1 32 bit</li> <li>• Microsoft Windows 8.1 64 bit</li> <li>• Microsoft Windows 10 32 bit</li> <li>• Microsoft Windows 10 64 bit</li> <li>• Windows Thin PC 32 bit</li> </ul>
Windows Embedded Standard-based thin client hardware	<ul style="list-style-type: none"> <li>• Installed RAM 2 GB</li> <li>• Free Physical Memory 128 MB</li> <li>• Free Disk Space 256 MB</li> <li>• CPU performance affects the maximum video resolution. With Windows Embedded Standard thin clients, the expected resolution depends on the CPU: <ul style="list-style-type: none"> <li>• Up to 720p with quad-core AMD GX-420CA SOC 2 GHz or similar</li> <li>• Up to 240p with dual-core AMD G-T56N 1.65 GHz or similar</li> <li>• Audio-only support with dual-core VIA Eden X2 U4200 1 GHz or similar CPU</li> </ul> </li> </ul> <p><b>Note</b> These hardware specifications are only guidelines for the expected resolutions. Other factors can affect video resolution.</p> <ul style="list-style-type: none"> <li>• DirectX 11 compatible GPU</li> <li>• USB 2.0 for USB camera and audio devices</li> </ul> <p><b>Note</b> Cisco Jabber Softphone for VDI for Windows does not require the Microsoft .NET Framework or any Java modules.</p>
Windows Embedded Standard-based thin client OS	<ul style="list-style-type: none"> <li>• Windows Embedded Standard 7 32 bit</li> <li>• Windows Embedded Standard 7 64 bit</li> <li>• Windows Embedded Standard 8 64 bit</li> <li>• Windows 10 IoT Enterprise</li> </ul>

Component	Requirements
Hosted virtual desktop OS (server-side)	<ul style="list-style-type: none"> <li>• Microsoft Windows 7 32 bit</li> <li>• Microsoft Windows 7 64 bit</li> <li>• Microsoft Windows 8 32 bit</li> <li>• Microsoft Windows 8 64 bit</li> <li>• Microsoft Windows 8.1 32 bit</li> <li>• Microsoft Windows 8.1 64 bit</li> <li>• Microsoft Windows 10 32 bit</li> <li>• Microsoft Windows 10 64 bit</li> </ul>
Connection broker for the hosted virtual desktop <a href="#">1</a>	<ul style="list-style-type: none"> <li>• Citrix XenDesktop 7.5 and later 7.x versions</li> <li>• Citrix XenApp 7.5 and later 7.x versions—Published Desktop and Published Application               <ul style="list-style-type: none"> <li><b>Important</b> Published Application is not supported in full-screen mode.</li> </ul> </li> <li>• VMware Horizon 6.0 (with View)—Published desktops only</li> <li>• VMware Horizon 6 version 6.1.0—Published desktops only</li> <li>• VMware Horizon 6 version 6.2.0—Published desktops only</li> <li>• VMware Horizon 7 version 7.x—Published desktops only</li> </ul>
Citrix Receiver or VMware Horizon Client <a href="#">2</a> (Installed on the thin client)	<ul style="list-style-type: none"> <li>• Citrix Receiver (ICA) for Windows 4.4.1000 and later 4.x versions</li> <li>• VMware Horizon Client for Windows 4.1.0, 4 and later 4.x version. (Versions 4.3 and 4.4 are not supported.)</li> </ul> <p>To enable JVDI support with versions 4.5 and later, check <b>32-bit Core Remote Experience on this 64-bit machine</b> during the VMWare Horizon installation (new install or upgrade). For more information about this setting, see the VMWare Horizon documentation.</p> <p><b>Important</b> Before you install the Cisco JVDI Client, install the Citrix Receiver or VMware Horizon Client on the thin client.</p> <p>If you change from a Citrix environment to a VMware environment (or from VMware to Citrix), reinstall the Cisco JVDI Client.</p>

Component	Requirements
Cisco Unified Communications client on the hosted virtual desktop:  Cisco Jabber for Windows or Cisco UC Integration™ for Microsoft Lync.	Cisco Jabber for Windows 12.1 running on the hosted virtual desktop (HVD).  Cisco Jabber Softphone for VDI is compatible with all future 12.1(x) Cisco Jabber for Windows versions.  For complete information about virtual environment compatibility, see the documentation for Cisco Jabber or Cisco UC Integration™ for Microsoft Lync.
Cisco Unified Communications Manager	<ul style="list-style-type: none"> <li>• Recommended CUCM Release 11.5(1)SU3 or later</li> <li>• Minimum CUCM Release 10.5</li> </ul>
Accessories	<p>For a complete listing of supported audio and video accessories, see <i>Unified Communications Endpoint and Client Accessories</i>, at <a href="http://www.cisco.com/c/en/us/products/unified-communications/uc_endpoints_accessories.html">http://www.cisco.com/c/en/us/products/unified-communications/uc_endpoints_accessories.html</a>.</p> <p><b>Important</b> Ensure that all Jabra devices are running the latest firmware. You can use the Jabra Direct to update the firmware. For more information visit: <a href="http://www.jabra.com">http://www.jabra.com</a>.</p>

<sup>1</sup> A connection broker is software that creates connections to hosted virtual desktops. A connection broker performs a number of tasks that include

- Validating the username and providing a connection for the user.
- Allowing the user to connect to a specific virtual desktop.

<sup>2</sup> The Citrix Receiver or VMware Horizon Client provides a user interface for the corresponding connection broker.

(PCoIP only)

## Considerations for Thin Clients

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

# Port Requirements



**Important** The Cisco JVDI Client installer does not add firewall rules.

If the Windows Firewall is enabled on the thin clients, you must add the Cisco JVDI Client (vxc.exe) as an exception. The first time that you start Cisco JVDI Client, a Windows Security Alert appears. To add the exception, check the networks for which you want to allow Cisco JVDI Client. For more information about how to configure the Windows Firewall, see the Microsoft documentation.

This requirement applies to all versions of the Windows Firewall, including Windows Defender.

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  <b>Note</b> 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. <ul style="list-style-type: none"> <li>• Stream Control Transmission Protocol (SCTP)</li> <li>• Transmission Control Protocol (TCP)</li> <li>• User Datagram Protocol (UDP)</li> </ul> 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 <b>Start/Stop Media Port</b> 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.	
G.711 A-law	
G.711 u-law	
G.729a	
Opus Opus is supported on Cisco Unified Communications Manager 11.0 or later.	



## CHAPTER 3

# Installation and Deployment

- [Deployment and Installation Workflow](#), on page 11
- [Install the Components Workflow](#), on page 12
- [Set up the Hosted Virtual Desktops Workflow](#), on page 13
- [Download the Cisco JVDI Client](#), on page 16
- [Download the Cisco JVDI Agent](#), on page 16
- [Cisco JVDI Client Installation](#), on page 16

## Deployment and Installation Workflow



**Important** The Cisco Jabber for Windows version must match your Cisco Jabber Softphone for VDI version. The Cisco JVDI Agent and Cisco JVDI Client versions must be the same.

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—Windows* 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 a hosted virtual desktop (HVD) is ready for you to install Cisco JVDI Agent.
- Step 3** Set up and configure the thin clients. Documentation for thin clients is available from the original equipment manufacturer (OEM).
- Step 4** Configure the network. See [Port Requirements, on page 9](#).
- Step 5** Install the Cisco Jabber Softphone for VDI components on the thin clients and the hosted virtual desktops. See [Install the Components Workflow, on page 12](#).  
After you install all required software on the HVD, you can clone the HVD.
- 

## Install the Components Workflow



**Important** The Cisco Jabber for Windows version must match your Cisco Jabber Softphone for VDI version. The Cisco JVDI Agent and Cisco JVDI Client versions must be the same.

---

### Procedure

---

- Step 1** [Download the Cisco JVDI Client, on page 16](#).
- Step 2** [Download the Cisco JVDI Agent, on page 16](#).
- Step 3** Have all users log out of the hosted virtual desktops.
- Step 4** On the thin client, install the Cisco JVDI Client.  
See [Cisco JVDI Client Installation, on page 16](#).
- Step 5** On the HVD, uninstall any previously installed versions of Cisco JVDI Agent or Cisco JVDI Agent. Also uninstall Cisco Unified Communications clients, such as Cisco Jabber.
- Step 6** On the HVD, install Cisco JVDI Agent.
- Step 7** On the HVD, install Cisco Jabber.  
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>.
-



# 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.  
**Important** Configure VMware to use PCoIP.  
If you are installing a 32-bit version of Cisco Jabber Softphone for VDI, see [VMware Installation—Required Setting, on page 13](#).
- 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.
- 

## VMware Installation—Required Setting

To enable Cisco Jabber Softphone for VDI (32-bit only) support with versions 4.5 and later, perform a custom installation of VMware Horizon.

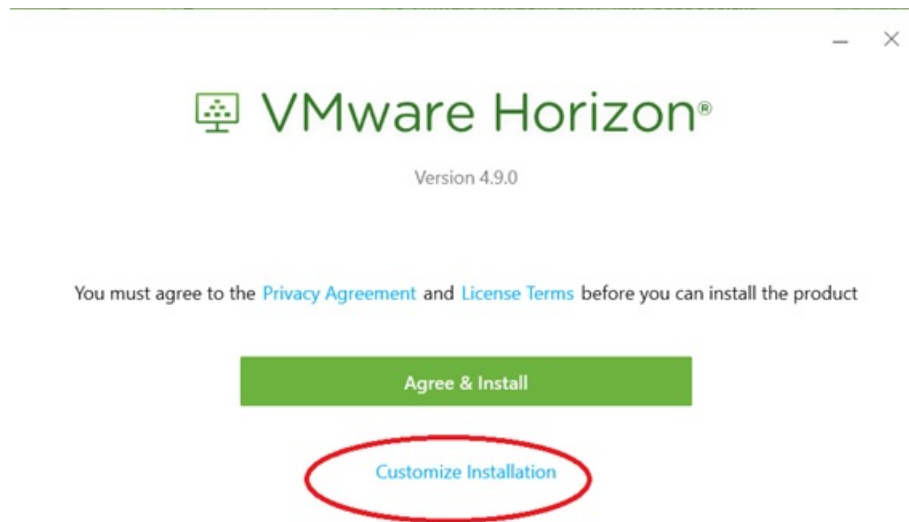


---

**Attention** This setting is not for 64-bit versions of Cisco Jabber Softphone for VDI.

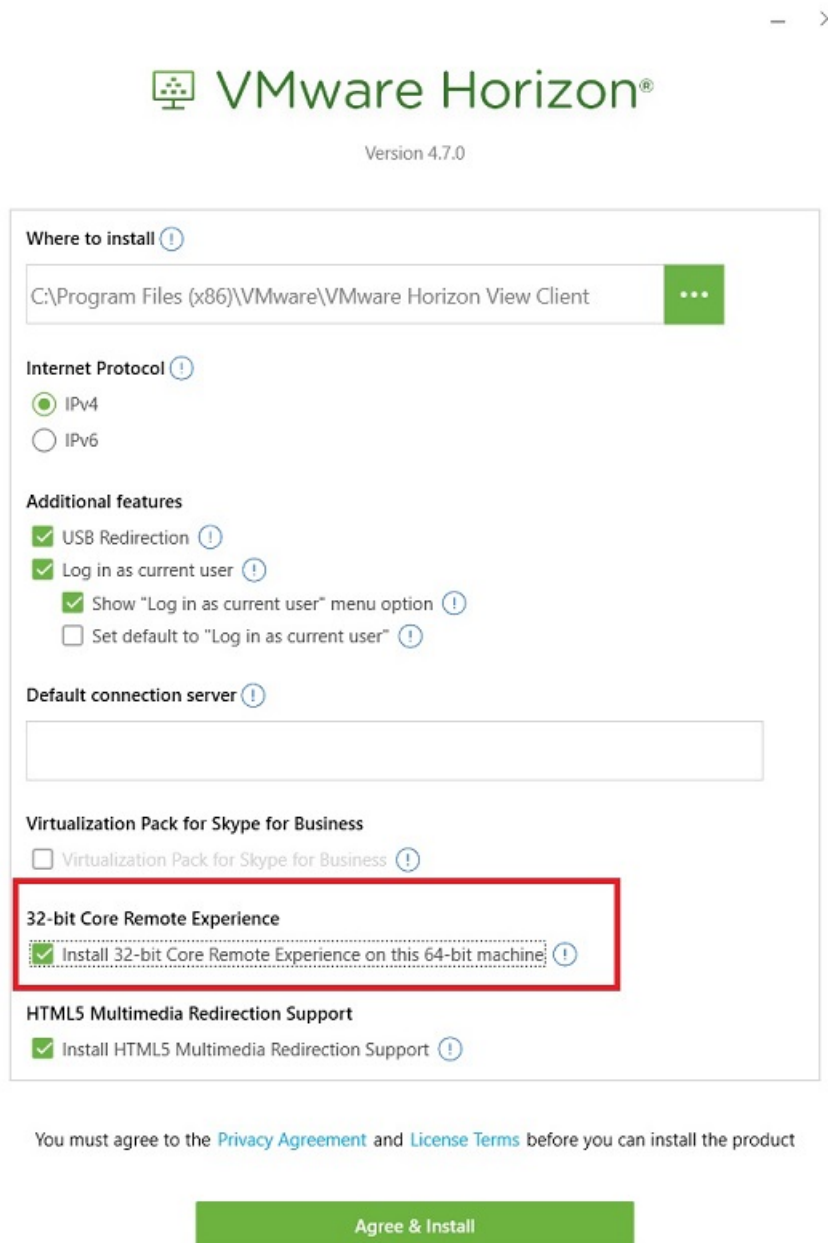
---

Figure 3: Select Customize Installation



Check the following setting during the installation (new install or upgrade): **32-bit Core Remote Experience on this 64-bit machine.**

Figure 4: VMware Customized Installation Settings



VMware Horizon®  
Version 4.7.0

Where to install ⓘ  
C:\Program Files (x86)\VMware\VMware Horizon View Client

Internet Protocol ⓘ  
 IPv4  
 IPv6

Additional features  
 USB Redirection ⓘ  
 Log in as current user ⓘ  
 Show "Log in as current user" menu option ⓘ  
 Set default to "Log in as current user" ⓘ

Default connection server ⓘ

Virtualization Pack for Skype for Business  
 Virtualization Pack for Skype for Business ⓘ

**32-bit Core Remote Experience**  
 Install 32-bit Core Remote Experience on this 64-bit machine ⓘ

HTML5 Multimedia Redirection Support  
 Install HTML5 Multimedia Redirection Support ⓘ

You must agree to the [Privacy Agreement](#) and [License Terms](#) before you can install the product

Agree & Install

For more information about this setting, see the VMware Horizon documentation.

## 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 Windows**.
- 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 Windows**.
- Step 3** From the list, choose the file for your release.
- Step 4** Click **Download** or **Add to cart** and follow the prompts.
- 

## Cisco JVDI Client Installation

### Prerequisites

Before you install Cisco JVDI Client on the thin clients, complete the following tasks:

- Install and set up the Citrix Receiver or VMware Horizon View Client.

Ensure that you are using a supported version of your Citrix or VMware product. For more information, see *Release Notes for Cisco Jabber Softphone for VDI for Windows* for your release.



---

**Important** The JVDI Client is a 32-bit application. When you install VMware Horizon View Client, choose **Customize Installation** and configure the following settings:

- Uncheck the **Virtualization Pack for Skype for Business** check box.
- Check the **Install 32-bit Core remote Experience on this 64-bit machine** check box.

---

- Obtain the Cisco JVDI Client zip file, and extract the contents.

Use one of the following methods to install Cisco JVDI Client:

- [Run the Microsoft Installer, on page 17](#)
- [Use the Command Line, on page 17](#)
- [Use the Group Policy Editor, on page 18](#)

## Run the Microsoft Installer

Run the Microsoft Installer (MSI) to install Cisco JVDI Client.

### Procedure

---

- Step 1** Double-click the CiscoJVDIClientSetup.msi file.
- Step 2** To open the executable file, click **OK**.
- Step 3** If the **Open File - Security Warning** appears, click **Run**.
- Step 4** Read the EULA and, if you agree, click **Accept and Install**.  
<http://www.cisco.com/go/eula>.
- Step 5** To complete the installation, click **Finish**.
- 

## Use the Command Line

### Procedure

---

- Step 1** Open a command window.
- Step 2** Enter the following command: `start /wait msixec.exe /i <path to MSI>\CiscoJVDIClientSetup.msi /quiet`.  
The `/quiet` switch specifies a silent installation.
-

## Use the Group Policy Editor

Use the Group Policy Management console to deploy Cisco JVDI Client to supported thin clients that are running a supported Microsoft Windows operating system.

### Before you begin

- Use Microsoft Orca to set the language code to 1033.
- Copy the modified Microsoft Installer (MSI) to a software distribution point for deployment. All computers to which you plan to deploy Cisco JVDI Client must be able to access the MSI on the distribution point.

### Procedure

---

- Step 1** Select **Start > Run**.
- Step 2** At the prompt, enter the following command: **GPMC.msc**.
- Step 3** Right-click on the appropriate domain in the left section.
- Step 4** Select **Create a GPO in this Domain, and Link it here**.
- Step 5** In the **New GPO** window, **Name** field, enter a name for the group policy object.
- Step 6** Leave the default value or select an option from the **Source Starter GPO** list, and then select **OK**.
- The new group policy appears in the list of group policies for the domain.
- Step 7** Select the group policy object under the domain in the left section.
- Step 8** From the **Security Filtering** section of the **Scope** tab, select **Add**.
- Step 9** Specify the computers and users to which you want to deploy Cisco JVDI Client.
- Step 10** Specify the MSI file.
- Step 11** Right-click the group policy object in the left section and then select **Edit**.
- The Group Policy Management Editor opens.
- Step 12** Select **Computer Configuration** and then select **Policies > Software Settings**.
- Step 13** Right-click **Software Installation** and then select **New > Package**.
- Step 14** Next to **File Name**, enter the location of the MSI file.

#### Example:

```
\\server\software_distribution
```

**Important** Enter the Uniform Naming Convention (UNC) path for the location of the MSI file. If you do not enter the UNC path, Group Policy cannot deploy Cisco JVDI Client.

- Step 15** Select the MSI file, and then select **Open**.
- Step 16** In the **Deploy Software** dialog box, select **Assigned**, and then select **OK**.
-

## Set the Language Code

Use Microsoft Orca to set the language code if you plan to use Group Policy to deploy Cisco JVDI Client. Microsoft Orca is available as part of the Microsoft Windows SDK for Windows 7 and .NET Framework 4 that you can download from the Microsoft website.

### Before you begin

Ensure that Microsoft Orca is installed.

### Procedure

---

- Step 1** Start Microsoft Orca.
  - Step 2** Select **File > Open**.
  - Step 3** Browse to the location of Cisco JVDI Client.
  - Step 4** Select Cisco JVDI Client, and then click **Open**.
  - Step 5** Select **View > Summary Information**.
  - Step 6** Set the Languages field to 1033.
  - Step 7** Select **OK**.
  - Step 8** Select **Tools > Options**.
  - Step 9** Select the **Database** tab.
  - Step 10** Select **Copy embedded streams during 'Save As'**.
  - Step 11** Select **Apply**, and then select **OK**.
  - Step 12** Select **File > Save As**.
  - Step 13** Select a location to which to save the modified Cisco JVDI Client file.
  - Step 14** Specify a name for the modified file, and then select **Save**.
-







## CHAPTER 4

# Configuration

---

- [Configuration Files, on page 21](#)
- [Set up Users on the Cisco Unified Communications Manager Workflow, on page 21](#)
- [Change a User Password, on page 25](#)

## 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.

---

## Set up Users on the Cisco Unified Communications Manager Workflow

### Procedure

---

- Step 1** [Create a CSF Device and a Directory Number for Each User, on page 22.](#)
- Step 2** [Associate New Devices with a User, on page 24.](#)
- Step 3** [Enable the CTI Protocol for Users, on page 24.](#)
- Step 4** [Configure Cisco Unified Communications Features for Users, on page 25.](#)

Enable the Unified Communications Manager IM and Presence Service. See the documentation for your version of Cisco Unified Communications Manager.

## Create a CSF Device and a Directory Number for Each User

You can use the same Cisco Unified Client Services Framework (CSF) devices for the virtual environment, as you do for the nonvirtual environment. We recommend that you create only one CSF device for each virtual user. If multiple devices exist for a virtual user, virtual Jabber automatically selects the first device in the list.

### Procedure

- Step 1** From Cisco Unified Communications Manager Administration, choose **Device > Phone**.
- Step 2** Select **Add New**.
- Step 3** From the **Phone Type** drop-down list, choose **Cisco Unified Client Services Framework**, and then select **Next**.
- Step 4** In the **Phone Configuration** window, enter the applicable information for the phone as follows:

Option	Description
<b>Device Name</b>	Enter a name to identify the Cisco Unified Client Services Framework device. The name can contain 1 to 15 characters, including alphanumeric characters. Periods, hyphens, and underscores are not supported. Typically the device name format is CSF<username>; however, including the user ID is optional. Example: CSFjohndoe.
<b>Description</b>	Enter a descriptive name for the phone. For example, enter <i>Richard-phone-on-computer</i> .
<b>Device Pool</b>	Choose <b>Default</b> or another profile that was previously created. The device pool defines sets of common characteristics for devices. These characteristics include the region, the date and time group, the softkey template, and Multilevel Precedence and Preemption (MLPP) information.
<b>Phone Button Template</b>	Choose <b>Standard Client Services Framework</b> . The phone button template determines the configuration of buttons on a phone and identifies which feature (such as line or speed dial) is used for each button. This option is required.
<b>Owner User ID</b>	To use an adjunct license with this device, choose the user ID from the list.
<b>Primary Phone</b>	To use an adjunct license with this device, choose the device name of the Cisco Unified IP Phone to associate with the client application.
<b>Allow Control of Device from CTI</b>	Always check this option in a virtual environment.
<b>Presence Group</b>	Choose <b>Standard Presence Group</b> .
<b>Device Security Profile</b>	Choose <b>Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile</b> .

Option	Description
<b>SIP Profile</b>	Choose <b>Standard SIP Profile</b> or another profile that was previously created. SIP profiles provide specific SIP information for the phone, such as registration and keepalive timers, media ports, and Do Not Disturb control.  <b>Important</b> If you choose <b>Secure Phone Profile</b> , do not specify the Certificate Authority Proxy Function (CAPF) authentication mode <b>By Null string</b> . Use of this setting with Cisco Jabber Softphone for VDI causes Jabber registration with Cisco Unified Communications Manager to fail.

**Step 5** Scroll down to the **Product Specific Configuration Layout** section, and set **Video Calling** to **Enabled**.

**Step 6** Select **Save**.

**Step 7** Select **Apply Config** if this button is available, and then confirm when prompted.

**Step 8** Select **Add a new DN** in the **Association Information** section that appears on the left side of the window.

**Step 9** Enter information for the directory number on the **Directory Number Configuration** window.

Option	Description
<b>Directory Number</b>	Enter the directory number (line) to assign to the device.
<b>Route Partition</b>	Enter the route partition. Partitions divide the route plan into logical subsets. These subsets include organization, location, and type of call.
<b>Display (Internal Caller ID)</b>	Enter the Caller ID. This entry is optional. The actual display depends on this entry and the configuration for the other party. For example, Cisco IP Phones display the Caller ID, but Cisco Jabber does not.
<b>Maximum Number of Calls</b>	Specify the maximum number of calls that can be presented to the application. This number includes all calls placed on hold plus the active call, regardless of which party initiated the calls.
<b>Busy Trigger</b>	Specify the number of calls (active and on hold). Incoming calls, above this limit receive a busy signal or are redirected to the Forward Busy Internal/External target (if the target is configured).

**Step 10** Select **Save**.

**Step 11** Select **Apply Config** if this button is available, and then confirm when prompted.

**Step 12** Scroll to the bottom of the **Directory Number Configuration** window, and then select **Associate End Users**.

**Step 13** In the **Find and List Users** window, use the search criteria to find the user who you want to associate with the directory number.

**Step 14** Check the box next to that username, and then select **Add Selected**.

The user is now associated with the DN.

**Step 15** In the **User Associated with Line** section of the window, select the username.

**Step 16** In the **End User Configuration** window, scroll down to the **Direct Number Associations** section.

**Step 17** From the **Primary Extension** drop-down list, choose the DN for the user.

**Step 18** In the **End User Configuration** window, under **Permissions Information**, select **Add to User Group** or **Add to Access Control Group**, depending on your version of Cisco Unified Communications Manager.

- Step 19** In the **Find and List User Groups** window, use the search criteria to find **Standard CCM End Users**.
- Step 20** Check the box next to **Standard CCM End Users**, and then select **Add Selected**.
- Step 21** In the **Find and List User Groups** window, use the search criteria to find **Standard CTI Enabled**.
- Step 22** Check the box next to **Standard CTI Enabled**, and then select **Add Selected**.
- Step 23** Select **Save**.

Cisco Unified Communications Manager reminds you that changes to line or directory number settings require a restart. However, you need only restart after you edit lines on Cisco Unified IP Phones that are running at the time of the modifications.

## Associate New Devices with a User



**Note** Perform this task in Cisco Unified Communications Manager.

### Procedure

- Step 1** From Cisco Unified Communications Manager Administration, choose **> User Management > End User**.
- Step 2** Search for the user in the **Find and List Users** window.
- Step 3** Select the user.
- Step 4** Select **Device Association** in the **Device Information** section.
- Step 5** Search for the devices that you require in the **User Device Association** window.
- Step 6** Select the devices that you require.
- For example, you can select a device whose type is Cisco Unified Client Services Framework, and a desk-phone device.
- Step 7** Select **Save Selected/Changes**.
- Step 8** Select **Back to User** from the menu in the **Related Links** navigation box at the top right of the window.
- Step 9** Select **Go**.
- Step 10** Verify that the devices are listed in the **Device Information** section in the **End User Configuration** window.

## Enable the CTI Protocol for Users

Enable the computer-telephony integration (CTI) protocol for each Cisco Jabber Softphone for VDI user.

### Procedure

- Step 1** In Cisco Unified Communications Manager Administration, click **User Management > End Users**.
- Step 2** Search for the user in the **Find and List Users** window.

- Step 3** Select the user.
- Step 4** In the **End User Configuration** window, scroll down to Permissions Information.
- Step 5** Click **Add to User Group**.
- Step 6** Select the following groups:
- Standard CCM End Users
  - Standard CTI Allow Control of All Devices
  - Standard CTI Enabled
- Step 7** Click **Save**.
- 

#### What to do next

Enable the Unified Communications Manager IM and Presence Service. See the documentation for your version of Cisco Unified Communications Manager.

## Configure Cisco Unified Communications Features for Users

For information about how to configure Cisco Unified Communications features for Cisco Jabber, see the deployment and installation guide for your release, available from <http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html>.

## Change a User Password

Use this procedure to change the password for a user only if LDAP Authentication is not enabled. If LDAP Authentication is enabled, the passwords are stored on the LDAP Server. For Cisco Unified Communications Manager 9.0 or later, this procedure applies only to passwords for users created locally.

#### Procedure

---

- Step 1** From Cisco Unified Communications Manager Administration, choose **Cisco Unified Communications Manager Administration > User Management > End User**.
- Step 2** Search for the user in the **Find and List Users** window.
- Step 3** Select the user.
- Step 4** In the **End User Configuration** window, in the **Password** field, enter a new password for the user.
- Step 5** In the **Confirm Password** field, enter the new password for the user again.
- Step 6** Select **Save**.
-





## CHAPTER 5

# Upgrade

---

- [Upgrade Workflow](#), on page 27
- [Upgrade Cisco Jabber for Windows](#), on page 28
- [Upgrade the Citrix Receiver or the VMware Client](#), on page 28
- [Change the Hosted Virtual Desktop Connection Type](#), on page 29

## 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)

The Cisco Jabber for Windows version must match your Cisco Jabber Softphone for VDI version. The Cisco JVDI Agent and Cisco JVDI Client versions must be the same.

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** 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** If Cisco Virtualization Experience Media Edition is installed, uninstall it.
- Step 5** Install the Cisco Jabber Softphone for VDI components on the thin clients and hosted virtual desktops.  
See [Install the Components Workflow, on page 12](#).
- 

## 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 Windows* for your release.



---

**Important** The Cisco Jabber for Windows version must match your Cisco Jabber Softphone for VDI version. The Cisco JVDI Agent and Cisco JVDI Client versions must be the same.

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** 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.
- 

## Upgrade the Citrix Receiver or the VMware Client

Perform this procedure to upgrade the Citrix Receiver or the VMware Horizon Client, with Cisco Jabber Softphone for VDI already installed. This procedure repairs Cisco JVDI Client.

### Procedure

---

- Step 1** Upgrade the Citrix Receiver or the VMware Horizon Client.  
See the documentation for your Citrix or VMware product.
- Step 2** Use one of the following methods to install Cisco JVDI Client:
- [Run the Microsoft Installer, on page 17](#)
  - [Use the Command Line, on page 17](#)



- [Use the Group Policy Editor, on page 18](#)

---

## Change the Hosted Virtual Desktop Connection Type

If you change the hosted virtual desktop connection type, you can use this procedure to repair Cisco Jabber Softphone for VDI.

You can change your connection type as follows:

- Citrix Receiver to VMware Horizon Client
- VMware Horizon Client to Citrix Receiver

### Procedure

---

- Step 1** Install the software for the new connection type, either Citrix Receiver or VMware Horizon Client.
- Step 2** Double click the CiscoJVDISetup.msi file.
- Step 3** To open the executable file, select **OK**.
- Step 4** If the Open File–Security Warning appears, select **Run**.
- Step 5** In the **Welcome** window, select **Next**.
- Step 6** In the **Program Maintenance** window, select **Modify** and then **Next**.
- Step 7** In the **Custom setup** window, select **Citrix Client Support** or **VMware Client Support** depending on which you installed and select **Next**.
- Step 8**
- Step 9** To proceed with modifying the installation, select **Install**.
- Note** During the modification of Cisco JVDI Client only components that were installed with the previous version are reinstalled.
- Step 10** To complete the installation, select **Finish**.
-





## CHAPTER 6

# Troubleshooting

- [Registry Keys, on page 31](#)
- [Verify That Cisco JVDI Client Is Running, on page 31](#)
- [Verify That Cisco JVDI Agent Is Installed, on page 32](#)
- [Confirm the Version of Cisco JVDI Client, on page 32](#)
- [Call Control Is Lost After a Network Failure, on page 32](#)
- [Call Is Lost After HVD Disconnection, on page 33](#)
- [Problem Reporting Tool, on page 33](#)

## Registry Keys

The Cisco JVDI Client installation program checks to ensure that either the Citrix Receiver or the VMware Horizon Client is already installed on the reused PC. In one of the following registry locations, the `InstallFolder` string-type registry key must be present:

- For Citrix, the installer searches in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Install\ICA Client` for the path to the Citrix installation.

**Example (from an x86 PC):** `[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Install\ICA Client] "InstallFolder"="C:\\Program Files\\Citrix\\ICA Client\\"`

- For VMware Horizon, the installer searches in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM` for the path to the VMware installation.

**Example (from an x64 PC):** `[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM] "ClientInstallPath"="C:\\Program Files\\VMware\\VMware View\\Client\\"`

## Verify That Cisco JVDI Client Is Running

Use Windows Task Manager to verify that Cisco JVDI Client is running.

In a Citrix environment, the Cisco Jabber Softphone for VDI processes start when the user signs in to their hosted virtual desktop (HVD). The processes stop when the session ends.

In a VMware environment, the Cisco Jabber Softphone for VDI processes start after the user signs in to their HVD and in to Cisco Jabber. The processes stop when the session ends.

#### Procedure

---

- Step 1** On the thin client desktop, right-click the taskbar and then select **Task Manager**.
  - Step 2** On the **Processes** tab, scroll down and look for the vxc.exe process.
- 

## 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 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.
- 

## Confirm the Version of Cisco JVDI Client

Cisco JVDI Client appears in the list of installed programs and features.

#### Procedure

---

- Step 1**
  - Step 2** On the thin client, open **Control Panel > Programs and Features**.
  - Step 3** Scroll down the list and locate Cisco JVDI Client.
  - Step 4** To confirm the version for Cisco JVDI Client, see the **Version** column.
- 

## 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 saves a problem report to the user's desktop, as a .zip file. 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. You can send the problem report to the Cisco Technical Assistance Center (TAC).

If a user experiences an error that does not crash the software, the user can run the PRT from the **Help** menu:

Cisco Jabber—**Help** > **Report a problem**

Users can generate a problem report from the Windows **Start** menu if Cisco Jabber is not running. You can access the tool from outside the application, from the Microsoft Windows **Start** menu.

Cisco Jabber—**Start** > **All Programs** > **Cisco Jabber** > **Cisco Jabber Problem Report**.



---

**Note** We recommend that users provide a description of the circumstances that lead up to the error. Users must accept the privacy agreement to run the PRT.

---

## 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.