Deployment and Installation Guide for Cisco Jabber Softphone for VDI—HP Thin Pro and Ubuntu Release 12.5

First Published: 2018-11-29

Last Modified: 2019-10-25

CONTENTS

CHAPTER 1

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 for HP Thin Pro and Ubuntu.

- Upgrading Cisco Jabber Softphone for VDI for HP Thin Pro and Ubuntu.

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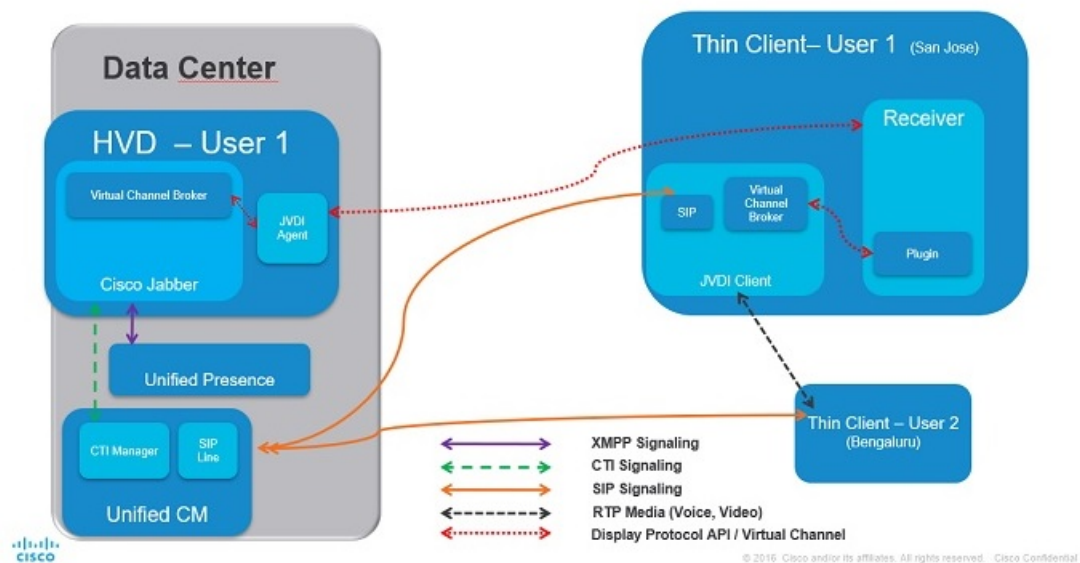
Cisco Jabber Softphone for VDI supports some audio and video accessories. For a complete listing of supported audio and video accessories, see *Unified Communications Endpoint and Client Accessories*, at http://www.cisco.com/c/en/us/products/unified-communications/uc_endpoints_accessories.html.

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

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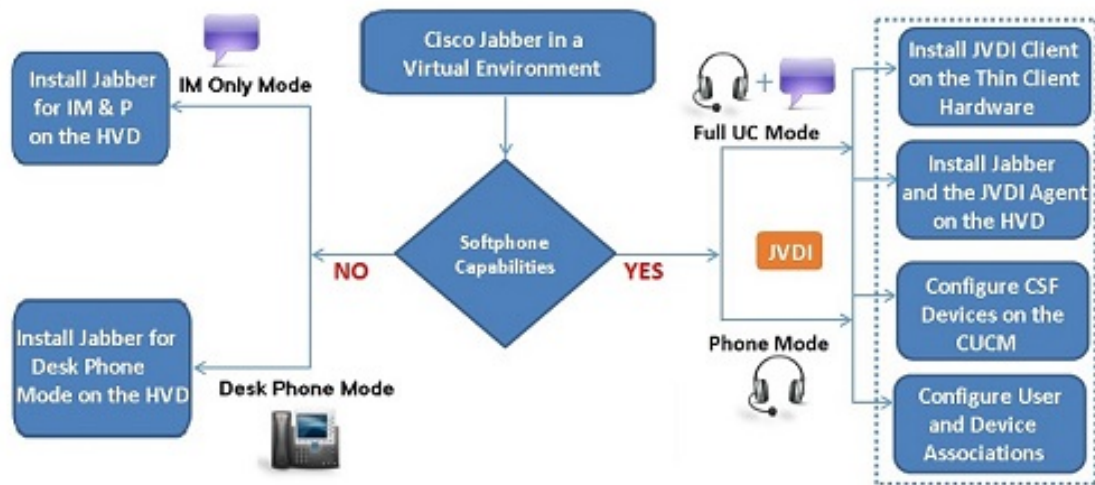
A Cisco Jabber Softphone for VDI deployment consists of the following components:

- Supported HP Thin Pro or Ubuntu thin clients.

  For more information about supported thin clients, see *Release Notes for Cisco Jabber Softphone for VDI for HP Thin Pro and Ubuntu*.

- 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 17.

- 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).

Requirements

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 and requirements listed in the table are supported.

Component	Requirements
HP Thin Pro thin clients—Hardware	The following client hardware is supported with HP Thin Pro 6.2: • HP t520 • HP t530 • HP t620 • HP t630 • HP t730 • HP mt21 The following client hardware is supported with HP Thin Pro 7: • HP t430 • HP t520 • HP t530 • HP t630 • HP t730 • HP mt21
HP ThinPro platform image	HP ThinPro 6.2: T7X62022 HP ThinPro 7: T7X70015 Support is limited for HP Thin Pro 7.
Ubuntu thin clients—Hardware	The following hardware is supported with Ubuntu 14.04 32b LTS: • Installed RAM 2 GB • Free Physical Memory 256 MB • Free Disk Space 256 MB • CPU: AMD G-T56N 1.65Ghz, or Intel Core2Duo T7500 2.2 GHz • USB 2.0 for USB camera and audio devices
Ubuntu	Ubuntu 14.04 i386 Ubuntu 16.04 i386 Support is limited for Ubuntu 16.04.

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 XenDesktop 6.5, 7.5, and later 7.x versions • Citrix XenApp 6.5, 7.5, and later 7.x versions—Published desktops only • VMware Horizon 6.0 (with View)—Published desktops only • VMware Horizon 6 version 6.1.0, 6.2.0, 7.0 and later 7.x versions—Published desktops only Citrix XenApp Published Application is not supported with Cisco Jabber Softphone for VDI for HP Thin Pro and Ubuntu.
Citrix Receiver or VMware Horizon Client [2] (Installed on the thin client)	**For HP Thin Pro 6.2.0** The HP Thin Pro image includes Citrix and VMware: • ICA Client: 13.5.0 or later (32 bit version required) • VMware 4.4.0 or later (32 bit version required) **For HP Thin Pro 7** • ICA Client is 13.10 (32 bit version required) • VMWare Horizon Client is 4.8 (32 bit version required) **For Ubuntu** • ICA Client V–13.3.0.344519 or later 13.3 versions • VMware Horizon View Client V–4.0.1-3698616
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 12.5(X) Cisco Jabber for Windows versions. For complete information about virtual environment compatibility, see the Jabber installation documentation for your release.

Component	Requirements
Cisco Unified Communications Manager	• Recommended CUCM Release 11.5(1)SU3 or later • Minimum CUCM Release 10.5
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 that include

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

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

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

(PCoIP only)

Considerations for Thin Clients

Thin clients must meet all system requirements. For more information, see *Release Notes for Cisco Jabber Softphone for VDI—HP Thin Pro and Ubuntu* for your release.

HP Thin Pro

HP Device Manager is the recommended deployment tool to deploy Virtualization Experience Media Edition to HP Thin Pro-based thin clients.

☞

Important Cisco does not support any management administrative method to deploy Cisco Jabber Softphone for VDI to HP Thin Pro-based thin clients. Support for adding and enabling add-ons is provided by HP, using HP Device Manager or other methods supported by HP.

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.	

CHAPTER **3**

Installation and Deployment

Deployment and Installation Workflow—HP Thin Pro

☞

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—HP Thin Pro and Ubuntu* for your release. Review 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 JVDI Agent.

Step 3   Set up and configure the thin clients.

Documentation for HP Thin Pro-based thin clients and for HP Thin Pro is available from the HP website. Ensure that the thin clients are ready for you to install the Cisco JVDI Client.

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 desktop. See Install the Components Workflow—HP Thin Pro, on page 13.

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

Deployment and Installation Workflow—Ubuntu

☞

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—HP Thin Pro and Ubuntu* 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 Jabber Softphone for VDI.

Step 3   Set up and configure the thin clients.

Have the hardware ready to install Cisco Jabber Softphone for VDI components.

Documentation for Ubuntu thin clients is available from the individual hardware vendors. Documentation for Ubuntu is available from the Ubuntu website.

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 desktop. See Install the Components Workflow—Ubuntu, on page 14.

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

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—HP Thin Pro

☞

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   Obtain the Cisco Jabber Softphone for VDI Debian (.deb) package and cisco-jvdi<xx.x.x>-pre-reqs.xar file from HP.

The <xx.x.x> variable in the filename is the Cisco Jabber Softphone for VDI release number. For assistance locating files on the HP site, contact HP support.

Have the Cisco Jabber Softphone for VDI files on hand and ready to install. If you plan to manually install Cisco JVDI Client on the thin clients, copy the files to a USB stick.

Step 2   Download the Cisco JVDI Agent, on page 16.

Have the Cisco JVDI Agent installation file on hand and ready to install on the hosted virtual desktop.

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

Step 4   On the thin client, install the Cisco Jabber Softphone for VDI files in the following order, either manually from a USB stick, or use HP Device Manager for mass deployments.

Order of installation:

    a.   Install cisco-jvdi12.0.x-pre-reqs-thinpro6.2.0-hp1d.xar.

    b.   Install the Cisco Jabber Softphone for VDI .deb package.

For more information about mass deployment, see the documentation for HP Device Manager 4.7, available from HP.

Step 5   On the HVD, uninstall any previously installed Cisco JVDI Agent.

Step 6   On the HVD, uninstall any previously installed Cisco Unified Communications clients, such as Cisco Jabber.

Step 7   On the HVD, install Cisco JVDI Agent.

Double-click the .msi file, and then follow the installation wizard steps.

Step 8   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.

Install the Components Workflow—Ubuntu

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   Obtain the Cisco Jabber Softphone for VDI deb package from the Ubuntu software center repository.

Have the Cisco Jabber Softphone for VDI deb package on hand and ready to install. You can place the file on a network share accessible from the thin clients, or copy it to a USB stick.

Step 2   Download the Cisco JVDI Agent, on page 16.

Have the Cisco JVDI Agent installation file on hand and ready to install on the hosted virtual desktop.

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

Step 4   On the thin client, use the terminal emulator to run the following command: **sudo apt-get update**, and then enter your password at the prompt.

Updates the list of repositories for the Ubuntu Software Center.

After the command finishes reading the package lists, you can close the terminal emulator.

Step 5   On the thin client, install the Cisco JVDI Client; enter your password at the authentication prompt.

When you double-click the Cisco Jabber Softphone for VDI deb package, the Ubuntu Software Center opens. After you click **Install**, the Ubuntu Software Center locates and installs the dependency libraries, and then installs the Cisco JVDI Client.

Step 6   On the HVD, uninstall any previously installed 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 Cisco JVDI Agent .msi and follow the installation wizard steps.

Step 9   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.

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 HP Thin Pro and Ubuntu**.

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 HP Thin Pro and Ubuntu**.

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

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

C H A P T E R 4

Configuration

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 18.

Step 2 Associate New Devices with a User, on page 20.

Step 3 Enable the CTI Protocol for Users, on page 20.

Step 4 Configure Cisco Unified Communications Features for Users, on page 21.

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
Device Name	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.
Description	Enter a descriptive name for the phone. For example, enter *Richard-phone-on-computer*.
Device Pool	Choose **Default** 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.
Phone Button Template	Choose **Standard Client Services Framework**. 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.
Owner User ID	To use an adjunct license with this device, choose the user ID from the list.
Primary Phone	To use an adjunct license with this device, choose the device name of the Cisco Unified IP Phone to associate with the client application.
Allow Control of Device from CTI	Always check this option in a virtual environment.
Presence Group	Choose **Standard Presence Group**.
Device Security Profile	Choose **Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile**.

Option	Description
SIP Profile	Choose **Standard SIP Profile** 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. **Important** If you choose **Secure Phone Profile**, do not specify the Certificate Authority Proxy Function (CAPF) authentication mode **By Null string**. 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
Directory Number	Enter the directory number (line) to assign to the device.
Route Partition	Enter the route partition. Partitions divide the route plan into logical subsets. These subsets include organization, location, and type of call.
Display (Internal Caller ID)	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.
Maximum Number of Calls	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.
Busy Trigger	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**.

C H A P T E R **5**

Upgrade

- Upgrade Workflow, on page 23
- Upgrade Cisco Jabber for Windows, on page 24

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

See the workflow for the corresponding platform: Install the Components Workflow—HP Thin Pro, on page 13 or Install the Components Workflow—Ubuntu, on page 14.

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 HP Thin Pro and Ubuntu* 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.

CHAPTER **6**

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 Version—HP Thin Pro

Procedure

Step 1   On the thin client, open the terminal console.
Step 2   Enter the following command: **lsb_release -a** .
Step 3   Look in the output for the HP Thin Pro version.

Example:
```
HP Thin Pro 5.2
```

Verify the Platform Version—Ubuntu

Procedure

Step 1	On the thin client, open **System Settings**.
Step 2	Select **Details**.

The version appears under the Ubuntu logo.

Example:

```
Ubuntu 14.04.x 32b LTS
```

Verify That the Cisco JVDI Client Is Installed

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

Procedure

Step 1	On the thin client, open the terminal console.
Step 2	Enter the following command: **dpkg -l	grep jvdi** .
Step 3	In the output, look for ii cisco-jvdi-client.

Example:

```
ii cisco-jvdi-client <xx.x.x.xxx> i386 Cisco JVDI Client
```

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

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.