Deployment and Installation Guide for Cisco Virtualization Experience Media Edition for Windows Release 11.5

First Published: December 17, 2015

Last Modified: December 17, 2015

CONTENTS

Cisco Virtualization Experience Media Edition Overview

Purpose of this Guide

This guide explains how to

- Install and configure Cisco Virtualization Experience Media Edition for Windows (VXME for Windows).
- Upgrade VXME for Windows.

About Cisco Virtualization Experience Media Edition

Cisco Virtualization Experience Media Edition (VXME) 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 VXME 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 VXME family of products are:

- Cisco Virtualization Experience Media Edition for SUSE Linux
- Cisco Virtualization Experience Media Edition for Windows
- Cisco Virtualization Experience Media Edition for Unicon eLux

For more information about Cisco VXME, visit http://www.cisco.com/e/en/us/products/collaboration-endpoints/virtualization-experience-media-edition/index.html.

Virtual Deployments

✎

Note In this deployment guide, the term *thin client* refers to reused PCs, or other supported client devices set up to provide access to hosted virtual desktops (HVD).

With Cisco Virtualization Experience Media Edition (Cisco VXME), thin client users can place and receive calls with their Cisco Unified Communications client (Cisco Jabber). Cisco VXME consists of the Cisco VXME Agent and the Cisco VXME Client. To reduce latency and to enhance media quality, VXME streams media between the endpoints without going through the hosted virtual desktops.

Cisco VXME also includes support for some accessories. For more information about supported accessories, see *Release Notes for Cisco Virtualization Experience Media Edition for Windows* for your release.

Use the following flowchart to determine whether you require VXME for your virtual environment.

Figure 1: Determine Whether You Need Cisco Virtualization Experience Media Edition for Windows
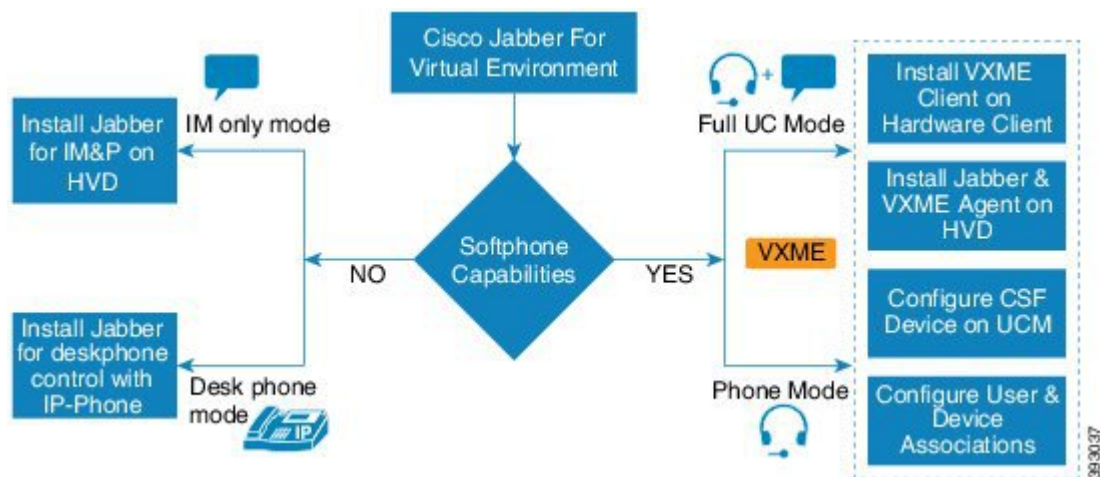
A Cisco VXME for Windows virtual deployment comprises the following components:

- Supported Windows thin clients

  For more information about the minimum requirements for supported thin clients, see the *Release Notes for Cisco Virtualization Experience Media Edition for Windows* for your release.

- Cisco VXME Client installed on the thin client

- Cisco VXME Agent installed on the HVD

- Cisco Jabber installed on the HVD

- Cisco Unified Communications Manager

Differences in the Virtual Environment

The user experience with Cisco Virtualization Experience Media Edition and a supported Cisco Unified Communications client is similar to the experience provided by a standard Cisco Unified Communications client 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.

- Users can choose to control their Cisco IP Phones or to use their computers to make and receive calls. The default phone selection is **Use my computer for calls**. After device selection, the Cisco Virtualization Experience Media Edition application starts the transfer of the phone configuration data for that user. For more information, see Configuration Files, on page 21.

- Users can manage their camera and audio devices by using the **Device Selector**, which is located in the Windows notification area. Users can also use the following tabs to manage their camera and audio devices from within their Cisco Unified Communications client:

  ◦ **File** > **Options** > **Audio**

  ◦ **File** > **Options** > **Video**

- If the thin client loses the connection to the network, the user is prompted to log back on to the HVD. If the connection failure occurs during a call, the call is lost. After reconnecting, the user can try to call the other party or send an IM. For the other party on the call, silence is the only indication that the call has dropped.

- By default, all calls send and receive video if both parties have video capability. Users can select their preference from the following options:

  ◦ **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 that the user places and receives. The default setting is **Always start calls with video**. Users can change this setting in **File** > **Options** > **Calls**.

  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 for the supported Cisco Unified Communications clients are different. For example, users cannot start Video Desktop Share (Binary Floor Control Protocol) from the call window. Video Desktop Share is supported only from the IM-chat window (Remote Desktop Protocol).

  Important   If Cisco Jabber is also installed on the thin clients, ensure that users exit Jabber before they sign in to their HVDs. If Cisco Jabber is running on the local desktop, and the user tries to sign in to Jabber on their HVD, Cisco VXME Client cannot register. Problems with accessories can also occur.

Filenames

The following table provides a list of the file types and names for this release.

File Type	Filename
Cisco Virtualization Experience Media Edition Client for Windows Release 11.5 (downloadable .zip file)	Cisco_VXME_Client_Windows-11.5.0.zip
VXME Client installer file (extracted from the downloaded .zip file)	CiscoVXMEClientSetup.msi
Cisco Virtualization Experience Media Edition Agent for Windows Release 11.5 (downloadable zip file)	Cisco_VXME_Agent-11.5.0.zip
VXME Agent installer file (extracted from the downloaded .zip file)	CiscoVXMEAgentSetup.msi

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.

Component	Requirements
Microsoft Windows-based thin client hardware	• Installed RAM 2 GB • Free Physical Memory 128 MB • Free Disk Space 256 MB • CPU Mobile AMD Sempron Processor 3600+, 2-GHz Intel Core 2 CPU, or T7400 2.16 GHz • DirectX 11 compatible GPU • USB 2.0 for USB camera and audio devices

Component	Requirements
Microsoft Windows-based thin client OS	• 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 • Windows Thin PC 32 bit **Note** Cisco Virtualization Experience Media Edition (VXME) for Windows does not require the Microsoft .NET Framework or any Java modules.

Windows Embedded Standard-based thin client hardware	• Installed RAM 2 GB
	
	• Free Physical Memory 128 MB
	
	• Free Disk Space 256 MB
	
	• CPU performance affects the maximum video resolution. With Windows Embedded Standard thin clients, the expected resolution depends on the CPU:
	
	  ◦ Up to 720p with quad-core AMD GX-420CA SOC 2 GHz or similar
	
	  ◦ Up to 240p with dual-core AMD G-T56N 1.65 GHz or similar
	
	  ◦ Audio-only support with dual-core VIA Eden X2 U4200 1 GHz or similar CPU
	
	  Note These hardware specifications are only guidelines for the expected resolutions. Other factors can affect video resolution.
	
	• DirectX 11 compatible GPU
	
	• USB 2.0 for USB camera and audio devices

Component	Requirements
Windows Embedded Standard-based thin client OS	• Windows Embedded Standard 7 32 bit • Windows Embedded Standard 7 64 bit • Windows Embedded Standard 8 64 bit **Note** Cisco Virtualization Experience Media Edition (VXME) for Windows does not require the Microsoft .NET Framework or any Java modules.
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	• Citrix XenDesktop 7.1, 7.5, or 7.6 • Citrix Xenapp 6.5, 7.5 or 7.6—Published desktops only • VMware Horizon View 5.3—Published desktops only • VMware Horizon 6.0 (with View)—Published desktops only • VMware Horizon 6 version 6.1.0—Published desktops only
Receiver or client (on the thin client)	Citrix Receiver (ICA) for Windows (Receiver Version and Installer Version): 4.3.100/14.3.100 VMware Horizon Client for Windows (32 or 64 bit): 3.5.2 **Important** Before you install Cisco VXME Client, install the Citrix Receiver or VMware Horizon Client on the thin client. If you upgrade your Citrix or VMware product, or change from a Citrix environment to a VMware environment, reinstall the Cisco VXME Client.

Component	Requirements
Cisco Unified Communications client on the hosted virtual desktop: • Cisco Jabber for Windows	Cisco Jabber for Windows 11.5 running on the hosted virtual desktop (HVD). Cisco VXME is compatible with all future 11.5(X) Cisco Jabber for Windows versions. For complete information about virtual environment compatibility, see the *Virtual Environments* section in the *Installation and Configuration Guide for Cisco Jabber for Windows* for your release.
Windows Server (Required for Citrix XenApp)	**Citrix Xenapp 6.5** • Microsoft Windows Server 2008 R2 • Windows Server 2008 R2 SP1 (Standard, Enterprise, Datacenter, and Foundation) **Citrix Xenapp 7.5 or 7.6** • Microsoft Windows Server 2008 R2 (Standard and Datacenter Editions) • Windows Server 2008 R2 SP1 (Standard, Enterprise, and Datacenter Editions) • Microsoft Windows Server 2012 (Standard and Datacenter Editions)
Cisco Unified Communications Manager	Cisco Unified Communications Manager version 9.x or later
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 the Jabra Direct to update the firmware. For more information visit: http://www.jabra.com.

Port Requirements

Note The Cisco VXME Client installer does not add firewall rules. You may need to disable the Windows Firewall on the endpoints, or add an exception to allow Cisco VXME Client.

The following table lists the ports or port ranges used by Cisco Virtualization Experience Media Edition for Windows.

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.

Important Cisco Virtualization Experience Media Edition uses the computer-telephony integration (CTI) protocol. Cisco Jabber for Windows on a hosted virtual desktop uses outbound TCP port 2748 to connect to the CTI gateway. The CTI gateway is the CTI Manager component of Cisco Unified Communications Manager.

For a complete listing of ports required by Cisco Jabber for Windows, see the planning guide for your release of Cisco Jabber.

Supported Codecs

Table 2: Supported Audio and Video Codecs

Audio Codec	Video Codec
G.722	H.264/AVC

Audio Codec	Video Codec
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.	

Installation

Deployment and Installation Workflow

Important Ensure that all component versions are supported and compatible. The Cisco Jabber for Windows version must match the Cisco Virtualization Experience Media Edition for Windows version. For details, see the "System Requirements" section of the release notes document for this release.

Procedure

	Command or Action	Purpose
Step 1	Read *Release Notes for Cisco Virtualization Experience Media Cisco Virtualization Experience Media Edition for Windows* for your release, 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	Read Requirements, on page 5.	Review the system requirements to confirm that all required hardware and software meet them.

	Command or Action	**Purpose**
		Failure to meet all requirements can result in a nonfunctional deployment.
Step 3	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 Virtualization Experience Media Edition (VXME).
Step 4	Set up and configure the thin clients. Documentation for thin clients is available from the original equipment manufacturer (OEM).	
Step 5	Configure the Network, on page 21. See also, Port Requirements, on page 8.	Configure important network settings.
Step 6	Set up Users on the Cisco Unified Communications Manager Workflow, on page 22.	• Add users and devices on the Cisco Unified Communications Manager. • Set up users on the Cisco Unified Communications Manager with Unified Communications features, such as Cisco Unified Communications Manager IM and Presence and WebEx integration.
Step 7	Install the Cisco VXME components on the thin clients and the hosted virtual desktop. See Install Cisco VXME Components Workflow, on page 12.	After you install all required software on the HVD, you can clone the HVD.
Step 8	Provide Links to the Documentation, on page 18.	Provide users with links to the documentation for their Unified Communications clients.

Related Topics

Set up the Hosted Virtual Desktops Workflow, on page 13

Install Cisco VXME Components Workflow

☞

Important The Cisco Jabber for Windows version must match the Cisco Virtualization Experience Media Edition for Windows version. See the "System Requirements" section of the release notes documentation for your Virtualization Experience Media Edition (VXME) release.

Procedure

	Command or Action	**Purpose**
Step 1	Download Cisco VXME Client, on page 14.	

	Command or Action	Purpose
Step 2	Download Cisco VXME Agent, on page 14.	
Step 3	On the thin client, install Cisco VXME Client. See Cisco VXME Client Installation, on page 14.	
Step 4	On the HVD, uninstall any previously installed Cisco VXME Agent and Cisco Unified Communications clients, such as Cisco Jabber, or Cisco UC Integration™ for Microsoft Lync.	
Step 5	On the HVD: Install Cisco VXME Agent, on page 18.	
Step 6	On the HVD, install Cisco Jabber.	

Related Topics

Set up the Hosted Virtual Desktops Workflow

☞

Important   Multiple registrations to the Cisco Unified Communications Manager are not supported. To help prevent multiple registrations, we recommend that you create only one hosted virtual desktop (HVD) for each user.

Procedure

	Command or Action	Purpose
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 VXME 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.

Command or Action	Purpose

Download Cisco VXME Client

Procedure

Step 1 Go to the following URL:
http://www.cisco.com/cisco/software/navigator.html

Step 2 Select **Products** > **Unified Communications** > **Unified Communications Applications** > **Messaging** > **Virtualization Experience Media Edition** > **Virtualization Experience Media Edition for Windows**.

Step 3 In the navigation tree, select your release.

Step 4 From the list, select the file for your release.

Step 5 Select **Download** or **Add to cart** and follow the prompts.

Download Cisco VXME Agent

Procedure

Step 1 Go to the following URL:
http://www.cisco.com/cisco/software/navigator.html

Step 2 Select **Products** > **Unified Communications** > **Unified Communications Applications** > **Messaging** > **Virtualization Experience Media Edition** > **Virtualization Experience Media Edition for Windows**.

Step 3 In the navigation tree, select your release.

Step 4 From the list, select the file for your release.

Step 5 Select **Download** or **Add to cart** and follow the prompts.

Cisco VXME Client Installation

Before you install Cisco VXME Client, 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 Virtualization Experience Media Edition for Windows* for your release.

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

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

Run the Microsoft Installer

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

Before You Begin

- 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 Virtualization Experience Media Edition for Windows* for your release.

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

Procedure

Step 1 Double-click the CiscoVXMEClientSetup.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

Use the command line to run the Microsoft Installer (MSI).

Before You Begin

- 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 Virtualization Experience Media Edition for Windows* for your release.

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

Procedure

Step 1   Open a command window.

Step 2   Enter the following command: **start /wait msiexec.exe /i <path to MSI>\CiscoVXMEClientSetup.msi /quiet**.
The **/quiet** switch specifies a silent installation.

Use the Group Policy Editor

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

> ☞
>
> **Important**   All computers or users to which you plan to deploy Cisco VXME Client must be in the same domain.

Before You Begin

- 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 Virtualization Experience Media Edition for Windows* for your release.

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

- 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 VXME 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 VXME 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 VXME 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**.

Related Topics

Set the Language Code

Use Microsoft Orca to set the language code if you plan to use Group Policy to deploy Cisco VXME 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 CiscoVXMEClientSetup.msi.

Step 4 Select CiscoVXMEClientSetup.msi, and then select **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 CiscoVXMEClientSetup.msi file.

Step 14 Specify a name for the modified file, and then select **Save**.

Related Topics

Install Cisco VXME Agent

Install Cisco VXME Agent on the hosted virtual desktops (HVD), before you install Cisco Jabber for Windows. Run the Microsoft Installer (MSI) on the hosted virtual desktop (HVD).

Before You Begin

Obtain the Cisco VXME Agent zip file, and extract the contents.

Procedure

Step 1 Double-click the CiscoVXMEAgentSetup.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**.

Provide Links to the Documentation

Create a Desktop Shortcut

Add a desktop shortcut to the user documentation. Users can click the shortcut to access the documentation and to get help.

Procedure

Step 1 On the Microsoft Windows desktop, right-click and point to **New**.

Step 2 Select **Shortcut**.

Step 3 Copy and paste the URL for the end-user documentation into the text box.
```
User Guides: http://www.cisco.com/en/US/products/ps12862/products_user_guide_list.html
```

Step 4 Select **Next**.

Step 5 Type a name for the shortcut.

Example:
Documentation/Help for Cisco VXME

Step 6 Select **Finish**.

Add a Link to the Citrix Landing Page

You can add a link to the Citrix landing page. Users can click the shortcut to access the documentation and to get help.

Note You must be a Desktop Delivery Controller (DDC) administrator.

Procedure

Step 1 Establish a Remote Desktop connection to the server running the Desktop Delivery Controller (DDC).

Step 2 In the navigation tree, under Access, select **Citrix Web Interface** > **XenApp Web Sites** > **Internal Site**.

Step 3 Under **Internal Site - Edit Settings**, select **Web Site Appearance**.

Step 4 In the **Customize Web Site Appearance - Internal Site** window, under **Options**, select **Content**.

Step 5 Select the language code (for example, English [en]), and then select **Edit**.

Step 6 In the **Edit Custom Text** window, check **Footer text (all screens)**.

Step 7 In the **Edit Custom Text** window, under Customize Footer Text, enter text to point the user to the online documentation.

Example:
Sample text
```
User Guides: http://www.cisco.com/en/US/products/ps12862/products_user_guide_list.html
```

Step 8 Select **Finish**, and then select **OK**.

Add a Link to the VMware Prelogin Banner

You can add a link to the VMware prelogin banner. Users can click the shortcut to access the documentation and to get help.

Note You must be a VMware Connection Server administrator.

Procedure

Step 1 Log in to the VMware Connection Server.

Step 2 Select **View Configuration - Global Settings**.

Step 3 Under the **General** section, select **Edit**.

Step 4 Check **Display a prelogin message**.

Step 5 Enter text to point the user to the online documentation URL.

Example:
Sample text
```
User Guides: http://www.cisco.com/en/US/products/ps12862/products_user_guide_list.html
```

Step 6 Select **OK**.

Configuration

-
-
-

Configure the Network

Related Topics

DHCP Pool Setup

If your network uses DHCP, specify the domain name in the DHCP pool. Without this setting, DHCP does not assign a domain to the thin clients. Therefore, the devices cannot register with the Cisco Unified Communications Manager, the client keypads are dimmed, and users cannot make calls.

Example:

```
ip dhcp pool Non-VXCM server
 network 10.2.209.0 255.255.255.0
 dns-server 10.2.25.11
 default-router 10.2.209.1
 domain-name rtpvxi.com
!
```

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 Virtualization Experience Media Edition 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

	Command or Action	Purpose
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 25.	
Step 4	Configure Cisco Unified Communications Features for Users, on page 26.	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

> **Note**   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, such as region, date and time group, 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**.
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.

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.

Option	Description
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 Virtualization Experience Media Edition (VXME) user.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **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 Select **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 Select **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

☞

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

- Cisco Virtualization Experience Media Edition (VXME)—Cisco VXME Client (thin client) and Cisco VXME Agent (HVD)
- Cisco Unified Communications software on the hosted virtual desktop (HVD)

Ensure that all component versions are supported and compatible. The Cisco Jabber for Windows version must match the Cisco Virtualization Experience Media Edition for Windows version. For details, see the "System Requirements" section of the release notes document for this release.

Procedure

	Command or Action	Purpose
Step 1	Read *Release Notes for Cisco Virtualization Experience Media Edition for Windows* for your release, 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	Read Requirements, on page 5.	Review the system requirements to confirm that all required hardware and software meet them.

	Command or Action	Purpose
		Failure to meet all requirements can result in a nonfunctional deployment.
Step 3	Install the VXME components on the thin clients and the hosted virtual desktop. See Install Cisco VXME Components Workflow, on page 12.	After you install all required software on the HVD, you can clone the HVD.
Step 4	Provide Links to the Documentation, on page 18.	Provide users with links to the documentation for their Unified Communications clients.

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 Virtualization Experience Media Edition for Windows* for your release.

Procedure

Step 1   Close Cisco Jabber and ensure that it is not running on the HVD.
   Important   If Cisco Jabber is running during the installation, exit and restart Cisco Jabber to enable virtualization.

Step 2   Install Cisco Jabber.

Upgrade the Citrix Receiver or the VMware Client

If you upgrade the Citrix Receiver or the VMware Horizon Client, and Cisco VXME Client is already installed, perform this procedure to repair Cisco VXME Client.

Before You Begin

Upgrade the Citrix Receiver or the VMware Horizon Client. See the documentation for your Citrix or VMware product.

Procedure

Step 1	Double click the file.
Step 2	To open the executable file, select **OK**.
Step 3	If the Open File - Security Warning appears, select **Run**.
Step 4	In the **Welcome** window, select **Next**.
Step 5	In the **Program Maintenance** window, select **Repair** and then **Next**.
Step 6	To proceed with repairing the installation, select **Install**.
Step 7	To complete the installation, select **Finish**.

Change the Hosted Virtual Desktop Connection Type

Use this procedure if Cisco VXME Client is already installed and you change the connection type as follows:

- Citrix Receiver to VMware Horizon Client

- VMware Horizon Client to Citrix Receiver

Before You Begin

Install the software for the new connection type, either Citrix Receiver or VMware Horizon Client.

Procedure

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

Troubleshooting

Registry Keys

The Cisco VXME 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 VXME Client Is Running

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

In a Citrix environment, the VXME 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 VXME 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 VXME Agent Is Installed

You can use the Windows Control Panel to verify that Cisco VXME 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 VXME Agent. The Cisco VXME Agent version appears in the **Versions** column.

Confirm the Version of VXME Client

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

Procedure

Step 1	On the thin client, open **Control Panel** > **Programs and Features**.
Step 2	Scroll down the list and locate Cisco VXME Client.
Step 3	Check the **Version** column to confirm the version for Cisco VXME Client.

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 Report

If users encounter a problem with Cisco Jabber, they can create a problem report. If Cisco Jabber encounters a problem and must close, the problem-reporting tool starts automatically, so that the user can create a problem report. Users can also generate a problem report from the Windows Start menu, if Cisco Jabber is not running.

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.

Important If there is a problem with the virtual channel, or if Cisco Jabber is not running, the problem report does not include logs from the thin client. For more information, see Virtual Channel Problem, on page 33.

Tip Advise users to include a memory dump if Cisco Jabber crashes.

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 instruct you to run the following executable: `C:\Program Files (x86)\Cisco Systems\Cisco VXME\CollectCiscoVXMEClientLogs.exe`. This executable gathers the logs from the thin client and saves them to the desktop as a CiscoVXMEClient-logs[timestamp].7z file. Users can still use the PRT to gather the logs from the hosted virtual desktop. Submit all logs gathered to TAC.