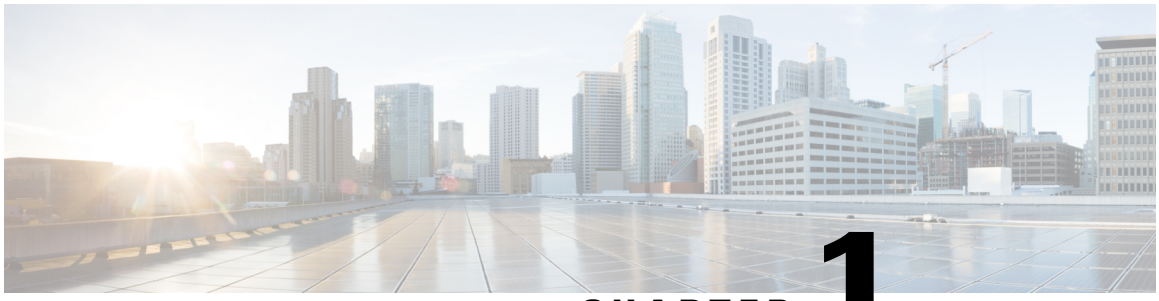
Deployment and Installation Guide for Cisco Virtualization Experience Media Engine for SUSE Linux Release 10.6

First Published: 2015-03-05

Last Modified: 2015-12-07

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

CONTENTS



CHAPTER 1

Cisco Virtualization Experience Media Engine Overview

Purpose of This Guide

The *Cisco Virtualization Experience Media Engine for SUSE Linux Deployment and Installation Guide* includes the following task-based information required to deploy and install Cisco Virtualization Experience Media Engine for SUSE Linux (VXME for SUSE Linux).

- Installation and configuration workflows and procedures that outline the processes to install and configure Cisco VXME for SUSE Linux
- Installation and configuration information for Cisco AnyConnect Secure Mobility Client in a Cisco VXME for SUSE Linux deployment
- Upgrade information for Cisco VXME for SUSE Linux

About Cisco Virtualization Experience Media Engine

Cisco Virtualization Experience Media Engine (VXME) extends the Cisco collaboration experience to virtual deployments. With a supported version of Cisco Jabber for Windows or Cisco UC Integration™ for Microsoft Lync, 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 Engine for SUSE Linux
- Cisco Virtualization Experience Media Engine for Windows

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

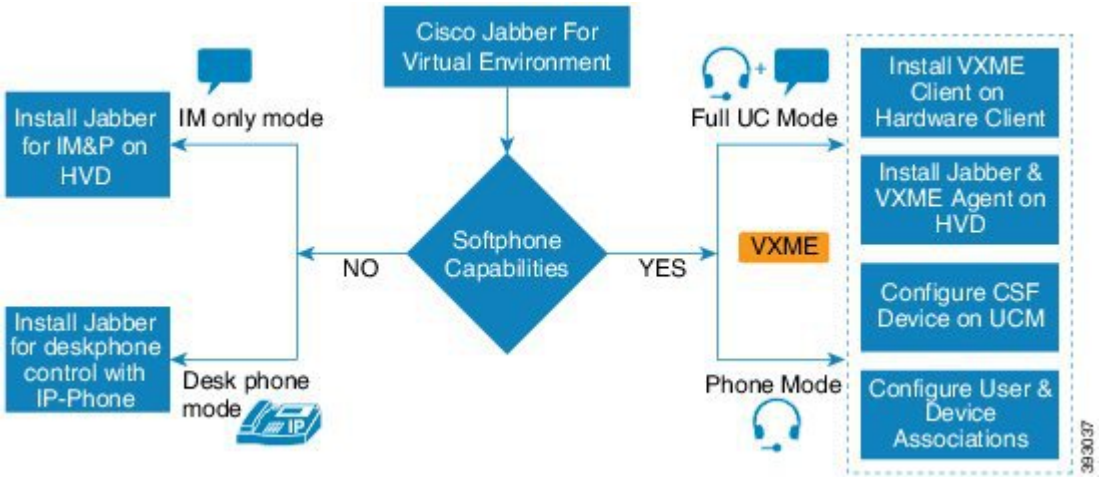
Virtual Deployments

With Cisco Virtualization Experience Media Engine (VXME), thin client users can place and receive calls with their Cisco Unified Communications application (Cisco Jabber or Cisco UC Integration™ for Microsoft Lync). Cisco Virtualization Experience Media Engine 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 Virtualization Experience Media Engine also supports some 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 VXME for your virtual environment.

Figure 1: Determine Whether You Need Cisco Virtualization Experience Media Engine for SUSE Linux



A Cisco VXME virtual deployment consists of the following components:

- Supported SUSE Linux thin clients

  For more information about supported thin clients, see *Release Notes for Cisco Virtualization Experience Media Engine for SUSE Linux*.

- Cisco VXME Client installed on the thin client
- Windows hosted virtual desktops (HVD), in a data center
- Cisco Jabber or Cisco UC Integration™ for Microsoft Lync installed on the HVD
- Cisco VXME Agent installed on the HVD
- Cisco Unified Communications Manager

Considerations for Thin Clients

SUSE Linux thin clients must meet all system requirements including a compatible base image version. For more information, see *Release Notes for Cisco Virtualization Experience Media Engine for SUSE Linux* for your release.

Wyse Device Manager 5.0 is the recommended deployment tool to deploy VXME to Dell Wyse thin clients.

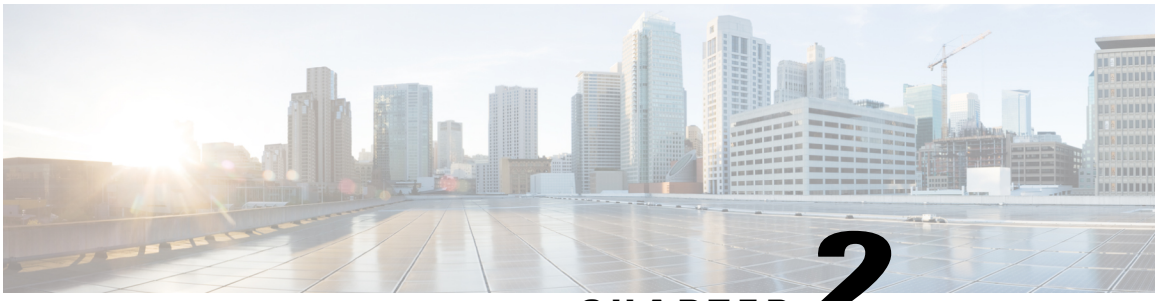
Important Cisco does not support any management administrative method to deploy VXME to Dell Wyse thin clients. Support for adding and enabling add-ons is provided by Dell Wyse, using Wyse Device Manager or other methods supported by Dell Wyse.

File Names

The following table lists the file types and names for this release.

File Type	File Name
Cisco Virtualization Experience Media Engine Client for SUSE Linux SP2 (downloadable .zip file)	Cisco_VXME_Client-10.6.0_SP2.zip
SP2 VXME .rpm file (extracted from zip file)	cisco_vxme_client-10.6.0-221.sletc11sp2.rpm
SP2 VXME Prerequisites .rpm file (extracted from zip file)	vxme-pre-reqs-10.6.0-23.sletc11sp2.rpm
Cisco Virtualization Experience Media Engine for SUSE Linux SP3 (downloadable .zip file)	Cisco_VXME_Client-10.6.0_SP3.zip
SP3 VXME .rpm file (extracted from zip file)	cisco_vxme_client-10.6.0-221.sletc11sp3.rpm
SP3 VXME Prerequisites .rpm file (extracted from zip file)	vxme-pre-reqs-10.6.0-23.sletc11sp3.rpm
Cisco Virtualization Experience Media Engine Agent for SUSE Linux Release 10.6 (downloadable zip file)	Cisco_VXME_Agent-10.6.0.zip
VXME Agent installer file (extracted from zip file)	CiscoVXMEAgentSetup.msi
Cisco AnyConnect for SUSE Linux SP2 (downloadable zip file)	Anyconnect_bundle-3.1.06073-69_SP2.zip
SP2 Cisco AnyConnect .rpm file (extracted from zip file)	anyconnect_bundle-3.1.06073-69.sletc11sp2sd.rpm
Cisco AnyConnect for SUSE Linux SP3 (downloadable zip file)	Anyconnect_bundle-3.1.06073-69_SP3.zip

File Type	File Name
SP3 Cisco AnyConnect .rpm file (extracted from zip file)	anyconnect_bundle-3.1.06073-69.sletc11sp3.rpm



CHAPTER 2

Deployment and Installation Workflows

New Deployment and Installation Workflow

Important You must ensure that all component versions are supported and compatible. The Cisco Jabber for Windows or Cisco UC Integration for Microsoft Lync version must match the Cisco Virtualization Experience Media Engine for SUSE Linux 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 Engine for SUSE Linux* for your release, available from http://www.cisco.com/c/en/us/support/collaboration-endpoints/virtualization-experience-media-engine/products-release-notes-list.html.	• Review the system requirements to confirm that all required hardware and software meets them. • Review the important notes for information about limitations or restrictions that may affect your deployment.
Step 2	Set up the Hosted Virtual Desktops, on page 9	
Step 3	Set up and configure the thin clients. Optional: See Enable AutoLogin, on page 24. Documentation for Dell Wyse thin clients is available from http:/ dell.com/wyse.	Deploy the base image to the thin clients and perform any other configuration required for your deployment.
Step 4	Set up Users on the Cisco Unified Communications Manager, on page 11	• Add users and devices on the Cisco Unified Communications Manager.

	Command or Action	Purpose
		• Set up users on the Cisco Unified Communications Manager with Cisco Unified Communications features, such as Cisco Unified Communications Manager IM and Presence and WebEx integration.
Step 5	Install Cisco Virtualization Experience Media Engine, on page 17	If your users do not require VPN access, you can skip the optional steps to install Cisco AnyConnect.
Step 6	Open Required Ports in Firewalls, on page 26.	
Step 7	Provide Links to the Documentation, on page 27	Provide users with links to the documentation for their Unified Communications clients.

Upgrade Workflow

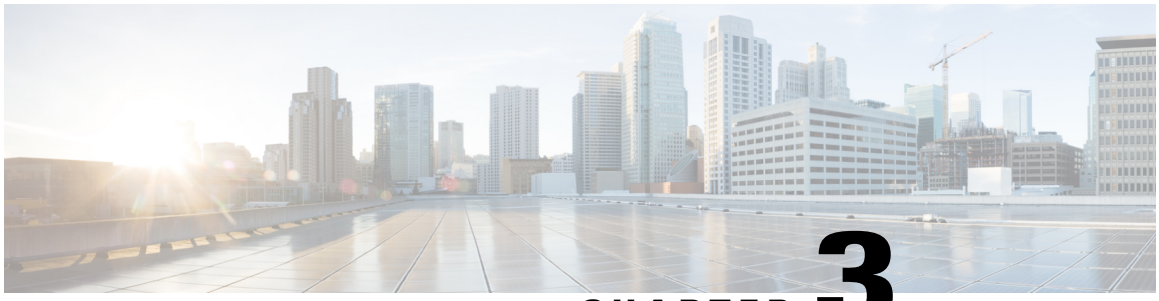
Important You must upgrade the platform image on the thin client, Cisco Virtualization Experience Media Engine, and the Cisco Unified Communications software on the hosted virtual desktop (HVD), for the Unified Communications features to work.

You must ensure that all component versions are supported and compatible. The Cisco Jabber for Windows or Cisco UC Integration for Microsoft Lync version must match the Cisco Virtualization Experience Media Engine for SUSE Linux 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 Engine for SUSE Linux* for your release, available from http://www.cisco.com/c/en/us/support/collaboration-endpoints/virtualization-experience-media-engine/products-release-notes-list.html.	• Review the system requirements to confirm that all required hardware and software meets them. • Review the important notes for information about limitations or restrictions that may affect your deployment.
Step 2	Upgrade the base image on the thin clients. Documentation for Dell Wyse thin clients is available from http:/ dell.com/wyse.	

	Command or Action	Purpose
Step 3	Install Cisco Virtualization Experience Media Engine, on page 17	If your users do not require VPN access, you can skip the optional steps to install Cisco AnyConnect.
Step 4	Provide Links to the Documentation, on page 27	Provide users with links to the documentation for their Unified Communications clients.



CHAPTER 3

Set up the Hosted Virtual Desktops

Build the Microsoft Windows HVD Image

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

Step 1 Log into 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.

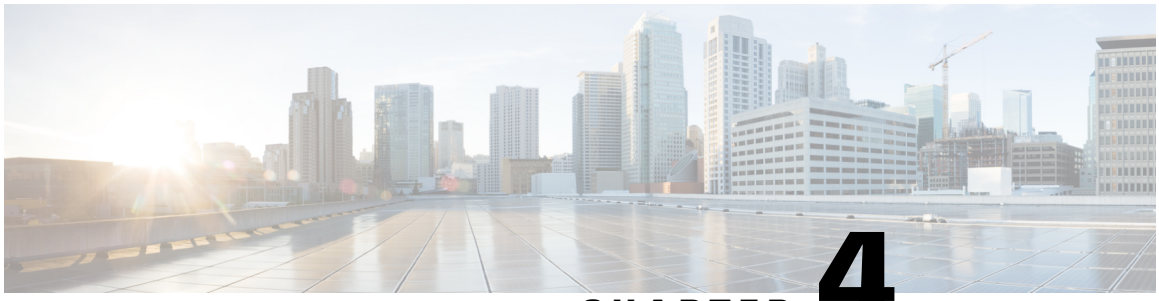
Step 3 Set up Citrix or VMware access to the HVDs.

Step 4 Install Cisco VXME Agent on the HVD—only if you are installing Cisco Jabber for Windows.
The Cisco UC Integration for Microsoft Lync installer includes Cisco VXME Agent. If you are installing Cisco UC Integration for Microsoft Lync, you can skip this step.

Step 5 Install Cisco Jabber or Cisco UC Integration for Microsoft Lync 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

See the administration guide for your release: http://www.cisco.com/c/en/us/support/unified-communications/uc-integration-tm-microsoft-lync/products-installation-guides-list.html

Step 6 Clone the HVD image.
For best practices for cloning Microsoft Windows HVD images, consult Microsoft.



CHAPTER 4

Set up Users on the Cisco Unified Communications Manager

Create a CSF Device and a Directory Number for Each User

Note Use the same Cisco Unified Client Services Framework (CSF) devices type for the virtual environment as you do for a nonvirtual environment. We recommend that you create only one CSF device for each virtual user. If multiple devices exist for a virtual user, Cisco Virtualization Experience Media Engine 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 Client 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.

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.

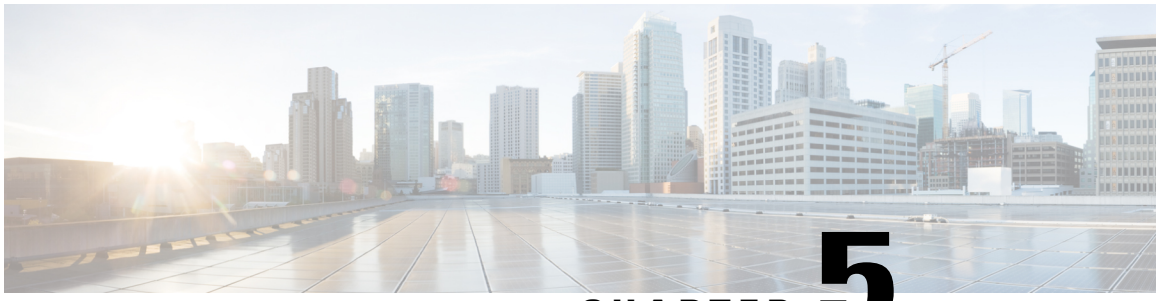
Step 5 In the **Confirm Password** field, enter the new password for the user again.

Step 6 Select **Save**.

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.
- Cisco UC Integration™ for Microsoft Lync: see the administration guide for your release, available from http://www.cisco.com/c/en/us/support/unified-communications/uc-integration-tm-microsoft-lync/products-installation-guides-list.html.



CHAPTER 5

Install Cisco Virtualization Experience Media Engine

Install Cisco VXME Components Workflow

Important The Cisco Jabber for Windows or Cisco UC Integration for Microsoft Lync version must match the Cisco Virtualization Experience Media Engine for SUSE Linux version. See the "System Requirements" section of the release notes documentation for your Virtualization Experience Media Engine release.

Procedure

	Command or Action	Purpose
Step 1	Download the Cisco VXME Client Add-on, on page 18	
Step 2	Download the Cisco VXME Agent, on page 18	
Step 3	(Optional)Download the Cisco AnyConnect Add-on, on page 19	Only perform this step if users require VPN connectivity.
Step 4	On the thin client, install the Cisco Virtualization Experience Media Engine (VXME) prerequisite add-on.	

	Command or Action	Purpose
Step 5	On the thin client install the Cisco Virtualization Experience Media Engine (VXME) add-on. See Create a Dell Wyse Device Manager Package, on page 19.	You can deploy Cisco AnyConnect at the same time.
Step 6	On the HVD, uninstall any previously installed versions of Cisco VXME Agent (formerly Cisco VXME Utilities) and Cisco Unified Communications clients, such as Cisco Jabber, Cisco UC Integration for Microsoft Lync, or Cisco Unified Personal Communicator.	
Step 7	On the HVD, install Cisco VXME Agent.	
Step 8	On the HVD, install Cisco Jabber or Cisco UC Integration for Microsoft Lync.	

Related Topics

File Names, on page 3

Download the Cisco VXME Client Add-on

Note The CiscoVXMEClient.zip file includes a prerequisite add-on, which you must install on the thin client, before you install the Cisco VXME Client add-on.

Procedure

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

Step 2 Choose **Products** > **Unified Communications** > **Unified Communications Applications** > **Messaging** > **Virtualization Experience Media Engine** > **Virtualization Experience Media Engine for SUSE Linux**.

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

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

Download the Cisco VXME Agent

Install Cisco VXME Agent on the hosted virtual desktops (HVD), before you install Cisco Jabber for Windows. If you plan to install Cisco UC Integration™ for Microsoft Lync, do not perform this procedure. Cisco UC Integration™ for Microsoft Lync includes Cisco VXME Agent.

Procedure

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

Step 2 Choose **Products** > **Unified Communications** > **Unified Communications Applications** > **Messaging** > **Virtualization Experience Media Engine** > **Virtualization Experience Media Engine for SUSE Linux**.

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

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

Download the Cisco AnyConnect Add-on

If users require VPN connectivity, download the Cisco AnyConnect add-on.

Procedure

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

Step 2 Choose **Products** > **Unified Communications** > **Unified Communications Applications** > **Messaging** > **Cisco Virtualization Experience Media Engine** > **Cisco Virtualization Experience Media Engine for SUSE Linux**.

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

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

Related Topics

File Names, on page 3

Create a Dell Wyse Device Manager Package

Wyse Device Manager is the recommended deployment tool to deploy the Cisco Virtualization Experience Media Engine add-on to the thin clients. See the Dell Wyse documentation for supported versions. You can also use this procedure if the thin clients are already running the required base image and you want to deploy an add-on.

Follow the optional steps in this procedure to deploy Cisco AnyConnect with the Cisco Virtualization Experience Media Engine add-on. In the procedure examples, <version> means <[Release Number]-[Build Number]-[Platform (SP2/SP3)].

Before You Begin

- Ensure that the thin clients are running the required firmware build; see *Release Notes for Cisco Virtualization Experience Media Engine for SUSE Linux* for your release. If necessary, contact Dell Wyse to get a compatible image.
- Obtain all of the required installation files: VXME, and if required, the optional AnyConnect VPN.
- Ensure that the thin clients are checked-in to Dell Wyse Device Manager (WDM). The devices should appear green in WDM.

Procedure

Step 1 On the server, on which you have WDM installed, extract the add-on files to a local folder.
The extracted add-on folder structure appears as follows:

```
~/<local folder>/addons/vxme-pre-reqs-<version>.rpm
~/<local folder>/addons/cisco_vxme_client-<version>.rpm
~/<local folder>/addons/directory
```

Step 2 (Optional) To deploy Cisco AnyConnect with Virtualization Experience Media Engine, extract anyconnect_bundle.<version>.zip.

Step 3 Copy vxme-pre-reqs-<version>.rpm and vxme-<version>.rpm to ~/CiscoVXME/CiscoVXME_x.x, where x.x is your release number.
The folder structure is as follows:

```
~/CiscoVXME/CiscoVXME_x.x/install-sletc-addons.sh
~/CiscoVXME/CiscoVXME_x.x/update-addons-list
~/CiscoVXME/CiscoVXME_x.x/vxme-pre-reqs-<version>.rpm
~/CiscoVXME/CiscoVXME_x.x/cisco_vxme_client-<version>.rpm
~/CiscoVXME/CiscoVXME_x.x.rsp
```

Step 4 (Optional) To deploy Cisco AnyConnect with Virtualization Experience Media Engine, copy the anyconnect_bundle<version>.rpm file to ~/CiscoVXME/CiscoVXME_x.x where x.x is your release number.

Step 5 (Optional) To deploy Cisco AnyConnect with Virtualization Experience Media Engine, add the following line to update-addons-list: UPDATE_ADDONS_LIST+=" anyconnect_bundle-<version>.rpm"

```
UPDATE_ADDONS_LIST+=" anyconnect_bundle-<version>.rpm"
```

Step 6 In the navigation pane of the Administrator Console, right-click **Package Manager** and then choose **New** > **Package**.

Step 7 In the **Package Wizard** window, select **Register a Package from a Script File (.RSP)**, and then select **Next**.

Step 8 Enter the path to the CiscoVXME_x.x.rsp file (where x.x is your release), and then select **Next**.

Tip You can select **Browse** to find and choose the file.

Step 9 In the Software Package Information dialog, check **Active**, and then select **Next**.
This step makes the WDM package active for distribution.

Step 10 To create and register the WDM package, select **Next**.

Step 11 Select **Finish**.
WDM copies the package to the Master Repository, where it appears under the appropriate category. The package is ready for distribution.

What to Do Next

Use the Default Device Configuration (DDC) method to upgrade the thin client.

For information about additional configuration required to enable Cisco AnyConnect VPN connections, see Cisco AnyConnect Secure Mobility Client, on page 31.

Related Topics

File Names, on page 3

Folder Structure

Note All package names, filenames (including .rsp and .ini files), and folders must be lower-case.

For example, assuming <packagename>.rsp is the RSP file, the folder structure required to register the package is as follows:

Folder	Description
~\<packagename>.rsp	The unique RSP file, located in the same folder as the matching root package folder.
~\<packagename>\	The root package folder. It stores the wlx folder and the add-ons folder. It also stores the following files, which are used for imaging and updating devices: • Latest-image.raw • Latest-image.raw.info
~\<packagename>\wlx	The main INI configuration folder. It stores the following: • wlx.ini file and $MAC.ini file • bitmap folder • certs folder • ini folder
~\<packagename>\wlx\bitmap	The folder where you can place custom images you plan to use.
~\<packagename>\wlx\certs	The folder where you can place the CA certificates that can be imported to a thin client. **Note** Use the Certs and ImportCerts INI parameters in the wlx.ini file to import the certificates to thin clients.
~ \<packagename>\wlx\ini	The folder where you can place the {username}.ini files.

Folder	Description
~\<packagename>\addons	The folder where you can place the add-ons you want to use. It also stores the folder file and the *.rpm packages available to be installed on the thin client. The folder file should list all available add-ons. The folder file is required in the add-ons folder to guarantee that add-ons are properly located.

Note If a folder does not contain a required file for the package, the folder can be omitted from the package folder structure. For example, if the package contains no graphics, the \wlx\bitmap folder is not required.

After you register the package, the thin client management program stores the package files in the software repository under c:\inetpub\ftproot\Rapport\<packagename>.

Caution Do not attempt to modify a registered package located in the Rapport folder. To modify a package, create and register a new package that includes the required changes.

Scripts

You use the following scripts when you create a Dell Wyse Device Manager package.

Note The examples for each script use variables for the filenames, which are different for each release.

install-sletc-addons.sh

```
#!/bin/bash
source /tmp/update-addons-list
WYSE_INIT_ADDON_UPDATE=/etc/wyseinit_factory_reset
NEED_REBOOT=no
for A in ${UPDATE_ADDONS_LIST} ; do
if [ -e /tmp/${A} ] ; then
/usr/sbin/addon-install /tmp/${A}
# Find WYSE_INIT addon among the list of
specified addons
WYSE_INIT=${A:0:9}
if [ "$WYSE_INIT" = "wyse_init" ] ; then
/bin/touch $WYSE_INIT_ADDON_UPDATE
/bin/sync
NEED_REBOOT=yes
fi
fi
done
sync
# WYSE_INIT addon needs reboot
if [ "$NEED_REBOOT" == "yes" ] ; then
/sbin/init 6
Fi
```

update-addons-list

```
# Quick guide
# Copy all the add-ons needs to be installed in to this directory
```

```
~install-sletc-addons/install-sletc-addons/
# Specify list of add-ons to be installed/updated preferably order
in which you wish to install as explained below
#
# Do not modify below line
UPDATE_ADDONS_LIST=
# Specify each add-on full name in separate line, with leading one
space enclosed inside quotes, as shown in below example
# Example:-
# Lets say you want to install following two add-ons
# abcd-xyz-1.1.1.sletc11sp3.rpm and aaaa-xxxx-2.2.2.sletc11sp3.rpm
# Specifiy these two add-ons as below
# UPDATE_ADDONS_LIST+=" abcd-xyz-1.1.1.sletc11sp3.rpm"
# UPDATE_ADDONS_LIST+=" aaaa-xxxx-2.2.2.sletc11sp3.rpm"
#
UPDATE_ADDONS_LIST+=" abcd-xyz-1.1.1.sletc11sp3.rpm"
UPDATE_ADDONS_LIST+=" aaaa-xxxx-2.2.2.sletc11sp3.rpm"
```

CiscoVXME_x.x.rsp

Note This RSP script is provided as an example; you may need to specify different parameters depending on your environment. For details about how to create RSP files, see the administration guide for your thin client management software.

```
[Version]
Number=CiscoVXME_x.x
Description=Cisco Virtualization Experience Media Cisco Virtualization Experience Media
Engine
OS=SLX
Category=Cisco
USE_Pxe=NO
[Script]
CO "SLX"
LU
SF "<regroot>/*" "/tmp/"
EX "dos2unix /tmp/update-addons-list"
EX "dos2unix /tmp/install-sletc-addons.sh"
EX "/bin/bash /tmp/install-sletc-addons.sh &"
EL
```

Schedule an Update or a Push

There are different methods that you can use to schedule an update or push a package to the thin clients. For more information about these methods, see the documentation for the thin clients and for the thin client management tool.

Important We strongly recommend that you use the Default Device Configuration (DDC) method to push packages to the thin clients. The Drag-and-Drop method may function, but it is only recommended in small environments or for test purposes. Drag-and-Drop does not function at all for thin clients behind a Cisco AnyConnect VPN.

Enable AutoLogin

AutoLogin is disabled by default (AutoLogin=no). If enabled, the AutoLogin feature automatically logs the user in as the Default User, unless you cancel the AutoLogin before the CountDown interval expires. You can cancel AutoLogin by pressing the ESC key. This feature is useful for kiosk environments.

To enable the AutoLogin feature, change the AutoLogin parameter in the wlx.ini file to AutoLogin=yes. For more information about how to edit the wlx.ini file, or about the AutoLogin or Countdown parameters, see the INI reference guide for the thin client.

User Mode

If you enable AutoLogin, the thin client automatically boots and signs in as the default user (*thinuser mode*), which restricts user access.

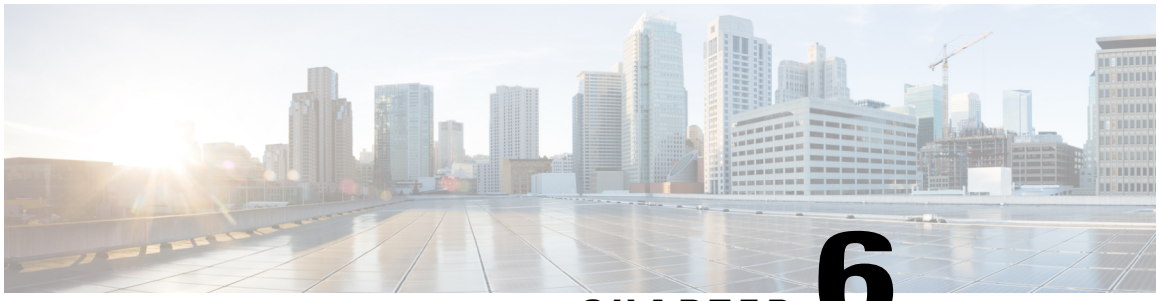
In thinuser mode, the FireFox shortcut does not appear in the Start menu and xterm does not appear in the Application Browser. Users can access System Information by clicking an icon in the notification area of the task bar. To set up access to FireFox, edit the wlx INI file to specify the required parameters.

Example:

```
CONNECT=BROWSER \
Description="Cisco Home Page" \
URL=http://www.cisco.com \
Resolution=FullScreen \
Mode=Normal
```

After application of the new wlx INI file, an icon for FireFox appears on the thin client desktop. For more information about how to edit the wlx INI file, see the INI reference documentation for your device.

Note Dell Wyse thin client users do not have access to the WDM icon in thinuser mode. This behavior is expected because users do not need this access. If you require access WDM to troubleshoot device check-in issues, you can open the application from xterm. For more information about how to manage Dell Wyse thin clients, see the administrator guides for your base image version.



CHAPTER 6

Configure the Network

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
!
```

Domain Name Resolution

If thin clients reside in a different domain than the Cisco Unified Communications Manager, the DNS server may be unable to resolve the domain name for the Cisco Unified Communications Manager.

To resolve this issue, edit the /etc/hosts file on the thin client. To save the change permanently, edit the wlx.ini file. Add the AddtoEtcHosts= parameter, and specify the IP, FQDN, and aliases for each Cisco Unified Communications Manager in the cluster. This parameter adds entries to the /etc/hosts file, where aliases are an optional space-separated list of hostnames.

For more information about how to edit the wlx.ini file, see the INI reference guide for the thin client.

Syntax

AddtoEtcHosts= "ip1 FQDN1 aliases1;ip2 FQDN2 aliases2"

Sample wlx.ini File

```
;************************************************************
;* General 1 *
;************************************************************
AddtoEtcHosts="10.200.252.2 CUCM123.cisco.com CUCM123;10.100.7.117 CUCM456.cisco.com CUCM456"

IniFileSource=cache

;************************************************************
;*                          Connections                     *
;************************************************************

Browser.Homepage=http://gwydlvm120

CONNECT=BROWSER \
Description="Citrix-HVD" \
URL=www.cisco.com \
AutoConnect=yes \
Sound=yes \
mode=normal
```

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.

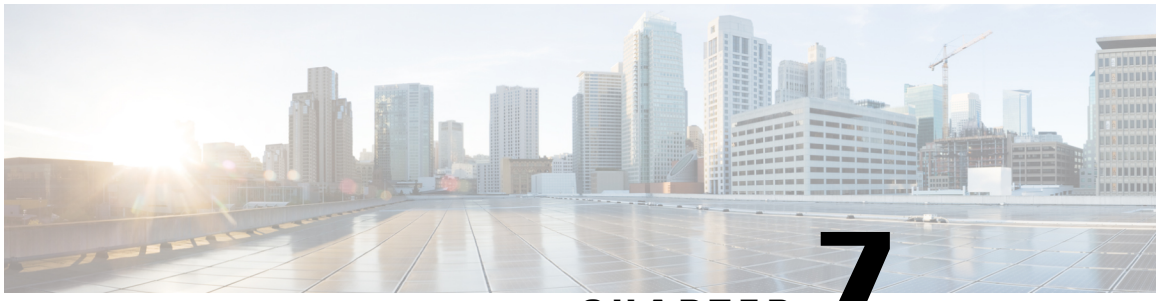
When users sign in to their supported Cisco Unified Communications application, Cisco Virtualization Experience Media Engine starts the download of the associated CNF file to the thin client. To ensure the successful transfer of the file, open the relevant ports in all firewall applications to allow 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.

Open Required Ports in Firewalls

If the network includes firewalls, you may have to open ports. See *Ports Reference Guide for Cisco Virtualization Experience Media Engine Release 9.0*, available from:

http://www.cisco.com/en/US/docs/voice_ip_comm/vxc/english/vxme/9.x_ports_ref/b_vxme_ports-reference-guide.html



CHAPTER 7

Provide Links to the Documentation

Create a Desktop Shortcut

Add a desktop shortcut to the user documentation, for users who do not connect to their hosted virtual desktops in kiosk mode. Users can click the shortcut to access the documentation and to get help.

Procedure

Step 1 Open the wlx.ini file for editing, by using your thin client management software (Dell Wyse Device Manager). Depending on your deployment, you may need to edit this file locally, in which case the filename is wnos.ini.

Step 2 Add the following lines:

```
CONNECT=BROWSER \
Description="Help Getting Started" \
URL=http://www.cisco.com/en/US/products/ps12862/products_user_guide_list.html \
Resolution=FullScreen \
Mode=Normal
```

Step 3 Optional. Add the icon parameter to change the shortcut icon.

```
Icon=image file
```

The image file must be located in the wlx/bitmap folder on the server. If you do not specify an image file, the default icon appears. Supported file types are PNG, JPEG, and GIF, and XPM for backward compatibility.

Step 4 Save the changes to the wlx.ini file.

Add a Link to the Citrix Landing Page

You can add a link to the Citrix landing page. This link is important for Citrix connections that operate in kiosk mode. In kiosk mode, the users have no access to the thin client desktop.

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. This link is important for VMware connections that operate in kiosk mode. In kiosk mode, the users have no access to the thin client desktop.

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**.

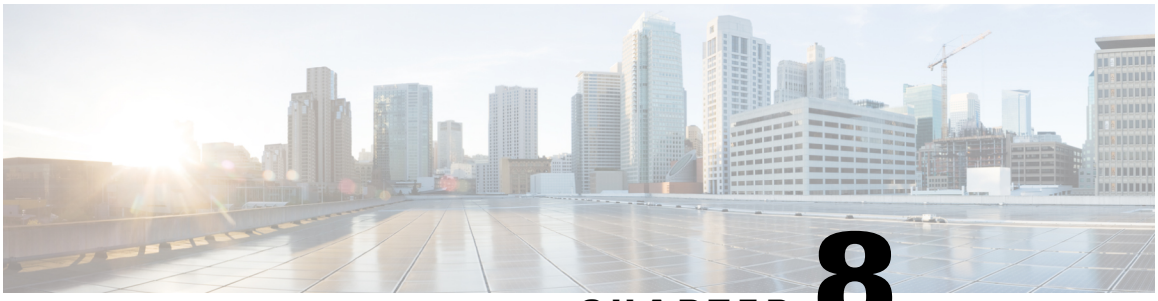
Step 4 Check **Display a prelogin message**.

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**.



CHAPTER 8

Cisco AnyConnect Secure Mobility Client

Cisco AnyConnect Feature Support

Cisco Virtualization Experience Media Engine supports Cisco AnyConnect Secure Mobility Client, Release 3.1. The Cisco AnyConnect Secure Mobility client provides remote users with secure VPN connections to the Cisco 5500 Series Adaptive Security Appliance (ASA). Cisco AnyConnect Secure Mobility client supports Cisco ASA version 8.0(4) or later and the Adaptive Security Device Manager (ASDM) 6.4(1) or later.

Cisco AnyConnect is available as a separate add-on that you can push to your devices using the standard add-on procedure.

Note Application upgrades of Cisco AnyConnect 3.1 from the ASA are not supported.

The following table shows the AnyConnect features supported on the thin clients.

Table 1: AnyConnect Feature Support

Feature	Supported on SUSE Linux-based Thin Clients
Datagram Transport Layer Security (DTLS) with SSL access to VPN	Yes
IPSec/IKEv2 support	No
Compression -Increases the communications performance between the security appliance and the client	Yes
Fallback from DTLS to TLS if DTLS fails	Yes
Certificate-only authentication	No

Feature	Supported on SUSE Linux-based Thin Clients
Machine certificate authentication for standalone mode	No
RSA SecurID integration	No
Smartcard support	No
Download certificate from ASA with Get Certificate	No
Simple Certificate Enrollment Protocol (SCEP) to set up and renew a certificate used for client authentication	No
GUI interface	Yes, Legacy
Minimize on connect	Yes
IPv6 VPN access-Allows access to IPv6 resources over a public IPv4 connection	No
Local LAN access	No
Local printer access through client firewall rules	No
Trusted network detection (TND)	No
Captive portal (hotspot) detection	No
Start Before Logon (SBL)	No
Autoconnect on start	Yes
Resume session after loss of connectivity	Yes
Auto update AnyConnect	N/A (update using Dell Wyse Device Manager)
Auto update AnyConnect profile	Yes
Diagnostic AnyConnect Reporting Tool (DART)	N/A
Federal Information Processing Standard (FIPS) security	Yes
Browser-based (clientless) VPN access	No
Endpoint assessment (Posture)	No
Endpoint remediation	No
Web security-Enforces acceptable use policies to protect endpoints from websites found to be unsafe	No
Network Access Manager (NAM) - L2	No

AnyConnect Profiles and the Cisco ASA

To enable Cisco AnyConnect connections, set up Cisco AnyConnect profiles on the Cisco Adaptive Security Appliance (ASA). Next, specify the required VPN INI connection parameters on the thin client. After you set up the required profiles and push the INI parameters to the client, users can then establish secure connections.

Before you provide the devices to your remote employees, push the required configuration to the devices on your local network first. You can then provide the preconfigured devices to remote users to operate behind the Cisco AnyConnect VPN.

Profile Setup on Cisco ASA

On the Cisco Adaptive Security Appliance (ASA), AnyConnect profiles provide basic information about connection setup, and users cannot manage or modify them. The profile is an XML file that lets you identify the secure gateway (Cisco ASA) hosts that you want to make accessible. In addition, the profile specifies extra connection attributes and constraints for a user. Usually, a user has a single profile file. This profile contains all the hosts needed by a user, and extra settings as needed.

By creating and assigning different profiles to group policies configured on the Cisco ASA, you can differentiate access to Cisco ASA features. The Cisco ASA automatically pushes the profile assigned to the user upon connection setup.

You can configure a profile using the AnyConnect profile editor, a GUI-based configuration tool launched from the Adaptive Security Device Manager (ASDM). The AnyConnect software package, version 3.0 and later, includes the editor. The editor starts when you load the AnyConnect package on the Cisco ASA as an SSL VPN client image.

For detailed configuration information, see the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Cisco AnyConnect Setup Using INI Parameters

To set up Cisco AnyConnect on the device, configure the Custom Connect INI parameter to create Cisco AnyConnect connections. Use the INI parameters to specify the Cisco Adaptive Security Appliance (ASA) address and settings.

Custom Connect Configuration

To create the Cisco AnyConnect connection, configure the Custom Connect parameter in your INI file. The Custom Connect parameter includes a Command option to enable Cisco AnyConnect at startup and to include a Cisco AnyConnect icon on the desktop.

```
CONNECT=Custom \
Description="ASA Connection" \
AutoConnect=Yes \
Reconnect=Yes \
ReconnectSeconds=100 \
Command=/opt/cisco/anyconnect/bin/vpnui
```

Note In the INI file, include the `INIFileSource=cache` parameter. This parameter ensures that devices use the local cached version of the INI file if they cannot access the INI files from Cisco VXC Manager. This parameter is important for devices running the Cisco AnyConnect VPN. These devices require a configuration to reference at bootup before connecting to the network over VPN.

Table 2: Custom Connect Options

Parameter	Description
AutoConnect={no, yes}	**Default is no.** Yes or no option to start a connection automatically at sign-on.
Command=<command or application to be executed from the client>	**Mandatory Option** Specifies a command or application to be executed from the client. For Cisco AnyConnect: Command=/opt/cisco/anyconnect/bin/vpnui
Description=<string description>	**Mandatory Option** Connection description. Provides a connection name for the Desktop icon and the Connection Manager. **Caution** The text must be enclosed in quotation marks if it contains spaces or punctuation characters. These characters are not allowed: & ‘ “ $? ! | ; ( ) [ ] { } \
Reconnect={no, yes}	**Default is no.** Yes or no option to automatically reconnect to an application server after a disconnection.
ReconnectSeconds=<value in seconds>	**Default is 30.** Specifies the amount of time in seconds (default is 30) to wait before automatic reconnection to an application server after a disconnection. Requires Reconnect=yes or 1.

Caution Do not insert any additional spaces at the end of lines in the INI file. Extra spaces may cause the device to parse the INI file incorrectly.

INI Parameters for Cisco ASA Settings

To complete the Cisco AnyConnect setup, specify the Cisco ASA address and settings using the following INI parameters. After you configure these settings and the Custom Connect parameter, push the updated INI file to your devices to enable VPN connections.

Table 3: Cisco AnyConnect INI Parameters

Parameter	Description
VPNGroup=<Group name>,... (optional)	Use this parameter if you configure groups on the Cisco ASA. This parameter specifies the name or names (separated by commas) that the Cisco AnyConnect Client can use for the VPN connection.
VPNHeadendAddress= <FQDN or IP address> (required)	Specifies the VPN headend FQDN or IP Address to autoconfigure the Cisco AnyConnect Client. For example, VPN.Cisco.com or 192.168.0.1.

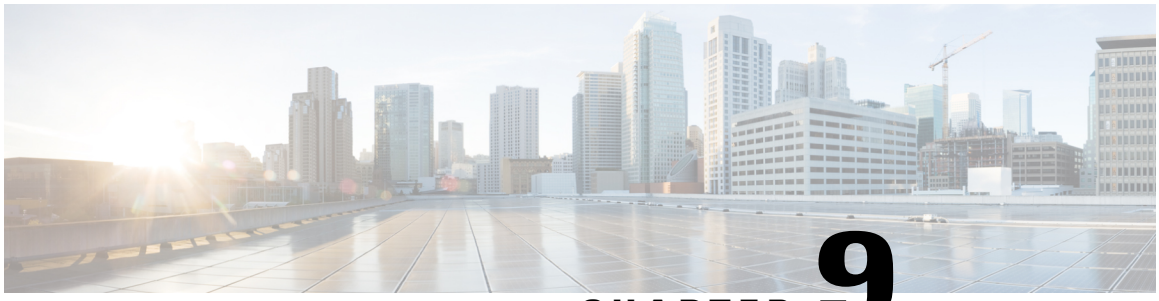
The following shows an example configuration:

```
VPNGroup= profilename
VPNHeadendAddress=192.168.0.1
```

Upgrades Over VPN

If you upgrade devices over a VPN connection, be aware of the following considerations:

- If the configured address discovery method for Dell Wyse Device Manager is DHCP, ensure that AnyConnect propagates these tags across the VPN.
- An image upgrade over a VPN can take a few hours (depending on the speed of the link). If the user disconnects from the VPN before the upgrade process is complete, the download starts from scratch at the next log in.



CHAPTER 9

Upgrade

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 Engine for SUSE Linux* 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 Cisco UC Integration™ for Microsoft Lync

Use this procedure to upgrade to a supported maintenance release of Cisco UC Integration™ for Microsoft Lync. For supported Cisco UC Integration™ for Microsoft Lync versions, see the "System Requirements" section in the *Release Notes for Cisco Virtualization Experience Media Engine for SUSE Linux* for your release.

Procedure

Step 1 Close Cisco UC Integration™ for Microsoft Lync and ensure that it is not running on the HVD.

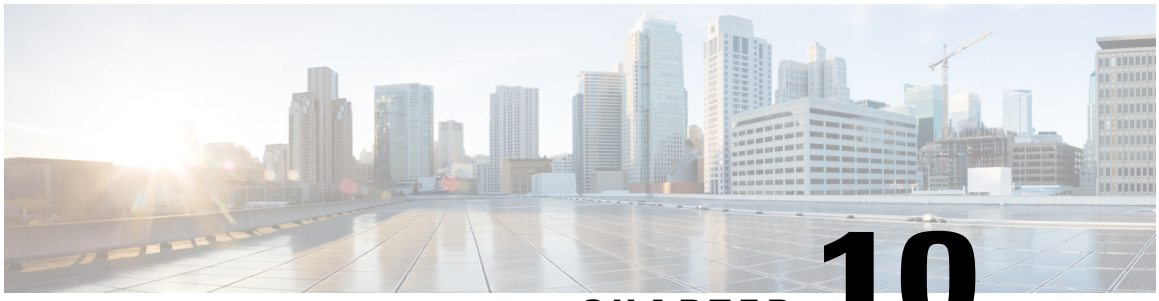
Important If Cisco UC Integration™ for Microsoft Lync is running during the installation, exit and restart Cisco UC Integration™ for Microsoft Lync to enable virtualization.

Step 2 Install Cisco UC Integration™ for Microsoft Lync.

Remove VXME from the Thin Clients

If you have a device running Cisco VXME, but you do not want to run Cisco VXME after the upgrade, you can remove VXME during the upgrade. If the AutoLogin paramenter is set to yes, and you do not perform the following step, the AutoLogin setting will persist on the device after the upgrade. That is, the device will continue to automatically login at boot using thinuser credentials.

If you want to disable the AutoLogin setting during an upgrade, you can set the preserve changes option in the RSP file to no (`set-preserve-changes no`), and then re-image the thin client with the latest base firmware. Alternately, you can edit the value for the parameter after the upgrade.



CHAPTER 10

Troubleshooting

Verify the Platform Base Image Version

You can open System Information to verify the build version.

Procedure

Step 1 In the notification area of the taskbar, click the System Information icon.

Step 2 Click the **Identity** tab.

Step 3 In the **System** section, look for the **Build** line.

Verify the Installation of Cisco VXME

You can use System Information to verify that Cisco Virtualization Experience Media Engine is installed, and to verify the versions of the add-ons.

Procedure

Step 1 Click the System Information icon in the notification area of the taskbar.

Step 2 Select the **Packages** tab.

Step 3 Scroll down the alphabetical list and look for vxme.
The add-on versions appear in the **Versions** column.

Confirm the Version of Cisco Virtualization Experience Media Engine

Note By default, SSH is disabled. For information about how to enable SSH, see the administration guide for your thin client.

Procedure

Step 1 Use SSH to connect to the thin client.

Step 2 Enter the following command: **rpm -qa | grep vxme** .
You can also use the **versionInfo** command.

Ensure That VXC Is Running on the Thin Client

The `vxc` process is part of Cisco Virtualization Experience Media Engine (VXME) and it must be running for VXME to function.

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:~>
```

Ensure That the Credentials Are Passed down the Virtual Channel

Procedure

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

Step 2 Turn off logging to remove the vxc_logs files.
vxc_run.sh -l off

Step 3 Turn logging back on and restart the thin client.
vxc_run.sh -l on

Step 4 Log in to the HVD and sign in to Cisco Jabber.

Step 5 Run the PRT and send the report to the PRT server.

Step 6 Download the report from the PRT server and extract the logs.

Step 7 Open the vxc.log file and search for `Attempting to connect to CUCM for`.

Lost Call Control After Network Failure

Users see a prompt to reconnect to their hosted virtual desktops (HVD). After they reconnect, Cisco Jabber or Cisco UC Integration for Microsoft Lync cannot control calls and their phones do not show as registered on the Logitech UC Keyboard.

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 or Cisco UC Integration for Microsoft Lync 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).

Log Files and Core Dumps

The default logging level is debug. You can use a script to disable and enable logging, for troubleshooting purposes. You can also enable core dumping. You must have administrator privileges to run the script, and log on to the thin client over SSH.

For information about how to enable or disable SSH, see the administration guide for the thin client.

For information about how to change the administrator or root password on the thin client, see the documentation for the thin client.

The following table lists and describes the options for the script. The script accepts two options (one for logging and one for core dumping).

Table 4: Logging Operations

Option	Description
`-l on`	Turn on logging for the thin client. This option creates the ciscolog.conf and writes logs to the /var/log/cisco folder. The script also restarts the thin client so the change takes effect immediately. The log file is /var/log/cisco/vxc.log. The log file for the Virtual Channel is: /var/log/cisco/VirtualChannel.log.
`-l off`	Turn off logging for the thin client. This option deletes the /var/log/cisco folder and the ciscolog.conf file. **Note** You cannot run the script to turn off logging from within the /var/log/cisco folder. The script also restarts the thin client so that the change takes effect immediately.
`-c on`	Turn on core dumping. This option adds a configuration line to /etc/security/limits.conf. The script also prompts you to restart the thin client for the changes to take effect. Core dumping is a system-wide policy; after you enable it, any process that crashes produces a core dump and saves it to /tmp. The filename format is: core_PROCESSNAME_TIMESTAMP. The system generates core files when a process crashes. The /tmp folder may contain multiple core files. The time stamp in the filename helps with the identification of the core files generated around the time of the incident under investigation.
`-c off`	Turn off core dumping. This option removes the configuration line from /etc/sysctl.conf. The script also prompts you to restart the thin client for the changes to take effect. **Important** If you turn off core dumping, the script deletes all core dumps from the /tmp folder.
`-h`	Display the usage help.

Script Example 1

```
vxc_run.sh –l off -c on
```
In this example, the script turns off logging and turns on core dumping.

Script Example 2

```
vxc_run.sh –l on
```
In this example, the script turns on logging.

Problem Reporting Tool

The Problem Reporting Tool (PRT) is a small program, which automatically runs if Cisco Jabber or Cisco UC Integration™ for Microsoft Lync encounters an unrecoverable error, or unhandled exception. 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.

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

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

Users can generate a problem report from the Windows **Start** menu if Cisco UC Integration™ for Microsoft Lync is not running. To access the tool from outside the application, choose **Start** > **All Programs** > **Cisco Systems, Inc** > **Report a problem**.

Advise users to include a memory dump with the problem report if their Cisco Unified Communications application crashes.

Note Users must accept the privacy agreement to run the PRT.

We recommend that users provide a description of the circumstances that lead up to the error. For more detailed information about how to run the PRT, see the Troubleshooting section in the applicable user guide.

Create a Problem Report After a Client Error

If Cisco Jabber or Cisco UC Integration™ for Microsoft Lync encounters a problem and must close, the problem-reporting tool starts automatically.

Procedure

Step 1 In the **Client Error** dialog box, choose a problem type.

Step 2 Enter a short description of the problem, and then click **Save Report**.

Note If your system administrator set up the feature, you can click **Send Report** to upload the problem report to a server. You do not need to save the file locally with this feature.

Step 3 In the **Save As** dialog box, choose the location to which you want to save the problem report, and then click **Save.**

Step 4 Send the file to your system administrator.

Create a Problem Report from the Help Menu

If you experience an issue with Cisco Jabber or Cisco UC Integration™ for Microsoft Lync, you can manually create a problem report from the **Help** menu.

Procedure

Step 1 Select **Help** > **Report a problem**.

Step 2 Select a problem area, and then click **Next**.

Step 3 Enter a short description of the problem, and then click **Next**.

Step 4 (Optional) To include a memory dump file, check the **Include memory dump** check box, and then click **Attach File**.
Include a memory dump if Cisco Jabber, Cisco UC Integration™ for Microsoft Lync, or Device Selector crashes.

Step 5 In the **Open** dialog box, select the memory dump file, and then click **Open**.

Step 6 Click **Save Report**.

Note If your system administrator set up the feature, you can click **Send Report** to upload the problem report to a server. You do not need to save the file locally with this feature.

Step 7 In the **Save As** dialog box, choose the location to which you want to save the problem report.

Step 8 Send the file to your system administrator.

Create a Problem Report from the Windows Start Menu

If you cannot sign in to Cisco Jabber or Cisco UC Integration™ for Microsoft Lync, you can create a problem report from the **Microsoft Windows Start** menu on the hosted virtual desktop. Only use this procedure if you cannot sign in to Cisco Jabber or Cisco UC Integration™ for Microsoft Lync because the problem report does not include the logs from the thin client.

Procedure

Step 1 Select **Start** > **All Programs** > **Cisco Systems, Inc** > **Report a problem**.
For Cisco UC Integration™ for Microsoft Lync, select **Start** > **All Programs** > **Cisco Systems, Inc** > **Report a problem**.

Step 2 Select a problem area, and then click **Next**.

Step 3 Enter a short description of the problem, and then click **Next**.

Step 4 (Optional) To include a memory dump file, check the **Include memory dump** check box, and then click **Attach File**.
Include a memory dump if Cisco Jabber, Cisco UC Integration™ for Microsoft Lync, or Device Selector crashes.

Step 5 In the **Open** dialog box, select the memory dump file, and then click **Open**.

Step 6 Click **Save Report**.

Note If your system administrator set up the feature, you can click **Send Report** to upload the problem report to a server. You do not need to save the file locally with this feature.

Step 7 In the **Save As** dialog box, choose the location to which you want to save the problem report.

Step 8 Send the file to your system administrator.

Gather Logs Manually

If the virtual channel goes down, the Problem Reporting Tool (PRT) cannot gather the Virtualization Experience Media Engine logs from the thin client. You can use Dell Wyse Device Manager (WDM) to gather the logs.

Before You Begin

You must have an FTP server set up, if you want to use FTP.

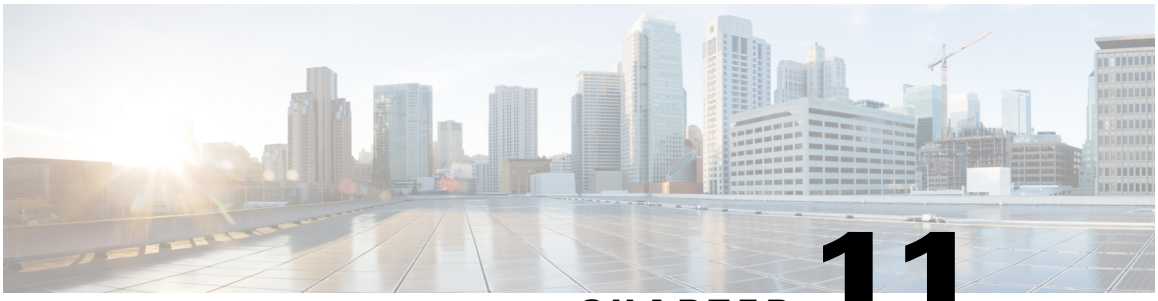
Procedure

Step 1 In WDM, right-click on the thin client and select **Execute Command**.

Step 2 In the **Execute** dialog box, enter the following command.
```
/usr/bin/collect-files
```
This step collects the logs and creates a compressed package.

Step 3 Send the file to the FTP server, by entering the following command.
Where 1.1.1.1 is the IP address of the FTP server:
```
/usr/bin/curl -T /root/VXC*.tar.gz ftp://1.1.1.1
```

Step 4 Remove the .tar.gz file, by entering the following command.
```
/bin/rm /root/vxc*.tar.gz
```



CHAPTER 11

Cisco Virtualization Experience Media Engine Reference Information

Differences in the Virtual Environment

The user experience with Cisco Virtualization Experience Media Engine and a supported Cisco Unified Communications client in a virtual environment is very similar to the experience provided by a standard Cisco Unified Communications client installation, with 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 Phone or to use their computer to make and receive calls. The default phone selection is **Use my computer for calls**. After device selection, the Cisco Virtualization Experience Media Engine application starts the transfer of the phone configuration data for that user. For more information, see Configuration Files, on page 26.
- Users 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**

Note With Cisco Jabber for Windows Release 10.5(1), the **Advanced** button that appears on the **Video** tab is not present in the virtual environment. With Cisco Jabber for Windows 10.5(2) the **Advanced** button does appear on the **Video** tab in the virtual environment.

- If a connection failure between the thin client and the HVD occurs, the user is prompted to log back on to the HVD. If the user has an active call, it is preserved. The user can end the call by using one of the

accessories, such as the keyboard. If the user does not have an accessory with which to end the call, the user can ask the other party to end the call. If there are held calls when the connection failure occurs, the parties on hold receive no notification of the connection failure. After logging back on to the HVD, the user can send an instant message (IM) to the parties that were left on hold.

- 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 initiate 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).

Supported Codecs

Supported Audio Codecs

- G.722
- G.722.1
  - G.722.1 32k
  - G.722.1 24k

Note G.722.1 is supported on Cisco Unified Communications Manager 8.6.1 or later.

- G.711
  - G.711 A-law
  - G.711 u-law
- G.729a

Supported Video Codecs

- H.264/AVC