Administration Guide for Cisco Virtualization Experience Client Manager 4.9

Last Modified: November 20, 2013

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

Administration Guide for Cisco Virtualization Experience Client Manager 4.9

CONTENTS

CHAPTER 7

Preface

Cisco Virtual Experience Client (VXC) Manager software is the premier enterprise solution for managing network intelligent devices simply, remotely, and securely. It enables IT professionals to easily organize, upgrade, control, and support thousands of Cisco VXC devices including Cisco VXC 6000 Series devices and Cisco VXC 2000 Series devices.

Note Cisco VXC 6215 clients run a Cisco-enhanced version of SUSE Linux firmware. Cisco VXC 2111/2211 PCoIP clients run PCoIP Zero Client firmware (also known as ThreadX firmware). Cisco VXC 2112/2212 ICA clients run WTOS firmware.

Cisco VXC Manager software uses industry standard communication protocols and a component-based architecture to efficiently manage your network devices. Its intuitive, simple, and powerful user interface is built to operate as a standard snap-in to the Microsoft Management Console (MMC). From one simple-to-use console, Cisco VXC Manager allows you to manage all of your network devices easily and quickly.

Audience

This guide is intended for administrators of the Cisco VXC Manager system. It provides information and detailed system configurations to help you design and manage a Cisco VXC Manager environment.

This guide is intended for experienced network administrators and Information Technology professionals who have installed and configured Windows operating systems and applications.

Organization

This manual is organized as described in the following table.

Chapter	Description
Preface	Describes the manual.
Chapter 1, “Getting Started”	Describes Cisco VXC Manager basics.
Chapter 2, “Device Manager”	Describes the Device Manager options and functions.
Chapter 3, “Package Manager”	Describes the Package Manager options and functions.

Chapter	Description
Chapter 5, “Update Manager”	Describes the Update Manager options and functions.
Chapter 6, “Report Manager”	Describes the Report Manager options and functions.
Chapter 7, “Configuration Manager”	Describes the Configuration Manager options and functions.
Appendix A, “Working with Groups and Views”	Describes how to work with groups and views within Cisco VXC Manager.
Appendix B, “About Cisco VXC Manager Security”	Describes security features.
Appendix C, “Upgrading Cisco VXC Manager Agents”	Describes upgrade procedures for the Cisco VXC Manager Agents (HAgent).
Appendix D, “Device Discovery, Device Imaging, and Mass Imaging Tool”	Describes the Mass Imaging Tool.
Appendix E, “Troubleshooting”	Describes troubleshooting procedures.
Appendix F, “Licensing and Sales Keys”	Describes licensing procedures for third-party clients.
Appendix G, “Additional Package Manager Procedures”	Describes additional package manager procedures for third-party clients.
Appendix H, “Cisco VXC Manager ScriptBuilder Tool and Scripting Language”	Describes the ScriptBuilder tool for third-party clients.
Appendix I, “Autogenic Imaging”	Describes Autogenic Imaging for third-party clients.

Related Documentation

For more information, see the documents available at the following URLs:

Cisco Virtualization Experience Client 2000 Series

http://www.cisco.com/en/US/products/ps11499/tsd_products_support_series_home.html

Cisco Virtualization Experience Client 6000 Series

http://www.cisco.com/en/US/products/ps11976/tsd_products_support_series_home.html

Cisco Virtualization Experience Client Manager

http://www.cisco.com/en/US/products/ps11582/tsd_products_support_series_home.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Document Conventions

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following convention:

Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

CHAPTER 1

Getting Started

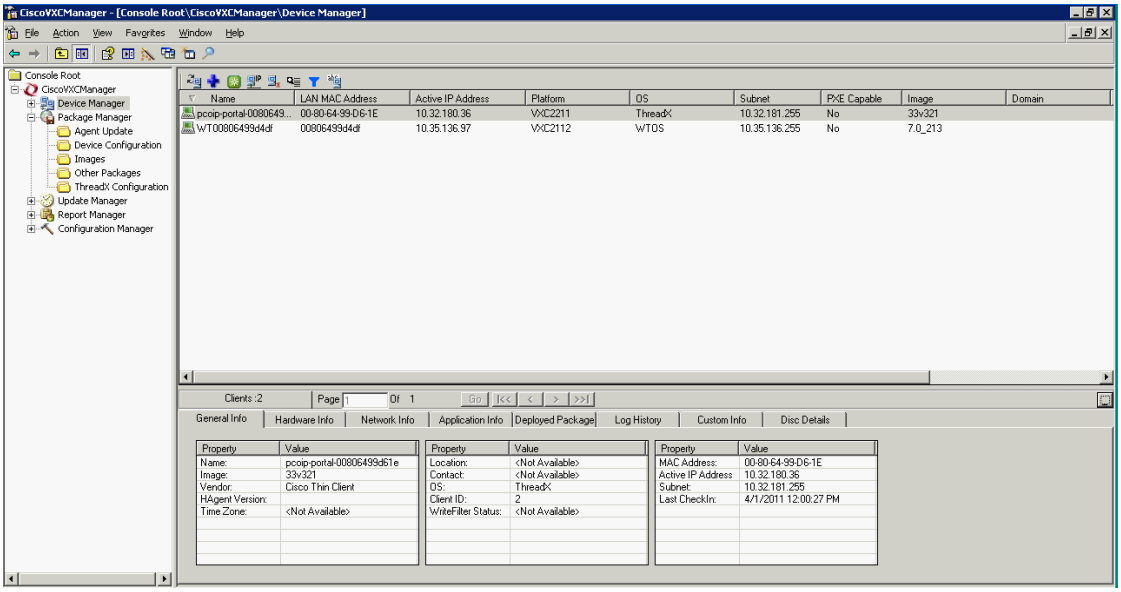
This chapter provides a brief overview of the functional areas within the Cisco VXC Manager Administrator Console. It also provides important information on the general features of the system to help you quickly get started as a Cisco VXC Manager administrator.

Getting to Know the Administrator Console

This section contains an overview of the areas and tools that comprise the Cisco VXC Manager Administrator Console (details on each item in the Administrator Console are provided in their respective chapters in this guide).

The Cisco VXC Manager Administrator Console is a snap-in to the Microsoft Management Console (MMC). It allows you to quickly view important information about the Cisco VXC Manager system, and helps you to easily perform all of the device management duties that are required to run and maintain your Cisco VXC Manager environment.

Figure 1-1 Cisco VXC Manager Administrator Console



The tree pane of the Administrator Console contains several functional managers (nodes). Each of these managers has a set of automated tools that help you to perform your administrator duties and daily activities in that functional area:

- Device Manager—View and manage the devices within your Cisco VXC Manager environment (see Device Manager, page 2-7).
- Package Manager—View and manage the Cisco VXC Manager packages (images, configurations, and so on) which can be distributed to managed devices (see Package Manager, page 3-31).
- Update Manager—View and manage the schedules for Cisco VXC Manager package distribution to managed devices, and the schedules for synchronizations between Remote Repositories and the Master Repository (see Update Manager, page 5-29).
- Report Manager—Create and view the Cisco VXC Manager reports (see Report Manager, page 6-45).
- Configuration Manager—Configure your Cisco VXC Manager system preferences and environment designs so that Cisco VXC Manager meets your specific needs (see Configuration Manager, page 7-61).

The top of the details pane of the Administrator Console contains various task command icons and features, and a listing of the items contained in the selected node or folder of the tree pane. For example, you can open a folder named Finance in which you have placed a View you have created to display all of the devices in your finance department.

The bottom of the details pane of the Administrator Console contains details and task options for the items listed in the top of the details pane. For example, if you choose a device listed in your finance department, the bottom of the details pane provides tabs (General Info, Hardware Info, Network Info, Application Info, Deployed Package, Log History, Custom Info, Disk Details, and Remote Sessions) that contain information on the various details of the device. To view the information you want about the device, click the appropriate tab.

Tip The panes of the Administrator Console allow you to drag and drop items for easy task performance.

Using Shortcut Menus

Cisco VXC Manager shortcut menus provide easy access to get things done throughout the system. You can right-click on an item or simply right-click the details pane of the Administrator Console to display the menu of available tasks you can do.

Along with specific tasks for each specific functional area (for example, creating a new report in the Reports Manager), notable shortcut menu items that are generally available in all functional areas include:

- All Tasks—Provides easy-to-follow wizards (see About Cisco VXC Manager Wizards, page 1-3).
- Refresh—Refreshes the current view displayed in a functional manager (for example, you can right-click in the details pane of the Device Manager and choose **Refresh** to refresh the view of the details pane).
- Export List—Exports the displayed list in the details pane to a .txt or .csv file for use (for example, export a list of Cisco VXC Manager packages for scheduling purposes).
- View—Customizes the look and feel of the Administrator Console.
- Arrange Icons and Line Up Icons—Organizes the icons on the details pane.
- Help—Provides context-sensitive help for the area in which you are working.

Tip Beyond these notable shortcut menu items, other shortcut menu items exist in each functional area to allow you to perform specific tasks in that specific functional area. For example, you can right-click a device in the details pane of the Device Manager and choose **Refresh Device Information** to request that the device send its latest information, such as the IP address, device name, installed applications, and so on. Also, you can right-click a device in the details pane of the Device Manager and choose **Get Logs** to create log files that you can view, and right-click a device and choose **View Log** to choose the log file you want to view (not supported on Cisco VXC 2112/2212).

About Cisco VXC Manager Wizards

Cisco VXC Manager provides easy-to-follow wizards for just about everything you need to do. You can quickly open a list of wizards (from which you can choose) to help you get things done from any of the managers in the tree pane of the Administrator Console. For example, you can right-click **Device Manager**, and then choose **All Tasks > Run Wizard** to open the list of wizards available for use.

Cisco VXC Manager wizards available for use include:

- View Wizard
- Package Wizard
- Package Distribution Wizard
- Software Repository Synchronization Wizard
- Report Wizard
- License Key Wizard
- ThreadX Device Settings

Using Cisco VXC Manager Toolbar Icons

Although Cisco VXC Manager shortcut menus provide easy access to get things done throughout the system, each functional manager also provides Cisco VXC Manager icons for use within that functional area (each has a pop-up description for easy identification in the Administrator Console).

Tip The Help icon (?) provides context-sensitive help from all functional managers.

Device Manager Icons

Standard toolbar Device Manager icons include (in order from left to right):

Figure 1-2 Device Manager – Standard Toolbar Icons

- Run a Wizard—Run one of the supported wizards available in the system.
- Change the View—Change the View to the available View you want.
- Create a New View—Create a customized View.

- Find Devices—Discover the devices in your environment according to your selections.
- Manually Add a Device—Manually add the devices you want.
- Find Device in View—Specify the View (path) in which the particular devices you want to find are located.

The Device Manager also includes the Device Manager Quick-Access toolbar (just above the details pane) containing frequently used Device Manager tools. Icons include (in order from left to right):

Figure 1-3 Device Manager – Quick-Access Toolbar Icons

- Refresh Device Information
- Manually Add a Device
- Remote Shadow (not supported on ThreadX/PCoIP devices)
- Change Device Information
- Reboot
- Shut Down (not supported on ThreadX/PCoIP devices running pre-3.5 firmware)
- Wake On LAN (not supported on ThreadX/PCoIP devices)
- Change Network Information (not supported on WTOS/ICA devices)
- Get Device Configuration (not supported on Cisco VXC devices)
- Get Device Images (not supported on Cisco VXC devices - requires PXE)
- Execute Command
- Delete Devices
- Diagnostic Report
- Create Device Filter

Package Manager Icons

The standard toolbar Package Manager icon is as follows:

Figure 1-4 Package Manager – Standard Toolbar Icon

Run a Wizard—Run one of the supported wizards available in the system.

Update Manager Icons

Standard toolbar Update Manager icons include (in order from left to right):

Figure 1-5 Update Manager – Standard Toolbar Icons

- Run a Wizard—Run one of the supported wizards available in the system.
- Scheduled Packages—Manage your scheduled Cisco VXC Manager packages for devices.

- Software Repository Synchronization—Initiate the Software Repository Synchronization process.

Report Manager Icons

Standard toolbar Report Manager icons include (in order from left to right):

Figure 1-6 Report Manager – Standard Toolbar Icons

- Run a Wizard—Run one of the supported wizards available in the system.
- Create New Report—Create one of the supported reports available in the system.
- System Log Archive—Export the archived records you want to a .txt or .csv file for use.

Configuration Manager Icons

Standard toolbar Report Manager icons include:

Figure 1-7 Report Manager – Standard Toolbar Icons

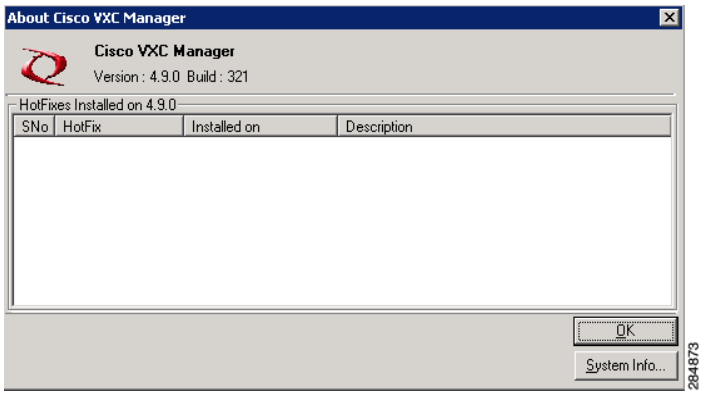
Run a Wizard—Run one of the supported wizards available in the system.

Knowing Your Cisco VXC Manager Version

To display the Cisco VXC Manager version and build number (as well as all installed hotfixes), right-click **CiscoVXCManager** (in the tree pane of the Administrator Console), and then choose **About Cisco VXC Manager**.

Tip You can also click **System Info** to open the System Information window to view system summary, hardware resources, components, and software environment details.

Figure 1-8 About Cisco VXC Manager



Some Initial Considerations

Before you begin using Cisco VXC Manager, consider the following:

- Additional Administrators—Adding the administrators you need ensures that you have the backup personnel necessary. Cisco recommends that you add at least one backup administrator account (see Managing User Permissions, page 7-94).
- System Design—Cisco VXC Manager installation provides you with the necessary components you need to begin adding devices to your Cisco VXC Manager system. However, it is best practice to be sure you have the subnets and repositories you want in your Cisco VXC Manager system before you begin adding devices to your Cisco VXC Manager system. Although you can add subnets and repositories at any time, getting your Cisco VXC Manager design set up before initial use is more convenient.

  For information on adding subnets, see Managing Subnets, page 7-90.

  For information on adding repositories, see Managing Software Repositories, page 7-87.

CHAPTER 2

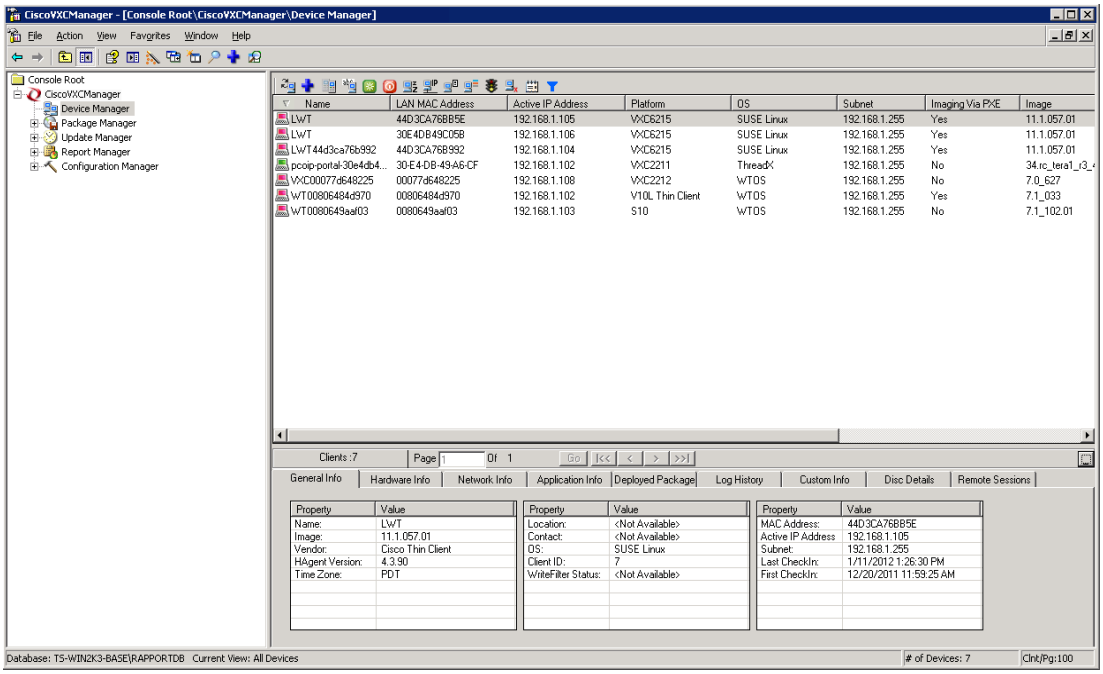
Device Manager

This chapter describes how to perform routine device management tasks using the Administrator Console. It provides information on managing the devices within your Cisco VXC Manager environment.

Managing Devices

Click **Device Manager** in the tree pane of the Cisco VXC Manager Administrator Console to open the Device Manager. The Device Manager allows you to quickly view and manage the devices within your Cisco VXC Manager environment (see Table 2-1). It also allows you to easily display the devices you want by using the available filtering and customizing features.

Figure 2-1 Device Manager



After you choose the devices you want (you can use Ctrl-click or Shift-click to choose multiple devices), you can then begin performing your tasks.

Tip For information on using available icons to perform Device Manager tasks, see Device Manager Icons, page 1-3. For information on setting your Device Manager preferences (device check-in, upgrade, and discovery), see Device Manager Preferences, page 7-73.

Table 2-1 provides a quick overview of what you can do using the Device Manager.

Table 2-1 Routine Device Manager Tasks

Tasks You Can Do	How	Details
Choose a View (defaults or one that you created) to use with Device Manager so you can quickly find the devices you want.	In the tree pane of the Administrator Console, right-click **Device Manager** and choose **Switch View** to open and use the Select Current Manager View dialog box.	After creating Views according to your device Group Types, Networks, and so on, choose a Current Manager View to view the devices you want (see Managing Views, page 7-63).
Create a Device Filter to use with Device Manager so you can quickly find the devices you want.	In the tree pane of the Administrator Console, right-click **Device Manager** and choose **Create Device Filter** to open and use the Filter Devices dialog box.	Creating a Device Filter, page 2-21
View device details of your selected devices.	Click the device details tab you want.	Viewing Device Details, page 2-10 **Tip** To set your preferences for device check-in, upgrade, and discovery, see Device Manager Preferences, page 7-73.
Search for the device that you want to use with Device Manager.	To determine the View (path) in which the particular devices you want to find are located, right-click **Device Manager**, and then choose **Find Device in View** to open and use the Find Device in View dialog box. To quickly find the particular devices you want, right-click any device name in the details pane, and then choose **Quick Find** to open and use the Quick Find dialog box.	Searching for a Device with Find Device in View and Quick Find, page 2-22 **Tip** Use the search tool best suited for your environment and needs.
Add a device to the system using Dynamic Discovery.	Cisco VXC Manager can discover the devices automatically using your preferences in the Preferences dialog box of the Configuration Manager.	Adding and Automatically Discovering Devices, page 2-13 and Adding Devices Using Manual Discovery, page 2-14
Add a device to the system manually.	Right-click **Device Manager**, and then choose **New > Device** to open and use the Add a Device dialog box.	Adding and Automatically Discovering Devices, page 2-13 and Adding Devices Manually, page 2-15
Change basic device information (device name, location, and so on).	Choose the devices you want, right-click the selection, and then choose **Change Device Information** to open and use the Change Client Information dialog box.	Changing Basic Device Information, page 2-16

Table 2-1 Routine Device Manager Tasks (continued)

Tasks You Can Do	How	Details
Change device network information (IP Address, DNS Server, and so on).	Choose the devices you want, right-click the selection, and then choose **Change Network Information** to open and use the Change Client Network Settings dialog box.	Changing Network Properties, page 2-17
Remotely shadow a device (to view and control a device remotely).	Right-click the device you want, and then choose **Remote Shadow** to open and use the VNC Authentication dialog box.	Remotely Shadowing Devices, page 2-20
Execute a DOS command on a device.	Right-click the device you want, and then choose **Execute Command** to open and use the Execute dialog box.	You can type executable commands for a given device (if the executable is not in the path of the device, you must provide a fully qualified path).
Configure the available device settings for a ThreadX device.	Right-click the ThreadX device you want, and then choose **ThreadX Device Settings** to open and use the ThreadX Device Information window.	Configuring ThreadX Device Information, page 2-18
Create a Diagnostic Report containing a summary of hardware and software information and a list of running processes.	Right-click the device you want and choose **Diagnostic Report** to view the Diagnostic Report.	Generating Diagnostic Reports, page 7-103
Create and view log files.	Right-click a device in the details pane of the Device Manager and choose **Get Logs** to open and use the Create Log File dialog box. To view a log file, right-click a device in the details pane of the Device Manager and choose **View Log** to open and use the View Logs dialog box.	Creating and Viewing Log Files, page 2-25
Shut down devices.	Choose the devices you want, right-click the selection, and then choose **Shut Down**.	
Reboot devices.	Choose the devices you want, right-click the selection, and then choose **Reboot**.	
Wake devices.	Choose the devices you want, right-click the selection, and then choose **Wake On LAN**.	

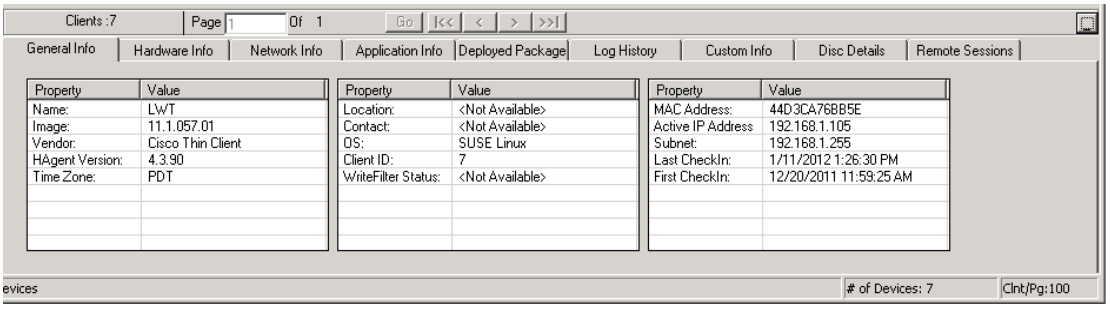
Table 2-1 Routine Device Manager Tasks (continued)

Tasks You Can Do	How	Details
Delete a Device from the system.	Choose the devices you want (you can use Ctrl-click or Shift-click to choose multiple devices), right-click the selected devices, choose **Delete Device**, and then confirm the deletion.	**Caution** If a device has been removed from a network before deleting a scheduled update for that device, the scheduled update may remain in a status of in-progress indefinitely. Before you delete a device, be sure there is no update scheduled for that device (in the tree pane of the Administrator Console, expand **Update Manager** and click **Scheduled Packages** to view any scheduled and in-progress device updates in the details pane).
Use the Package Distribution Wizard to schedule a package for distribution.	Select the devices you want (you can use Ctrl-click or Shift-click to select multiple devices), right-click the selected devices, choose **Package Distribution Wizard** to open and use the Package Distribution Wizard.	Using the Package Distribution Wizard to Schedule a Package for Distribution, page 2-26
Use the Remote Task Manager to view Applications, Processes, and Performance for any selected device.	Select the single device you want, right-click the selected device, choose **Remote Task Manager** to open and use the Remote Task Manager.	Using the Remote Task Manager to View Applications, Processes, and Performance for a Device, page 2-27

Viewing Device Details

The General Info tab is displayed in the bottom of the details pane by default (see Figure 2-1).

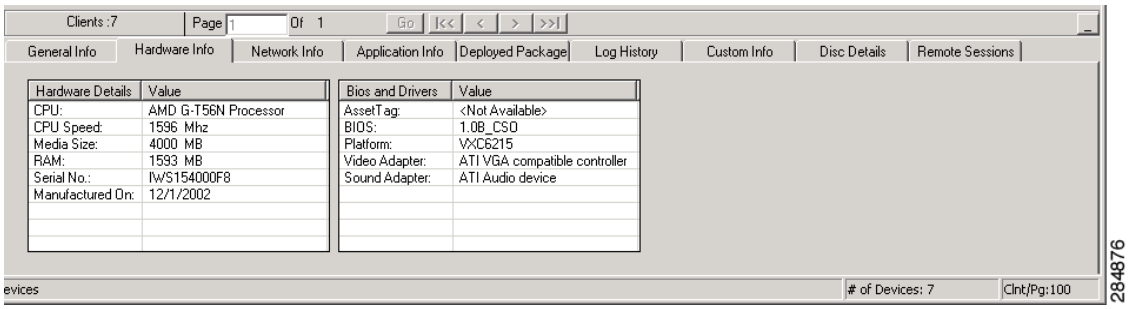
Figure 2-2 General Info Tab



Tip To view the General Info and related tabs, you may need to maximize the Cisco VXC Manager Administrator Console, and then click the plus icon (+) at the bottom of the details pane.

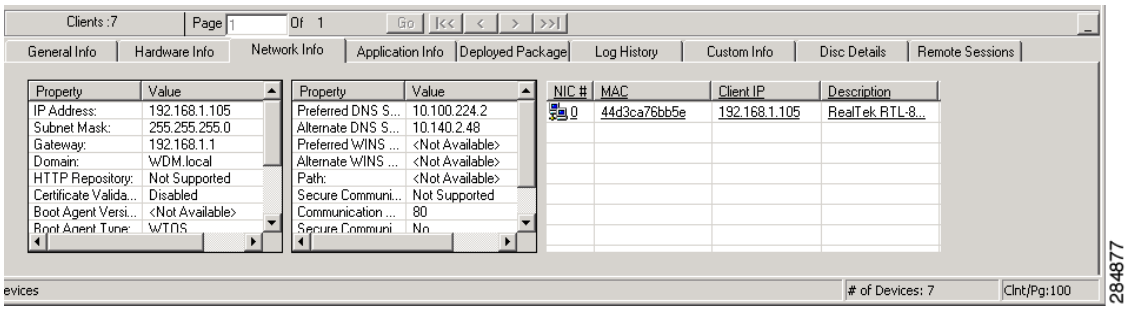
The Hardware Info tab (see Figure 2-3) displays the detailed hardware information, including the partition details of the disk from which the OS is booted and boot agent information for the device.

Figure 2-3 Hardware Info Tab



The Network Info tab (see Figure 2-4) displays the detailed network information for the selected device, including the communication details between different components of Cisco VXC Manager.

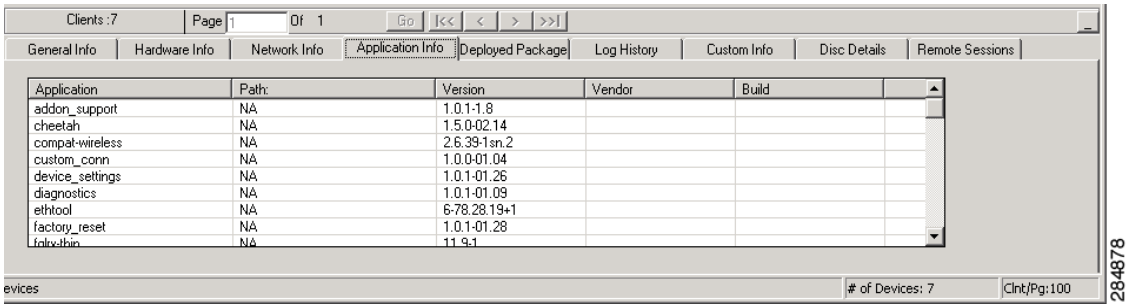
Figure 2-4 Network Info Tab



The Application Info tab (see Figure 2-5) displays the list of the applications installed on the device.

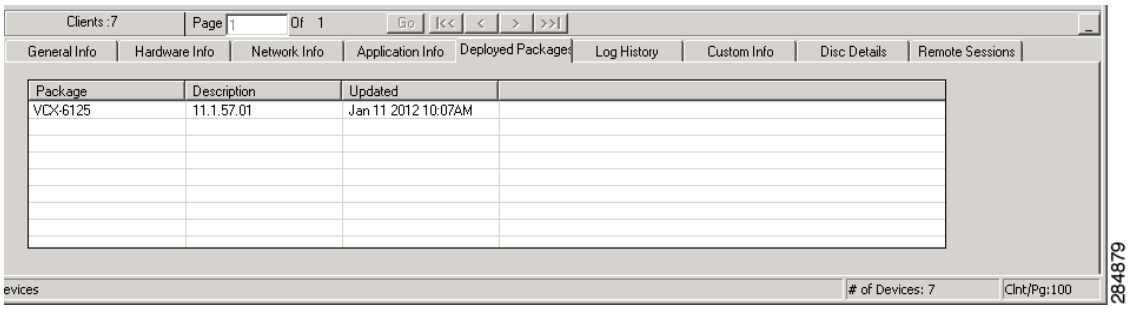
Note Cisco VXC 2112/2212 ICA devices do not display any application information as WTOS only contains a single firmware file and does not support separate application modules.

Figure 2-5 Application Info Tab



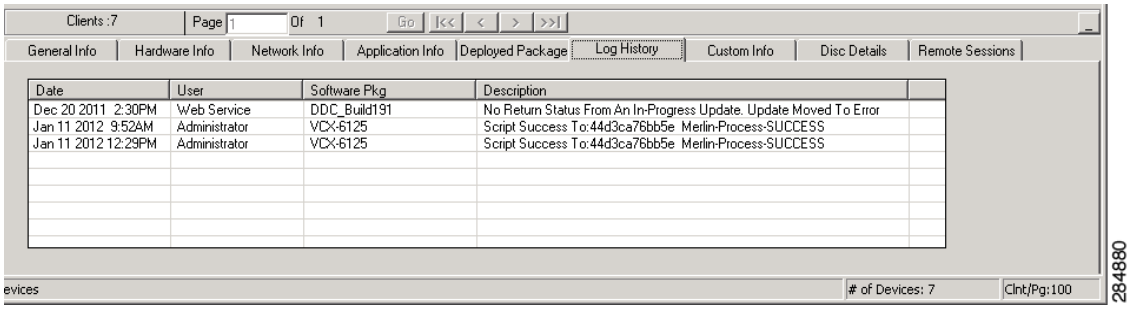
The Deployed Package tab (see Figure 2-6) displays the list of all Cisco VXC Manager packages distributed to the device.

Figure 2-6 Deployed Package Tab



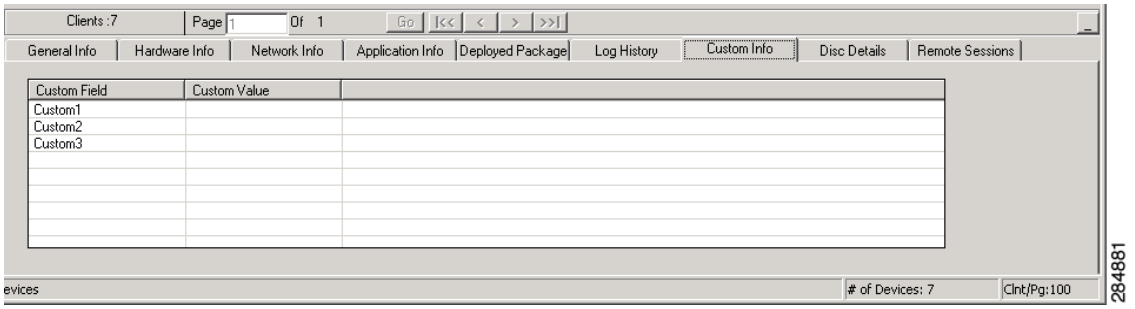
The Log History tab (see Figure 2-7) displays the list of all logs corresponding to Cisco VXC Manager package distribution for the selected device.

Figure 2-7 Log History Tab



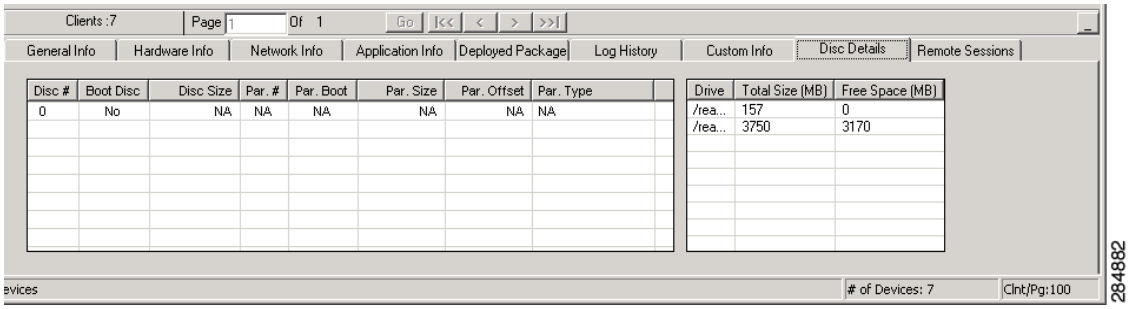
The Custom Info tab (see Figure 2-8) displays all custom information (such as, location, contact, and so on) for the selected device.

Figure 2-8 Custom Info Tab



The Disk Details tab (see Figure 2-9) displays the list of all disks including their partition details existing in the selected device.

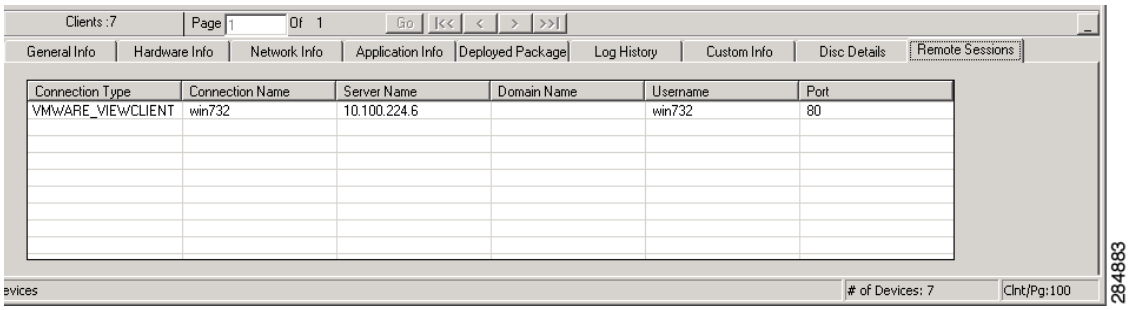
Figure 2-9 Disc Details Tab



The Remote Sessions tab (see Figure 2-10)displays all remote information (connection type, connection name, server name, and so on) for the selected device.

Note The Remote Session tab does not display session information for Mozilla Firefox connections on the Cisco VXC 6215.

Figure 2-10 Remote Sessions Tab



Adding and Automatically Discovering Devices

Cisco VXC Manager becomes aware of the devices in your network using either dynamic discovery or a manual process. After Cisco VXC Manager identifies the devices in the network, it stores information about them in the Cisco VXC Manager Database. You can then use Cisco VXC Manager to manage the devices.

Devices with the Cisco VXC Manager Agent (also referred to as the HAgent) installed must be linked to the Web Service so that the devices can check-in regularly. At check-in time, the Cisco VXC Manager Agent provides the Web Service with device information such as device name, hardware information (such as platform, flash size, memory, CPU, asset number, serial number), network information (such as WINS, DNS, IP address, Domain Name, subnet), image number, and so on. There are five ways in which devices can be linked to the server that contains the Web Service:

- Set Up a DHCP Server—(Recommended for WTOS clients and SUSE Linux clients) Linking is accomplished through DHCP Option Tags 186 and 192 which allow the DHCP server to supply the Cisco VXC Manager Agent with the proper Cisco VXC Manager Web Server IP address and port. See Configuring the DHCP Server, page D-1.
- DHCP Option Tags and DNS SRV Records—(Required for ThreadX clients) See Configuring the DHCP Server, page D-1, Configuring a DNS Service Location (SRV) Resource Record for ThreadX Devices, page D-7, and Configuring a Cisco VXC Manager Server Host Name in the DNS Server, page D-9 for details.

- Enable DHCP Options for HTTP Discovery—Cisco VXC Manager services includes a DHCP Proxy that will respond to DHCP Inform requests from Cisco VXC Manager Agents with the Web Server IP address and port.
- Manual Discovery—Initiate discovery from the server to find devices by either Subnet Broadcast or IP Range. Cisco VXC Manager Agents will respond to the server discovery by storing the discovering Web Server IP address and port and begin regular check-ins.
- Manual Device Setup—Manually enter the Web Server IP address and port on each device. You can do this through the Cisco VXC Manager Control Panel applet on the device (if supported by the device).

You can add devices to Cisco VXC Manager either by having Cisco VXC Manager discover the devices using Dynamic Discovery or by manually adding devices.

Using Dynamic Discovery, the Cisco VXC Manager Agent checks in periodically with the Cisco VXC Manager Web Service. This form of check-in is based on pull communications because the Cisco VXC Manager Agent initiates communications. For more information on using Cisco VXC Manager to discover devices, see Adding Devices Using Manual Discovery, page 2-14.

When you add devices manually, you instruct Cisco VXC Manager to discover devices on command. This method uses push communications because the Cisco VXC Manager Server initiates the operation. When you choose this method of adding devices, you can specify whether to add devices through a UDP broadcast or through a TCP connection to every device within a subnet or an IP Range setting. For more information on manually adding devices to Cisco VXC Manager, see Adding Devices Manually, page 2-15.

Adding Devices Using Manual Discovery

With new devices that come with the Cisco VXC Manager Agent pre-installed, you must link the Cisco VXC Manager Agent on the devices to the Cisco VXC Manager Web Service. Once the link is established, the devices check in periodically using Dynamic Discovery.

Use the following guidelines to manually discover devices with the Device Manager:

Procedure

Step 1 In the tree pane of the Administrator Console, right-click **Device Manager** and click **Find Devices** to open the Find Devices dialog box.

Step 2 Using the radio buttons, specify whether to discover devices by subnet or IP range.

Step 3 (Optional) To discover devices by IP range:

a. Click the **IP Ranges** option.

b. From the Network List pane, choose either individual IP ranges (use Shift or Ctrl to choose multiple subnets) or all IP ranges by clicking **Select All** (the maximum number of ranges that can be selected at any given time for discovery is 100).

Step 4 (Optional) To discover devices by subnet:

a. Click the **Subnets** option.

b. If you enabled the Show Subnet Hierarchy preference (see Subnet Preferences, page 7-85) and you want to choose a subnet hierarchy level to find devices, choose a subnet hierarchy level from the Network Hierarchy pane. The corresponding broadcast addresses for the subnets in the hierarchy will be displayed on the Network List pane.

If you did not enable the Show Subnet Hierarchy preference, continue with the next step.

c. From the Network List pane, choose either individual broadcast addresses (use Shift or Ctrl to choose multiple subnets) or all broadcast addresses by clicking **Select All**.

Note The maximum number of subnets that can be selected at any given time for discovery is 100. Initially, Cisco VXC Manager will discover up to approximately 50 subnets (always starting from the first subnet). To discover any remaining subnets, you must restart the discovery.

Step 5 Click **OK**. Cisco VXC Manager begins discovering the devices according to your selections. The details pane displays both the newly discovered devices along with devices that have been discovered previously.

Adding Devices Manually

Cisco VXC Manager also allows you to manually add devices to the Cisco VXC Manager Database (for example, in cases where technical issues prevent you from discovering a device that is otherwise operating normally, or in cases where the operating system of a device has become corrupt and the device does not operate normally).

Use the following guidelines when adding devices manually:

Procedure

Step 1 In the tree pane of the Administrator Console, right-click **Device Manager**, and then choose **New > Device** to open the Add a Device dialog box.

Step 2 Use the following guidelines:

- Name—Machine name of the device as you want it to be displayed in the Device Manager.
- MAC Address—Media Access Control (MAC) address of the device, which uniquely identifies the device on the network. Be sure to enter the MAC address accurately or Cisco VXC Manager will not be able to communicate with the device.
- IP Address—Internet Protocol address of the device. This identifies the device on a TCP/IP network. Network messages are routed to the device based on the IP address.
- Media Size—Enter the flash memory size of the device in megabytes (for example, 32, 48, 96, and so on).
- Operating System—Installed operating system of the device.
- Platform—Hardware platform for the device.
- Callisto-2—Choose this option if the device is a Callisto-2 device.
- Subnet—The subnet for the device.
- Imaging via PXE—Choose this option if the device is capable of being imaged by Cisco VXC Manager (the device supports the Preboot EXecute Environment).

Step 3 After completing your configurations click **OK**. The newly added device appears in the details pane. If you have created a View corresponding to any of the device group type characteristics, the device is automatically incorporated into the appropriate View.

Changing Device Properties

Device Properties consist of basic properties and network properties. You can change basic properties by using the procedures in Changing Basic Device Information, page 2-16. You can change the network properties by using the procedures in Changing Network Properties, page 2-17.

Changing Basic Device Information

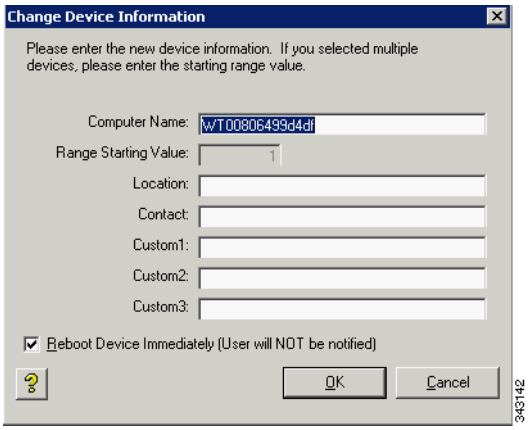
Caution This section does not apply to Cisco VXC 2111/2211 clients running ThreadX firmware.

Procedure

Step 1 Switch to the view containing the devices you want to change.

Step 2 Choose the devices you want to change, right-click the selection, and then choose **Change Device Information** to open the Change Device Information dialog box.

Figure 2-11 Change Device Information



Step 3 Use the following guidelines:

- Computer Name—Enter a descriptive name for the computer (or range of computers, if you selected multiple devices).
- Range Starting Value—If you selected multiple devices, an incremental number will be appended to the name of each device. Enter the starting number for the range of devices.
- Location—Enter a descriptive location where the device or devices reside. For example, San Jose headquarters, 2nd floor.
- Contact—Enter the name of the person who can serve as a contact for the device or devices in the range.
- Custom1, Custom2, Custom3—Enter any additional information that you want to maintain along with the device or group of devices (asset tracking data, a service date, a date of acquisition, or any other information that is useful to you).

Step 4 Depending on whether or not you want to reboot the device or devices automatically after changing the information (devices are updated only after a reboot) check or uncheck **Reboot Device Immediately** (be aware that if you choose to reboot immediately, users will not be notified that the device will be rebooted). Note that Write Filter devices ignore this option and will reboot immediately.

Step 5 Click **OK** to open the details pane displaying the newly updated device information after the devices have rebooted and checked-in.

Changing Network Properties

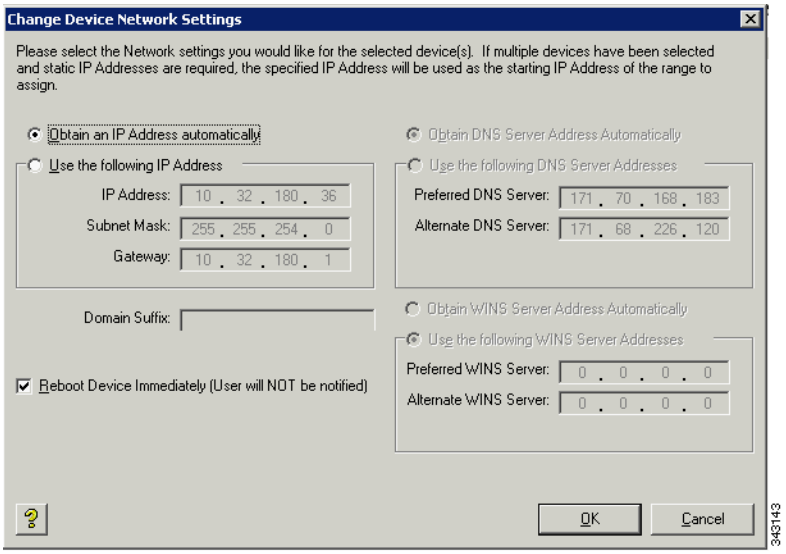
Caution This section does not apply to Cisco VXC 2112/2212 clients running WTOS firmware.

Procedure

Step 1 Switch to the view containing the devices you want to change.

Step 2 Choose the devices you want to change, right-click the selection, and then choose **Change Network Information** to open the Change Device Network Settings dialog box.

Figure 2-12 Change Device Network Settings



Step 3 Depending on whether or not you want to assign a static IP Address for the selected devices, complete one of the following:

- If no, click **Obtain an IP Address automatically** and continue with the next step.
- If yes, click **Use the following IP Address** and complete the fields in the IP Address section.

Tip For the IP Address section—If you selected multiple devices in step 2, the IP Address you enter is the starting address for the range of addresses that includes all of the devices you selected. All ranges must fall within a Class C subnet. If a group of devices are assigned a range of IP Addresses that would cross a Class C, Cisco VXC Manager issues an error message blocking the operation.

Step 4 Depending on whether or not you want to assign a static DNS Server Address for the selected devices, complete one of the following:

- If no, click **Obtain DNS Server Address Automatically** and continue with the next step.
- If yes, click **Use the following DNS Server Addresses** and complete the fields in the DNS Server Address section.

Step 5 If you want to add a Domain Name as a suffix to the device names for the selected devices, enter the Domain Name in the Domain Suffix field (for example, if you add as a suffix the Domain Name **DFW1.cisco.com** to a device named Device1, the result is: Device1.DFW1.cisco.com).

Step 6 Depending on whether or not you want to assign a static WINS Server Address for the selected devices, complete one of the following:

- If no, click **Obtain WINS Server Address Automatically** and continue with the next step.
- If yes, click **Use the following WINS Server Addresses** and complete the fields in the WINS Server Address section.

Step 7 Depending on whether or not you want to reboot the device or devices automatically after updating the information (devices are updated only after a reboot) check or uncheck the **Reboot Device Immediately** check box (be aware that if you choose to reboot immediately, users will not be notified that the device will be rebooted). Note that Write Filter devices ignore **Reboot Device Immediately** and will reboot.

Step 8 Click **OK**. The details pane will display the newly updated network information after the devices have rebooted and checked-in.

Configuring ThreadX Device Information

Caution This section is applicable only to Cisco VXC 2111/2211 clients running ThreadX firmware for PCoIP.

Use the following guidelines to configure ThreadX device information.

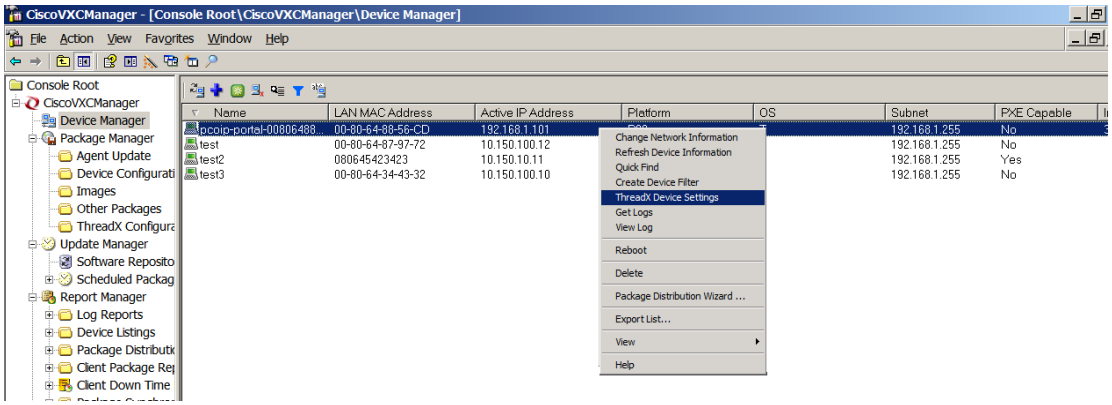
Configuration Settings—Cisco VXC Manager supports the following configurations on the device side:

- Label settings
- Time Zone settings
- Video settings
- Global settings for RDP

Note Cisco does not provide support for RDP network implementations with the Cisco VXC 2111/2211 clients.

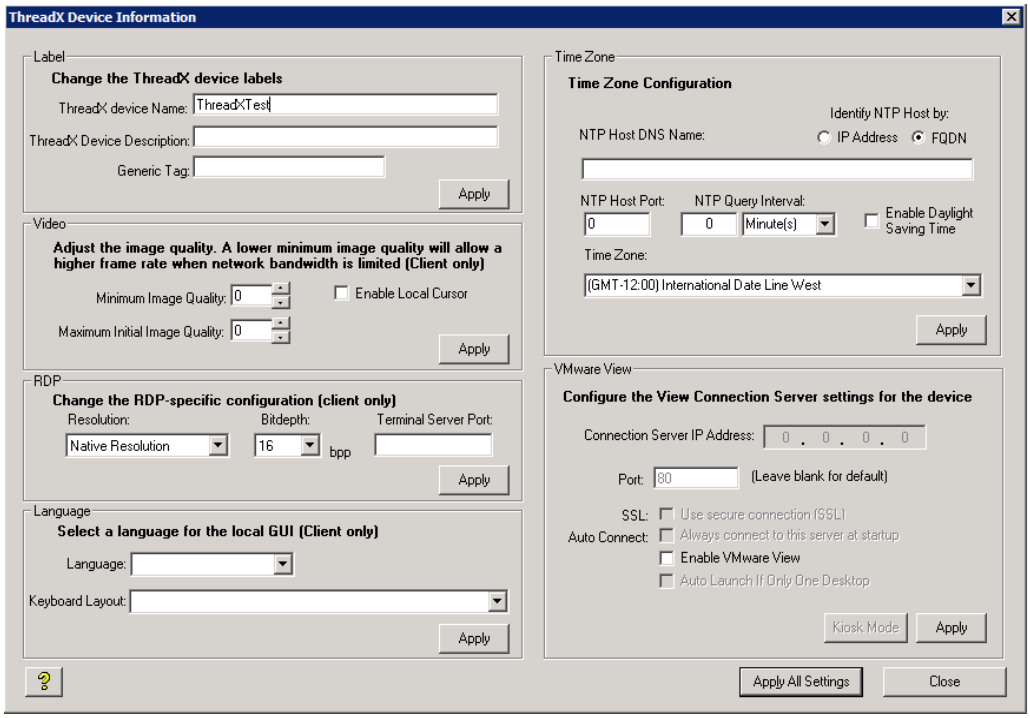
- VMware View settings

Figure 2-13 ThreadX Device Settings Menu Option



To configure the available device settings for a device, right-click a device and choose the **ThreadX Device Settings** menu option to open and use the ThreadX Device Information window.

Figure 2-14 ThreadX Device Information

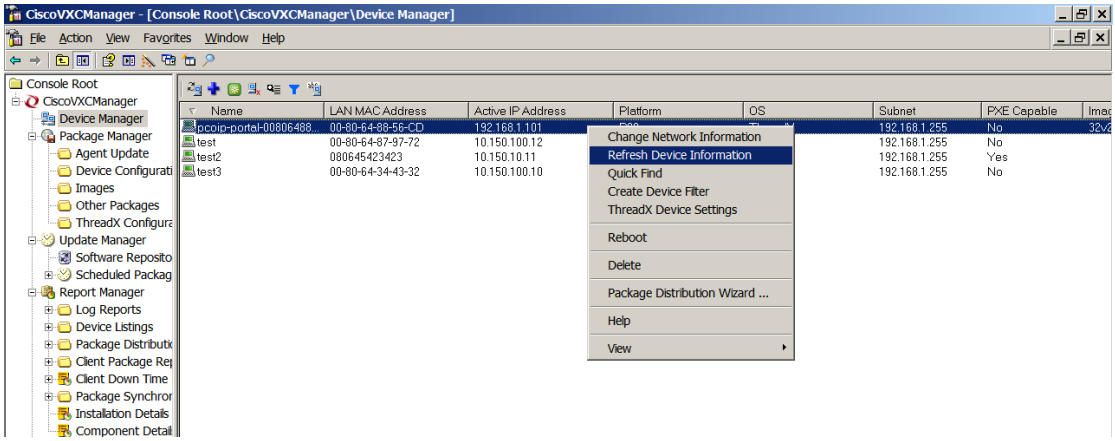


After you configure the device settings, click **Apply** to apply a single configuration set or click **Apply All Settings** to apply the entire configuration set at one time.

Tip To configure the available device settings for multiple devices, right-click the devices you want in the list of devices and choose the **ThreadX Device Settings** menu option to open and use the ThreadX Device Information window. In this case, only the Apply All Settings command button is available for use (the Apply command button for each configuration set is disabled).

Refresh Device Information—To manually refresh the device information, right-click a device and choose the **Refresh Device Information** menu option.

Figure 2-15 Refresh Device Information Menu Option



Reboot—To manually reboot the device, right-click a device and choose the **Reboot** menu option.

Remotely Shadowing Devices

Viewing and controlling a device remotely (shadowing a device) is useful to help a user with a particular application and to troubleshoot device problems.

Caution This section is not applicable to Cisco VXC 2111/2211 clients running ThreadX firmware for PCoIP.

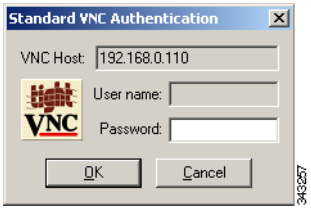
Procedure

Step 1 Switch to the view containing the device you want to shadow.

Step 2 In the Device Manager details pane, right-click the device you want to shadow and choose **Remote Shadow**.

Step 3 The Standard VNC Authentication dialog box prompts you for a VNC host, username and password.

Figure 2-16 VNC Authentication



Step 4 Enter the VNC host, username and password you set up earlier for VNC authentication and click **OK** (note that some manufacturers hard-code passwords into their devices, requiring you to contact the manufacturer to obtain the device password). A window displays the device screen and allows you to run applications and control the device from the Administrator Console.

Step 5 To end the shadowing, close the viewer.

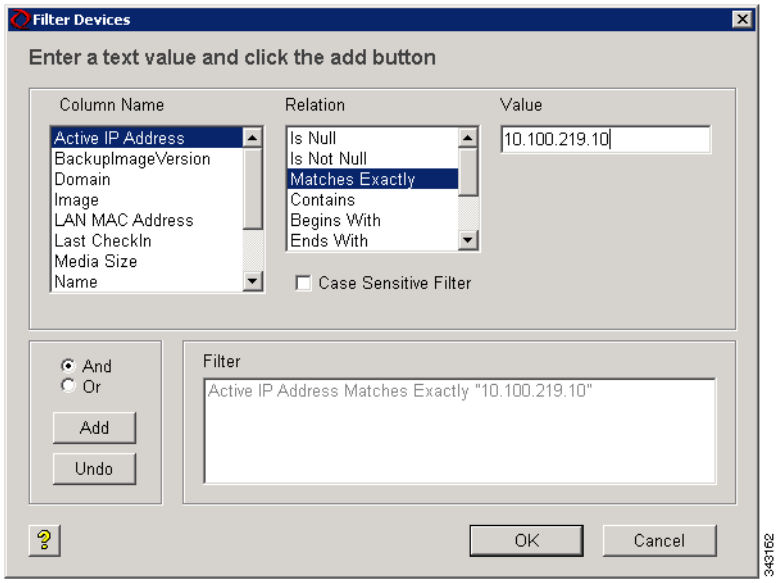
Creating a Device Filter

Create a Device Filter with Device Manager to quickly find the devices you want.

Procedure

Step 1 In the tree pane of the Administrator Console, right-click **Device Manager** and choose **Create Device Filter** to open the Filter Devices dialog box.

Figure 2-17 Device Filter



Step 2 Use the following guidelines when creating the filter:

- Choose the item you want in the Column Name list to display the Relation selections available for that Column Name.
- After you choose the item in the Relation list, you may need to enter a Value to be able to use the Case Sensitive Filter check box (depending on the item you choose).
- After you configure your item, you can add your item (click **Add**) to the Filter pane.
- When you add more than one item, you can click either the **And** radio button or the **Or** radio button before adding your item (click **Add**) to the Filter pane.
- To remove an item from the Filter pane, click **Undo**.

Step 3 After completing your criteria, click **OK** to create the filter for use.

Tip To use the Device Filter, right-click **Device Manager**, and then choose **Find Devices** to display the devices that match your filter criteria.

Editing a Device Filter

In the tree pane of the Administrator Console, right-click **Device Manager**, and then choose **Edit Device Filter** to open and use the Filter Devices dialog box.

Deleting a Device Filter

In the tree pane of the Administrator Console, right-click **Device Manager**, and then click **Remove Device Filter**.

Searching for a Device with Find Device in View and Quick Find

While you can use either of the Cisco VXC Manager search tools to find the devices you want, use the search tool best suited for your environment and needs as follows:

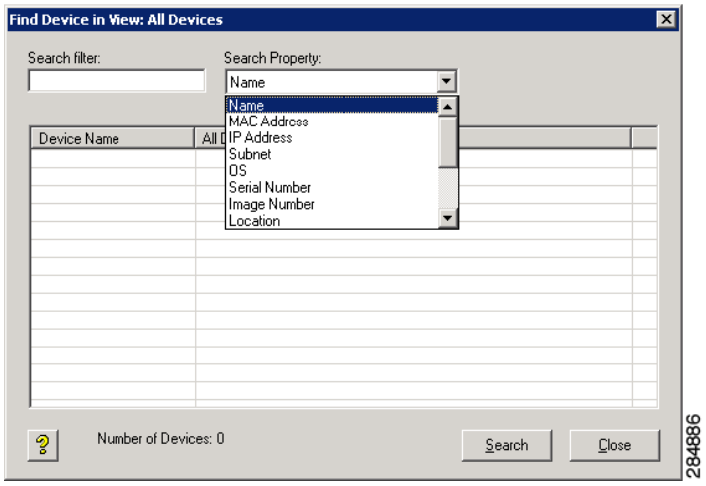
- Find Device in View—Useful in multiview environments to determine the View (path) in which the particular devices you want to find are located (see Using Find Device in View, page 2-22).
- Quick Find—Useful in single-view environments to quickly find the particular devices you want (see Using Quick Find, page 2-23).

Using Find Device in View

In the tree pane of the Administrator Console, right-click **Device Manager**, and then choose **Find Device in View** to open the Find Device in View dialog box displaying a list of all the devices in the view and the view path next to each device.

Tip You can also use the **Find Device in View** icon to open the dialog box.

Figure 2-18 Find Device in View Search

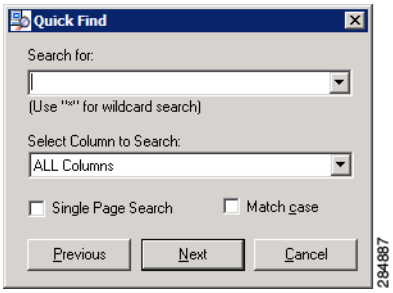


You can use the Search Filter field (enter your text) and Search Property field (choose a property) to filter and find the devices you want.

Using Quick Find

Right-click any device name in the Device Manager view and choose **Quick Find** to open and use the Quick Find dialog box.

Figure 2-19 Quick Find Search

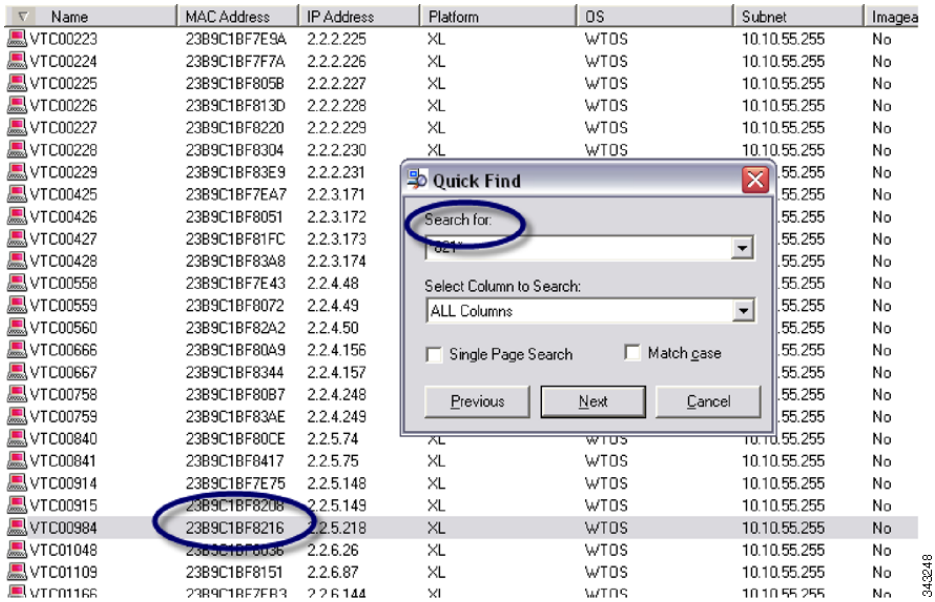


Tip Only devices in the currently displayed view can be searched.

Use the following guidelines when searching:

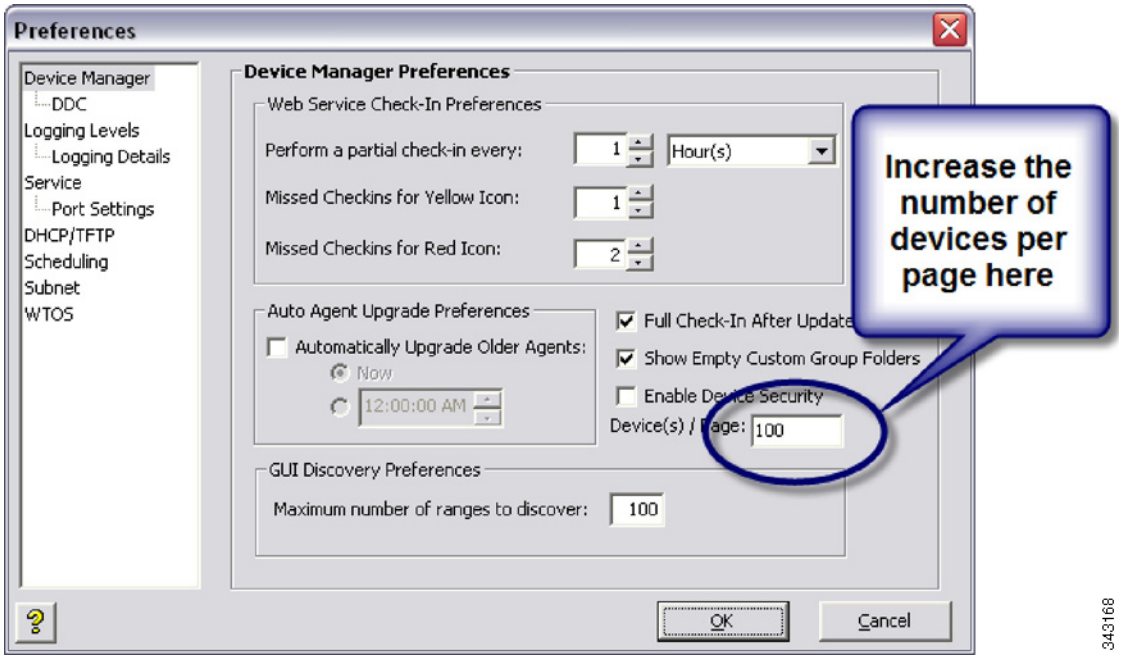
- Search for Options—There are two options for the Search For field:
  - Enter a search term, for example, **ABC**.
  - Choose a search term used previously from the drop-down menu. Your last 20 searches are displayed in this list.
- Wildcards—You can use wildcards in the Search for field. Enter an asterisk (*) at the beginning, the end, or both the beginning and end of an entry to represent additional characters.
- Select Column to Search Options—Allows you to search for your entry in all displayed columns or a specific column only.
- Single Page Search and Match Case Options—Use these check boxes to restrict your search to a single page or to consider the case of the letters in the Search for field.
- Direction of Your Search—Click **Previous** or **Next** to determine the direction of your search. Click **Next** to search forward from the top of each page to the bottom and from that page to the following page. Click **Previous** to search backward from the bottom of each page to the top and from that page to the previous page.
- Stop a Search—Click **Stop Searching** during a search.
- Results—When the search finds a device, the row that represents the device is highlighted in the Device Manager window (you can then click **Previous** or **Next** to find additional results). If your search produces no matches, the “Device not found” message appears.

Figure 2-20 Successful Search Results



Tip Searching across pages is much slower than searching the same number of devices when they are all displayed on a single page. To improve search performance, increase the number of devices displayed per page and enable the Single Page Search feature in the Quick Find dialog box. To increase the number of devices displayed on a page, use the Device Manager Preferences window, as shown in Figure 2-21.

Figure 2-21 Devices Displayed on a Single Page

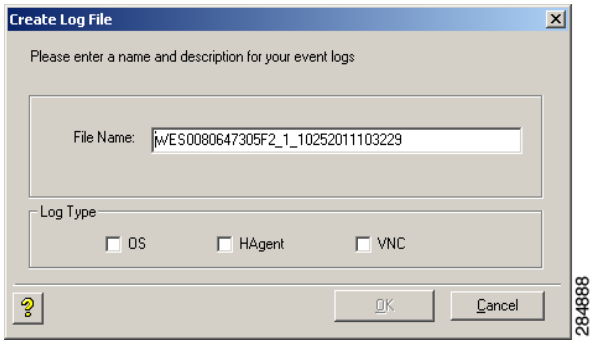


Creating and Viewing Log Files

To create log files that you can view, right-click a device in the details pane of the Device Manager and choose **Get Logs** (enter a name, choose the type of log file you want, and then click **OK**).

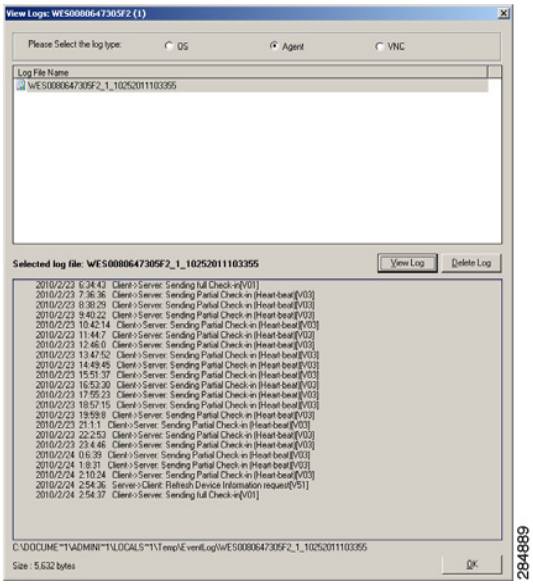
Note Support of this feature is platform dependent. It is supported only on Cisco VXC 6215 and Cisco VXC 2111/2211.

Figure 2-22 Creating Log Files



To choose the log file you want to view, right-click a device in the details pane of the Device Manager and choose **View Log** (choose the type of log file you want, choose the log file name you want, and then click **View Log**).

Figure 2-23 Viewing Log Files



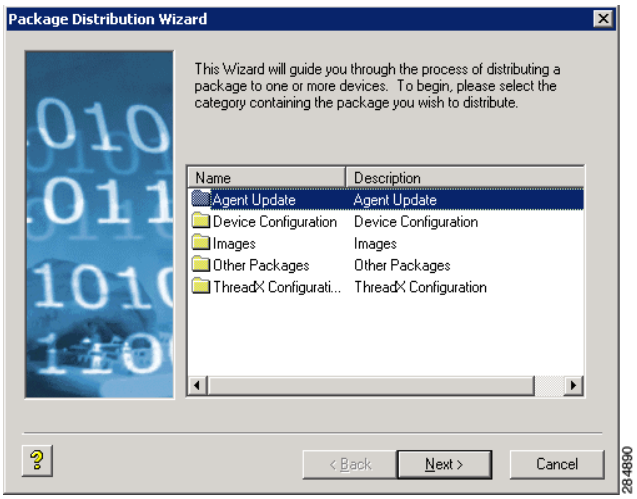
Tip To delete the log files you no longer need, choose a log file name and click **Delete Log**.

Using the Package Distribution Wizard to Schedule a Package for Distribution

Step 1 Switch to the view containing the devices you want.

Step 2 In the Device Manager details pane, choose the devices to which you want to schedule a package distribution (you can use Ctrl-click or Shift-click to choose multiple devices), right-click the selected devices, and then choose **Package Distribution Wizard** to open the Package Distribution Wizard.

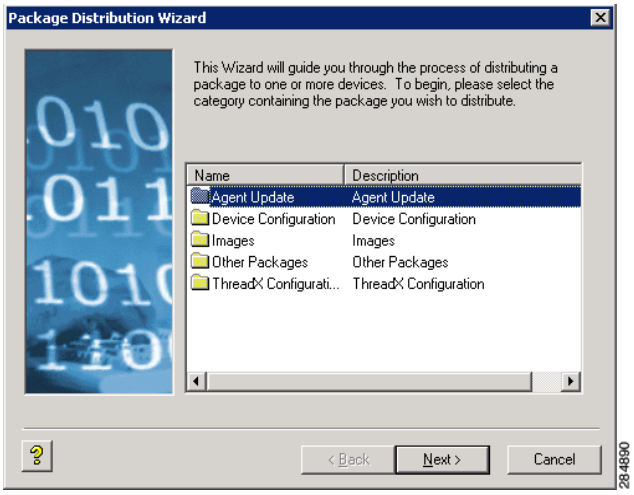
Figure 2-24 Package Category Selection



Step 3 Choose the package category folder that contains the registered package you want to distribute and click **Next**.

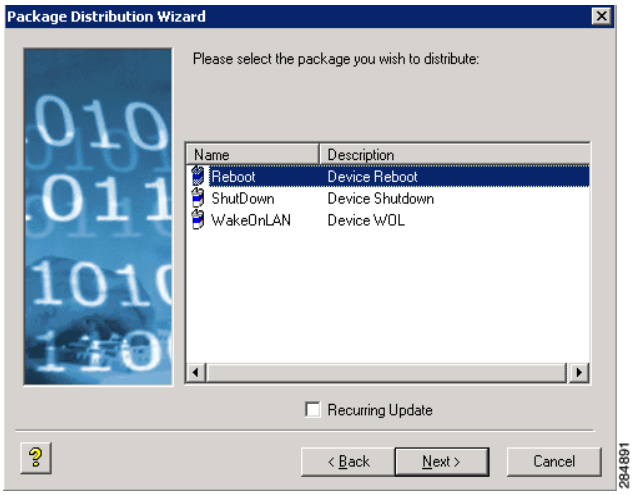
Note Only images that support the operating system and flash size of the previously selected device groups view are displayed.

Figure 2-25 Package Selection



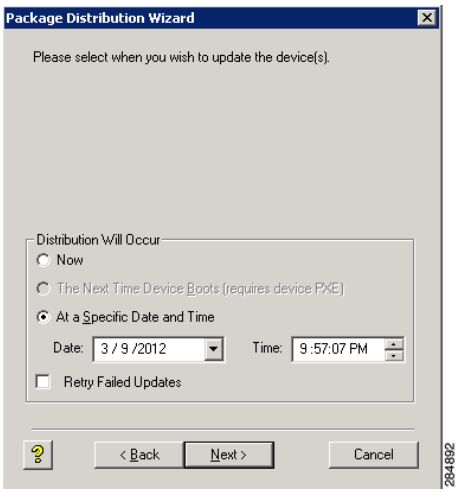
Step 4 Choose the package you want and click **Next**.

Figure 2-26 Package Schedule



Step 5 Choose the scheduling options for the distribution, and then click **Next**.

Figure 2-27 Create Schedule



Step 6 Choose the imaging option you want and click **Next**.

Step 7 After the package schedule is completed (update creation process is complete in the database), click **Finish**.

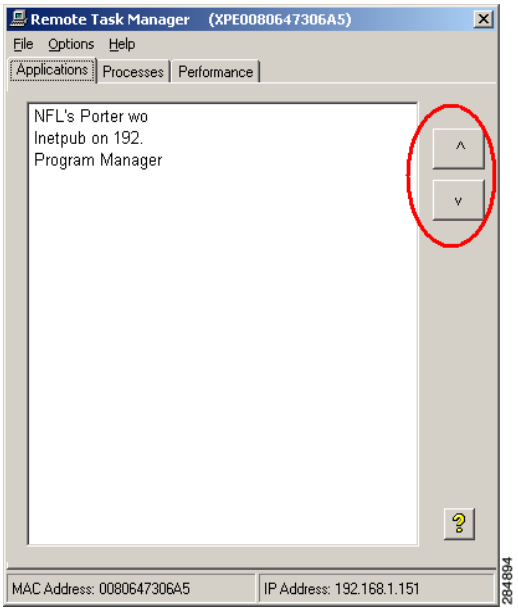
Using the Remote Task Manager to View Applications, Processes, and Performance for a Device

Step 1 Switch to the view containing the device you want.

Step 2 In the Device Manager details pane, choose the single device for which you want to view the applications, processes, and performance.

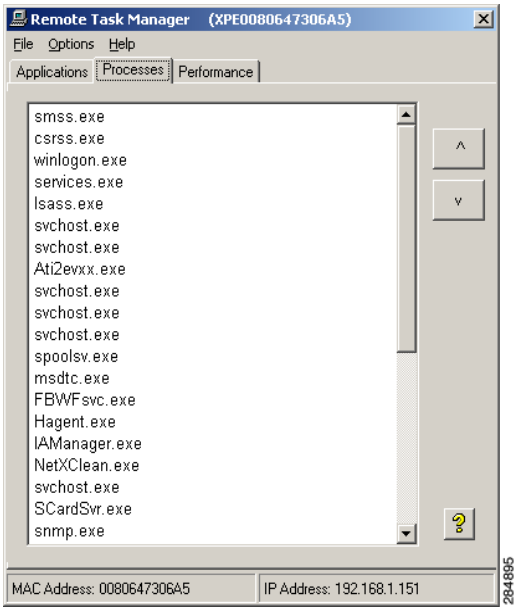
Step 3 Right-click the selected device, and then choose **Remote Task Manager** to open the Remote Task Manager.

Figure 2-28 Applications Tab



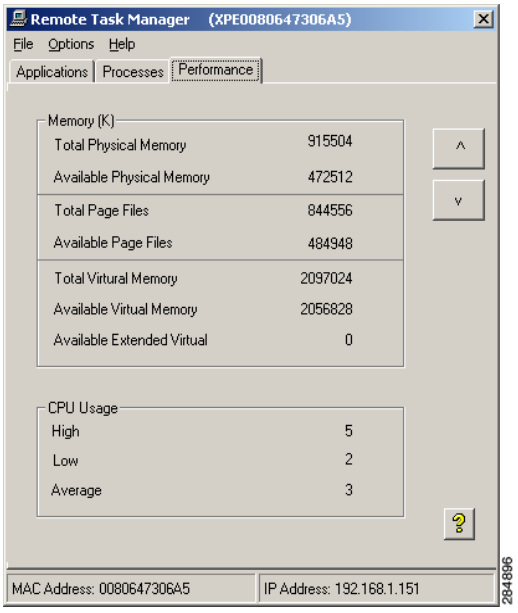
Step 4 On the Applications tab you can view the applications of the selected device (the window title bar displays the name of the device; the Mac address and IP address are displayed in the window status bar). You can also use the up arrow and down arrow to quickly display the information for the next or the previous device in the Device Manager details pane you previously selected. To refresh information, click **Options > Refresh**.

Figure 2-29 Processes Tab



Step 5 On the Processes tab you can view running processes of the selected device (the window title bar displays the name of the device; the Mac Address and IP Address are displayed in the window status bar). You can also use the up-arrow and down-arrow to quickly display the information for the next or the previous device in the Device Manager details pane you previously selected.

Figure 2-30 Performance Tab



Step 6 On the Performance tab you can view the Memory, Total Page Files, Total Virtual Memory, and CPU Usage fields for the selected device (the window title bar displays the name of the device; the MAC address and IP address are displayed in the window status bar). You can also use the up-arrow and down-arrow to quickly display the information for the next or the previous device in the Device Manager details pane you previously selected.

CHAPTER 3

Package Manager

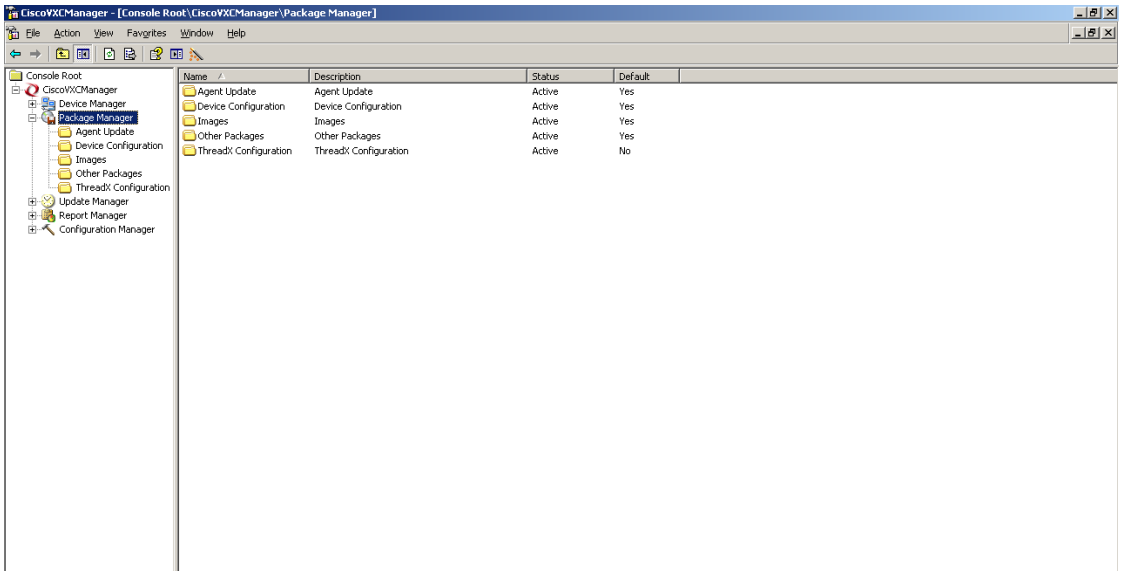
This chapter describes how to perform routine Cisco VXC Manager package management tasks using the Administrator Console. It provides information on managing the Cisco VXC Manager packages (software, images, configurations, and so on) that can be distributed to the devices within your Cisco VXC Manager environment.

For detailed instructions for managing packaging for Cisco VXC clients, see Chapter 4, “Cisco VXC Firmware and Configuration Upgrade Procedures”.

Managing Cisco VXC Manager Packages

Click **Package Manager** in the tree pane of the Cisco VXC Manager Administrator Console to open the Package Manager. The Package Manager allows you to quickly view and manage the Cisco VXC Manager packages that can be distributed to the devices within your Cisco VXC Manager environment (see Table 3-1). It also allows you to easily display the Cisco VXC Manager packages you want by using the available filtering and customizing features.

Figure 3-1 Package Manager



Before you use the Package Wizard to create and register Cisco VXC Manager packages, you should understand the update distribution process and the contents of Cisco VXC Manager packages, know the location of the existing Cisco VXC Manager packages that you want to register, and ensure that the devices from which you are getting images or configurations already have the Cisco VXC Manager Agent (HAgent) installed. After Cisco VXC Manager packages are registered, you can distribute them as updates to the devices within your Cisco VXC Manager network (see Update Manager, page 5-29).

Tip If you intend to perform Cisco VXC Manager package registration and scheduling for all of the devices in your Cisco VXC Manager system at the same time, the Cisco VXC Manager Mass Imaging Tool can be a convenient way for you to easily perform these tasks (see Using the Cisco VXC Manager Mass Imaging Tool, page D-17).

Table 3-1 provides a quick overview of what you can do using the Package Manager.

Table 3-1 Routine Package Manager Tasks

Tasks You Can Do	How	Details
Create and register a Cisco VXC Manager package from a script file so it is ready to be distributed.	In the tree pane of the Administrator Console, right-click **Package Manager**, choose **New > Package** to open the Package Wizard, choose the **Register a Package from a Script File (.RSP)** option, and then follow the wizard.	Register a Package from a Script File (.RSP), page 3-35 **Tip** For information on script files, see Cisco VXC Firmware and Configuration Upgrade Procedures, page 4-1
Create and register a configuration from a device running Enhanced SUSE Linux Enterprise so it is ready to be distributed.	In the tree pane of the Administrator Console, right-click **Package Manager**, choose **New > Package** to open the Package Wizard, choose the **Register a Configuration from a** Device option, and then follow the wizard. **Tip** You can also right-click the reference device and choose **Get Device Configuration** to open and use the Package Wizard.	Registering a Configuration from Devices Running Enhanced SUSE Linux Enterprise, page 3-36
Create and register a ThreadX package so it is ready to be distributed.	Use the guidelines in Updating the PCoIP Client Configuration (Building and Registering a ThreadX Package), page 4-11. After you create these packages, you can drag and drop a package to the devices you want, and then schedule their deployment accordingly.	Updating the PCoIP Client Configuration (Building and Registering a ThreadX Package), page 4-11
View the details of a registered Cisco VXC Manager package.	In the tree pane of the Administrator Console, expand **Package Manager** and choose the folder that contains the Cisco VXC Manager package. In the details pane, right-click the Cisco VXC Manager package and choose **Properties**.	Viewing the Details of a Registered Cisco VXC Manager Package, page 3-37

Table 3-1 Routine Package Manager Tasks (continued)

Tasks You Can Do	How	Details
View and change the script of a registered Cisco VXC Manager package.	In the tree pane of the Administrator Console, expand **Package Manager** and choose the folder that contains the Cisco VXC Manager package. In the details pane, right-click the Cisco VXC Manager package and choose **View Package Script** to open and use the Package Script dialog box.	Viewing and Changing the Script of a Registered Cisco VXC Manager Package, page 3-39  **Caution** You cannot modify the script for default Cisco VXC Manager packages

Table 3-1 Routine Package Manager Tasks (continued)

Tasks You Can Do	How	Details
Export the script of a registered Cisco VXC Manager package to a folder you want.	In the tree pane of the Administrator Console, expand **Package Manager** and choose the folder that contains the Cisco VXC Manager package. In the details pane, right-click the Cisco VXC Manager package and choose **Export Package Script** to open and use the Browse for Folder dialog box.	Exporting the Script of a Registered Cisco VXC Manager Package, page 3-40
Delete a registered Cisco VXC Manager package from the system.	In the tree pane of the Administrator Console, expand **Package Manager** and choose the folder that contains the Cisco VXC Manager package. In the details pane, right-click the Cisco VXC Manager package, choose **Delete**, and then confirm the deletion. **Tip** You can use Ctrl-click or Shift-click to choose multiple Cisco VXC Manager packages.	You cannot delete default Cisco VXC Manager packages. You cannot delete a registered Cisco VXC Manager package that is scheduled for distribution; you must first delete the scheduled update as described in Managing the Schedules for Device Updates, page 5-29 before you can delete a registered Cisco VXC Manager package. **Caution** When you delete a registered Cisco VXC Manager package that has never been distributed, Cisco VXC Manager also deletes it from the Cisco VXC Manager Repository. The Cisco VXC Manager package is recoverable only if you have a copy of it outside of Cisco VXC Manager. In such a case, you can re-register the Cisco VXC Manager package. **Tip** If you delete a Cisco VXC Manager package that has already been distributed, you can recover it from the Backup folder of the Cisco VXC Manager Repository and re-register it. When archived, a Cisco VXC Manager package receives a date-stamped name, therefore, before re-registering an archived Cisco VXC Manager package, you must rename it to its original name.

Register a Package from a Script File (.RSP)

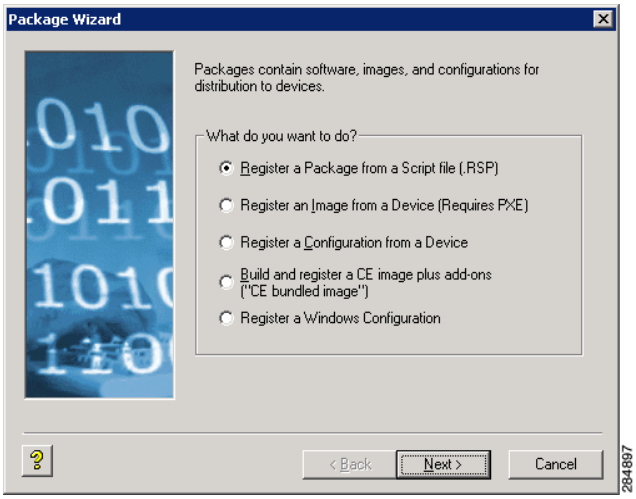
Caution When you register Cisco VXC Manager packages, be sure you have write permissions to the directory where the Cisco VXC package files are located and to the configured Cisco VXC Manager software repository location. If you attempt to register a package without the correct write permissions, registration errors can occur.

Use the following procedure to register a package from an RSP script file.

Procedure

Step 1 In the tree pane of the Administrator Console, right-click **Package Manager** and choose **New > Package** to open the Package Wizard.

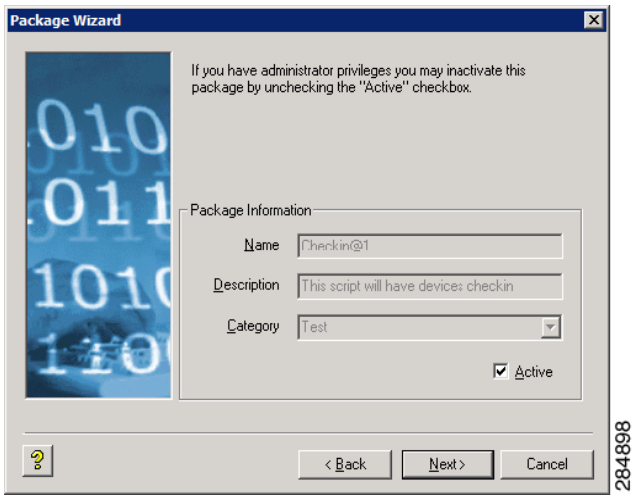
Figure 3-2 Package Wizard



Step 2 Choose the **Register a Package from a Script File (.RSP)** option and click **Next**.

Step 3 Enter the File Path to the Cisco VXC Manager script (RSP) file for the Cisco VXC Manager package (for example, push_9V92_S550_512.rsp) you want to register (you can use **Browse** to find and choose a file), and then click **Next** to open the Software Package Information dialog box.

Figure 3-3 Software Package Information



Step 4 The Software Package Information dialog box displays the Name, Description, and Category of the Cisco VXC Manager package specified in the RSP file.

Step 5 Depending on whether or not you want to have the Cisco VXC Manager package distributed (active for distribution), check or uncheck the **Active** check box.

Step 6 Click **Next**. The wizard notifies you that is ready to create and register the new Cisco VXC Manager package.

Step 7 Click **Next** to create and register the Cisco VXC Manager package.

Step 8 After the Cisco VXC Manager package has been created and registered, click **Finish**. Cisco VXC Manager copies the package to the Master Repository and displays the package under the appropriate category. The Cisco VXC Manager package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

Registering a Configuration from Devices Running Enhanced SUSE Linux Enterprise

This Package Wizard option pulls a configuration from a device (such as a reference device) to easily configure (clone) similar devices within your Cisco VXC Manager installation.

Tip This functionality is supported only on clients running Enhanced SUSE Linux Enterprise.

Prior to using the Package Wizard to pull and register the configuration from a Reference Device, ensure that:

- The reference device supports Pre-boot Execute Environment (PXE).
- You have configured the reference device to fulfill your specifications.
- You have tested the reference device and resolved any issues.

After you ensure your reference device is ready, you can continue using the Package Wizard to pull and register the configuration from the device in accordance with the following procedure.

Procedure

Step 1 In the tree pane of the Administrator Console, right-click **Package Manager** and choose **New > Package** to open the Package Wizard.

Tip You can also right-click the Reference Device in the details pane of the Device Manager and choose **Get Device Configuration** to open the Package Wizard.

Step 2 Choose the **Register a Configuration from a Device** option and click **Next**.

Step 3 Enter a name and description for the Cisco VXC Manager package (the new Cisco VXC Manager package will remain inactive until Cisco VXC Manager successfully retrieves the configuration from the Reference Device).

Step 4 Click **Next**. The wizard notifies you that is ready to create and register the new Cisco VXC Manager package.

Step 5 Click **Next** to create and register the Cisco VXC Manager package.

Step 6 After the Cisco VXC Manager package has been created and registered, click **Finish**. The Cisco VXC Manager package is copied to the Master Repository and is displayed under the appropriate category. The Cisco VXC Manager package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

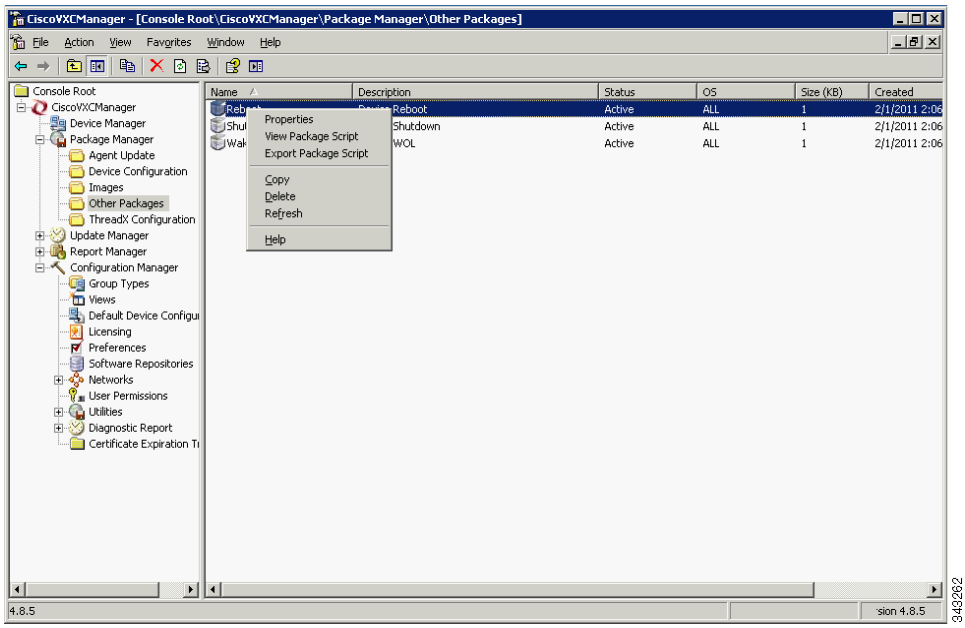
Viewing the Details of a Registered Cisco VXC Manager Package

Use the following procedure to view the details of a registered Cisco VXC Manager package.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Package Manager** and choose the folder that contains the Cisco VXC Manager package you want to view.

Figure 3-4 Cisco VXC Manager Package Properties



Step 2 In the details pane, right-click the Cisco VXC Manager package and choose **Properties** to open the Edit Package dialog box displaying the details of the Cisco VXC Manager package.

Figure 3-5 Edit Package

The Edit Package dialog box contains the following fields:

- Name—Name of the Cisco VXC Manager package.
- Description—Description of the Cisco VXC Manager package.
- Active—If selected, allows distribution of the Cisco VXC Manager package to a device; if cleared, the Cisco VXC Manager package cannot be distributed to a device.
- Operating System—The operating system for which this Cisco VXC Manager package is compatible.
- Size—Size of the Cisco VXC Manager package in kilobytes.
- Date Created—Cisco VXC Manager package creation date and time.

Viewing and Changing the Script of a Registered Cisco VXC Manager Package

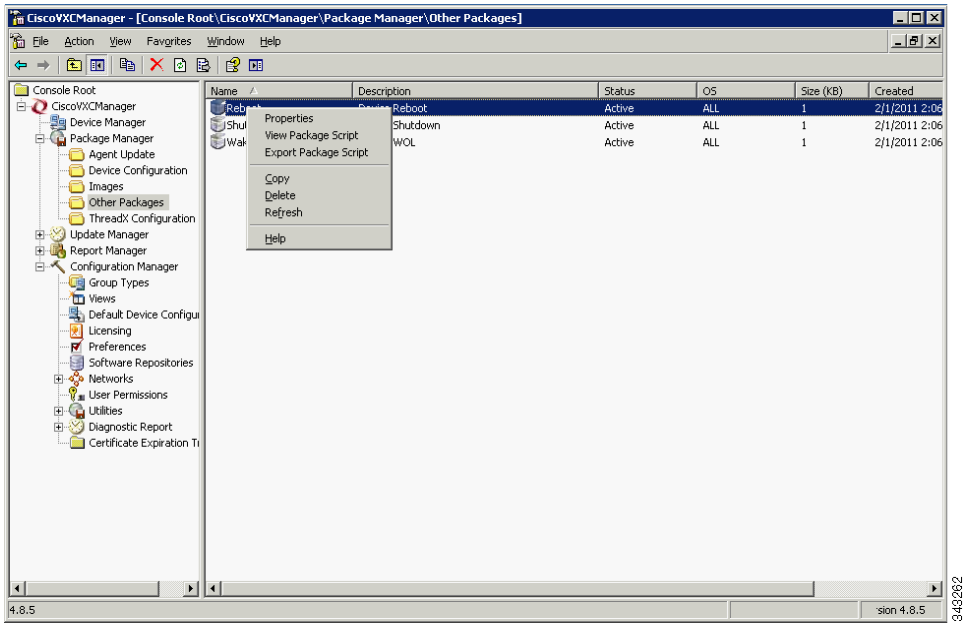
Cisco VXC Manager Scripting Language is a simplified scripting language that you can use to build your own Cisco VXC Manager packages. You can also use it to perform basic tasks such as copying files and modifying the registry of the devices that Cisco VXC Manager manages. Cisco VXC Manager Scripting Language is not a programming language (it does not support looping, branching, and the use of subroutines). However, it does contain a small command set to allow it to perform a variety of routine functions such as checking the operating system version on a given device.

Caution You cannot modify the script for default Cisco VXC Manager packages.

Procedure

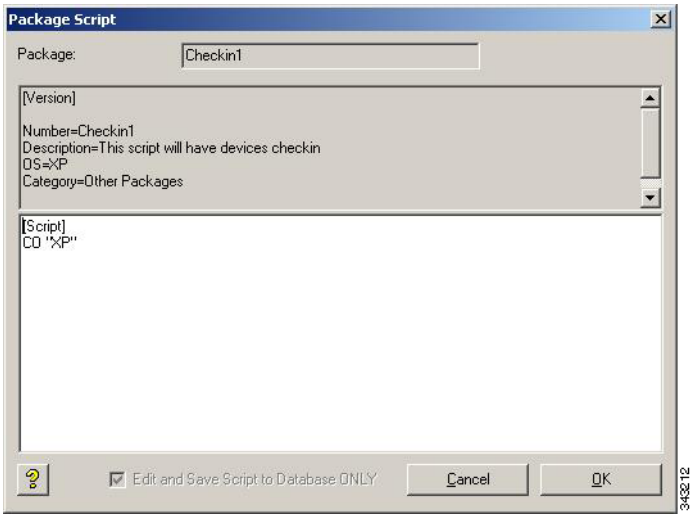
Step 1 In the tree pane of the Administrator Console, expand **Package Manager** and choose the folder that contains the Cisco VXC Manager package you want to view.

Figure 3-6 View Cisco VXC Manager Package Script



Step 2 In the details pane, right-click the Cisco VXC Manager package and choose **View Package Script** to open the Package Script dialog box displaying the script of the Cisco VXC Manager package.

Figure 3-7 Package Script



Step 3 Choose the **Edit and Save Script to Database ONLY** check box and then make your changes to the script of the RSP file.

Step 4 After completing your changes, click **OK**.

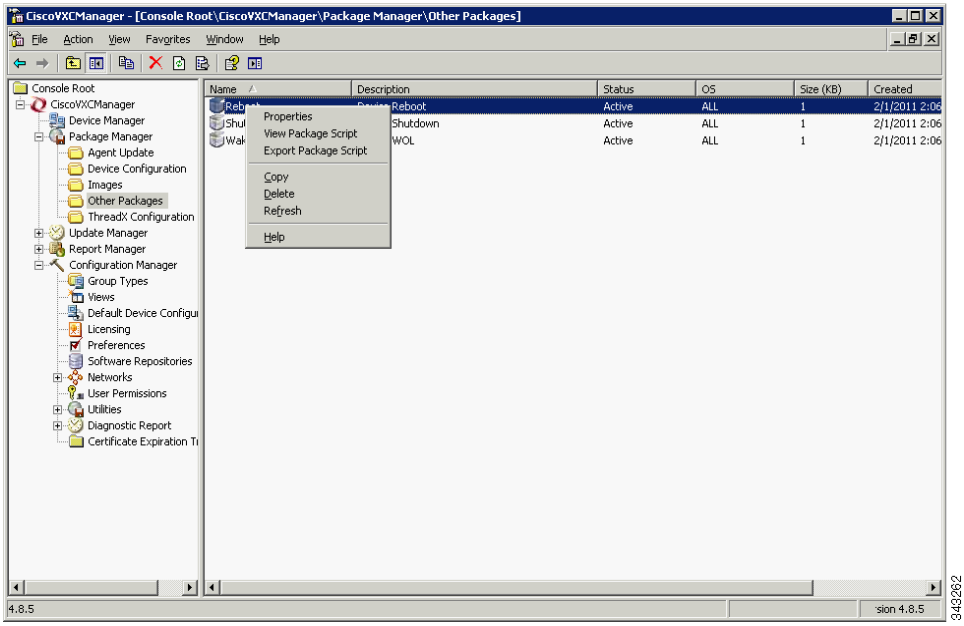
Exporting the Script of a Registered Cisco VXC Manager Package

Use the following procedure to export the script of a registered Cisco VXC Manager package.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Package Manager** and choose the folder that contains the Cisco VXC Manager package you want to view.

Figure 3-8 View Cisco VXC Manager Package Script



Step 2 In the details pane, right-click the Cisco VXC Manager package, and choose **Export Package Script** to open the Browse for Folder dialog box.

Step 3 Choose the folder to which you want to export the script, and then confirm.

CHAPTER 4

Cisco VXC Firmware and Configuration Upgrade Procedures

This chapter provides information on the procedures required to upgrade firmware images and configurations on Cisco VXC 6215 clients (running SUSE Linux firmware), Cisco VXC 2211/2211 PCoIP clients (running ThreadX firmware), and Cisco VXC 2112/2212 ICA clients (running WTOS firmware) using Package Manager.

It contains the following information:

Cisco VXC 6215 Upgrade Procedures

You can use Cisco VXC Manager to manage Cisco VXC 6215 clients using similar procedures as those required for the management of the Cisco VXC 2112/2212 ICA-protocol clients.

Management Architecture

The following sections provide a brief overview of the features of the Cisco VXC 6215 that are relevant for its management. For more information on the Cisco VXC 6215, see *Cisco Virtualization Experience Client 6215 Administration Guide*.

Operating System: Cisco-Enhanced SUSE Linux

Cisco VXC 6215 clients run a Cisco-enhanced version of SUSE Linux that is optimized to run Internet browsers, virtualization clients, remote desktop protocols, and other productivity software like unified communications.

Cisco VXC Manager Agent: HAgent for SUSE Linux

The Cisco VXC Manager Agent, also referred to as the HAgent, is installed on the Cisco VXC 6215 for communicating management messages with the Cisco VXC Manager.

INI files for Client Configuration

Cisco VXC 6215 uses INI files for configuration of the device. See *Cisco Virtualization Experience Client 6215 INI Files Reference Guide* for details.The INI settings are applied at boot time or when a user logs out of a device.The INI files can be automatically deployed to Cisco VXC 6215 using an FTP server (see "Appendix A: Central Configuration: Automating Updates and Configurations" of the *Cisco Virtualization Experience Client 6215 Administration Guide*) or using the Default Device Configuration (DDC) mechanism of Cisco VXC Manager (see Updating the Cisco VXC 6215 Operating System Image, page 4-2).

Device Discovery

Upon boot up, the Cisco VXC 6215 clients follow the automated discovery process described in Adding and Automatically Discovering Devices, page 2-13. Administrators can also run the manual discovery process described in Adding Devices Manually, page 2-15. After a client has checked in (or registered) with Cisco VXC Manager, it appears in the Cisco VXC Manager interface and can then be managed. During the first check-in, the Cisco VXC Manager Agent for the client also provides a complete hardware and software inventory. To refresh this information, right-click a device in the details pane of the Device Manager and choose **Refresh Device Information**.

Heartbeats and Health Status

Cisco VXC Manager Agents on the Cisco VXC 6215 send heartbeat check-ins according to the interval specified in the Configuration Manager preferences. The default check-in time is one hour.

Updating the Cisco VXC 6215 Operating System Image

To update the firmware image on the Cisco VXC 6215, perform the following procedure.

Note If the Cisco VXC 6215 is running the Voice and Video Firmware Add-on, after you upgrade the Base VDI firmware, you must install the compatible release of the Voice and Video Firmware Add-on. See Register a Package to Enable a Cisco Add-On, page 4-6.

Procedure

Step 1 Download or copy the OS image from the Cisco Software Download page at the following URL: http://www.cisco.com/cisco/software/navigator.html

Choose **Products > Voice and Unified Communications > IP Telephony > Virtualized Endpoints > Cisco Virtualization Experience Client 6000 Series > Cisco Virtualization Experience Client 6215**.

Step 2 On the server where you have Cisco VXC Manager installed, extract the zipped OS image files to a local folder.

Step 3 In the extracted wlx.ini file, do not modify the existing parameters, but add any additional INI configurations you require.

Note If you have existing INI configurations on your clients, you must copy and paste these parameters into the wlx.ini that you push with the update; otherwise, the clients will lose the pre-existing configurations.

Step 4 Register the package (see Register a Package from a Script File (.RSP), page 3-35). When you are prompted for an RSP file during the package registration process, browse and choose the RSP file that is contained in the unzipped package.

Step 5 To upgrade the Cisco VXC 6215, you can use Default Device Configuration or use the Drag-and-Drop method (see Managing Default Device Configurations, page 7-66 and Scheduling Device Updates Using the Drag-and-Drop Method, page 5-35)

Note If you downgrade a Cisco VXC 6215 thin client from a newer Image DDC (for example, DDC_10) to any older Image DDC (for example, DDC_09), and then try to re-apply the newer image DDC to the client, the operation fails. To successfully re-apply the newer image DDC (DDC_10) to the thin client after a downgrade, you must first rename the newer image DDC using Cisco VXC Manager (for example, to DDC_10a).

Packaging and Deploying Cisco VXC 6215 Add-On Packages

This section describes how to perform additional Cisco VXC Manager package management tasks for the Cisco VXC 6215 add-on packages.

Note This section contains additional Package Manager procedures that are applicable only to the Cisco VXC 6215 add-ons.

Cisco VXC 6215 Default Add-Ons

The Cisco VXC 6215 firmware includes default add-ons that provide increased security for the thin client and minimize the exposure of the SUSE Linux base operating system to users, while still providing users with useful functionality.

Add-ons are feature-specific software components that provide additional customized functionality on the Cisco VXC 6215 thin clients without affecting the underlying operating system files.

The Cisco add-on applications bundled by default on the Cisco VXC 6215 include the following:

Autologin

The Autologin (autologin-1.0-2.sletc11sp1.rpm) add-on allows the Cisco VXC 6215 to boot using the thin user credentials without requiring the user to provide the credentials.

After the thin client boots up, the login screen initially appears, and after approximately 10 to 15 seconds, the thin client automatically logs the user into the thin client using thinuser/thinuser as the default username and password.

Caution For proper operation of the Cisco VXC 6215, the Autologin add-on must always be enabled and running on the thin client (the default configuration). Do not remove or disable the Autologin add-on as this is an unsupported configuration. Operation with the Autologin add-on enabled is the only supported mode of operation. If you do remove the Autologin add-on, you must reinstall it by reinstalling the latest Base VDI Firmware Release available on cisco.com.

CiscoConfig

The CiscoConfig add-on (ciscoconfig-1.0-2.sletc11sp1.rpm) provides additional functionality to the user beyond that provided by the Autologin add-on. With the CiscoConfig add-on, the Cisco VXC 6215 provides access to additional applications including system information, display settings, Cisco VXC Manager settings, and the Firefox Browser though the Application Browser (**Computer > More Applications**).

Caution As the CiscoConfig add-on is required for proper functioning of the Autologin add-on, the CiscoConfig add-on must always be enabled and running on the thin client (the default configuration). If you do remove the CiscoConfig add-on, you must reinstall it by reinstalling the latest Base VDI Firmware Release available on cisco.com.

Ssh_opt

The Cisco VXC 6215 can support remote connections to the thin client using SSH. To provide increased security, the ssh_opt add-on (ssh_opt-1.0-1.0.sletc11sp1.rpm) disables SSH functionality by default. To allow remote SSH access to the client, the administrator can disable this add-on.

Note To enable the SSH functionality on the Cisco VXC 6215 devices using Cisco VXC Manager, in the Device Manager, right-click the device and choose **Execute Command**. In the Execute Command dialog box, type **/etc/init.d/sshd start** to enable the SSH functionality. If the Ssh_opt add-on is installed on the Cisco VXC device, then the Ssh_opt add-on sets the OpenSSH idle timeout to 30 mins and the maximum timeout to 60 mins. (These default SSH idle timeout values cannot be modified.)

Optional Voice and Video Firmware Add-On

To support Unified Communications on the Cisco VXC 6215, you must purchase and install the Voice and Video Firmware add-on. The optional Voice and Video Firmware add-on provides Unified Communications functionality for Cisco UC Integration for Microsoft Lync and Cisco Unified Personal Communicator.

With the Voice and Video Firmware add-on, users in a virtual environment can use Cisco UC Integration for Microsoft Lync or Cisco Unified Personal Communicator from their thin clients. The Voice and Video Firmware runs on the thin client, and Cisco UC Integration for Microsoft Lync or Cisco Unified Personal Communicator runs on the Windows hosted virtual desktop.

Power Management Settings with Voice and Video Firmware Add-On

By default, the Cisco VXC 6215 supports a power management setting (EnergyWise) whereby the clients enter the sleep mode after a specified period of time. When the Voice and Video Firmware add-on is enabled, this power management setting is disabled, and the clients do not enter the sleep mode.

For more information on the optional Voice and Video Firmware add-on, see the *Deployment Guide for Voice and Video Firmware for Cisco Virtualization Experience Client 6215.*

Downloading the Cisco VXC Add-On Software Packages

To download the Cisco VXC 6215 add-on software packages, follow these steps:

Procedure

Step 1 From your workstation, access http://www.cisco.com/cisco/software/navigator.html.

Step 2 Sign in with your Cisco.com user ID and password.

Step 3 On the Download Software page:

a. Choose **Products > Voice and Unified Communications > IP Telephony > Virtualized Endpoints**.

b. When the next page appears, choose **Cisco Virtualization Experience Client 6000 Series**.

c. Choose **Cisco Virtualization Experience Client 6215**.

d. In the the Add Ons folder, choose the add-on you require.

e. Click the **Download** button next to the WinZip file to launch a window with detailed information about the selected release and to add it to the Download Cart.

Step 4 Verify that the software and image information are what you want, and click **Proceed With Download**.

Step 5 Accept the conditions by entering the appropriate information into the User Details section and by clicking **Accept**.

Step 6 Read the Cisco End User License Agreement, and click **Agree**.

Step 7 Download and save the Cisco VXC 6215 add-on zip file to your workstation.

Step 8 Locate the saved file on the host or workstation, and unzip the file to your local drive or disk.

Managing Cisco VXC Manager Add-On Packages

Click **Package Manager** in the tree pane of the Cisco VXC Manager Administrator Console to open the Package Manager. The Package Manager allows you to quickly view and manage the Cisco VXC Manager packages that can be distributed to the devices within your Cisco VXC Manager environment.

Before using the Package wizard to create and register Cisco VXC Manager packages, you must understand the update distribution process and the contents of Cisco VXC Manager packages, know the location of the existing Cisco VXC Manager packages that you want to register, know the location of the base image, and know the add-ons you want to add to it when you create the bundled images. You must also ensure that the devices from which you will be getting images or configurations already have the Cisco VXC Manager Agent installed. After Cisco VXC Manager packages are registered, you can distribute the packages as updates to the devices within your Cisco VXC Manager network (see Update Manager, page 5-29).

Register a Package to Enable a Cisco Add-On

Use the following procedure to enable a Cisco add-on.

Procedure

Step 1 On the server on which you have Cisco VXC Manager installed, extract the add-on files to a local folder (see Downloading the Cisco VXC Add-On Software Packages, page 4-5).

Note Assuming an add-on named ciscoaddontest1, the extracted add-on folder structure appears as follows:
~/ciscoaddontest1/wlx/wlx.ini
~/ciscoaddontest1/ADDONS/<rpmfilename>.rpm
~/ciscoaddontest1/ADDONS/directory
~/ciscoaddontest1.rsp

Step 2 In the extracted wlx.ini file, do not modify the existing parameters, but add any additional INI configurations you require.

Note If you have existing INI configurations on your clients, you must copy and paste these parameters into the wlx.ini that you push with the add-on; otherwise, the clients will lose the pre-existing configurations.

Step 3 In the tree pane of the Administrator Console, right-click **Package Manager** and choose **New > Package** to open the Package wizard.

Step 4 Click the **Register a Package from a Script File (.RSP)** option and click **Next**.

Step 5 Enter the file path to the Cisco VXC Manager script file (RSP) file for the Cisco VXC Manager package (for example, ciscoaddontest1.rsp) you want to register (you can use Browse to find and choose a file), and then click **Next** to open the Software Package Information dialog box.
The wizard obtains and displays the name, description, and category of the Cisco VXC Manager package.

Step 6 To have the Cisco VXC Manager package active for distribution, check the **Active** check box.

Step 7 Click **Next**.
The wizard notifies you that it is ready to create and register the new Cisco VXC Manager package.

Step 8 Click **Next** to create and register the Cisco VXC Manager package.

Step 9 After the Cisco VXC Manager package is created and registered, click **Finish**.
The Cisco VXC Manager package is copied to the Master Repository and is displayed under the appropriate category. The Cisco VXC Manager package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

Register a Package to Disable a Cisco Add-On

There are two methods that you can use to disable a Cisco add-on, using either a remove-packages.sh file or a RemoveAddons INI parameter, as described in the following procedures.

Note You can uninstall add-ons using Cisco VXC Manager; however, when you upgrade the device to a new version of firmware, these add-ons may be reenabled in the updated firmware.

Disabling an Add-On Using the remove-packages.sh File

Use the following procedure to disable a Cisco add-on using the remove-packages.sh file.

Procedure

Step 1 On the server on which you have Cisco VXC Manager installed, create a new folder for the add-on.

Step 2 Within this folder, create an RSP file with a name that starts with the ciscoaddon prefix, for example, ciscoaddon-remove1.rsp.

Step 3 To disable an add-on package, verify that the content of the RSP file is as follows:

```
[Version]
Number=ciscoaddon-remove1
Description=Remove sample Cisco Add-on package
OS=SLX
Category=Other Packages
USE_Pxe=NO

[Script]
CO "SLC"
LU
SF "<regroot">/*" "/tmp/"
EX "dos2unix /tmp/remove=packages.sh"
EX 'sh /tmp/remove-packages.sh"
EL
RB
```

Step 4 In the RSP script, ensure that the "Number=" segment has the exact same value as the RSP filename.

Step 5 In the add-on folder, create a subfolder with a name that matches the RSP file name, for example, ciscoaddon-remove1.

Step 6 Within the subfolder you created, create the remove-packages.sh file.

The contents of the remove-packages.sh file must be as follows:

```
#!/bin/bash
for addon in ciscoaddon-remove1
do
/usr/sbin/addon-remove $addon
done
```

Note The folder structure and the corresponding files for the add-on deployment must be as follows:
~ /ciscoaddon-remove1.rsp
~ /ciscoaddon-remove1/remove-packages.sh

Step 7 In the tree pane of the Administrator Console, right-click **Package Manager** and choose **New > Package** to open the Package wizard.

Step 8 Click the **Register a Package from a Script File (.RSP)** option and click **Next**.

Step 9 Enter the file path to the Cisco VXC Manager script (RSP) file for the Cisco VXC Manager package (for example, ciscoaddon-remove1.rsp) you want to register (you can use Browse to find and choose a file), and then click **Next** to open the Software Package Information dialog box.
The wizard obtains and displays the name, description, and category of the Cisco VXC Manager package.

Step 10 Depending on whether you want to have the Cisco VXC Manager package distributed (active for distribution), check or uncheck the **Active** check box.

Step 11 Click **Next**.
The wizard notifies you that it is ready to create and register the new Cisco VXC Manager package.

Step 12 Click **Next** to create and register the Cisco VXC Manager package.

Step 13 After the Cisco VXC Manager package has been created and registered, click **Finish**.
The Cisco VXC Manager package is copied to the Master Repository and is displayed under the appropriate category. The Cisco VXC Manager package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

Disabling an Add-On Using the RemoveAddons INI Parameter

Use the following procedure to disable a Cisco add-on using the RemoveAddons INI parameter.

Procedure

Step 1 On the server on which you have Cisco VXC Manager installed, create a new folder for the add-on.

Step 2 Within this folder, create an RSP file with a name that starts with the ciscoaddon prefix, for example, ciscoaddon-remove2.rsp.

Step 3 If you want to disable an add-on package, verify that the content of the RSP file is as follows:

```
[Version]
Number=ciscoaddon-remove2
Description=Push and parse wlx.ini and image update package
OS=SLX
Category=Other Packages
USE_Pxe=NO

[Script]
EX "/bin/regset --persist System IniFileSource server"
RP "<regroot>"
EX "/usr/bin/perl /etc/addons.d/dispatcher.d/60.fetchIni eth0 up"
EX "/usr/bin/perl /sbin/dhcp2registry"
EX "/usr/sbin/thinclient-config --set-update-mode addons"
```

```
EX "sync"
EX "sleep 2"
RB
```

Step 4 In the RSP script, ensure that the “Number=” segment has the exact same value as the RSP filename and folder name.

Step 5 Within the add-on folder, create a subfolder with a name that matches the RSP file name, for example, ciscoaddon-remove2.

Step 6 Within this folder, create a subfolder named **wlx**.

Step 7 Within the wlx folder, create a wlx.ini file.

Note The folder structure and the corresponding files for the add-on deployment must be as follows:
`~/ciscoaddon-remove2/wlx/wlx.ini`
`~/ciscoaddon-remove2.rsp`

Step 8 Verify that the content of the wlx.ini file is as follows:

```
Update.Preserve_changes=Yes
Update.Mode=Addons
RemoveAddons=ciscoaddon-remove2.rpm
```

Step 9 In the wlx.ini file, ensure that the “RemoveAddons=” segment has the exact same value as the RPM filename of the add-on to remove.

Note If you are removing multiple add-ons, then you must specify all the RPM files in a comma-separated list in the RemoveAddon segment. For example:
RemoveAddons=ciscoaddon-remove2.rpm,ciscoaddon-remove3.rpm,ciscoaddon-remove4.rpm

Step 10 In the tree pane of the Administrator Console, right-click **Package Manager** and choose **New > Package** to open the Package wizard.

Step 11 Choose the **Register a Package from a Script File (.RSP)** option and click **Next**.

Step 12 Enter the file path to the Cisco VXC Manager script (RSP) file for the Cisco VXC Manager package (for example, ciscoaddontest1.rsp) you want to register (you can use Browse to find and choose a file), and then click **Next** to open the Software Package Information dialog box.
The wizard obtains and displays the name, description, and category of the Cisco VXC Manager package.

Step 13 Depending on whether you want to have the Cisco VXC Manager package distributed (active for distribution), check or uncheck the **Active** check box.

Step 14 Click **Next**.
The wizard notifies you that it is ready to create and register the new Cisco VXC Manager package.

Step 15 Click **Next** to create and register the Cisco VXC Manager package.

Step 16 After the Cisco VXC Manager package is created and registered, click **Finish**.
The Cisco VXC Manager package is copied to the Master Repository and is displayed under the appropriate category. The Cisco VXC Manager package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

Updating the Cisco VXC 6215 Client Configuration

Use this procedure to create a SUSE Linux package to upgrade the Cisco VXC 6215 client configuration.

Procedure

Step 1 Create a folder to contain the client configurations, for example 6215Configs.

Step 2 In the 6215Configs folder, create an RSP file named SLE1.rsp with the following content:

```
[Version]
Number=SLE1
OS=SLX
Category=Other Packages
USE_Pxe=NO
[Script]
RP "<regroot>"
EX "/usr/bin/perl /sbin/dhcp2registry"
EX "/usr/sbin/thinclient-config --set-update-mode both"
EX "/usr/sbin/thinclient-config --set-force-image-update no"
EX "sync"
EX "sleep 2"
RB
RB
```

where the "Number=" segment must have the exact same value as the RSP file name.

Note This RSP script is provided as an example; you may need to reconfigure the parameters depending on your environment.

Step 3 Also in the 6215Configs folder, create a subfolder using the same name as the RSP file name, for example SLE1.

Step 4 In the SLE1 folder, create a subfolder named wlx.

Step 5 In the wlx folder, create a file named wlx.ini that contains the required configuration. (See *Cisco Virtual Experience Client 6215 INI Files Reference Guide* for more information.) For example:

- Location and name of .rsp image:

  C:\VXC-M\6215Configs\SLE1.rsp
- Location and name of wlx directory:

  C:\VXC-M\6215Configs\SLE1\wlx
- Location and name of wlx.ini file in wlx directory:

  C:\VXC-M\6215Configs\SLE1\wlx\wlx.ini

Step 6 In the tree pane of the Administrator Console, expand **Package Manager**.

Step 7 In the details pane, right-click **Other Packages** and choose **New > Package**.

Step 8 Choose **Register a Package from a Script file (.RSP)** and click **Next**.

Step 9 Click **Browse** to choose the file path of the .rsp package file you want to register (For example: C:\VXC-M\6215Configs\SLE1.rsp) and click **Open**.

Step 10 Click **Next** to display the Package Wizard summary.

Step 11 Click **Next** to see the Package Registration Progress screen.

Step 12 Click **Next** to create the package.

Step 13 After the package is created and registered, click **Finish**.

Step 14 To upgrade the Cisco VXC 6215, you can use Default Device Configuration or use the Drag-and-Drop method (see Managing Default Device Configurations, page 7-66 and Scheduling Device Updates Using the Drag-and-Drop Method, page 5-35).

Cisco VXC 2111/2211 PCoIP Client Upgrade Procedures

The following sections describe how to update the PCoIP firmware image and client configurations:

Updating the PCoIP Firmware Image

To update the firmware image on a Cisco VXC PCoIP client, perform the following procedure.

Procedure

Step 1 Download the PCoIP image package from the Cisco Software Download page at the following URL:

http://www.cisco.com/cisco/software/navigator.html?mdfid=283759601&i=rm

Step 2 On the server where you have Cisco VXC Manager installed, extract the zipped firmware files to a local folder.

Step 3 Register the package (see Register a Package from a Script File (.RSP), page 3-35). When you are prompted for an RSP file during the package registration process, browse and choose the RSP file that is contained in the unzipped package.

Note To upgrade the image on PCoIP devices, the Category parameter in the RSP file must be set to Images (Category=Images).

Step 4 To upgrade the Cisco VXC 2111/2211, you can use Default Device Configuration or use the Drag-and-Drop method (see Managing Default Device Configurations, page 7-66 and Scheduling Device Updates Using the Drag-and-Drop Method, page 5-35)

Updating the PCoIP Client Configuration (Building and Registering a ThreadX Package)

You can configure the following configuration packages for mass deployment to ThreadX devices:

- **VMwareView Packages**: You can deploy a VMwareView package to the ThreadX devices to configure the VM server settings.
- **Video Packages**: You can deploy a video package to ThreadX devices to configure global video settings such as minimum and maximum image quality settings.

- **RDP Packages**: You can deploy an RDP package to ThreadX devices to configure global RDP settings.

Note Cisco does not provide support for RDP network implementations with the Cisco VXC 2111/2211 PCoIP clients running ThreadX firmware.

- **Additional configuration packages**: You can also deploy additional configuration packages including: timezone and international language settings.

After configuring these packages, you can use DDC or drag and drop to schedule the deployment of the packages to the devices you want (for more information on scheduling packages, see Update Manager, page 5-29).

Tip You can use the sample ThreadX packages that are bundled with Cisco VXC Manager. To create customized packages, modify these sample ThreadX packages, which you can then deploy to ThreadX devices. The sample ThreadX packages are located in the ThreadX Configuration folder (under the Package Manager node).

Customizing the Existing Sample ThreadX Packages

Use the following guidelines to customize the existing sample ThreadX packages.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Package Manager > ThreadX Configuration**.

Step 2 In the details pane, right-click the desired sample package and choose **View Package Script** to open the Package Script dialog box displaying the script of the Cisco VXC Manager package.

Step 3 Check the **Edit and Save Script to Database ONLY** check box and then configure the parameters as desired.

Step 4 After completing your changes, click **OK**.

Step 5 Schedule the package update using Default Device Configuration (see Managing Default Device Configurations, page 7-66) or using the Drag-and-Drop method (see Scheduling Device Updates Using the Drag-and-Drop Method, page 5-35).

Creating New ThreadX Packages

Use the following guidelines to configure additional customized ThreadX packages based on the existing ThreadX packages.

Procedure

Step 1 Create a folder to contain the new package (for example, VMwareViewTest1).

Step 2 In the tree pane of the Administrator Console, expand **Package Manager > ThreadX Configuration**.

Step 3 In the details pane, right-click the desired package and choose **Export Package Script**.

Step 4 Browse to the folder you created in Step 1, and click **OK**.

Step 5 Rename the exported RSP file to match the name of the folder you created in Step 1 (for example, VMwareViewTest1.rsp).

Step 6 Use a text editor to edit the RSP file script for the requirements of your environment.

The following shows an example VMwareView script:

```
[Version]
Number=VMWareViewTest1
Description=ThreadX VMWareView Configuration
OS=TDC
Category=ThreadX Configuration
[Script]
IP=10.10.10.1
SSL=0
AutoLaunchIfOnlyOneDesktop=0
AutoConnect=0
Enable Kiosk Mode=1
Enable custom username=1
Username=user123
Password=
```

Be sure that the Number= segment has the exact same value as the RSP file name and folder name (this naming convention applies to all packages).

Step 7 Register the package (see Register a Package from a Script File (.RSP), page 3-35).

Step 8 Schedule the package update using Default Device Configuration (see Managing Default Device Configurations, page 7-66) or using the Drag-and-Drop method (see Scheduling Device Updates Using the Drag-and-Drop Method, page 5-35).

Supported Parameters for ThreadX VMware View Packages

You can use a VMware View package to configure View Connection Server settings on ThreadX devices. To configure a VMware View package, see Customizing the Existing Sample ThreadX Packages, page 4-12 and Creating New ThreadX Packages, page 4-12. The following table describes the parameters supported in the script of a VMware View package.

Table 4-1 VMWare View Package Parameter Definitions

Parameter	Definition
IP=	Connection server IP address
Port=	Port number (integer value between 1 and 65535).
SSL=	Use secure connection (SSL). Enter 0 for no, 1 for yes.
AutoLaunchIfOnlyOneDesktop=	Auto Launch if only one desktop. Enter 0 for no, 1 for yes.
AutoConnect=	Always connect to this server at startup. Enter 0 for no, 1 for yes.
Enable Kiosk Mode=	Enter 0 for no, 1 for yes.
Enable custom username=	Enter 0 for no, 1 for yes.

Table 4-1 VMWare View Package Parameter Definitions

Parameter	Definition
Username=	User name if enable custom username is true (Enable custom username=1)
Password=	Specifies the password for the specified username.

VMware View Package Example

The following shows an example script for a VMware View package.

```
[Version]
Number=VMWareView_Test
Description=Test Script
OS=TDC
Category=ThreadX Configuration
[Script]
IP=10.100.5.5
Port=999
SSL=1
AutoLaunchIfOnlyOneDesktop = 1
AutoConnect=1
Enable Kiosk Mode=1
Enable custom username = 1
Username=Tester
Password=PW
```

Supported Parameters for ThreadX Language Packages

You can use a Language package to configure language and keyboard settings on ThreadX devices. To configure a Language package, see Customizing the Existing Sample ThreadX Packages, page 4-12 and Creating New ThreadX Packages, page 4-12. The following sections describe the parameters supported in the script of a Language package.

Language=

The Language= parameter allows you to set the language for the On Screen Display GUI on the device.

Table 4-2 Language Parameter Values

Language	Parameter Value
Chinese-Simplified	zh_CN
Chinese-Traditional	zh_TW
English	en
French	fr
German	de
Greek	el
Italian	it
Japanese	ja

Table 4-2 Language Parameter Values

Language	Parameter Value
Korean	ko
Portuguese	pt
Spanish	es

Keyboard Layout=

The Keyboard Layout= parameter sets the layout and language of the keyboard according to the language selected.

Table 4-3 Keyboard Layout Parameter Values

Keyboard Layout Language	Parameter Value
Belgian ISO-8859-1	be.iso
Belgian ISO-8859-1 (accent keys)	be.iso.acc
Danish Codepage 865	danish.cp865
Danish ISO-8859-1	danish.iso
Danish ISO-8859-1 (accent keys)	danish.iso.acc
Dutch ISO-8859-1 (accent keys)	dutch_iso.acc
Finnish Codepage 850	finnish.cp850
Finnish ISO-8859-1	finnish.iso
Finnish ISO-8859-1 (accent keys)	finnish.iso.acc
French Canadian ISO-8859-1 (accent keys)	fr.ca.iso.acc
French Dvorak-like	fr.dvorak
French Dvorak-like (accent keys)	fr.dvorak.acc
French ISO-8859-1	fr.iso
French ISO-8859-1 (accent keys)	fr.iso.acc
German Codepage 850	german.cp850
German ISO-8859-1	german.iso
German ISO-8859-1 (accent keys)	german.iso.acc
Greek ISO-8859-7 (104 keys)	el.iso07
Italian ISO-8859-1	it.iso
Japanese 106/109	jp.106
Japanese 106x (ctrl and shift swapped)	jp.106x
Korean Dubeolsik ISO-8859-1	kr.iso
Latin American	latinamerican
Latin American (accent keys)	latinamerican.iso.acc
Lithuanian	lt.iso
Norwegian Dvorak	norwegian.dvorak

Table 4-3 Keyboard Layout Parameter Values (continued)

Keyboard Layout Language	Parameter Value
Norwegian ISO-8859-1	norwegian.iso
Norwegian ISO-8859-1 (accent keys)	norwegian.iso.acc
Polish ISO-8859-2 (Programmers)	pl.iso2.pro
Portuguese ISO-8859-1	pt.iso
Portuguese ISO-8859-1 (accent keys)	pt.iso.acc
Russian	ru.iso
Spanish ISO-8859-1	spanish.iso
Spanish ISO-8859-1 (accent keys)	spanish.iso.acc
Spanish ISO-8859-15 (accent keys)	spanish.iso15.acc
Swedish Codepage 850	swedish.cp850
Swedish ISO-8859-1	swedish.iso
Swedish ISO-8859-1 (accent keys)	swedish.iso.acc
Swiss-French Codepage 850	swissfrench.cp850
Swiss-French ISO-8859-1	swissfrench.iso
Swiss-French ISO-8859-1 (accent keys)	swissfrench.iso.acc
Swiss-German Codepage 850	swissgerman.cp850
Swiss-German ISO-8859-1	swissgerman.iso
Swiss-German ISO-8859-1 (accent keys)	swissgerman.iso.acc
Turkish Q ISO-8859-9	tr.iso9.q
Turkish Q ISO-8859-9 (accent keys)	tr.iso9.q.acc
United Kingdom Codepage 850	uk.cp850
United Kingdom Codepage 850 (ctrl and caps swapped)	uk.cp850.ctrl
United Kingdom ISO-8859-1	uk.iso
United Kingdom ISO-8859-1 (ctrl and caps swapped)	uk.iso.ctrl
United States of America dvorak	us.dvorak
United States of America dvorakx	us.dvorakx
United States of America Emacs optimized layout	us.emacs
United States of America ISO-8859-1	us.iso
United States of America ISO-8859-1 (accent keys)	us.iso.acc
United States of America ISO-8859-1 (ctrl and caps swapped)	us.pc.ctrl
United States of America lefthand dvorak	us.dvorakl

Table 4-3 Keyboard Layout Parameter Values (continued)

Keyboard Layout Language	Parameter Value
United States of America righthand dvorak	us.dvorakr
United States of America Traditional Unix Workstation	us.unix

Language Package Example

The following shows an example script for a ThreadX Language package.

```
[Version]
Number=Language_Test
Description=Test Script
OS=TDC
Category=ThreadX Configuration
[Script]
Language=en
Keyboard Layout=us.iso
```

Supported Parameters for ThreadX TimeZone Packages

You can use TimeZone packages to specify the time zone on ThreadX devices. To configure a TimeZone package, see Customizing the Existing Sample ThreadX Packages, page 4-12 and Creating New ThreadX Packages, page 4-12.

The following tables describe the parameters supported in the script of a TimeZone package.

Table 4-4 TimeZone Package Parameter Definitions

Parameter	Definition
NTP Server=	NTP Host DNS Name (IP Address or FQDN)
Query Interval=	NTP Query Interval (integer value - number of seconds) Valid range is: 900–60480000.
Port=	NTP Host Port (integer value between 1 and 65535)
Enable Daylights Saving=	Enable Daylight Saving Time. Enter 0 for no, 1 for yes.
Time Zone=	See the following table for possible values.

Table 4-5 Time Zone Parameter Values

Time Zone	Parameter Value
(GMT-12:00) International Date Line West	gmt_minus_1200_international_date_line_west
(GMT-11:00) Midway Island, Samoa	gmt_minus_1100_midway_island
(GMT-10:00) Hawaii	gmt_minus_1000_hawaii
(GMT-09:00) Alaska	gmt_minus_0900_alaska
(GMT-08:00) Pacific Time (US & Canada)	gmt_minus_0800_pacific_time
(GMT-08:00) Tijuana, Baja California	gmt_minus_0800_tijuana

Table 4-5 Time Zone Parameter Values (continued)

Time Zone	Parameter Value
(GMT-07:00) Arizona	gmt_minus_0700_arizona
(GMT-07:00) Chihuahua, La Paz, Mazatlan - New	gmt_minus_0700_chihuahua_new
(GMT-07:00) Chihuahua, La Paz, Mazatlan - Old	gmt_minus_0700_chihuahua_old
(GMT-07:00) Mountain Time (US & Canada)	gmt_minus_0700_mountain_time
(GMT-06:00) Central America	gmt_minus_0600_central_america
(GMT-06:00) Central Time (US & Canada)	gmt_minus_0600_central_time
(GMT-06:00) Guadalajara, Mexico City, Monterrey - New	gmt_minus_0600_guadalajara_new
(GMT-06:00) Guadalajara, Mexico City, Monterrey - Old	gmt_minus_0600_guadalajara_old
(GMT-06:00) Saskatchewan	gmt_minus_0600_saskatchewan
(GMT-05:00) Bogota, Lima, Quito, Rio Branco	gmt_minus_0500_bogota
(GMT-05:00) Eastern Time (US & Canada)	gmt_minus_0500_eastern_time
(GMT-05:00) Indiana (East)	gmt_minus_0500_indiana
(GMT-04:30) Caracas	gmt_minus_0430_caracas
(GMT-04:00) Atlantic Time (Canada)	gmt_minus_0400_atlantic_time
(GMT-04:00) La Paz	gmt_minus_0400_la_paz
(GMT-04:00) Manaus	gmt_minus_0400_manaus
(GMT-04:00) Santiago	gmt_minus_0400_santiago
(GMT-03:30) Newfoundland	gmt_minus_0330_newfoundland
(GMT-03:00) Brasilia	gmt_minus_0300_brasilia
(GMT-03:00) Buenos Aires, Georgetown	gmt_minus_0300_buenos_aires
(GMT-03:00) Greenland	gmt_minus_0300_greenland
(GMT-03:00) Montevideo	gmt_minus_0300_montevideo
(GMT-02:00) Mid-Atlantic	gmt_minus_0200_mid_atlantic
(GMT-01:00) Azores	gmt_minus_0100_azores
(GMT-01:00) Cape Verde Is.	gmt_minus_0100_cape_verde_is
(GMT) Casablanca, Monrovia, Reykjavik	gmt_plus_0000_casablanca
(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London	gmt_plus_0000_greenwich_mean_time
(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	gmt_plus_0100_amsterdam
(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague	gmt_plus_0100_belgrade
(GMT+01:00) Brussels, Copenhagen, Madrid, Paris	gmt_plus_0100_brussels
(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb	gmt_plus_0100_sarajevo
(GMT+01:00) West Central Africa	gmt_plus_0100_west_central_africa
(GMT+01:00) Windhoek	gmt_plus_0100_windhoek
(GMT+02:00) Amman	gmt_plus_0200_amman

Table 4-5 Time Zone Parameter Values (continued)

Time Zone	Parameter Value
(GMT+02:00) Athens, Bucharest, Istanbul	gmt_plus_0200_athens
(GMT+02:00) Beirut	gmt_plus_0200_beirut
(GMT+02:00) Cairo	gmt_plus_0200_cairo
(GMT+02:00) Harare, Pretoria	gmt_plus_0200_harare
(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius	gmt_plus_0200_helsinki
(GMT+02:00) Jerusalem	gmt_plus_0200_jerusalem
(GMT+02:00) Minsk	gmt_plus_0200_minsk
(GMT+03:00) Baghdad	gmt_plus_0300_baghdad
(GMT+03:00) Kuwait, Riyadh	gmt_plus_0300_kuwait
(GMT+03:00) Moscow, St. Petersburg, Volgograd	gmt_plus_0300_moscow
(GMT+03:00) Nairobi	gmt_plus_0300_nairobi
(GMT+03:30) Tehran	gmt_plus_0330_tehran
(GMT+04:00) Abu Dhabi, Muscat	gmt_plus_0400_abu_dhabi
(GMT+04:00) Baku	gmt_plus_0400_baku
(GMT+04:00) Caucasus Standard Time	gmt_plus_0400_caucasus_standard_time
(GMT+04:00) Yerevan	gmt_plus_0400_yerevan
(GMT+04:30) Kabul	gmt_plus_0430_kabul
(GMT+05:00) Ekaterinburg	gmt_plus_0500_ekaterinburg
(GMT+05:00) Islamabad, Karachi, Tashkent	gmt_plus_0500_islamabad
(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi	gmt_plus_0530_chennai
(GMT+05:30) Sri Jayawardenepura	gmt_plus_0530_sri_jayawardenepura
(GMT+05:45) Kathmandu	gmt_plus_0545_kathmandu
(GMT+06:00) Almaty, Novosibirsk	gmt_plus_0600_almaty
(GMT+06:00) Astana, Dhaka	gmt_plus_0600_astana
(GMT+06:30) Yangon (Rangoon)	gmt_plus_0630_yangon
(GMT+07:00) Bangkok, Hanoi, Jakarta	gmt_plus_0700_bangkok
(GMT+07:00) Krasnoyarsk	gmt_plus_0700_krasnoyarsk
(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi	gmt_plus_0800_beijing
(GMT+08:00) Irkutsk, Ulaan Bataar	gmt_plus_0800_irkutsk
(GMT+08:00) Kuala Lumpur, Singapore	gmt_plus_0800_kuala_lumpur
(GMT+08:00) Perth	gmt_plus_0800_perth
(GMT+08:00) Taipei	gmt_plus_0800_taipei
(GMT+09:00) Osaka, Sapporo, Tokyo	gmt_plus_0900_osaka
(GMT+09:00) Seoul	gmt_plus_0900_seoul
(GMT+09:00) Yakutsk	gmt_plus_0900_yakutsk
(GMT+09:30) Adelaide	gmt_plus_0930_adelaide

Table 4-5 Time Zone Parameter Values (continued)

Time Zone	Parameter Value
(GMT+09:30) Darwin	gmt_plus_0930_darwin
(GMT+10:00) Brisbane	gmt_plus_1000_brisbane
(GMT+10:00) Canberra, Melbourne, Sydney	gmt_plus_1000_canberra
(GMT+10:00) Guam, Port Moresby	gmt_plus_1000_guam
(GMT+10:00) Hobart	gmt_plus_1000_hobart
(GMT+10:00) Vladivostok	gmt_plus_1000_vladivostok
(GMT+11:00) Magadan, Solomon, Is., New Caledonia	gmt_plus_1100_magadan
(GMT+12:00) Auckland, Wellington	gmt_plus_1200_auckland
(GMT+12:00) Fiji, Kamchatka, Marshal Is.	gmt_plus_1200_fiji
(GMT+13:00) Nuku'alofa	gmt_plus_1300_nukualofa

TimeZone Package Example

The following shows an example script for a TimeZone package.

```
[Version]
Number=TimeZone_Test
Description=Test Script
OS=TDC
Category=ThreadX Configuration
[Script]
NTP Server=10.100.5.5
Query Interval=3600
Port=9999
Enable Daylights Saving=1
Time Zone=gmt_minus_1000_hawaii
```

Supported Parameters for ThreadX Video Packages

You can use a Video package to configure video image quality settings on ThreadX devices. To configure a Video package, see Customizing the Existing Sample ThreadX Packages, page 4-12 and Creating New ThreadX Packages, page 4-12. The following table describes the parameters supported in the script of a Video package. A lower image quality allows a higher frame rate when network bandwidth is limited.

Table 4-6 Video Package Parameter Definitions

Parameter	Definition
Cursur_enable=	Enable Local Cursor. Enter 0 for no, 1 for yes.
Min_Img_Qty=50	Minimum Image Quality. Range: 30 to 100.
Max_Img_Qty=80	Maximum Image Quality. Range: 30 to 100.

Video Package Example

The following shows an example script for a Video package.

```
[Version]
Number=Video_Test
Description=Test Script
OS=TDC
Category=ThreadX Configuration
[Script]
Cursur_enable=1
Min_Img_Qty=50
Max_Img_Qty=80
```

Cisco VXC 2112/2212 ICA Client Upgrade Procedures

The following sections describe how to update the ICA firmware image and client configurations:

- Updating the ICA Firmware Image, page 4-21
- Updating the ICA Client Configuration (Building and Registering a WTOS package), page 4-22

Note When Cisco VXC Manager deploys packages to Cisco VXC 2112/2212 ICA devices, it notifies the devices to download the updated firmware or configuration from a specific folder location on the server. The ICA devices then update themselves but do not notify the Cisco VXC Manager server.

Updating the ICA Firmware Image

To update the firmware image on a Cisco VXC ICA client, perform the following procedure.

Procedure

Step 1 Download the OS image from the Cisco Software Download page at the following URL:

http://www.cisco.com/cisco/software/navigator.html?mdfid=283759601&i=rm

Step 2 On the server where you have Cisco VXC Manager installed, extract the zipped firmware files to a local folder.

Step 3 Register the package (see Register a Package from a Script File (.RSP), page 3-35). When you are prompted for an RSP file during the package registration process, browse and choose the RSP file that is contained in the unzipped package.

Note To upgrade the image on ICA devices, the Category parameter in the RSP file must be set to Images (Category=Images).

Step 4 Configure the following WTOS preferences:

a. In the tree pane of the Preferences dialog box, click **WTOS**.

b. Ensure that the WTOS Root Path field contains **WNOS**.

c. Click **OK**.

Step 5 To upgrade the Cisco VXC 2112/2212, use Default Device Configuration (see Managing Default Device Configurations, page 7-66).

Note ICA Clients only support the Default Device Configuration method for upgrades. They do not support drag and drop.

Updating the ICA Client Configuration (Building and Registering a WTOS package)

Use this procedure to update the ICA client configuration using a WTOS package.

Procedure

Step 1 Create a folder to contain the client configurations, for example **ICAConfigs**.

Step 2 In the ICAConfigs folder, create an RSP file named ICA1.rsp with the following content:

```
[Version]
Number=ICA1
Description=Package for ICA client upgrade
OS=BL
Category=Images
Imagetype=Merlin
Mediasize=128
[Script]
```

where the “Number=” segment must have the exact same value as the RSP file name.

Step 3 Also in the ICAConfigs folder, create a subfolder using the same name as the RSP file name, for example **ICA1**.

Step 4 In the ICA1 folder, create a subfolder named **WNOS**.

Step 5 In the WNOS folder, create a file named wnos.ini that contains the required configuration. (See *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide* for more information, including sample .ini files.)

For example:

- Location and name of RSP image:

  C:\VXC-M\ICAConfigs\ICA1.rsp
- Location and name of WNOS directory:

  C:\VXC-M\ICAConfigs\ICA1\WNOS
- Location and name of wnos.ini file in WNOS directory:

  C:\VXC-M\ICAConfigs\ICA1\WNOS\wnos.ini

Step 6 Register the package (see Register a Package from a Script File (.RSP), page 3-35).

Step 7 Ensure the following additional WTOS preferences are configured appropriately:

a. In the tree pane of the Preferences dialog box, click **WTOS**.

b. Ensure that the WTOS Root Path field contains **WNOS**.

c. Click **OK**.

Step 8 To upgrade the Cisco VXC 2112/2212, use Default Device Configuration (see Managing Default Device Configurations, page 7-66).

Note In the Default Device Configuration wizard, on the Primary Definition tab, choose the name of the package you just registered in the Qualifying OS Image field to update the ICA client configuration.

Upgrading Clients Using a Remote Repository

Cisco VXC Manager supports a built-in scalability feature in the form of remote repositories. In order to preserve bandwidth and perform upgrades more efficiently, you can configure a remote repository that is closer to the physical location of your devices. The configuration of a remote repository involves setting up the remote repository, registering the repository in Cisco VXC Manager, syncing packages with the remote repository, and specifying which subnet is associated with which repository.

In the current release, the only method of assigning devices to a remote repository is by device subnet.

For more information, see Understanding Cisco VXC Manager Repositories, page 7-86, Scheduling a Remote Repository Synchronization, page 5-38, and Adding Subnets to Cisco VXC Manager Manually, page 7-91.

Understanding the Cisco VXC Manager Package Structure

A Cisco VXC Manager Package structure consists of two components:

- The Package script (RSP) file (ImgXL24.rsp)
- The Package folder that contains the required application or image files (ImgXL24)

In order for a Package to function properly, these two components must adhere to the following structural rules:

- The Package script file must have an .rsp extension. You can create and edit an RSP file using Notepad.
- The Package folder must have the same name as the Package script file.
- The Number= parameter in the [Version] section of the Package script file should match the value reported by the device to the Client Manager. This becomes extremely important when using the Default Device Configuration feature.
- All the files referenced by the Package script file must be within the Package folder or a subfolder within.
- All command arguments should be enclosed in double-quotes and are separated by spaces ONLY.
- All registry paths are delimited with backslashes (‘\’) and are within quotes.
- Do not use abbreviations for the root registry keys (e.g. use HKEY_LOCAL_MACHINE, not HKLM).
- All filenames are delimited with backslashes (‘\’) and are within quotes.
- Neither path names nor registry branches should ever end with a backslash.

- In general, a script is aborted if a command fails. If you do not want the script to abort if a command fails, then appended the command with and asterisk (*). (Note not all commands support this).
- <REGROOT> (e.g. <regroot>\sourcefile.txt) points to the root directory of the registered package (e.g. c:\inetpub\ftproot\rapport\<packagename>).

Tip <regroot> is a pointer that tells the Cisco VXC Manager Service to look in a specific location on the Cisco VXC Manager server (not the device) for Package application files. <regroot> finds the Cisco VXC Manager Master Repository and identifies the folder contained within that is holding the needed Package files.

Understanding the Script File Structure

A Cisco VXC Manager script (RSP) file is one of two components that make up a Cisco VXC Manager Package:

- The Package script (RSP) file (ImgXL24.rsp)
- The Package folder that contains the required application or image files (ImgXL24)

The Package script (RSP) file must conform to a specific structure and should contain two sections:

- Version
- Script

Version

The Version section contains information required for package registration and distribution purposes. The following describes each of the elements of the Version section:

[Version] - Required section header

Number= - Must be the same as the Package Script File name

Description= - A brief description of what the Package is to achieve

OS= -The Operating System the Package is intended for

USE_REMOTE= - YES/NO, specifies whether or not a Remote Repository (if it exists) should be used. Default is YES. (OPTIONAL)

DEPLOYEDSW= - YES/NO defines whether package should be added to the Cisco VXC Manager deployed package table for device. Default is YES. (OPTIONAL)

Category= - The Cisco VXC Manager Package Manager category in the Administrator Console where the package will reside. Note if the category does not exist it will be created.

Image Category Special Tags

[Version] - Required section header

ImageSize= - size of image in Megabytes

BootFloppy= - name of bootfloppy; default is RAPPORT

IMAGE= - name of image file to be used; by default Cisco VXC Manager uses the first file found in the package folder (excluding CRC.text)

Command= - the image operation to be performed

Script

The Script section contains the commands that are carried out when the script is distributed. Each command is executed in order as they appear within the [Script] section.

Recommended Scripting Template

```
[Version]
Number=Script name (matching the RSP_ file name and Package folder name)
Description=Detailed description with version number and valid images
OS=XX
Category=Other Packages
[Script]
Written by: Your Name and Company
; ..........................................................................
; >Check the Operating System
; >Check the Image Version
; ..........................................................................
CO "NT"
CI “XXXX”
; ..........................................................................
; >Check Free Space
; >Check Minimum Memory, if necessary
; >Check User, if necessary
; ..........................................................................
CF “X” “XXX”
CR “XXXX”
CU “XXXXXXXX”
; ..........................................................................
; > Query User then lock Workstation
; ..........................................................................
QU
LU*
; ..........................................................................
; >Add Commands Here
; ..........................................................................
;SF “<regroot>\files\x.xxx” “c:\yyyy\zzzz”
;EX “c:\yyyy\zzzz”
;DF “c:\yyyy\zzzz”
;MR “<regroot>\xxxx.reg”
;SP "c:\windows\system.ini" "DISPLAY" "screen-size" "640"
; ..........................................................................
; >End Lockout
; ..........................................................................
EL*
; ..........................................................................
; >Reboot, if necessary
; ..........................................................................
RB
---------------------------------------------------------------------------
```

Version

The Version section contains information required for package registration and distribution purposes.

BootFloppy=

Specifies the boot floppy Cisco VXC Manager uses during the imaging process:

- Rapportitf.0 (Cisco VXC Manager Imaging agent for imaging)

Category=

Defines the category for the Package. If you type a different category name in Category=, and then register the Package using Cisco VXC Manager, a folder is created under the Package Manager with that name.

Tip A package can be moved from one category to another by changing Category= and re-registering the package.

Command=

The image operation to be performed.

Example: Command=%ImageWrite%

Possible Values:

- %ImageWrite% (This value writes to the DiskOnChip)
- %ImageRead% (This value reads from the DiskOnChip)

DeployedSW=

This defines whether the package should be added to the Cisco VXC Manager deployed package table for the device.

DEPLOYEDSW=Yes or No - Default is Yes if not specified or specified incorrectly. This option is used primarily in conjunction with DDC. If a DDC has Enforce Sequence enabled any package sent to the device will trigger the DDC to re-image the device (thereby removing all packages). Using DeployedSW=No allows the user to send packages to devices without logging their distribution, thereby not triggering a DDC operation.

Description=

Allows the script developer to add a short description about the Package. The description is a comment line and is not parsed by Cisco VXC Manager when the script is executed.

Image=

This defines the file name to be used when reading or writing an image.

Image=filename - The default is the first file found in <regroot> excluding CRC.txt.

ImageSize=

Identifies for Cisco VXC Manager the size of image being sent to a client.

Values: 8, 16, 24, 32, 48, 64, 72, 80, 96, 128, 144, 192, 256, 512, 1024

Number=

Identifies for Cisco VXC Manager the name of the Package. The name of the Package script (RSP) file must match the Number= parameter. For example, if the Package script name is ImgXL24.rsp, you must have Number=ImgXL24 in the [Version] section of ImgXL24.rsp.

Example:

```
[Version]
Number=[Number reported by device in Device Manager under Image]
Description=Image to Write to Device
OS=NT
Category=Images
USE_PXE=YES
USE_REMOTE=NO
DEPLOYEDSW=YES
IMAGE=[xyz24xl.img]
IMAGESIZE=24
```

OS=

Defines the Operating System the device is running.

Values:

- BL WTOS
- SLX SUSE Linux
- TDC ThreadX

Use_Remote=

This defines whether the package should use a Remote Repository assigned to its subnet or if it should always use the Master.

Use_Remote=Yes or No - Default is Yes, if not specified or specified incorrectly.

CHAPTER 5

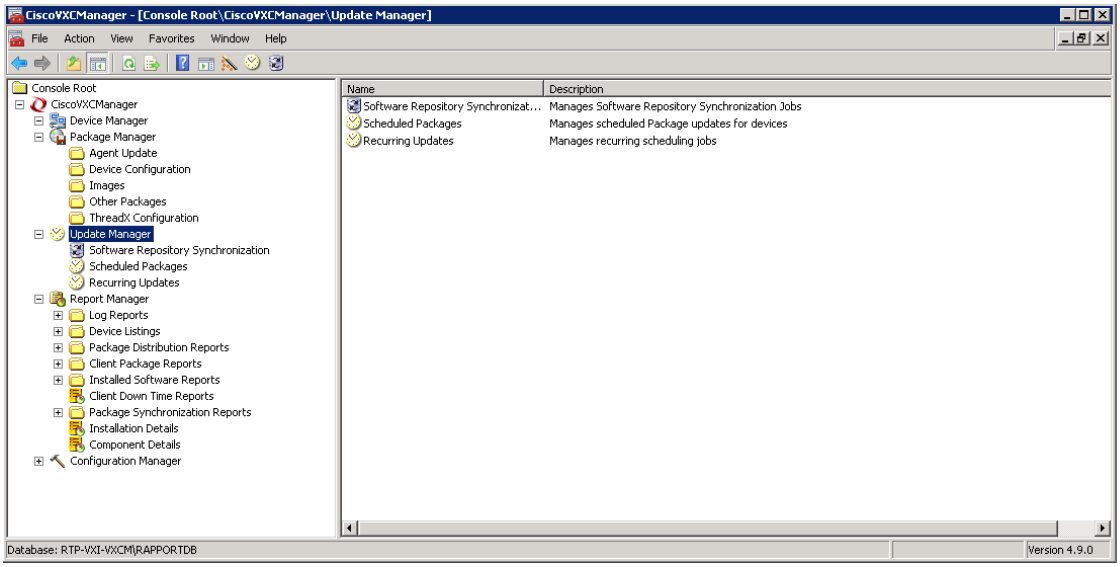
Update Manager

This chapter describes how to perform routine device update management tasks using the Administrator Console. It provides information on managing the device updates in your Cisco VXC Manager system and the schedules for synchronizations between Remote Repositories and the Master Repository.

Managing the Schedules for Device Updates

Click **Update Manager** in the tree pane of the Cisco VXC Manager Administrator Console to open the Update Manager. The Update Manager allows you to quickly view and manage the device updates (schedules of the Cisco VXC Manager packages registered in the Cisco VXC Manager database that are ready to be distributed to devices) within your Cisco VXC Manager environment (see Table 5-1). It also allows you to view and manage the schedules for synchronizations between Remote Repositories and the Master Repository.

Figure 5-1 Update Manager



Before using the Update Wizard to schedule device updates, you should understand the update distribution process and the contents of the registered Cisco VXC Manager packages, know the identity of the Cisco VXC Manager packages that you want to distribute, and ensure that the devices to which you will be pushing images or configurations are recognized by the Cisco VXC Manager system (for

example, they have been discovered by Cisco VXC Manager). After the Cisco VXC Manager packages in the Cisco VXC Manager database are scheduled for distribution, they will be distributed as updates to the devices within your Cisco VXC Manager network according to your schedules and preferences.

Tip If you intend to perform Cisco VXC Manager package registration and scheduling for all of the devices in your Cisco VXC Manager system at the same time, the Cisco VXC Manager Mass Imaging Tool can be a convenient way for you to easily perform these tasks (see Using the Cisco VXC Manager Mass Imaging Tool, page D-17).

Table 5-1 provides a quick overview of what you can do using the Update Manager.

Table 5-1 Routine Update Manager Tasks

Tasks You Can Do	How	Details
Use the Package Distribution Wizard to schedule a registered Cisco VXC Manager package so that it will be distributed as an update.	In the tree pane of the Administrator Console, expand **Update Manager**, right-click **Scheduled Packages**, and then choose **New > Update** to open and use the Package Distribution Wizard.	Scheduling Device Updates Using the Package Distribution Wizard, page 5-32
Use the Drag-and-Drop method to schedule a registered Cisco VXC Manager package so that it will be distributed as an update (useful for environments with a large number of devices and Views).	Complete the instructions in Scheduling Device Updates Using the Drag-and-Drop Method, page 5-35.	Scheduling Device Updates Using the Drag-and-Drop Method, page 5-35
Use the Default Device Configuration method to schedule a registered Cisco VXC Manager package so that it will be distributed as an update (useful if you have a group of devices that have the same OS and media size on which you want to enforce your specified configurations automatically).	Complete the instructions in Scheduling Device Updates Using the Default Device Configuration, page 5-36.	Scheduling Device Updates Using the Default Device Configuration, page 5-36
View the schedules of Cisco VXC Manager packages that will be distributed as updates.	In the tree pane of the Administrator Console, expand **Update Manager** and click **Scheduled Packages** (the details pane displays any scheduled and in-progress device updates).	
Change a previously scheduled update or recurring update (the schedule of a Cisco VXC Manager package that will be distributed as an update).	In the tree pane of the Administrator Console, expand **Update Manager** and click **Scheduled Packages**. In the details pane, right-click the previously scheduled or recurring update and choose **Properties** to open and use the Edit Updatesor Recurring Scheduler dialog box.	Changing a Scheduled Device Update for a Cisco VXC Manager Package, page 5-37

Table 5-1 Routine Update Manager Tasks (continued)

Tasks You Can Do	How	Details
Delete a previously scheduled update (the schedule of a Cisco VXC Manager package that will be distributed as an update).	In the tree pane of the Administrator Console, expand **Update Manager** and choose **Scheduled Packages**. In the details pane, right-click the previously scheduled update, choose **Delete**, and then confirm the deletion. **Tip** You can use Ctrl-click or Shift-click to choose multiple Cisco VXC Manager packages.	You cannot delete in-progress device updates for a Cisco VXC Manager package. **Tip** If you have an in-progress update that cannot be fulfilled (for example, a device problem), you can move the update to an error state (right-click on the update and choose **Move to Error**) and then delete it.
Choose an Update Manager View (a default or one that you created) to use with Scheduled Packages so you can quickly find the devices you want.	In the tree pane of the Administrator Console, expand **Update Manager**, right-click **Scheduled Packages**, and then choose **Switch View** to open and use the Select Current Manager View dialog box.	After creating Views according to your device Group Types, Networks, and so on, selecting a Current Manager View makes it easy to view the devices you want (see Managing Views, page 7-63).
Use the Remote Software Repository Synchronization Wizard to manually schedule a synchronization.	In the tree pane of the Administrator Console, expand **Update Manager**, right-click **Software Repository Synchronization**, and then choose **New > Remote SW Repository Synch** to open the Remote Software Repository Synchronization Wizard.	Manually Scheduling a Synchronization (Using the Remote Software Repository Synchronization Wizard), page 5-39
Set up or change an automatic synchronization.	Complete the instructions in Configuring an Automatic Synchronization, page 5-39.	Configuring an Automatic Synchronization, page 5-39 **Note** Automatic synchronization is the default set during installation. Use these instructions if you ever need to change a manual synchronization schedule back to an automatic schedule, or simply need to change the time settings on your current automatic schedule.
View the schedules of remote repository synchronizations.	In the tree pane of the Administrator Console, expand **Update Manager** and click **Software Repository** (the details pane displays any scheduled, error-state, or in-progress remote repository synchronizations).	

Table 5-1 Routine Update Manager Tasks (continued)

Tasks You Can Do	How	Details
Change the schedule of a remote repository synchronization.	In the tree pane of the Administrator Console, expand **Update Manager** and click **Software Repository Synchronization**. In the details pane, right-click the scheduled synchronization and choose **Properties** to open and use the Synchronize Remote Software Repository dialog box.	Changing a Remote Software Repository Synchronization, page 5-42
Delete a previously scheduled remote repository synchronization.	In the tree pane of the Administrator Console, expand **Update Manager** and click **Software Repository Synchronization**. In the details pane, right-click the previously scheduled synchronization, choose **Delete**, and then confirm the deletion.	You cannot delete in-progress remote repository synchronizations.

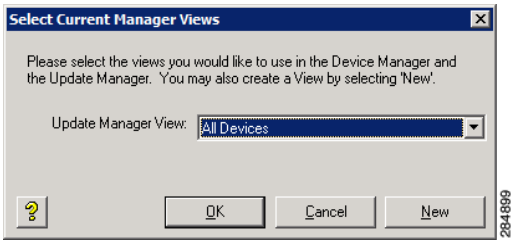
Scheduling Device Updates Using the Package Distribution Wizard

Use the following procedure to schedule updates using the Package Distribution Wizard.

Procedure

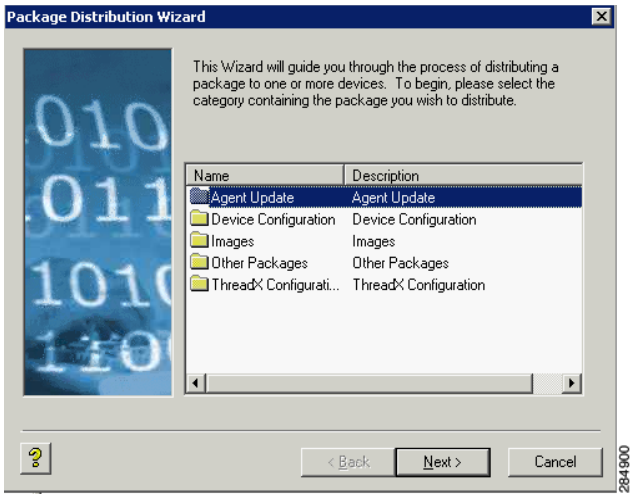
Step 1 In the tree pane of the Administrator Console, expand **Update Manager**, right-click **Scheduled Packages**, choose **Switch View** to open the Update Manager View dialog box, choose the view that contains the group or groups of devices you want to receive the update, and then click **OK** (note that you can use **New** to create a new view).

Figure 5-2 Choose View



Step 2 In the tree pane of the Administrator Console, right-click **Scheduled Packages** and choose **New > Update** to open the Package Distribution Wizard.

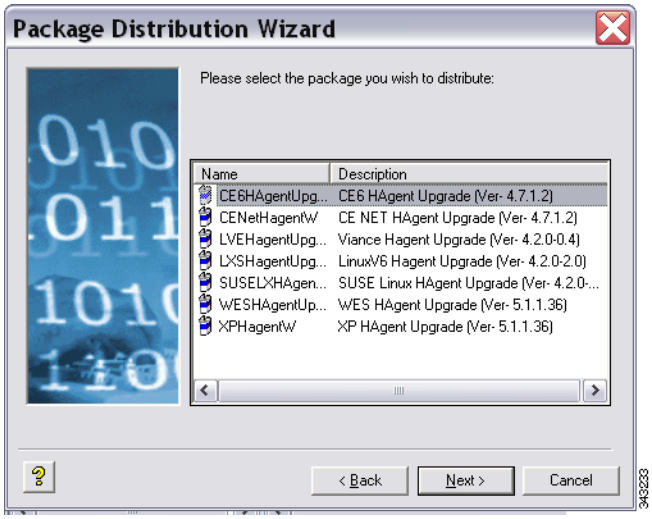
Figure 5-3 Package Distribution Wizard



Step 3 Choose the folder that contains the registered Cisco VXC Manager package you want to distribute and click **Next**.

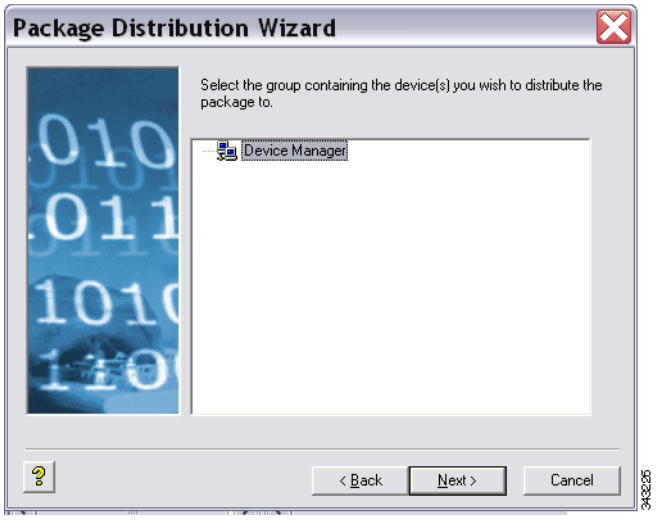
Note Only images that support the operating system and flash size of the previously selected device groups view will be displayed.

Figure 5-4 Choose the Cisco VXC Manager Package



Step 4 Choose the Cisco VXC Manager package you want and click **Next**.

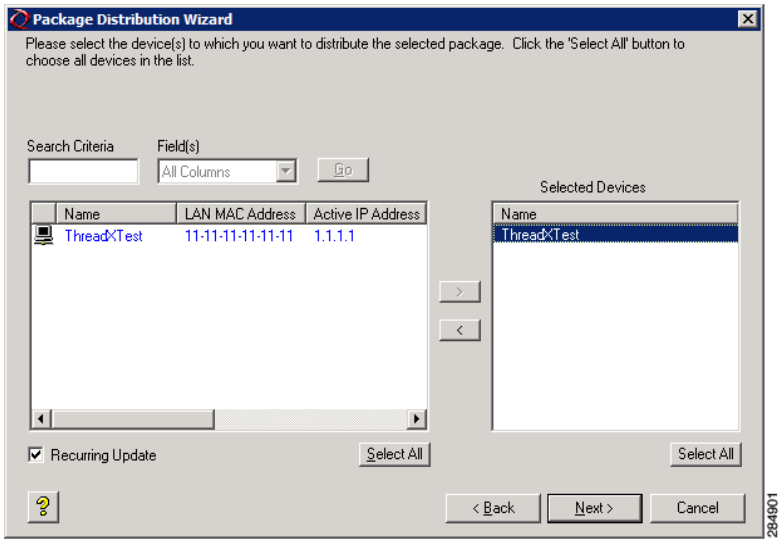
Figure 5-5 Choose Client Groups



Step 5 Choose the group of devices you want to receive the update (to choose all of the groups in the hierarchy, choose **Device Manager** at the top of the hierarchy) and click **Next**.

Tip The device groups you see depend on the Update Manager View you selected in Step 1.

Figure 5-6 Choose Clients



Step 6 Choose the devices you want to receive the update (you can use Ctrl-click or Shift-click to choose multiple devices; or click **Select All** if you want to choose all of the devices in the list), check or uncheck the **Recurring Update** check box (allowing you to schedule on a recurring basis), and click **Next**.

Step 7 Depending on whether or not any of the devices you selected are serviced by a Remote Repository (for example, the Cisco VXC Manager package with the update is contained in a Remote Repository), complete one of the following:

- If no, the wizard prompts you to choose when the update or recurrence pattern should occur. Choose the time and date for the update, click **Next**, and then continue with Step 8.

- If yes, and you have set up your preferences to synchronize Remote Repositories, the wizard prompts you for the synchronization information. Enter the information, click **Next**, and then continue with Step 8.

Step 8 When prompted to create the updates click **Next**.

Step 9 After the wizard notifies you that the updates have been created, click **Finish**.

Scheduling Device Updates Using the Drag-and-Drop Method

Caution This section is not applicable to Cisco VXC 2112/2212 clients running WTOS firmware.

You can use the drag-and-drop method to schedule a registered Cisco VXC Manager package so that it will be distributed as an update (useful for environments with a large number of devices and Views). Drag-and-drop can push only one package at a time to your devices. To push multiple packages to your devices at the same time, you must use DDC.

Tip You can create the View you want (a folder that includes the devices to which you want to distribute a Cisco VXC Manager package) by using the instructions in Managing Views, page 7-63.

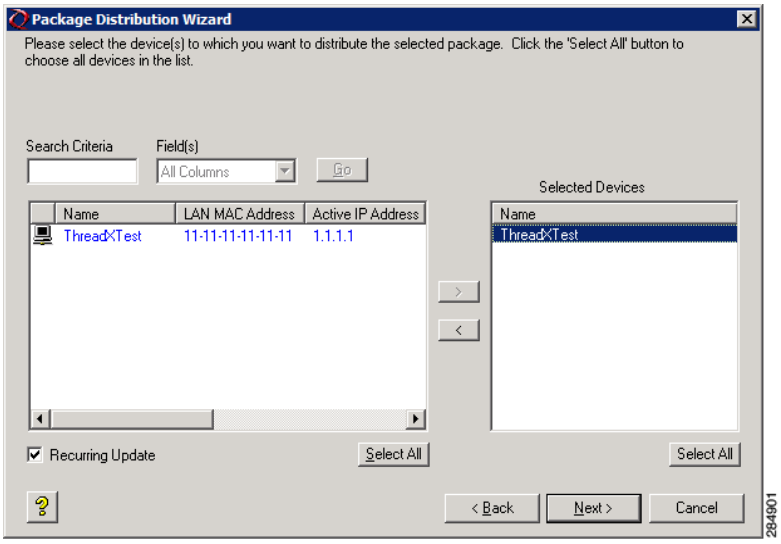
Procedure

Step 1 In the tree pane of the Administrator Console, expand **Package Manager** and click the folder that contains the Cisco VXC Manager package you want to distribute so that it is displayed in the details pane.

Step 2 In the tree pane of the Administrator Console, expand **Device Manager** so that the folder containing the devices (the View) to which you want to distribute the Cisco VXC Manager package is displayed in the tree pane.

Step 3 Click and drag the Cisco VXC Manager package you want to distribute from the details pane and drop the Cisco VXC Manager package onto the folder in the tree pane containing the devices (the View) to which you want to distribute the Cisco VXC Manager package.

Figure 5-7 Choose Devices



Step 4 In the Package Distribution Wizard that appears, choose the devices you want to receive the Cisco VXC Manager package, click the arrow to move them to the Selected Devices list (you can use Ctrl-click or Shift-click to choose multiple devices; or click **Select All** if you want to choose all of the devices in the list), check or uncheck the **Recurring Update** check box (allowing you to schedule on a recurring basis for time, day, and range of dates after you click **Next**; for example, every two weeks on Monday at 3:00 a.m. with no end date), and then click **Next**.

Step 5 Depending on whether or not any of the devices you selected are serviced by a Remote Repository (for example, the Cisco VXC Manager package with the update is contained in a Remote Repository), complete one of the following:

- If no, the wizard prompts you to choose when the update or recurrence pattern should occur. Choose the time and date for the update, click **Next**, and then continue with Step 6.
- If yes, and you have set up your preferences to synchronize Remote Repositories, the wizard prompts you for the synchronization information. Enter the information, click **Next**, and then continue with step 6.

Step 6 When prompted to create the updates click **Next**.

Step 7 After the wizard notifies you that the updates have been created, click **Finish**.

After you configure a DDC for Cisco VXC clients, the clients are updated to the selected OS version automatically: either at their regularly scheduled check-in time or according to the update time set in the Device Manager DDC preferences in Configuration Manager. You can also right-click the Cisco VXC client you want to upgrade, and choose **Reboot** to perform a manual upgrade.

Scheduling Device Updates Using the Default Device Configuration

If you have a group of devices that have the same OS and media size, you can assign a Default Device Configuration (DDC) to update the devices automatically. A DDC allows you to set default configurations for a group of devices and ensures that the devices conform to your configurations. That is, if there is any deviation from your default configurations, Cisco VXC Manager reverts the devices

back to your specified configurations automatically (Cisco VXC Manager automatically sends the Cisco VXC Manager packages in the DDC to the devices according to your schedule and without your intervention).

Procedure

Step 1 Identify the devices to which you want to assign a DDC, and create a suitable View to isolate the target devices (a DDC can be applied only to a group of devices that have the same OS and media size).

Tip You can create the View you want (a folder that includes the devices to which you want to distribute a Cisco VXC Manager package) by using the instructions in Managing Views, page 7-63.

Step 2 Identify the registered Cisco VXC Manager packages (in the Cisco VXC Manager Database) that you want to include in the DDC.

Tip DDCs also allow you to determine the sequence in which the Cisco VXC Manager packages are distributed to the devices.

Step 3 Use the procedures in Managing Default Device Configurations, page 7-66 to create and assign the DDC you want.

Changing a Scheduled Device Update for a Cisco VXC Manager Package

Use the following procedure to change a scheduled device update for a Cisco VXC Manager Package.

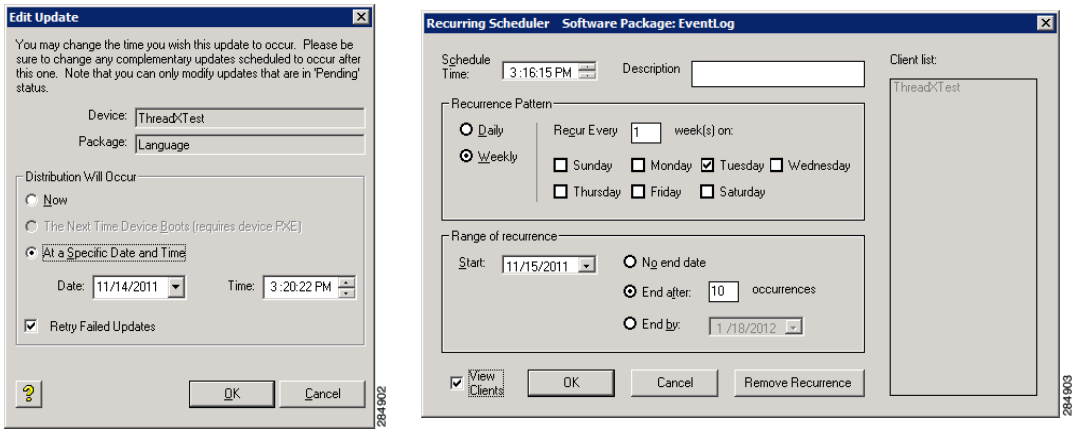
Caution You cannot edit in-progress device updates. If a device has been removed from a network before deleting a scheduled update for that device, the scheduled update may remain in a status of in-progress indefinitely. Before you delete a device, be sure there is no update scheduled for that device.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Update Manager**, and then depending on your scheduled package click **Scheduled Packages** or **Recurring Updates**. The details pane displays any scheduled, error-state, or in-progress device updates.

Step 2 Right-click the scheduled or recurring device update you want to change and choose **Properties** to open the Edit Updates or **Recurring Scheduler** dialog box.

Figure 5-8 Edit Updates/Recurring Scheduler



Step 3 Make your changes (the ability to choose the **Next Time the Device Boots** option requires that the device supports PXE and that you set up your preferences to allow updates to occur at PXE if you are using PXE-based imaging—see PXE Based Imaging, page D-12).

Tip If the scheduled device update is linked to a Remote Repository, you may see two update rows in the details pane of the Software Repository Synchronization window. The first row is for an update to synchronize the Remote Repository with the Master Repository (if necessary). The second row is for the actual update to the devices that are serviced by the Remote Repository. You can edit either or both of these updates. However, you cannot reschedule the synchronization update (between the Remote Repository and the Master Repository) to occur after the update for the corresponding devices.

Step 4 After completing your changes, click **OK**.

Scheduling a Remote Repository Synchronization

Cisco VXC Manager packages in Remote Repositories can be synchronized using either of the following methods:

- Configuring an Automatic Synchronization—This is the default set during installation. With Automatic synchronization enabled, the remote repository synchronizes with the master repository when a client device receives an update for a Cisco VXC Manager package that is not included in the repository assigned to the client subnet (see Configuring an Automatic Synchronization, page 5-39).

Note Cisco VXC 2111/2211 PCOIP devices and Cisco VXC 2112/2212 ICA devices do not support automatic synchronization of Remote Repositories. You must manually schedule a synchronization for these devices.

Automatic Synchronization only occurs when a client requires a package that does not already exist on the Remote Repository for that client. If you configure a package on the Master Repository that is not applicable to clients on a particular subnet, the Remote Repository for that subnet does not perform a synchronization to obtain this package. As such, the contents of a Remote Repository do not always match the Master Repository.

To fully synchronize the Remote Repository to the Master Repository, you can perform a manual synchronization prior to deploying the package.

- Manually Scheduling a Synchronization—Using the Remote Software Repository Synchronization Wizard, you can set up the specific schedules you need (see Manually Scheduling a Synchronization (Using the Remote Software Repository Synchronization Wizard), page 5-39).

Configuring an Automatic Synchronization

By default, Cisco VXC Manager uses automatic synchronization of the Remote Repository with the Master Repository. If you ever need to change a manual synchronization schedule back to an automatic schedule, or simply need to change the time settings on your current automatic schedule, use the following guidelines:

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, and then click **Preferences**.

Step 2 In the details pane, double-click **Scheduling Preferences** to open the Preferences dialog box.

Step 3 In the left pane of the Preferences dialog box, click **Scheduling** to open the Scheduling Preferences dialog box.

Step 4 Enter the general scheduling preferences you want (see Scheduling Preferences, page 7-83).

Step 5 Check the **Auto-synch Remote Software Repository** check box and set the **Max. Retry Count** you want (5 is generally recommended).

Step 6 Choose the **Imaging Option** you want (see Scheduling Preferences, page 7-83).

Step 7 Click **OK**.

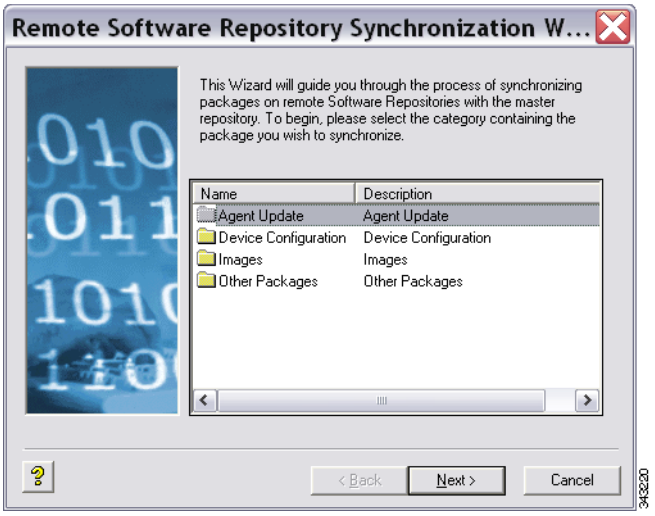
Manually Scheduling a Synchronization (Using the Remote Software Repository Synchronization Wizard)

Use the following procedure to manually schedule a synchronization.

Procedure

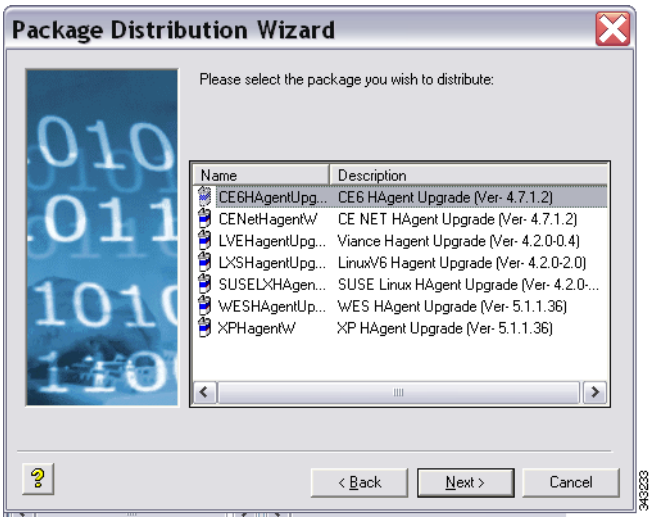
Step 1 In the tree pane of the Administrator Console, expand **Update Manager**, right-click **Software Repository Synchronization**, and then choose **New > Remote SW Repository Synch** to open the Remote Software Repository Synchronization Wizard.

Figure 5-9 Remote Software Repository Synchronization Wizard



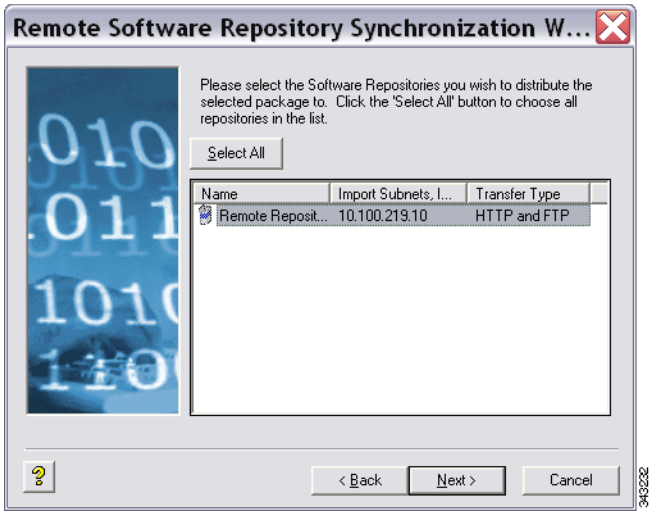
Step 2 Choose the category containing the Cisco VXC Manager package you want to synchronize, and then click **Next**.

Figure 5-10 Choose the Cisco VXC Manager Package



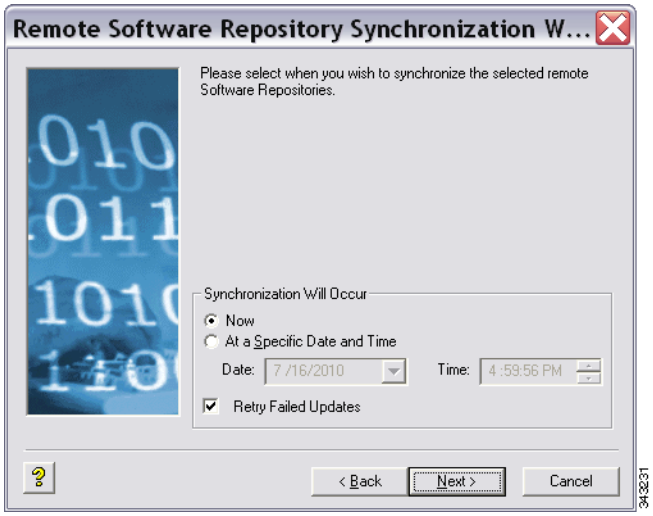
Step 3 Choose the Cisco VXC Manager package you want to synchronize, and then click **Next**.

Figure 5-11 Choose the Software Repository



Step 4 Choose the repositories to which you want the Cisco VXC Manager package distributed, and then click **Next**.

Figure 5-12 Choose the Scheduling Options



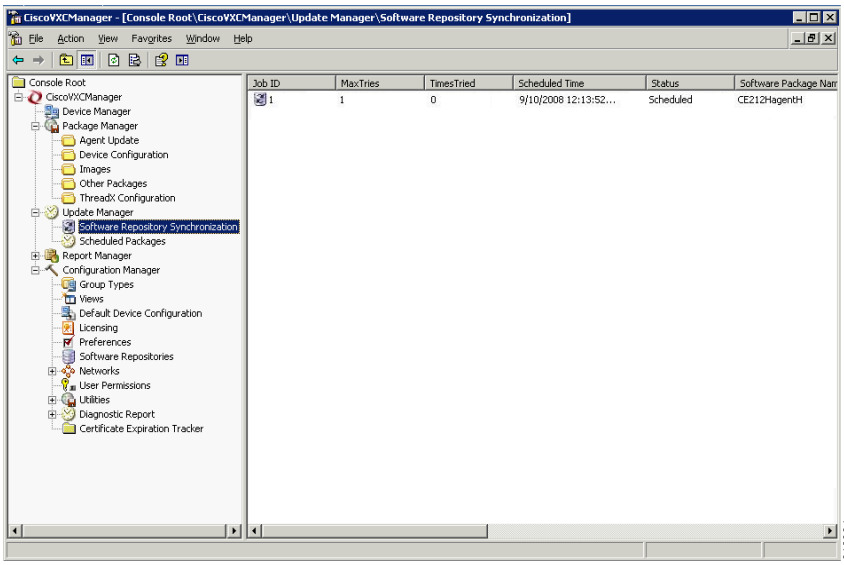
Step 5 Choose the scheduling options for the synchronization, and then click **Next**.

Step 6 When prompted to create the schedule click **Next**.

Step 7 After the wizard notifies you that the schedule has been created, click **Finish**.

Step 8 To verify the repository synchronization is scheduled, navigate to **CiscoVXCManager > Update Manager > Repository Synchronization** and view the synchronization details in the details pane.

Figure 5-13 Repository Synchronization



Changing a Remote Software Repository Synchronization

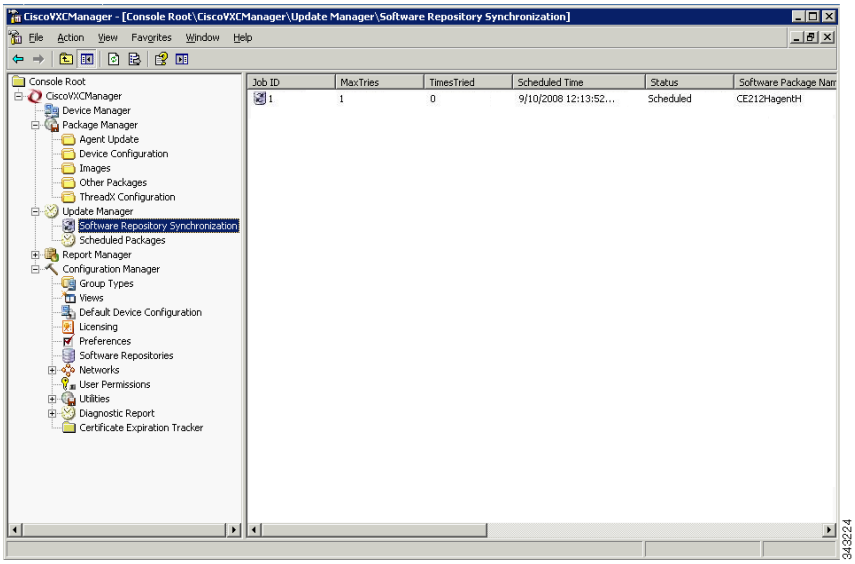
Use the following procedure to change a remote software repository synchronization.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Update Manager**, and then click **Software Repository Synchronization**.

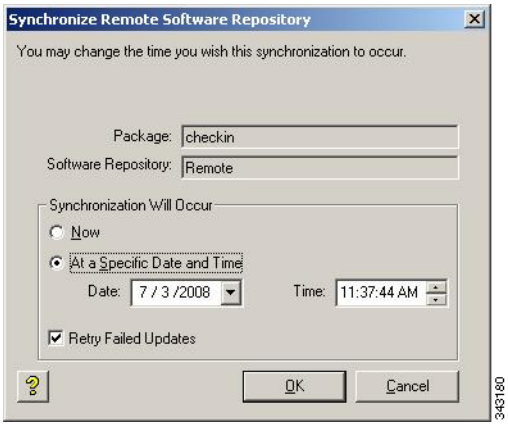
Step 2 The details pane displays any scheduled, error-state, or in-progress repository synchronizations.

Figure 5-14 Software Repository Synchronization



Step 3 Right-click the scheduled repository synchronization you want to change, and then choose **Properties** to open the Edit Synchronize Remote Software Repository dialog box.

Figure 5-15 Edit Synchronize Remote Software Repository



Step 4 Make your changes.

Step 5 After completing your changes, click **OK**.

CHAPTER 6

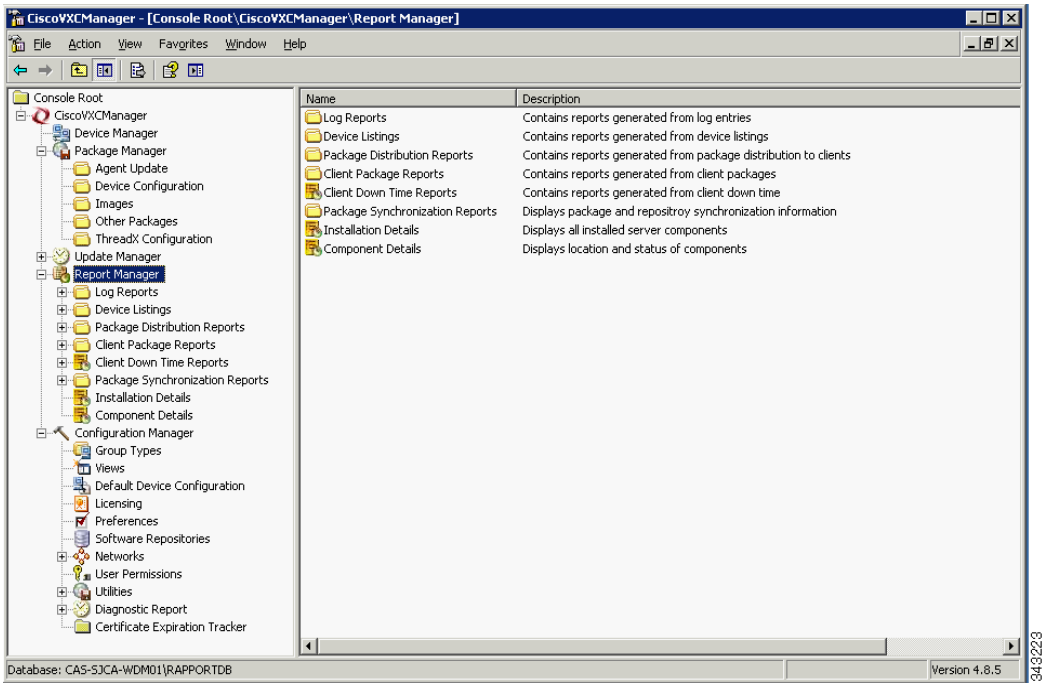
Report Manager

This chapter describes how to create and manage Cisco VXC Manager reports using the Administrator Console. It provides information and instructions to help you generate various reports on your Cisco VXC Manager environment.

Creating and Managing Reports

Click **Report Manager** in the tree pane of the Cisco VXC Manager Administrator Console to open the Report Manager. The Report Manager allows you to quickly create and manage the reports available about your Cisco VXC Manager environment (see Table 6-1). It also allows you to easily display the current information from your devices according to the criteria you set in the report.

Figure 6-1 Report Manager



Tip To choose the columns you want displayed within the details pane for a report, right-click the details pane containing the report and choose **View > Add/Remove Columns** to open and use the Add/Remove Columns dialog box.
To export a report to a .txt or .csv file, right-click the Report Manager folder you want (for example, **Log Reports**), choose **Export List**, and then use the Export to a File dialog box.

Table 6-1 provides a quick overview of what you can do using the Report Manager.

Table 6-1 Routine Report Manager Tasks

Tasks You Can Do	How	Details
Create a report listing activities related to all Cisco VXC Manager components according to your logging preferences (for example, all administrator activities within a start and end time).	In the tree pane of the Administrator Console, expand **Report Manager**, right-click **Log Reports**, and then choose **New > Report** to open and use the Report Wizard.	Log Reports, page 6-47 **Tip** To set your logging preferences, see Logging Preferences, page 7-75.
Create a report listing managed devices according to your criteria (for example, all devices according to operating system).	In the tree pane of the Administrator Console, expand **Report Manager**, right-click **Device Listings**, and then choose **New > Report** to open and use the Report Wizard.	Device Listings, page 6-48
Create a report with information about managed devices according to the Cisco VXC Manager packages you have distributed (for example, all devices according to a specific Cisco VXC Manager package update).	In the tree pane of the Administrator Console, expand **Report Manager**, right-click **Package Distribution Reports**, and then choose **New > Report** to open and use the Report Wizard.	Package Distribution Reports, page 6-49
Create a report with information about the Cisco VXC Manager packages you have distributed according to the devices in your Cisco VXC Manager environment (for example, all Cisco VXC Manager package updates according to a specific Cisco VXC Manager device).	In the tree pane of the Administrator Console, expand **Report Manager**, right-click **Client Package Reports**, and then choose **New > Report** to open and use the Report Wizard.	Client Package Reports, page 6-50
Create a report with information about the software installed on the devices in your Cisco VXC Manager environment according to your criteria (for example, software according to subnet).	In the tree pane of the Administrator Console, expand **Report Manager**, right-click **Installed Software Reports**, and then choose **New > Report** to open and use the Report Wizard.	Installed Software Reports, page 6-51
Create a Client Down Time report to view information about the down-time period for specific devices in your Cisco VXC Manager environment.	In the tree pane of the Administrator Console, expand **Report Manager**, right-click **Client Down Time Reports**, and then choose **New > Report** to open and use the Report Wizard.	Client Down Time Reports, page 6-53
Display an Installation Details report to view information about the installed components of Cisco VXC Manager.	In the tree pane of the Administrator Console, expand **Report Manager** and choose **Installation Details** to view the report in the details pane.	Installation Details Report, page 6-54

Table 6-1 Routine Report Manager Tasks (continued)

Tasks You Can Do	How	Details
Display a Component Details report to view information about the running components of Cisco VXC Manager.	In the tree pane of the Administrator Console, expand **Report Manager** and choose **Component Details** to view the report in the details pane.	Component Details Report, page 6-55
Create a Package Synchronization History report to view the details of Cisco VXC Manager package synchronizations for each Cisco VXC Manager package in the Master Repository with a Remote Repository.	In the tree pane of the Administrator Console, expand **Report Manager**, expand **Package Synchronization Reports**, and then choose **Package Synchronization History** to view the report in the details pane.	Package Synchronization History Reports, page 6-56. See also Package Synchronization Reports, page 6-56.
Create an Unsynchronized Packages report to view the details of Cisco VXC Manager package synchronizations that have not taken place for Cisco VXC Manager packages in the Master Repository with a Remote Repository.	In the tree pane of the Administrator Console, expand **Report Manager**, expand **Package Synchronization Reports**, and then choose **Unsynchronized Packages Report** to view the report in the details pane.	Unsynchronized Packages Reports, page 6-57. See also Package Synchronization Reports, page 6-56.
Create an Orphaned Package report to view the details of Cisco VXC Manager packages that still remain in the Remote Repository while the related Cisco VXC Manager packages have been deleted in the Master Repository.	In the tree pane of the Administrator Console, expand **Report Manager**, expand **Package Synchronization Reports**, and then choose **Orphaned Package Report** to view the report in the details pane.	Orphaned Package Reports, page 6-59. See also Package Synchronization Reports, page 6-56.

Log Reports

Log Reports provide information about the activities related to all Cisco VXC Manager components according to your logging preferences (see Logging Preferences, page 7-75).

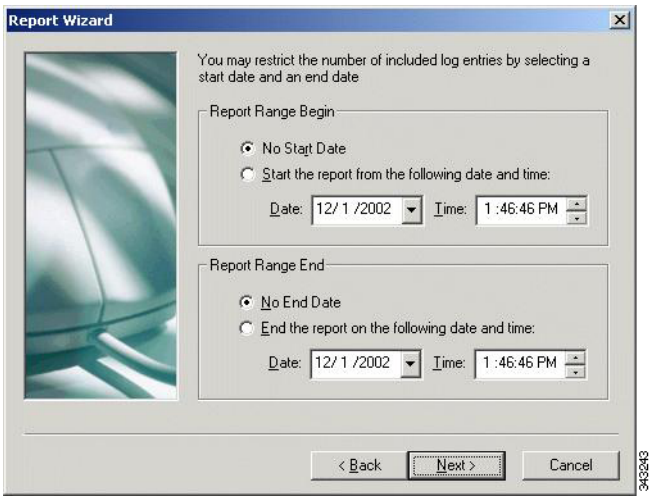
Tip After you create a Log Report, Cisco VXC Manager automatically saves the criteria and there is no need to create that report again. Each time you view the report (click the report name in the appropriate folder) you see current information according to the criteria you set. You can also refresh a report by right-clicking the folder containing the report and selecting **Refresh**.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Report Manager**, right-click **Log Reports** and choose **New > Report** to open the Report Wizard.

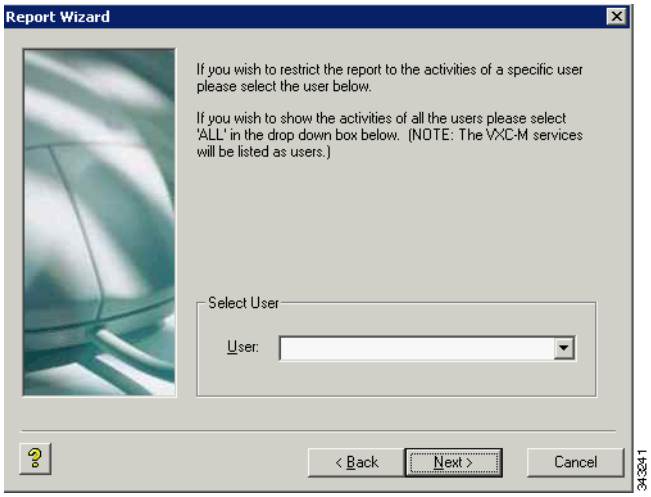
Step 2 Enter a name and description for the report (so you can easily recognize it later) and click **Next**.

Figure 6-2 Start and End Options



Step 3 Set the start and end options you want, and then click **Next**.

Figure 6-3 Specify Users



Step 4 Choose the option you want from the User list, and then click **Finish** to create the report.

Device Listings

The Device Listings report provides information about the devices in your Cisco VXC Manager environment according to your grouping (“listing”) criteria.

Tip Once you create a Device Listings report, Cisco VXC Manager automatically saves the criteria and there is no need to create that report again. Each time you view the report (click the report name in the appropriate folder) you see current information according to the criteria you set. You can also refresh a report by right-clicking the folder containing the report and choosing **Refresh**.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Report Manager**, right-click **Device Listings** and choose **New > Report** to open the Report Wizard.

Step 2 Use the following guidelines when creating the report:

- Enter a name and description for the report (so you can easily recognize it later).
- Choose a Group you want in the Select a Group list to display the Group Selections available for that Group.
- After selecting the item in the Group Selections list you want, you can add it (click **Add**) to the Selected Items pane using either the **AND** option or the **OR** option.
- When adding more than one item in the Group Selections list from the same Group to the Selected Items pane, you must use the **OR** condition.
- When selecting across different Groups, you can use only one selection condition, either **AND** or **OR**. For example, if you choose the **OS** and **Subnet Groups**, and the selection condition is **AND**, the report will list only the devices that meet both the **OS** and **Subnet** criteria. Conversely, if the selection condition for the same two Groups is **OR**, the report will list all devices that match the **OS** criteria (regardless of subnet) and all devices that match the **Subnet** criteria (regardless of OS).
- The conditions **AND** and **OR** are global. After you apply the **AND** or **OR** condition to the first two selection Groups, that same condition applies to all other selections across other Groups you choose.
- To remove an item from the Selected Items pane, choose the item and click **Remove**.
- To remove all items from the Selected Items pane, click **Clear All**.

Step 3 After completing your criteria, click **OK** to create the report.

Package Distribution Reports

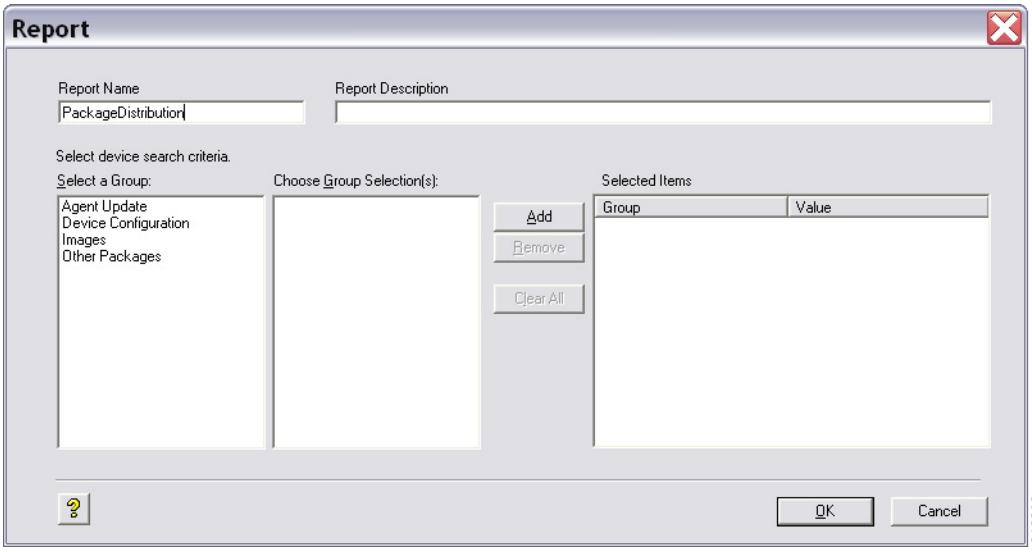
Package Distribution Reports provide information about managed devices according to the Cisco VXC Manager packages you have distributed.

Tip Once you create a Package Distribution Report, Cisco VXC Manager automatically saves the criteria and there is no need to create that report again. Each time you view the report (click the report name in the appropriate folder) you see current information according to the criteria you set. You can also refresh a report by right-clicking the folder containing the report and choosing **Refresh**.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Report Manager**, right-click **Package Distribution Reports** and choose **New > Report** to open the Report Wizard.

Figure 6-4 Package Distribution Reports Criteria



Step 2 Use the following guidelines when you create the report:

- Enter a name and description for the report (so you can easily recognize it later).
- Choose a Group you want in the **Select a Group** list to display the Group Selections available for that Group.
- After selecting the items in the Group Selections list you want, you can add them (click **Add**) to the Selected Items pane.
- To remove an item from the Selected Items pane, choose the item (for example, **Update5XPE**) and click **Remove**.
- To remove all items from the Selected Items pane, click **Clear All**.

Step 3 After completing your criteria, click **OK** to create the report.

Client Package Reports

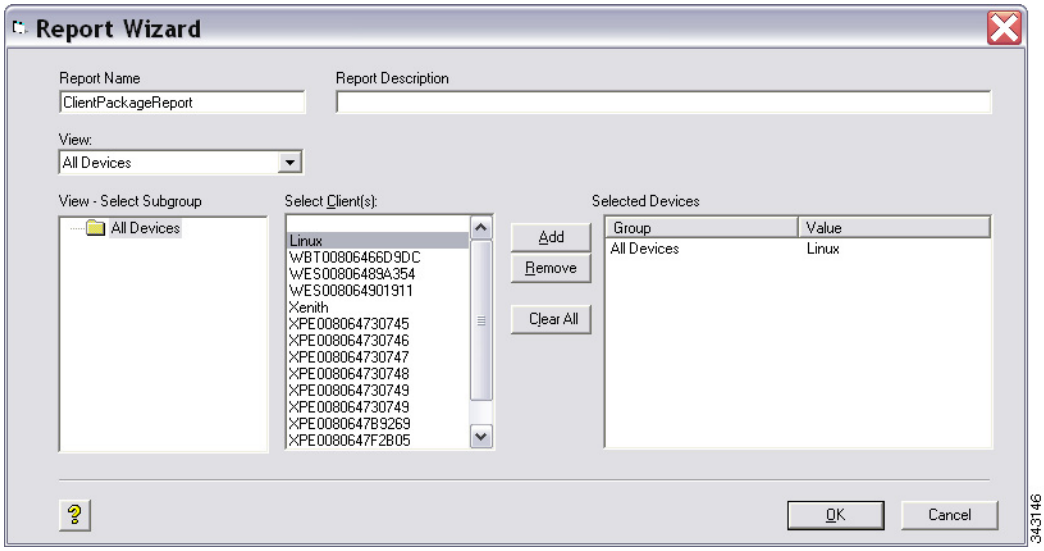
Client Package Reports provide information about the Cisco VXC Manager packages you have distributed according to the devices in your Cisco VXC Manager environment.

Tip Once you create a Client Package Report, Cisco VXC Manager automatically saves the criteria and there is no need to create that report again. Each time you view the report (click the report name in the appropriate folder) you see current information according to the criteria you set. You can also refresh a report by right-clicking the folder containing the report and choosing **Refresh**.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Report Manager**, right-click **Client Package Reports** and choose **New > Report** to open the Report Wizard.

Figure 6-5 Client Package Reports Criteria



Step 2 Use the following guidelines when creating the report:

- Enter a name and description for the report (so you can easily recognize it later).
- Choose a view that contains the devices you want in the View list (for information on creating a View, see Managing Views, page 7-63).
- Choose a Subgroup that contains the devices you want in the View - Select Subgroup list to display the clients available for that subgroup.
- After you choose the items in the Select Clients list, click **Add** to add them to the Selected Devices pane.
- To remove an item from the Selected Devices pane, choose the item (for example, **WES008**) and click **Remove**.
- To remove all items from the Selected Devices pane, click **Clear All**.

Step 3 After you complete your criteria, click **OK** to create the report.

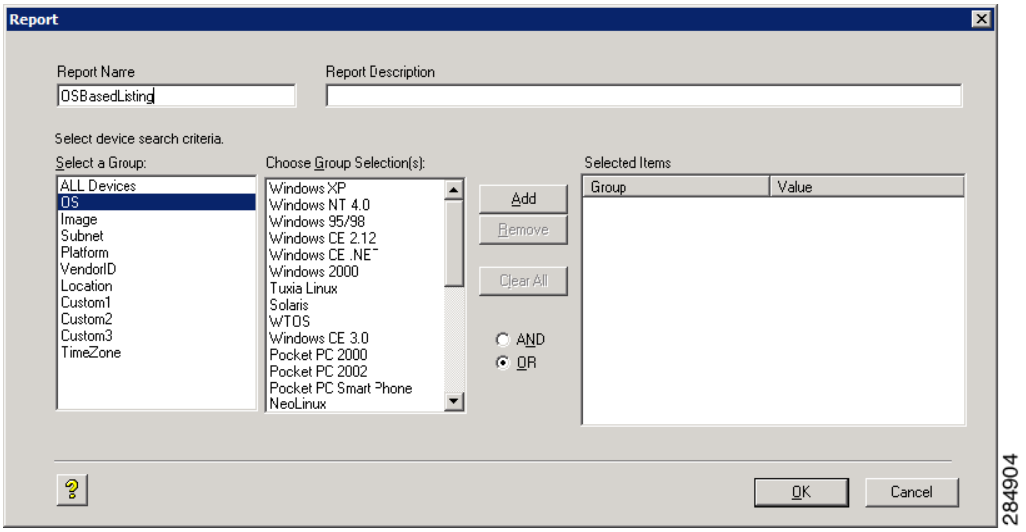
Installed Software Reports

Installed Software Reports provide information about the software installed on the devices in your Cisco VXC Manager environment according to your criteria.

Tip After you create an Installed Software report, Cisco VXC Manager automatically saves the criteria and you do not need to create that report again. Each time you view the report (click the report name in the appropriate folder) you see current information according to the criteria you set. You can also refresh a report by right-clicking the folder containing the report and selecting **Refresh**.

Step 1 In the tree pane of the Administrator Console, expand **Report Manager**, right-click **Installed Software Reports** and choose **New > Report** to open the Report Wizard.

Figure 6-6 Report Wizard



Step 2 Use the following guidelines when creating the report:

- Enter a name and description for the report (so you can easily recognize it later).
- Choose the software you want in the Select Software list to display the version available for that Software.
- Choose the version you want in the Select Version list.
- Depending on whether or not the software is already installed on the devices, choose **Yes** or **No**.
- Choose a group you want in the Select a Group list to display the Group Selections available for that group.
- After selecting the item in the Group Selections list you want, you can add it (click **Add**) to the Selected Items pane using either the AND option or the OR option.
- When adding more than one item in the Group Selections list from the same group to the Selected Items pane, you must use the OR condition. For example, if you choose **SUSE Linux** and **ThreadX** from the OS group, you must use the OR condition (the report will display all devices that run any of the selected operating systems).
- When selecting across different groups, you can use only one selection condition, either AND or OR. For example, if you choose the OS and Subnet groups, and the selection condition is AND, the report will list only the devices that meet both the OS and Subnet criteria. Conversely, if the selection condition for the same two groups is OR, the report will list all devices that match the OS criteria (regardless of subnet) and all devices that match the Subnet criteria (regardless of OS).

- The conditions AND and OR are global. After you apply the AND or OR condition to the first two selected groups, that same condition applies to all other selections across other groups you choose.
- To remove an item from the Selected Items pane, choose the item (for example, SUSE Linux) and click **Remove**.
- To remove all items from the Selected Items pane, click **Clear All**.

Step 3 After completing your criteria, click **OK** to create the report.

Client Down Time Reports

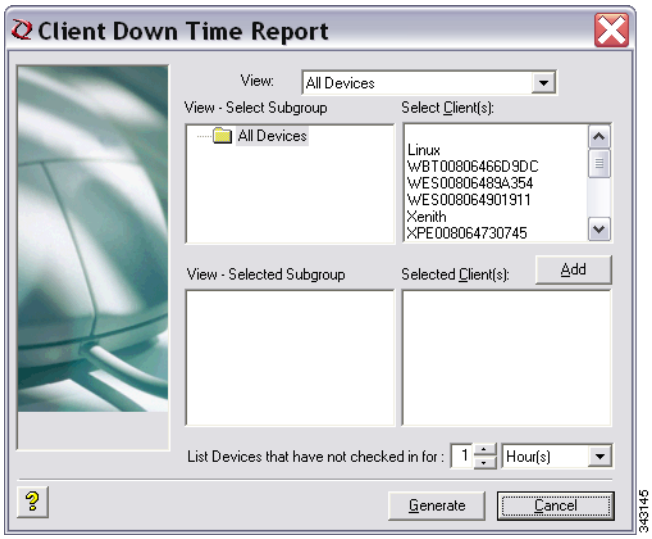
Client Down Time Reports provide information about the downtime period for specific devices in your Cisco VXC Manager environment.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Report Manager** and click **Client Down Time Reports**.

Step 2 In the toolbar, click the **Create A New Report** icon .

Figure 6-7 Client Down Time Reports Criteria



Step 3 Use the following guidelines when creating the report:

- Choose a view that contains the devices you want in the View list (for information on creating a View, see Managing Views, page 7-63).
- Choose a subgroup that contains the devices you want in the Select Subgroup list to display the Clients available for that Subgroup.
- After selecting the items in the Select Clients list you want, you can add them (click **Add**) to the Selected Subgroups pane and Selected Clients pane.
- Enter the time values you want in the List Devices That Have Not Checked In For fields.

Step 4 After completing your criteria, click **Generate** to create the report.

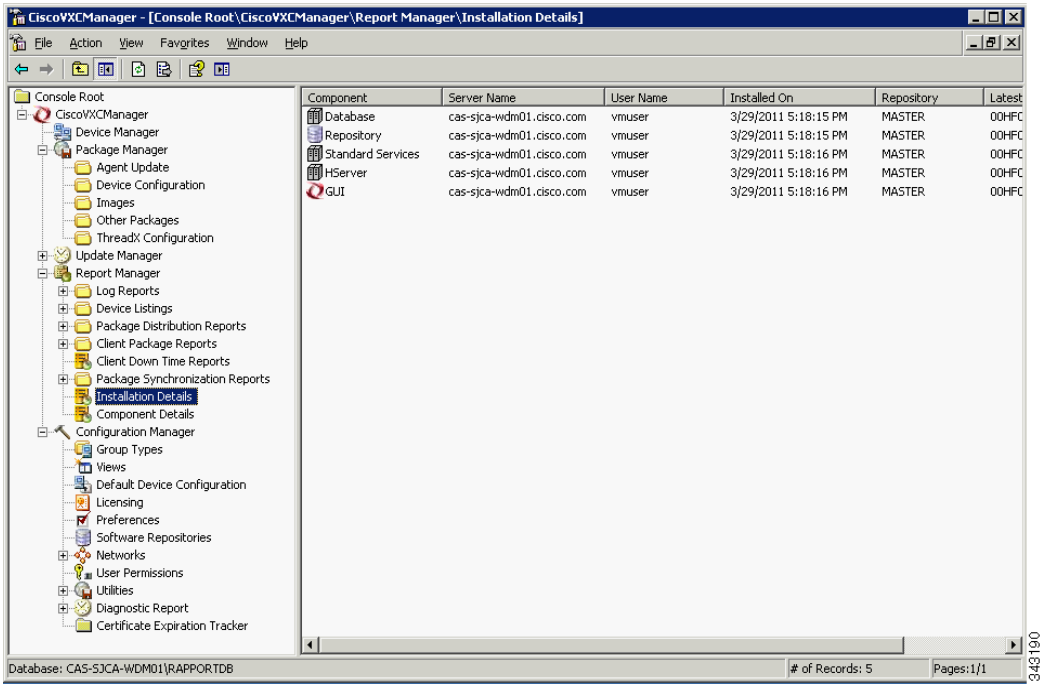
Installation Details Report

Installation Details reports provide information about the installed components of Cisco VXC Manager.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Report Manager** and choose **Installation Details** to view the report in the details pane.

Figure 6-8 Installation Details



Step 2 You can view:

- Component—Name of Cisco VXC Manager component
- Server Name—Name of the server in which the Cisco VXC Manager component is installed
- User Name—Login ID of the User of the server
- Installed On—The date and time when the Cisco VXC Manager component was installed
- Repository—Name of the main Cisco VXC Manager repository
- Latest Hot Fix ID—ID of the latest Cisco VXC Manager hotfix installed on the server

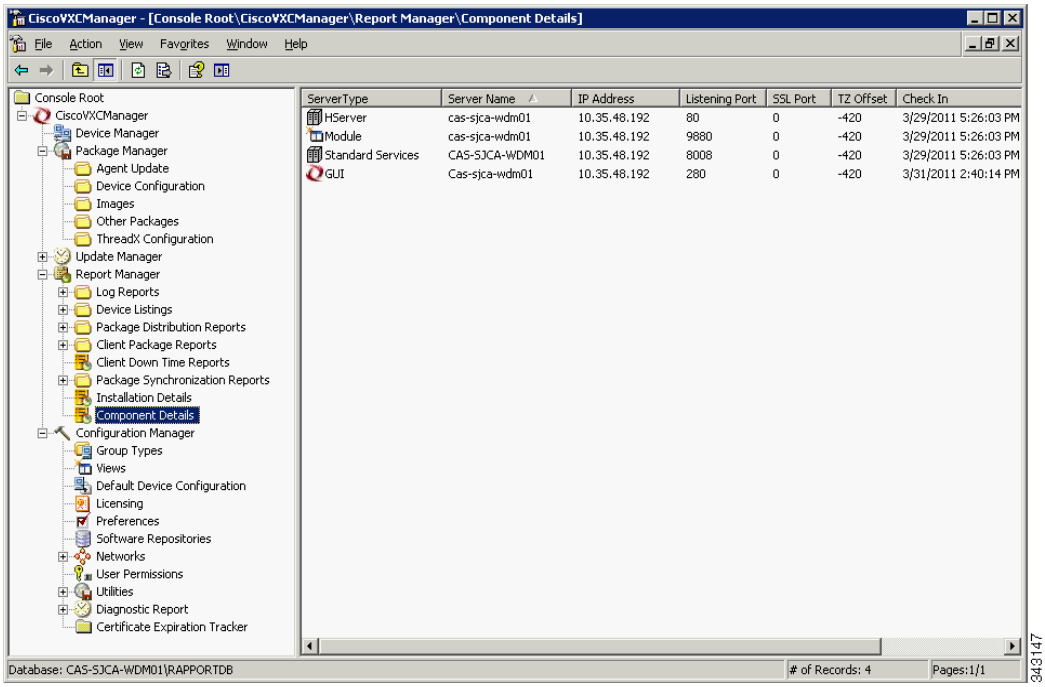
Component Details Report

Component Details reports provide information about the running components of Cisco VXC Manager.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Report Manager** and choose **Component Details** to view the report in the details pane.

Figure 6-9 Component Details



Step 2 You can view:

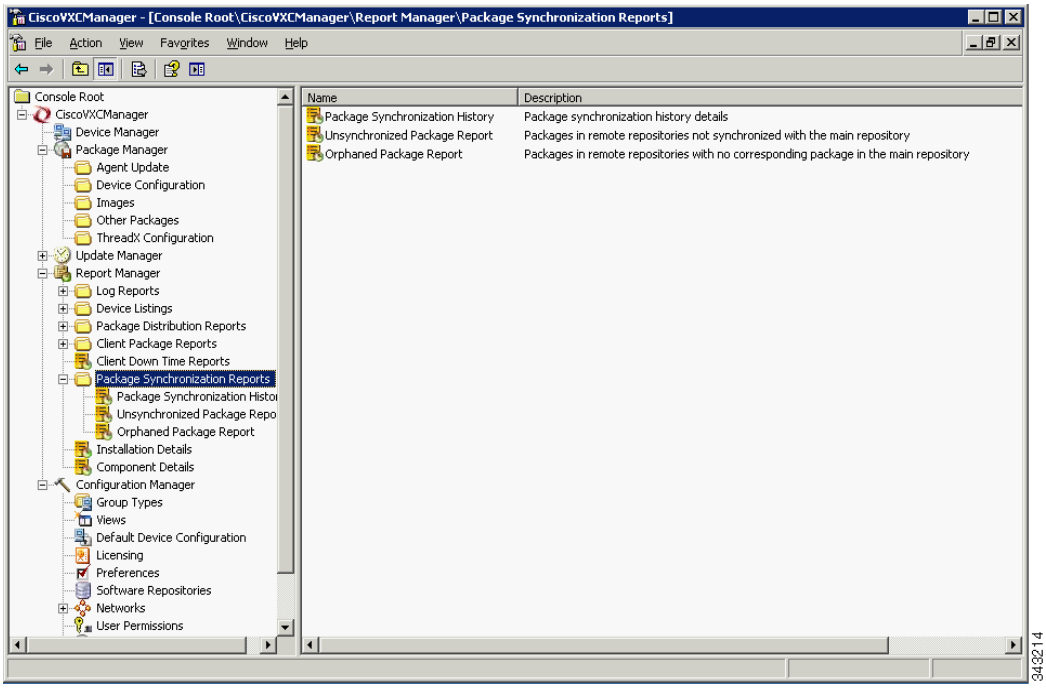
- Server Type—Name of Cisco VXC Manager component
- Server Name—Name of the server in which the Cisco VXC Manager component is installed
- IP Address—IP Address of the server in which the Cisco VXC Manager component is installed
- Listening Port—Port number where the specific component is communicating
- SSL Port—SSL Port Number
- TZ Offset—The value of the offset between the local time zone and GMT
- Check In—The date and time when the specific component checked in
- Check Out—The date and time when the specific component checked out

Package Synchronization Reports

Package Synchronization Reports provide information about the synchronization of Cisco VXC Manager packages between the Master Repository and Remote Repositories. There are three types of Package Synchronization Reports that you can view and export:

- Package Synchronization History—Displays the synchronization details of all Cisco VXC Manager packages with a Remote Repository (see Package Synchronization History Reports, page 6-56).
- Unsynchronized Package Report—Displays a row for each Cisco VXC Manager package for which the version is different between the Master Repository and Remote Repository (see Unsynchronized Packages Reports, page 6-57).
- Orphaned Package Report—Displays the list of Cisco VXC Manager packages which are present in the Remote Repository but have no corresponding Cisco VXC Manager package in the Master Repository (see Orphaned Package Reports, page 6-59).

Figure 6-10 Package Synchronization Reports



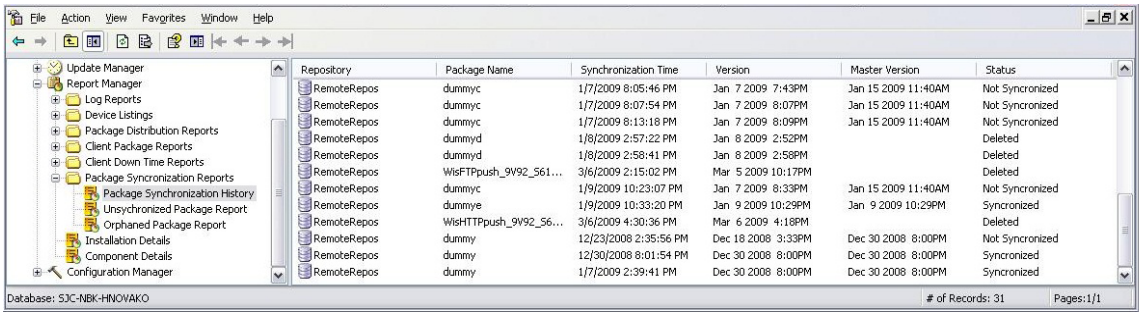
Package Synchronization History Reports

Package Synchronization History reports display the details of Cisco VXC Manager package synchronizations for each Cisco VXC Manager package in the Master Repository with a Remote Repository. One row is displayed for each time a Cisco VXC Manager package is synchronized with a Remote Repository. A Cisco VXC Manager package synchronized with n Remote Repositories will display n rows each time that Cisco VXC Manager package is synchronized.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Report Manager**, expand **Package Synchronization Reports**, and then choose **Package Synchronization History** to view the report in the details pane.

Figure 6-11 Package Synchronization History



Step 2 One row is displayed for each time a Cisco VXC Manager package is synchronized between the Master Repository and a Remote Repository. The number of rows displayed for a specific a Cisco VXC Manager package equals the number of times that Cisco VXC Manager package has been synchronized. You can view:

- Repository—Name of the Remote Repository for which the Cisco VXC Manager package was synchronized
- Package Name—Name of the Cisco VXC Manager package
- Synchronization Time—The time the Cisco VXC Manager package was synchronized with the Remote Repository. Note that the Cisco VXC Manager packages scheduled for synchronization (but not yet started) do not have a synchronization time displayed.
- Version—Only valid for the most recent synchronization of that Cisco VXC Manager package
- Master Version—Current version of the Cisco VXC Manager package in the Master Repository
- Status—Comparison of the version of the Cisco VXC Manager package between the Master Repository and a Remote Repository at the current time as follows:
  - Synchronized—The Cisco VXC Manager packages are the same.
  - Not Synchronized—The Cisco VXC Manager packages are different.
  - Deleted—The Cisco VXC Manager package in the Master Repository has been deleted (if the related Cisco VXC Manager package still remains in the Remote Repository, you can view it in the Orphaned Package report as described in Orphaned Package Reports, page 6-59).

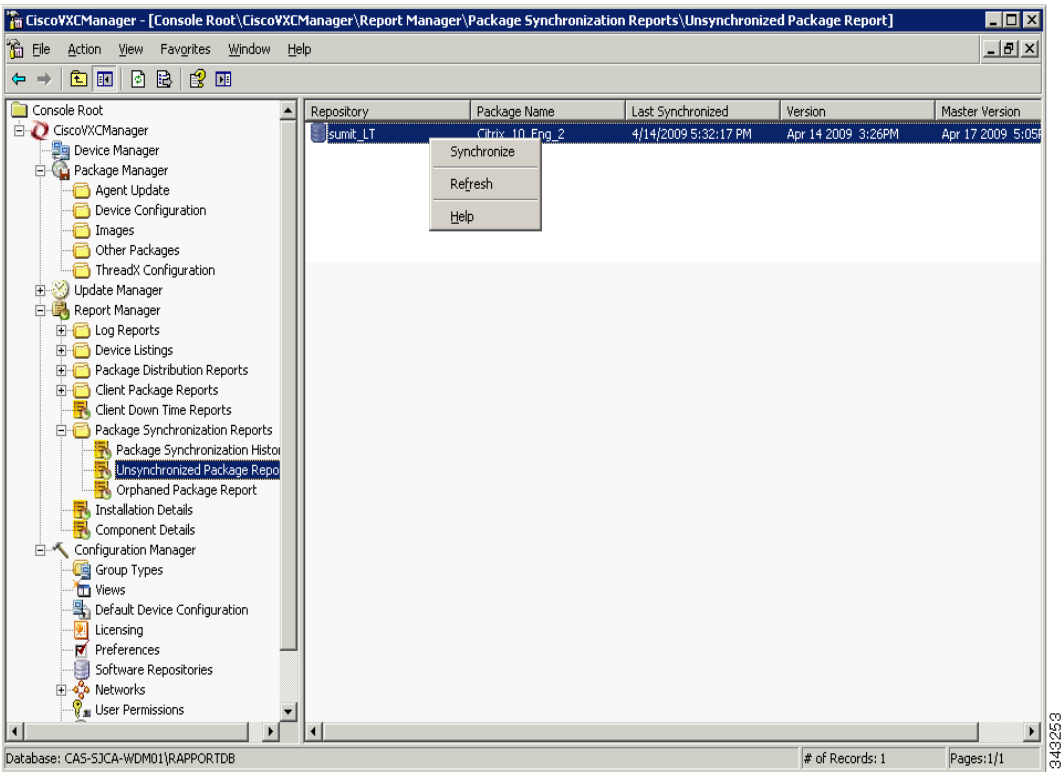
Unsynchronized Packages Reports

Unsynchronized Packages reports display the details of Cisco VXC Manager package synchronizations that have not taken place for Cisco VXC Manager packages in the Master Repository with a Remote Repository. One row is displayed for each Cisco VXC Manager package that is not synchronized with a Remote Repository. The versions of that Cisco VXC Manager package between the Master Repository and a Remote Repository are different at the current time.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Report Manager**, expand **Package Synchronization Reports**, and then choose **Unsynchronized Packages Report** to view the report in the details pane.

Figure 6-12 Unsynchronized Packages Report



Step 2 One row is displayed for each time a Cisco VXC Manager package is not synchronized between the Master Repository and a Remote Repository. The number of rows displayed for a specific Cisco VXC Manager package equals the number of times that Cisco VXC Manager package has not been synchronized. You can view:

- Repository—Name of the Remote Repository for which the Cisco VXC Manager package was not synchronized
- Package Name—Name of the Cisco VXC Manager package
- Last Synchronized—Time of the most recent synchronization (this time record is also displayed in the Package Synchronization History report for the Cisco VXC Manager package)
- Version—Current version of the Cisco VXC Manager package in the Remote Repository
- Master Version—Current version of the Cisco VXC Manager package in the Master Repository

Tip To synchronize an unsynchronized Cisco VXC Manager package immediately, right-click the Cisco VXC Manager package and choose **Synchronize**.

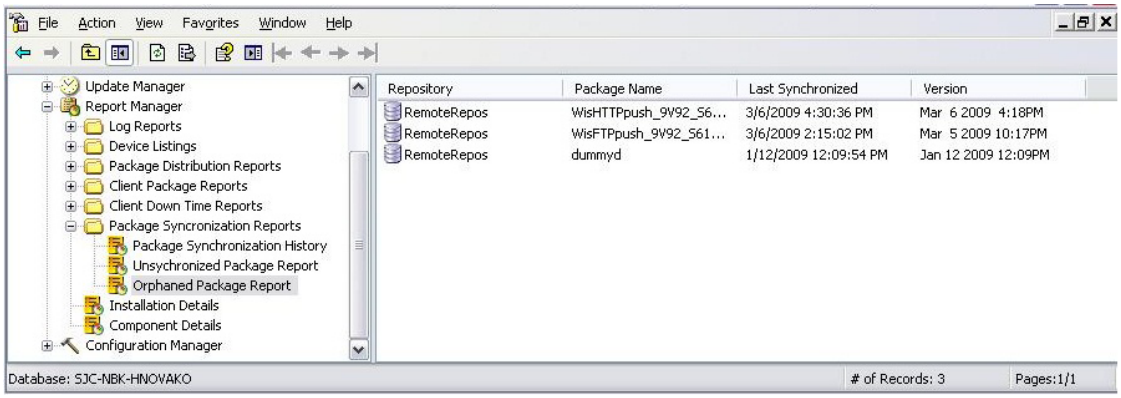
Orphaned Package Reports

Orphaned Package reports display the details of Cisco VXC Manager packages that still remain in the Remote Repository while the related Cisco VXC Manager packages have been deleted in the Master Repository. One row is displayed for each orphaned Cisco VXC Manager package that remains in a Remote Repository.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Report Manager**, expand **Package Synchronization Reports**, and then choose **Orphaned Package Report** to view the report in the details pane.

Figure 6-13 Orphaned Package Report



Step 2 One row is displayed for each orphaned Cisco VXC Manager package that remains in a Remote Repository. You can view:

- Repository—Name of the Remote Repository that contains the orphaned Cisco VXC Manager package
- Package Name—Name of the Cisco VXC Manager package
- Last Synchronized—Time of the most recent synchronization (this time record is also displayed in the Package Synchronization History report for the Cisco VXC Manager package)
- Version—Current version of the Cisco VXC Manager package in the Remote Repository

CHAPTER 7

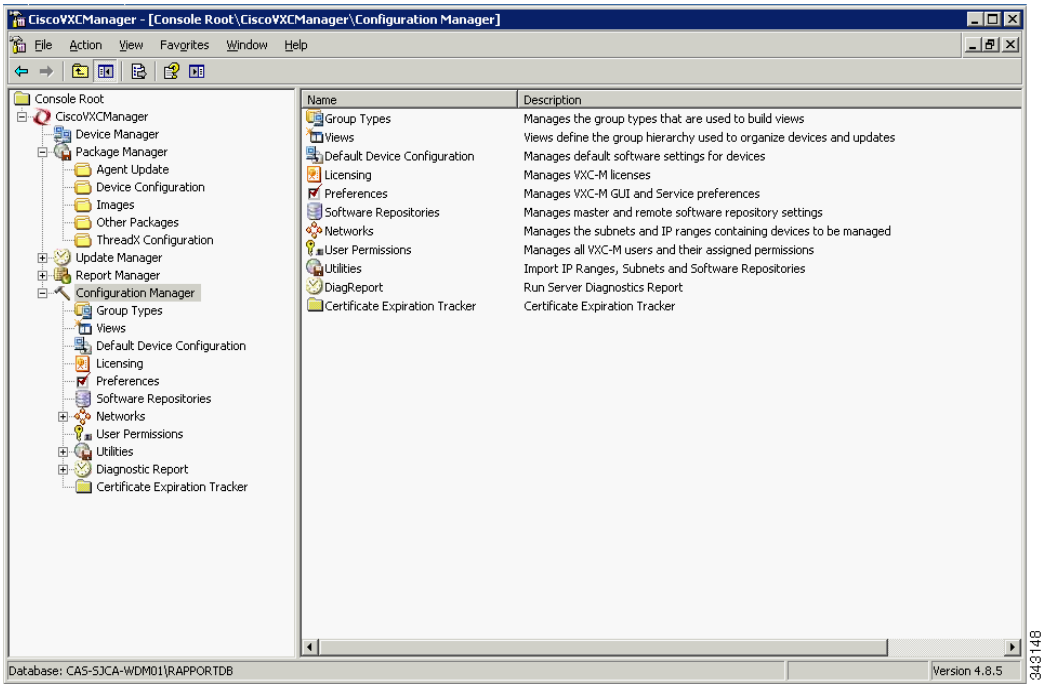
Configuration Manager

This chapter describes how to perform routine Cisco VXC Manager configuration management tasks using the Administrator Console. It provides information on managing the configuration settings and preferences of your entire Cisco VXC Manager system.

Managing Cisco VXC Manager Configuration Settings and Preferences

Click **Configuration Manager** in the tree pane of the Cisco VXC Manager Administrator Console to open the Configuration Manager. The Configuration Manager allows you to quickly view and manage essential functionalities within your Cisco VXC Manager environment. It also allows you to easily modify the design of your Cisco VXC Manager environment as your needs require (for example, you can expand necessary features of your Cisco VXC Manager environment as your company needs grow).

Figure 7-1 Configuration Manager



The Configuration Manager allows you to manage Cisco VXC Manager:

- Group Types (see Managing Group Types, page 7-62)
- Views (see Managing Views, page 7-63)
- Default Device Configurations (see Managing Default Device Configurations, page 7-66)
- Preferences (see Configuring Preferences, page 7-73)
- Software Repositories (see Understanding Cisco VXC Manager Repositories, page 7-86)
- Networks (see Managing Networks, page 7-90)
- User Permissions (see Managing User Permissions, page 7-94)
- Utilities (see Using Cisco VXC Manager Utilities, page 7-98)
- Diagnostic Reports (see Generating Diagnostic Reports, page 7-103)
- Certificate Expiration Trackers (see Using the Certificate Expiration Tracker, page 7-104)

Managing Group Types

Group Types allow you to create or build the Views you need for easy device and update organization and management. After creating the Group Types you need, you can create a View of devices you must manage (such as WTOS devices on a certain subnet in a certain building), and then use that View (for example, with Device Manager) so you can quickly find those devices and perform your tasks.

For convenience, Cisco VXC Manager provides several predefined Group Types by default: OS, Platform, Image/Firmware Image Number, Subnet, Location, TimeZone, VendorID, Custom1, Custom2, and Custom3. Cisco VXC Manager also allows you to create the custom Group Types you need. By combining predefined Group Types and custom Group Types, you can achieve high levels of granularity in your Views (for information on creating Views, refer to Managing Views, page 7-63). For more information on Group Types and Views, see Understanding Group Types and Views, page A-1.

This section contains information on:

- Creating Custom Group Types, page 7-62
- Editing Custom Group Types, page 7-63
- Deleting Custom Group Types, page 7-63

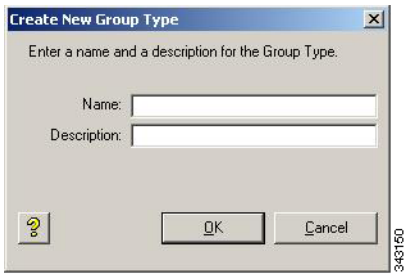
Creating Custom Group Types

Use the following procedure to create custom group types.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, right-click **Group Types**, and then choose **New > Group** to open the Create New Group Type dialog box.

Figure 7-2 Create New Group Type



Step 2 Enter the name and description.

Step 3 Click **OK** to add the Group Type to the list of available Group Types that you can use when assigning devices to groups (see Assigning Devices to Groups, page A-3).

Editing Custom Group Types

In the tree pane of the Administrator Console, expand **Configuration Manager**, click **Group Types**, right-click on the Group Type you want to edit, and then choose **Properties** to open and use the Edit Group Type dialog box. Note that you cannot edit a predefined Group Type.

Deleting Custom Group Types

In the tree pane of the Administrator Console, expand **Configuration Manager**, click **Group Types**, right-click on the Group Type you want to delete, choose **Delete**, and then click **Yes** to confirm. Note that you cannot delete a predefined Group Type.

Managing Views

Cisco VXC Manager Views allow you to visually organize or filter your devices functionally so that you can more easily manage them. Views consist of hierarchies of folder groups, whether the folders are for a Group Type (predefined and/or custom), a Group Instance (within a Group Type), or any combination of these items. For more information on Group Types and Views, see Understanding Group Types and Views, page A-1.

This section contains information on:

Creating Views

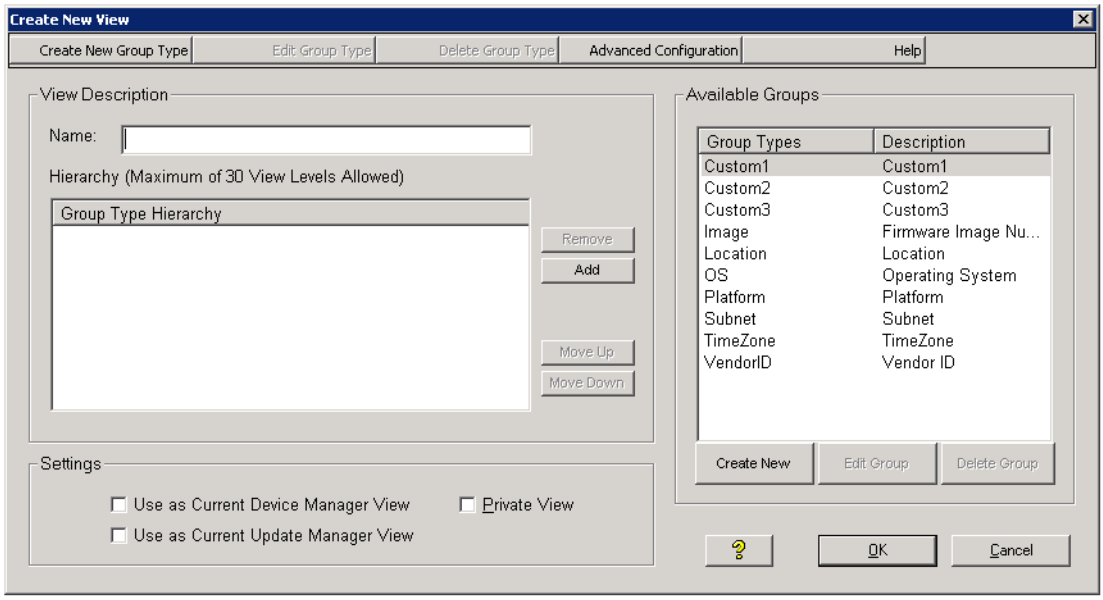
Use the following procedure to create views.

Tip Be sure you have created the group types you need to create or build the views you want (see Managing Group Types, page 7-62).

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, right-click **View**, and then choose **New > View** to open the Create New View dialog box.

Figure 7-3 Create New View



Step 2 Use the following guidelines when creating the View:

- Enter a Name for the View (so you can easily recognize it later).
- Choose a Group Type you want in the Available Groups list, and then add it (click **Add**, double-click it, or drag-and-drop it to the position you want) to the Group Type Hierarchy pane (you can also use the **Create New**, **Edit Group**, and **Delete Group** command buttons as needed for convenience—see Managing Group Types, page 7-62).
- You can continue to choose the Group Types in the Available Groups list you want to add to the View (up to 30 levels).
- When adding Group Types to the View, you can choose an item in the Group Type Hierarchy list and use the **Remove**, **Move Up**, and **Move Down** command buttons as needed to build the Group Type Hierarchy you want for the View.
- To have the current View you are building automatically displayed as the default view when you click on **Device Manager** in the tree pane of the Administrator Console, check the **Use as Current Device Manager View** check box. Any previous default view is replaced by this new default view (and moved to the Select Current Manager View list you can use when switching views).

- To have the current View you are building automatically selected during the update creation process (and displayed as the default view when you click on **Update Manager** in the tree pane of the Administrator Console—the default while viewing the scheduled Cisco VXC Manager packages), check the **Use as Current Update Manager View** check box. Any previous default view is replaced by this new default view (and moved to the Select Current Manager View list you can use when switching views).
- To have the current View you are building available only to you, the current user, check the **Private View** check box. Uncheck the check box (the default) to make the view available to all administrators authorized to use Cisco VXC Manager.

Tip You can also use the **Advanced Configuration** command button to make further configurations as described in Using Advanced View Configuration Options, page 7-65.

Step 3 After you have finished configuring the View you want, click **OK** to add the View to the available Views that you can use.

Editing Views

In the tree pane of the Administrator Console, expand **Configuration Manager**, click **Views**, right-click on the View you want to edit, and then choose **Properties** to open and use the Edit View dialog box.

Deleting Views

In the tree pane of the Administrator Console, expand **Configuration Manager**, click **Views**, right-click on the View you want to delete, choose **Delete**, and then click **Yes** to confirm.

Tip You cannot delete a View that is currently in use with either the Device Manager or Update Manager (you must switch to a different View before you can delete it).

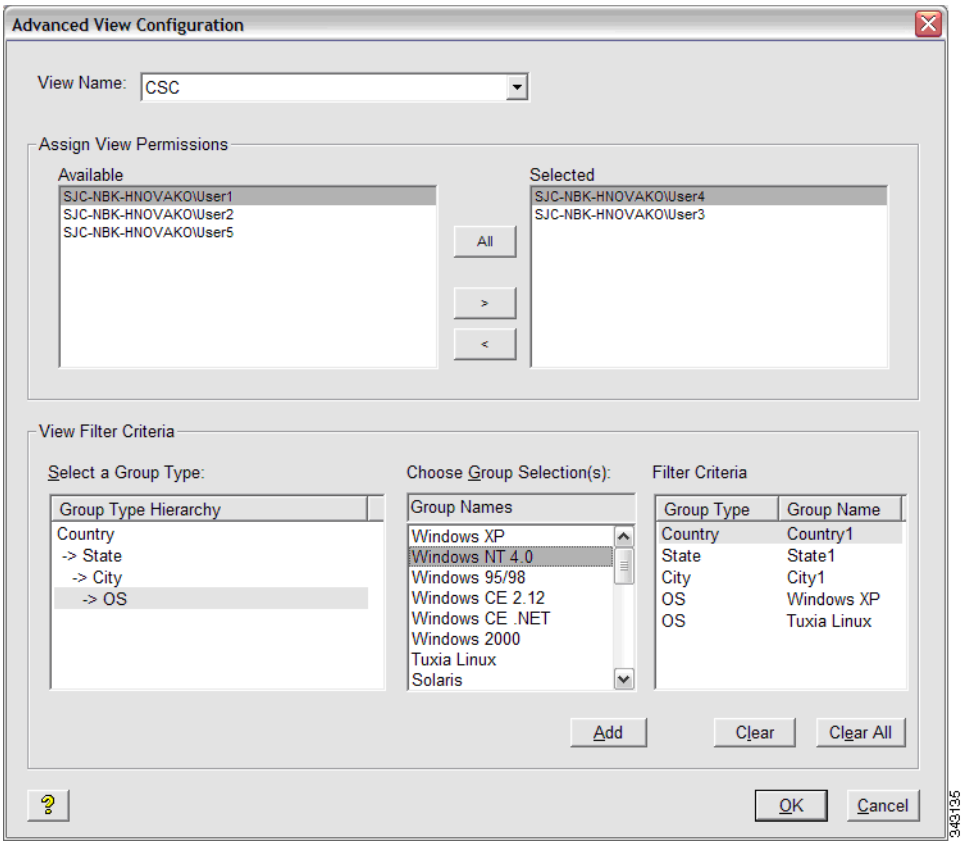
Using Advanced View Configuration Options

Administrators can use the Advanced View Configuration options (Assign View Permissions and View Filter Criteria) for easier user and device administration with Views.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, click **Views**, right-click on a View you want to further configure with the Advanced View Configuration options, and then choose **Advanced Filter** to open and use the Advanced View Configuration dialog box.

Figure 7-4 Advanced View Configuration



Step 2 Use the following guidelines:

- To give permissions to access the selected View to different users, choose the users in the Available list, and then use the command buttons (or double-click the users) to assign the users to the Selected pane (click **All** to assign all available users).
- To assign filter criteria for each or any of the Groups Types in the Group Type Hierarchy of the View, choose a Group you want in the Select a Group list to display the Group Selections available for that Group, choose the item in the Group Selections list you want to include in the filter criteria for the View, and then add it (click **Add** or double-click the item) to the Filter Criteria pane (use **Clear** or **Clear All** as needed to remove selection).

Step 3 After selecting the Advanced View Configuration options you want, click **OK**.

Managing Default Device Configurations

The Default Device Configuration (DDC) functionality allows you to configure default configurations for a group of devices. This functionality ensures that the device conforms to your configurations. If there is any deviation from your default configurations, Cisco VXC Manager reverts the device back to your specified configurations. This feature automates the recovery of failed devices, the re-purposing of existing devices, and the addition of new devices within an existing infrastructure.

Caution Before creating and assigning a DDC to update devices automatically, you must register the appropriate Cisco VXC Manager packages that contain the settings, applications, or image updates you want to assign as a DDC. You must also check the **Enable Default Device Configuration** check box in the Default Device Configuration dialog box, as described in Device Manager Preferences, page 7-73.

This section contains information on:

Configuring Default Device Configuration Preferences

Use the following procedure to configure Default Device Configuration (DDC) and scheduling preferences for DDC image upgrades.

Procedure

Step 1 In the tree pane of the Administrator Console, choose **Configuration Manager > Preferences**.

Step 2 In the details pane, double-click **Device Manager Preferences**.

Step 3 In the tree pane of the Preferences dialog box, click **DDC**.

Step 4 Under Default Device Configuration, check the **Enable Default Device Configuration** check box.

Step 5 Under Time to Schedule DDC Reconciliation, click **Upon Checkin**.

Step 6 In the tree pane of the Preferences dialog box, click **Scheduling**.

Step 7 Under Imaging Option, click **Merlin**.

Step 8 Click **OK**.

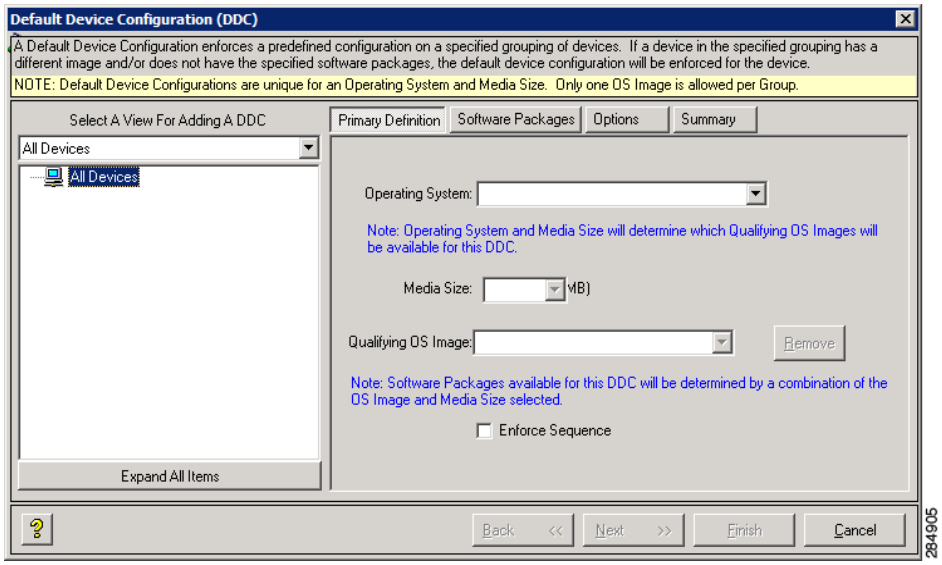
Creating and Assigning Default Device Configurations

Use the following procedure to create and assign Default Device Configurations.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, right-click **Default Device Configuration**, and choose **New > Default Device Configuration** to open the Default Device Configuration Wizard.

Figure 7-5 Default Device Configuration Wizard—Primary Definition Tab



Step 2 Use the following guidelines for the Primary Definition tab:

- Select A View For Adding A DDC—Choose the View that includes the groups of the devices to which you intend to assign the DDC. After you choose a View, the View Hierarchy pane shows the various groups and levels of that View (you can use **Expand All Items** to display all levels in your View). In the View Hierarchy pane, choose the group folder that contains the devices to which you want to assign the DDC.
- Operating System—Choose the operating system of the devices to which you want to assign the DDC.
- Media Size—Enter the media size (in MBs) of the devices to which you want to assign the DDC. The Cisco VXC Manager script package file for any Cisco VXC Manager packages to be used in a DDC must specify the media size value of the intended target devices in the imagesize parameter under the [Version] section of script (for example, Imagesize=32). For more information on scripts, refer to Cisco VXC Manager ScriptBuilder Tool and Scripting Language, page H-1.

Tip For ThreadX devices the Media Size must be 0, for WTOS devices the media size must be 128, and for SUSE Linux devices the Media Size must be 4000.

- Qualifying OS Image—Choose the image associated with the OS you want to form the basis for the DDC that you want to assign. (Choosing an image is not mandatory. You can choose **No Image** from the list to avoid imaging; simply choose the settings and other add-ons without choose an image.) If you do choose an image, the image package must be named to correspond with the image number displayed by the Device Manager.

Tip For SUSE Linux devices, choose No Image.

- Remove—Click **Remove** to remove the image associated with the group in a DDC. Use this button to remove the group from the DDC definition.

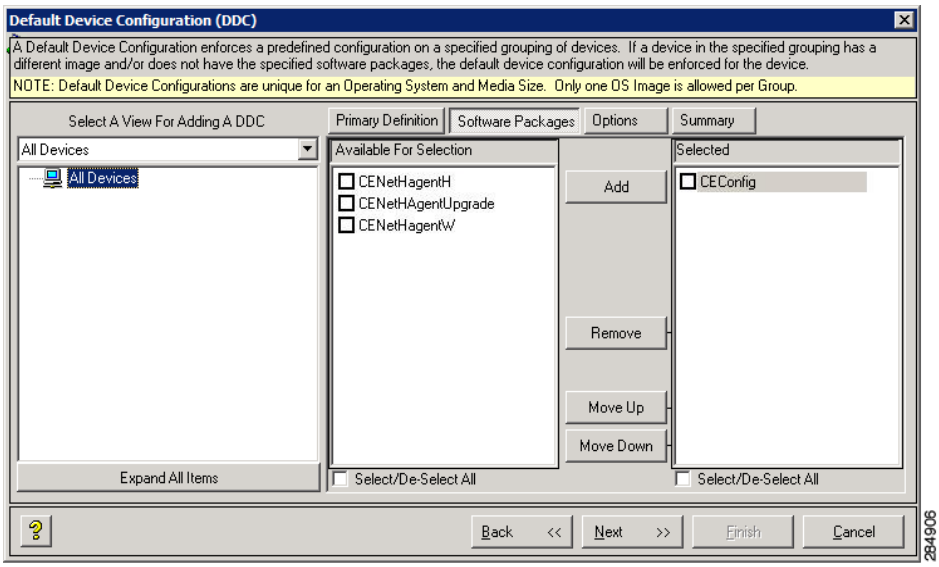
Tip You can assign different images and packages to different View folders.

- Enforce Sequence—Depending on whether or not you want the Cisco VXC Manager packages that are a part of the DDC to be the only packages allowed for the devices (that is no other packages can be sent to the devices), check or uncheck **Enforce Sequence**.

Caution If you check **Enforce Sequence,** this parameter may interfere with any Cisco VXC Manager packages that are sent or scheduled to a device outside the DDC process.

Step 3 After configuring your settings, click **Next** to open the Software Packages tab.

Figure 7-6 Default Device Configuration Wizard—Software Packages Tab



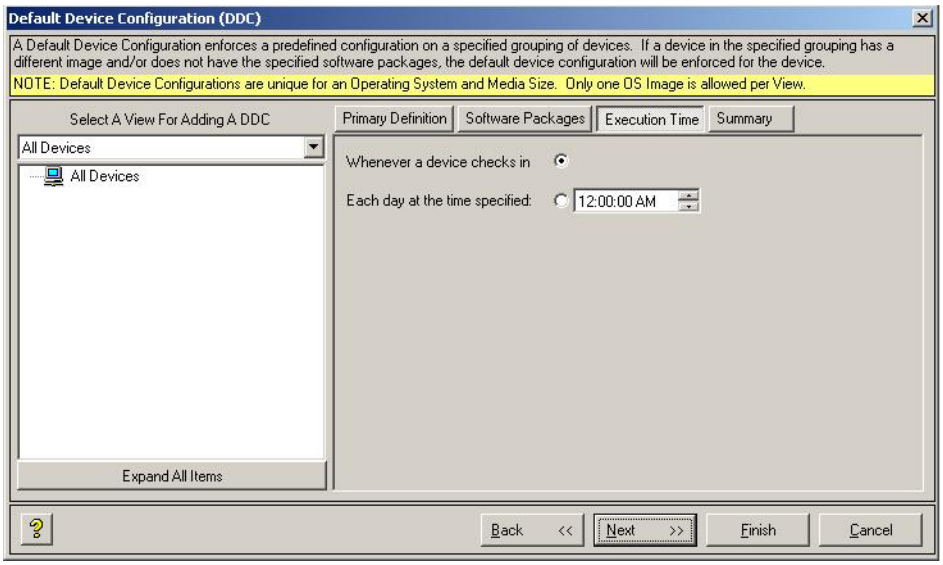
Step 4 Choose the Cisco VXC Manager packages in the Available For Selection list that you want to include in the DDC and click **Add** to move them to the Selected list.

Tip Click **Add** and **Remove** to move as many packages as you want to (and from) the Selected list. Check or uncheck **Select/De-Select All** to check or uncheck all package check boxes in the Available For Selection list or the Selected list. Click **Move UP** and **Move Down** to change the order of the Cisco VXC Manager packages in the Selected list. When you move the mouse over the listed software packages, a tooltip displays a description of the corresponding package.

Step 5 (Optional) To add different OS images and software packages to specific groups within your view, you can return to the Primary Definition tab and complete steps 2 through 4 for each group you want.

Step 6 After configuring your settings, click **Next** to open the Options tab.

Figure 7-7 Default Device Configuration Wizard—Options Tab



Step 7 Use the following guidelines for the Options tab:

- Execute DDC:

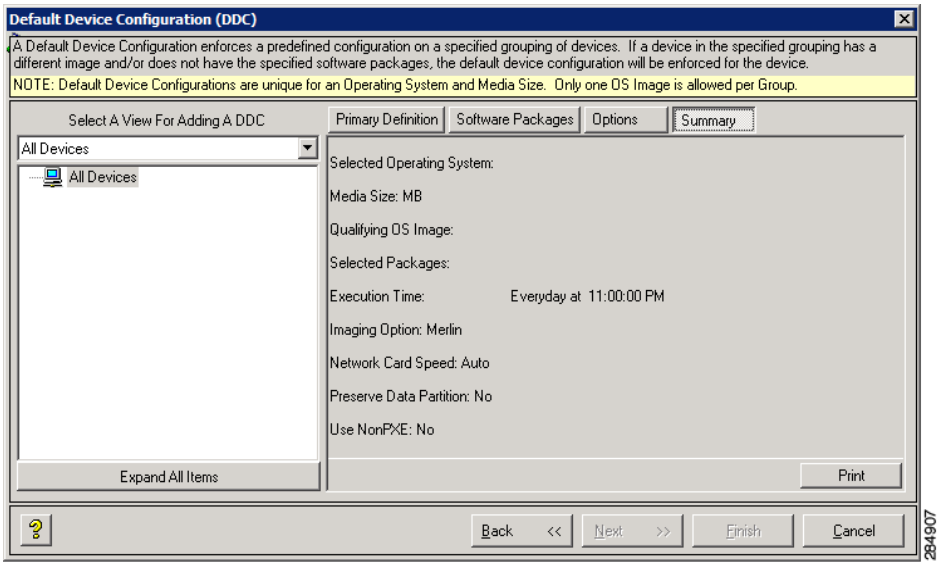
  Click either the **Whenever a device checks in** radio button or the **Each day at the time specified** radio button for DDC execution (if you click the **Each day at the time specified** radio button, be sure to enter or choose the time you want).

- Options:
  - Check the **Preserve Data Partition** check box if you want to preserve any existing custom data partition you have on the client (outside of the partition used by the firmware).
  - Check the **Use Non PXE** check box if you are imaging using Non-PXE.

Tip The Preserve Data Partition option is only available for use with clients using multiple data partitions totaling 4 GB or larger, allowing you to remove the partition used for custom data that is not write filter protected (this is the custom data partition outside of the partition used for write filter protected firmware).

Step 8 After configuring your settings, click **Next** to open the Summary tab.

Figure 7-8 Default Device Configuration Wizard—Summary Tab



Step 9 View the Summary tab to ensure that you have configured the DDC the way you want (if not, click **Back** and make your changes), and then click **Finish** to open the details pane displaying the newly assigned DDC.

The DDC is identified by its Operating System and Media Size. The next time a device from the View you specified checks-in or is discovered, and meets the Operating System and Media Size criteria, it is automatically assigned the DDC.

Tip For information on viewing the Summary of a DDC in your Cisco VXC Manager system, see Viewing the Summary of a Default Device Configuration, page 7-71.

Editing Default Device Configurations

In the tree pane of the Administrator Console, expand **Configuration Manager**, click **Default Device Configuration**, right-click on the DDC you want to edit, and then choose **Properties** to open and use the Edit Default Device Configuration dialog box.

Deleting Default Device Configurations

In the tree pane of the Administrator Console, expand **Configuration Manager**, click **Default Device Configuration**, right-click on the DDC you want to delete, choose **Delete**, and then click **Yes** to confirm.

Viewing the Summary of a Default Device Configuration

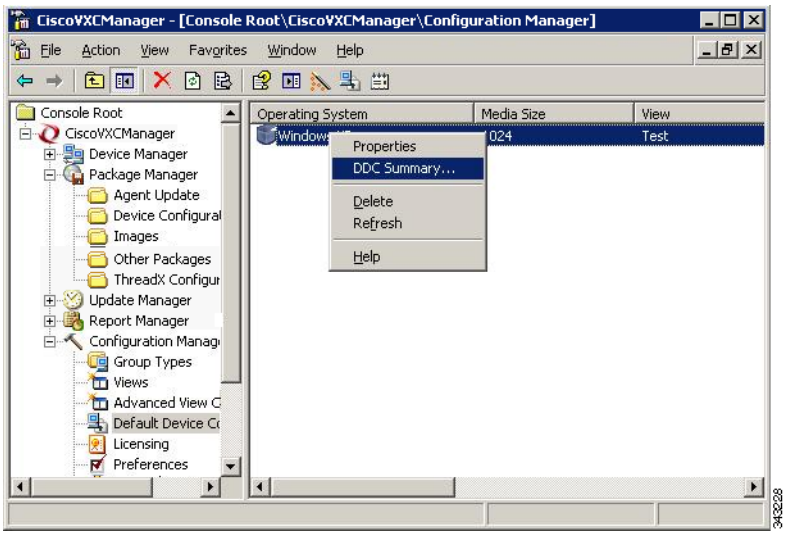
Use the following procedure to view the summary of a Default Device Configuration.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager** and choose **Default Device Configuration** to display your existing DDCs.

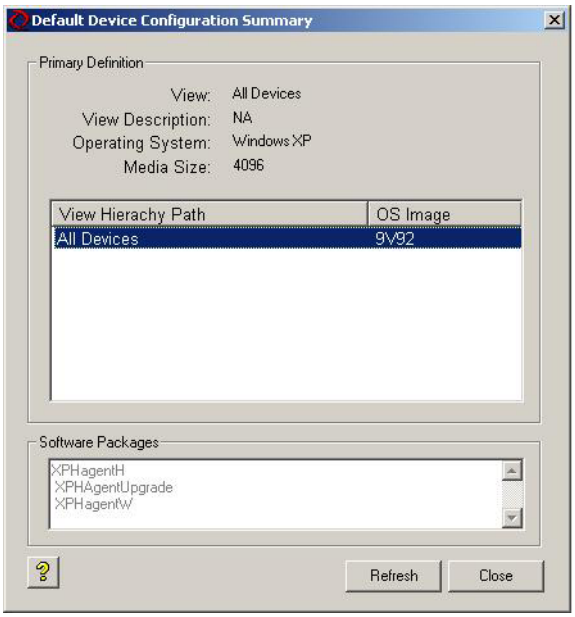
Step 2 Right-click the DDC for which you want to see the summary and choose **DDC Summary**.

Figure 7-9 Choose DDC Summary Option



Step 3 The Summary page for the specific DDC appears.

Figure 7-10 DDC Summary



Configuring Preferences

Use the following procedure to configure preferences.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, and then click **Preferences** to display the list of preferences available in the details pane.

Step 2 Double-click the name of the preference you want to configure to open and use the Preferences dialog box.

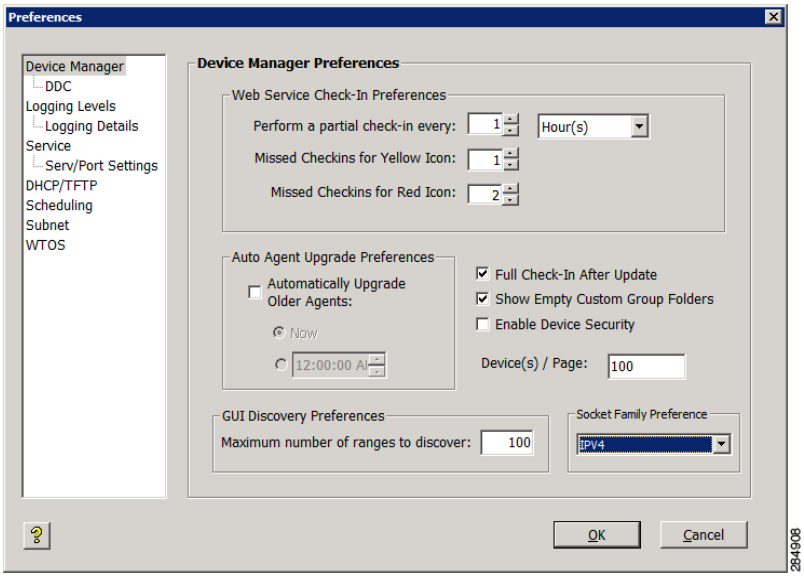
Step 3 Depending on the preferences you want to configure, refer to the following:

- Device Manager Preferences, page 7-73
- Logging Preferences, page 7-75
- Service Preferences, page 7-78
- DHCP/TFTP Preferences, page 7-82
- Scheduling Preferences, page 7-83
- Subnet Preferences, page 7-85
- WTOS Preferences, page 7-85

Device Manager Preferences

Double-click **Device Manager** in the list of preferences to open the Device Manager Preferences dialog box.

Figure 7-11 Device Manager Preferences

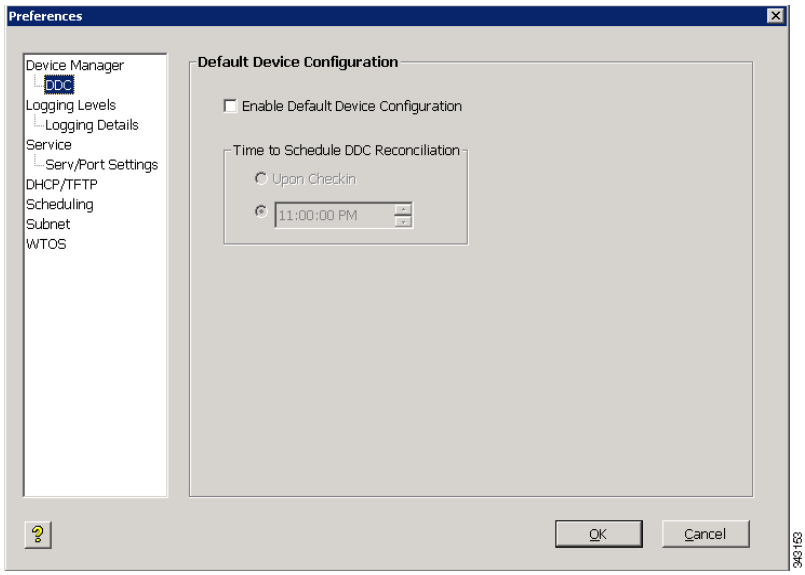


Use the following guidelines:

- Web Service Check-In Preferences area:
  - Perform a partial check-in every—Set the partial check-in frequency of all devices by selecting a number and a time unit (minutes, hours, days). The default is 1 Hour. Partial check-ins occur regularly at the specified interval to ascertain device health status (red, yellow, green). Partial check-ins require less network bandwidth than a full check-in (important for large Cisco VXC Manager installations with thousands of devices). Changes to check-in frequencies do not take effect until after the previously set check-in time or if devices are refreshed.
  - Missed Check-ins for Yellow Icon—Choose the number of missed check-ins before the icon for the device turns yellow to indicate there might be a problem with the device.
  - Missed Check-ins for Red Icon—Choose the number of missed check-ins before the icon for the device turns red to indicate there might be a serious problem with the device.
- Auto Agent Upgrade Preferences area:
  - Automatically Upgrade Older Agents—Check this check box to enable Auto-Agent Upgrades of Cisco VXC Manager Agents (HAgent), and then choose an option: Now to upgrade older Agents at the time Cisco VXC Manager discovers the Agent; or Clock to set a time at which Cisco VXC Manager will update older versions of Cisco VXC Manager Agents after discovering them (preferably, this should be a time of low network activity to avoid overloading your network with Agent upgrade transactions).
  - Full Check-In After Update—Check this check box to cause a device to check-in with the Web Service after the device receives and executes the files in a Cisco VXC Manager package.
  - Show Empty Custom Group Folders—Check this check box if you want to display any empty folders in the Device Manager when you create custom Group Types for your Views (for information on the effects this option has on device organization, see Understanding the Show Empty Custom Group Folders Option, page A-2).
  - Enable Device Security—Check this check box to ensure that Cisco VXC Manager Agents are managed only by an authorized Cisco VXC Manager installation (for more information on Cisco VXC Manager security, see About Cisco VXC Manager Security, page B-1).
  - Device(s) / Page—Enter the number of devices to display on the Devices page.
- GUI Discovery Preferences area:
  - Maximum number of ranges to discover—Enter the maximum number of ranges you want to discover.
  - Socket Family Preference—Choose the option you want (IPV4, Dual Stack, or IPV6).

Click **DDC** in the Device Manager tree to open the Default Device Configuration dialog box.

Figure 7-12 Default Device Configuration



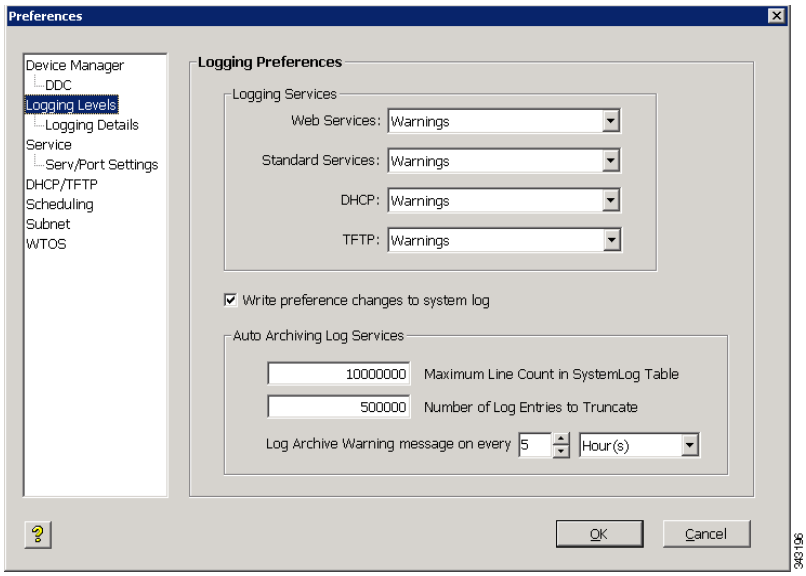
Use the following guidelines:

- Enable Default Device Configuration—Check this check box to allow devices to use DDCs for automatic upgrades (see Managing Default Device Configurations, page 7-66).
- Time to Schedule DDC Reconciliation area—Click the desired radio button: **Upon Check-in** if you want the DDC to occur when a device checks-in with the Web Service; or a custom time to specify the time of the day after which you want the DDC to occur (note that this is not the actual time when a DDC is reconciled, as the actual time depends on the frequency of check-ins you set in the Device Manager Preferences dialog box).

Logging Preferences

Double-click **Logging Preferences** in the list of preferences to open the Logging Preferences dialog box.

Figure 7-13 Logging Preferences



Use the following guidelines:

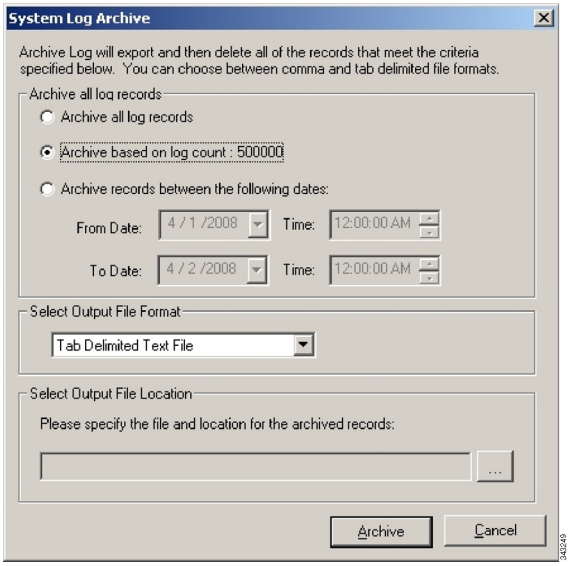
- Logging Services area—Choose the logging level for each of the communication protocols. Options include:
  - Errors—Consisting of simple error messages.
  - Warning—Consisting of warnings in addition to error messages (this is the default option).
  - Informational—Consisting of other information items in addition to error and warning messages.
  - Debug—Consisting of all information in Errors, Warning, Informational, and additional debugging data that might be useful for troubleshooting.
- Write Preferences changes to system log—Check this check box to keep logging level changes in the system log table.
- Auto Archiving Log Services area—Configure the size of the system log table and warning message frequency:
  - Maximum Line Count in SystemLog Table—Enter the number of records allowed before archiving occurs; valid values are from 500000 to 10000000; the default value is 10000000
  - Number of Log Entries to Truncate—Enter the number of records to be archived; valid values depend upon the value specified in the Maximum Line Count in SystemLog Table field; if the maximum line count value is 5000, valid values for log entries to truncate are from 500 to 4999. If the maximum line count is set to 10000000, the valid values for log entries to truncate are from 500 to 999999.

Tip The value for the Number of Log Entries to Truncate is always less than the value for the Maximum Line Count in SystemLog Table.

  - Log Archive Warning message on every—Edit the time interval for displaying the circular logging warning message (default interval is every 5 hours). When the value you set for the Maximum Line Count in SystemLog Table is exceeded, the Archive Logs warning message

appears. The first time the line count exceeds the configured limit, a warning message appears immediately. If you choose **OK**, the System Log Archive window appears (if you choose **Cancel**, you will see the warning again at the next configured warning message interval).

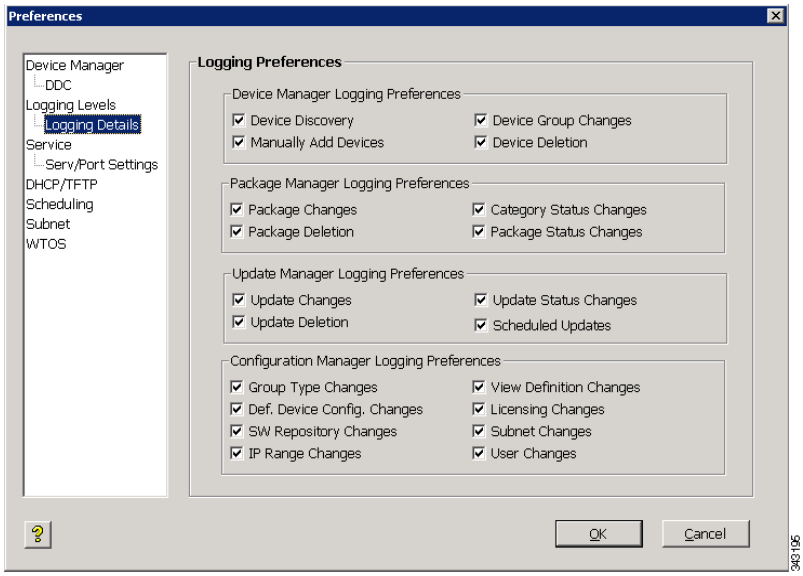
Figure 7-14 System Log Archive Window



Use the options and list menus to choose the logs to be archived, the output file format, and output file location. After you are finished setting the options, click **Archive**.

Click **Logging Details** in the Logging Levels tree to open the Logging Details Preferences dialog box where you can make further selections.

Figure 7-15 Logging Details Preferences

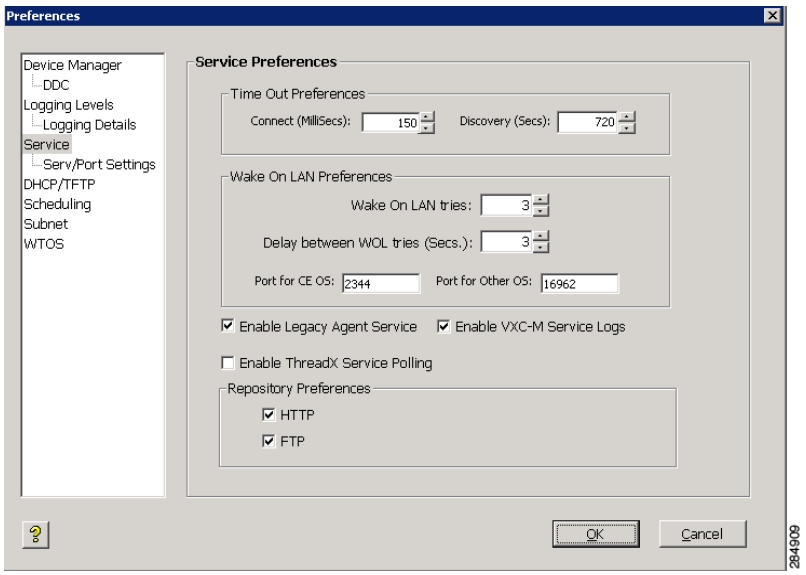


Tip Category Status Changes refers to whether a Cisco VXC Manager package changed from one category to another (for example, if you edit the script file for a Cisco VXC Manager package and change it from Image to Client Configuration), while Package Status Changes refers to whether a package changes from active to inactive or inactive to active.

Service Preferences

Double-click **Service Preferences** in the list of preferences to open the Service Preferences dialog box. Use this dialog box to set global service preferences and repository communication preferences.

Figure 7-16 Service Preferences



Use the following guidelines:

- Time Out Preferences area—Set the values in the Connect (Millisecs) field (number of milliseconds during which Cisco VXC Manager attempts to connect to a device, whether through the Web Service or the Standard Service, before timing out) and the Discovery (Secs) field (maximum time allotment for Cisco VXC Manager to discover all of the devices in your network).
- Wake On LAN Preferences area—Set the values in the Wake On LAN tries field (number of times that the service attempts to perform a WOL command before stopping) and the Delay between WOL tries (Secs) field (length of time Cisco VXC Manager pauses before it attempts another WOL command to the same device).
- Port for CE OS—Not supported on Cisco VXC devices.
- Port for Other OS—Specify a custom Wake On LAN port other than the default UDP port 16962.
- Enable Legacy Agent Service—Check this check box to communicate with older versions of Cisco VXC Manager Agents.
- Enable VXC-M Service Logs—Check this check box to start or stop the service log during Cisco VXC Manager start up.
- Enable ThreadX Service Polling—Check this check box to poll ThreadX devices.

- Repository Preferences area—Check **HTTP**, **FTP**, or both for the transfer protocol. The Repository Preferences settings determines the protocol (**HTTP** or **FTP**) that is used to communicate with a Repository during Cisco VXC Manager package registration, Cisco VXC Manager package deletion, Remote Software Repository Synchronization, and Cisco VXC Manager package updates for client devices.

Tip This is a global option that applies only when the Cisco VXC Manager Administrator Console is started. To start or stop the service logs for a particular session, right-click **CiscoVXCManager** to open and use the stop or start service log toggle option (shown in Figure 7-18 and Figure 7-18) to start or stop the service log.

Caution The Master Software Repository must support the protocols selected in the Repository Preferences. For details about the way Repository Preferences for Cisco VXC Manager package registration and Cisco VXC Manager package updates affect client devices, see Table 7-1 and Table 7-2.

Figure 7-17 Start Service Log

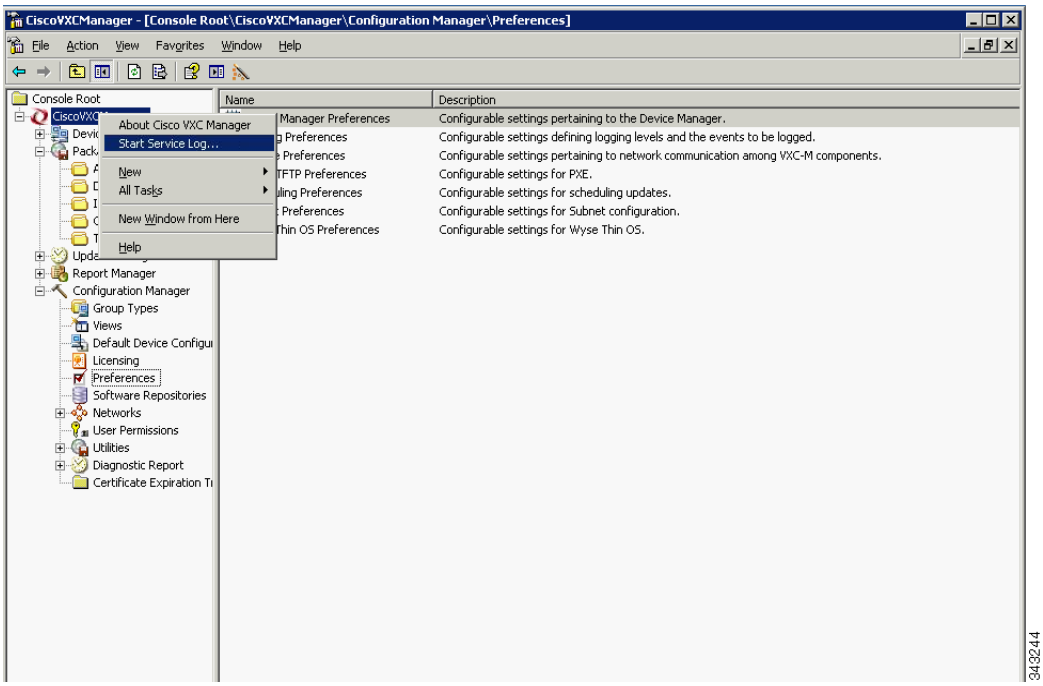


Figure 7-18 Stop Service Log

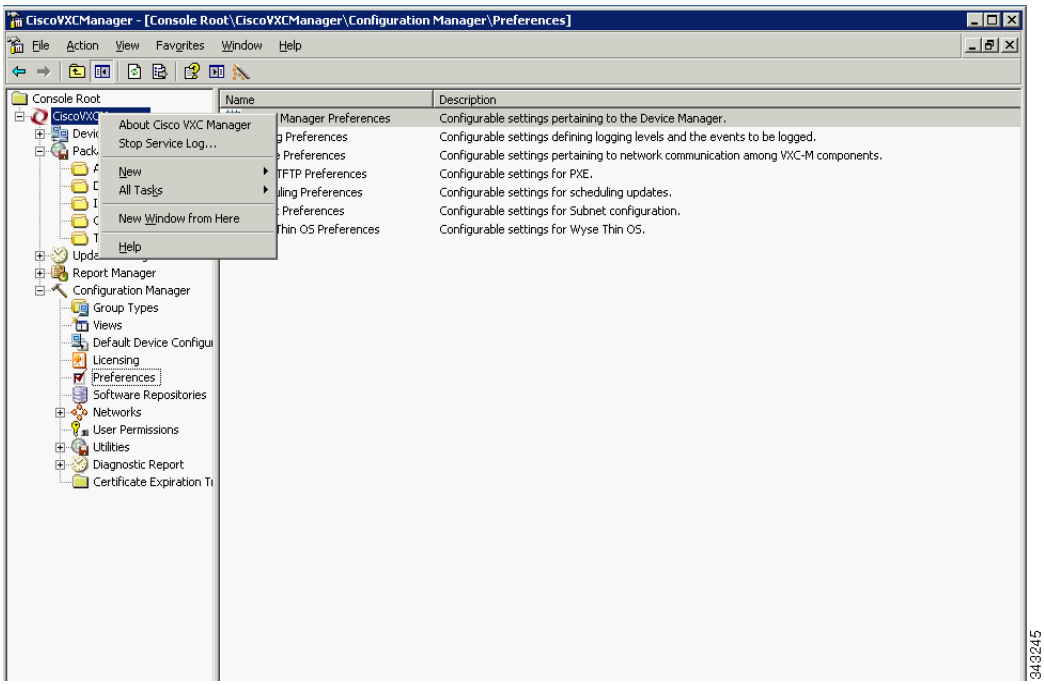


Table 7-1 Protocol Used to Register Cisco VXC Manager Packages to Master Software Repository

Global Repository Preference Setting	Master Repository Preference Setting	Cisco VXC Manager Transfer Protocol
HTTP	HTTP(S)	HTTP(S) only
FTP	FTP	FTP only
FTP	HTTP(S) and FTP	FTP only
HTTP and FTP	HTTP(S) and FTP	HTTP(S) and FTP HTTP(S) is attempted and used if successful; if it fails, FTP is used.

Table 7-2 Protocol Used to Register Cisco VXC Manager Packages to Master Software Repository

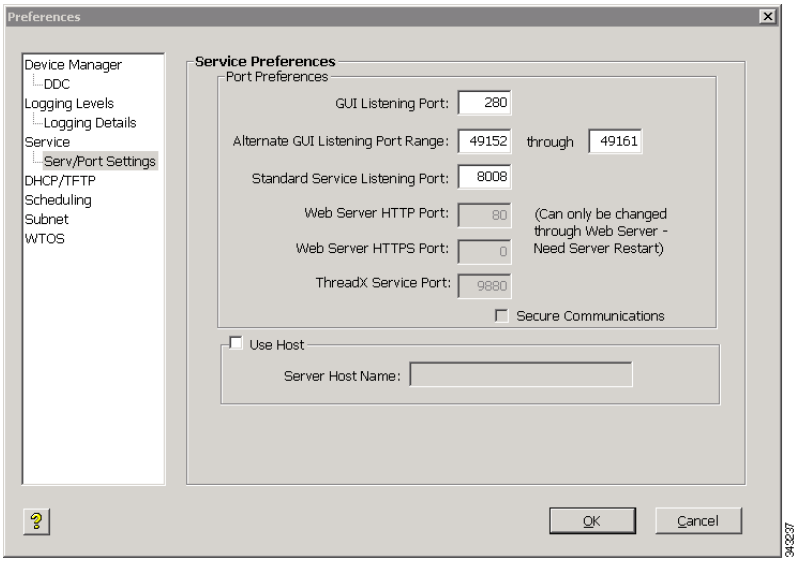
Global Repository Preference Setting	Preference Setting for Repository Used by Client	Protocol Used to Transfer Package
HTTP	FTP	HAgent on client device uses Master HTTP(S) repository only
HTTP	HTTP(S) and FTP	HAgent on client device uses assigned HTTP(S) repository only
FTP	FTP	HAgent on client device uses assigned FTP repository only

Table 7-2 Protocol Used to Register Cisco VXC Manager Packages to Master Software Repository

Global Repository Preference Setting	Preference Setting for Repository Used by Client	Protocol Used to Transfer Package
FTP	HTTP(S)	HAgent on client device uses Master FTP repository only
FTP	HTTP(S) and FTP	HAgent on client device uses assigned FTP repository only
HTTP and FTP	HTTP(S)	HAgent on client device uses assigned HTTP(S) repository only
HTTP and FTP	FTP	HAgent on client device uses assigned FTP repository only
HTTP and FTP	HTTP(S) and FTP	HAgent on client device tests connection for assigned HTTP(S) repository and if successful, uses assigned repository via HTTP(S). If the connection fails, HAgent uses assigned repository via FTP.

Click **Serv/Port Settings** in the Service tree to open the Port Settings Preferences dialog box.

Figure 7-19 Port Settings Preferences



Use the following guidelines:

- **Port Preferences** area:
  - **GUI Listening Port and Alternate GUI Listening Port Range**—Ports through which the Web Service listens for incoming Cisco VXC Manager Agent requests.
  - **Standard Service Listening Port**—Port through which the Standard Services listens for device check-in activity.

- **Web Server HTTP Port**—Port Cisco VXC Manager uses to issue real-time commands (such as Quick Device Commands or device updates at a specific time). Normally this is port 80. Note that you can change this port only through your Web Server.
- **Web Server HTTPS Port**—Port Cisco VXC Manager uses to issue real-time commands (such as Quick Device Commands or device updates at a specific time). Normally this is port 443. Note that you can change this port only through your Web Server.

Caution The configured port, either HTTP or HTTPS, determines the communication protocol between the components of Cisco VXC Manager.

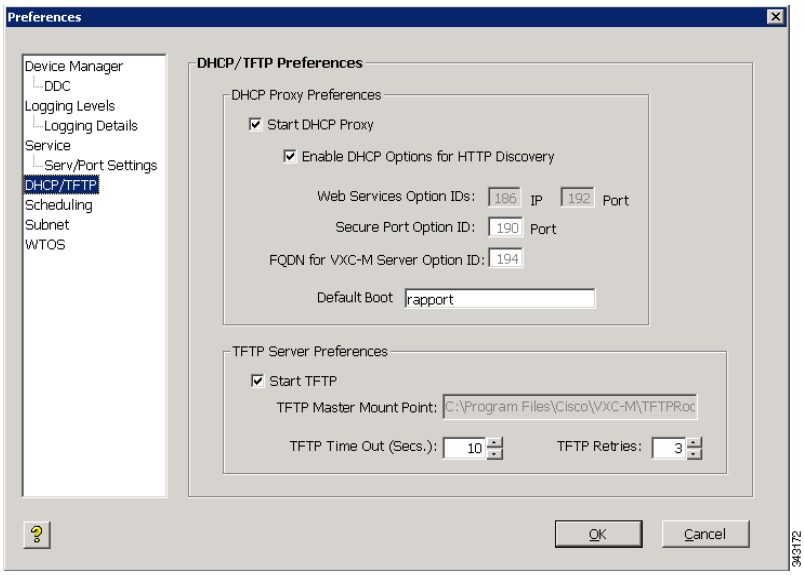
- **ThreadX Service Port**—Port Cisco VXC Manager uses to issue real-time commands (such as Quick Device Commands or device updates at a specific time). Normally this is port 9880. Note that you can change this port only through your Web Server.
- **Secure Communications**—This is a read-only box that indicates the communication between the components of Cisco VXC Manager (as well as devices) is secure (checked) or not secure (unchecked).

- **Use Host**—You can check **Use Host** to have the Cisco VXC Manager Agent use the Server Host Name you enter to connect to the server. Note that the Server Host Name will have a default value of the host machine and an administrator can change this value to a different host name (useful in cases of request forwarding through an HTTP Proxy).

DHCP/TFTP Preferences

Double-click **DHCP/TFTP Preferences** in the list of preferences to open the DHCP/TFTP Preferences dialog box.

Figure 7-20 DHCP/TFTP Preferences



Use the following guidelines:

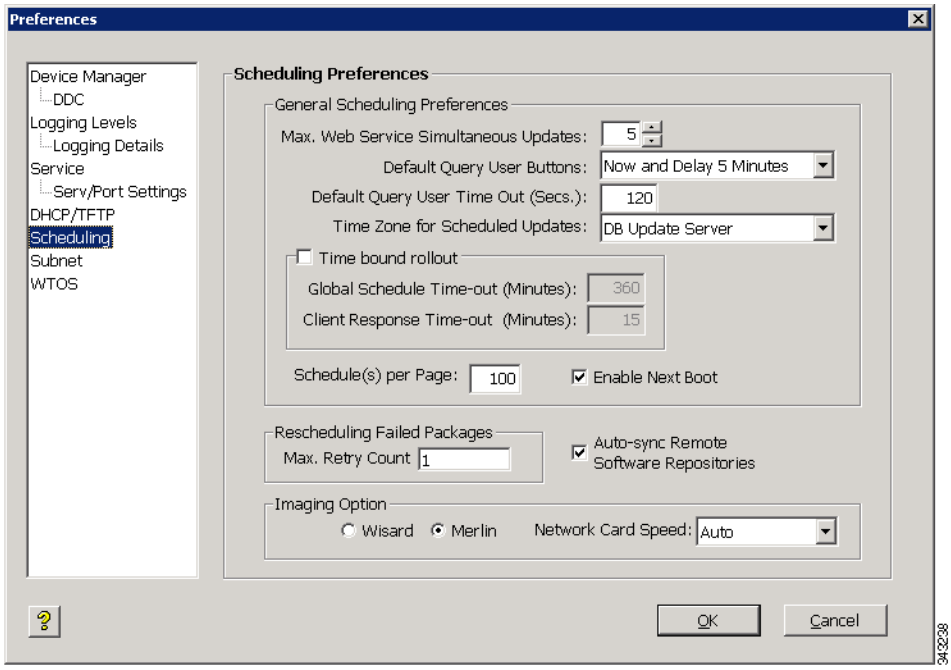
- DHCP Proxy Preferences area:

  - Start DHCP Proxy—Check this check box to allow Cisco VXC Manager to serve as a Dynamic Host Configuration Protocol (DHCP) proxy.
  - Enable DHCP Options for HTTP Discovery—Check this check box to allow the Web Service to use DHCP when discovering devices.
  - Default Boot Image—Enter the name of the folder where the default boot images are kept. Typically, this is the Trivial File Transfer Protocol (TFTP) root directory below the FTP home directory used by the Master Repository.
- TFTP Server Preferences area:
  - Start TFTP—Check this check box to allow Cisco VXC Manager to use TFTP when updating devices.
  - TFTP Master Mount Point—Displays the TFTP mount point that Cisco VXC Manager set during installation. Typically, this is the TFTP root directory (Cisco VXC Manager) below the FTP home directory used by the Master Repository.
  - TFTP Time Out (Secs.)—Specify the length of time (in seconds) that Cisco VXC Manager waits for a connection to the TFTP service before attempting to reconnect.
  - TFTP Retries—Specify the number of times that Cisco VXC Manager attempts to connect to the TFTP service before failing.

Scheduling Preferences

Double-click **Scheduling Preferences** in the list of preferences to open the Scheduling Preferences dialog box.

Figure 7-21 Scheduling Preferences



Use the following guidelines:

- General Scheduling Preferences area:

  - Max. Web Service Simultaneous Updates—Specify the maximum number of updates that Cisco VXC Manager can perform concurrently to devices with Cisco VXC Manager Agents.
  - Default Query User Buttons—Choose the option you want for the list. This entry is a global override. If a Cisco VXC Manager script package file (RSP file) contains QU and no arguments, the defaults specified in this field dictate what options the user sees when the QU statement executes as part of a device update.
  - Default Query Time Out (Secs.)—Specify the length of time that the user options are displayed before the script proceeds without user input.
  - Time Zone for Scheduled Updates—Choose the Cisco VXC Manager Time Zone that will be in effect when you schedule device updates. Options include DB Update Server (the time zone defined by the physical location of the Cisco VXC Manager Database), Console (the time zone defined by the physical location of the Cisco VXC Manager Administrator Console), and Device (the time zone defined by the physical location of the device that will undergo the actual update). For example: assuming the Console is at time 0, the Cisco VXC Manager Database is at +1, and the device is at +2; if you choose Console as the time zone and schedule an update for 1:00 PM, then the update starts at the following local times at each location: 1:00 PM at the Console, 2:00 PM at the Database, and 3:00 PM at the device. With the same settings for the Cisco VXC Manager Database and the device, if the current Console time is 1:00 PM, then an update scheduled for 1:00 PM would occur at the following Console times for each setting: Console: 1:00 PM at the Console; Cisco VXC Manager Database: 12:00 PM at the Console; Device: 11:00 AM at the Console.
  - Schedule(s) / Page—Enter the number of scheduled Cisco VXC Manager packages to display on the Scheduled Packages page.
  - Enable Next Boot—Check this check box to allow Cisco VXC Manager to update devices after their next reboot.
  - Time Bound Rollout—Enables or disables the garbage collector feature for scheduled updates. When you check this check box, the settings of the Global Schedule Time-out and the Client Response Time-out determine whether the scheduled updates enter an error state or remain in the scheduled state indefinitely.

    - Global Schedule Time-out (Minutes)—Specify the time period after which all the outstanding scheduled updates will be moved to error state.

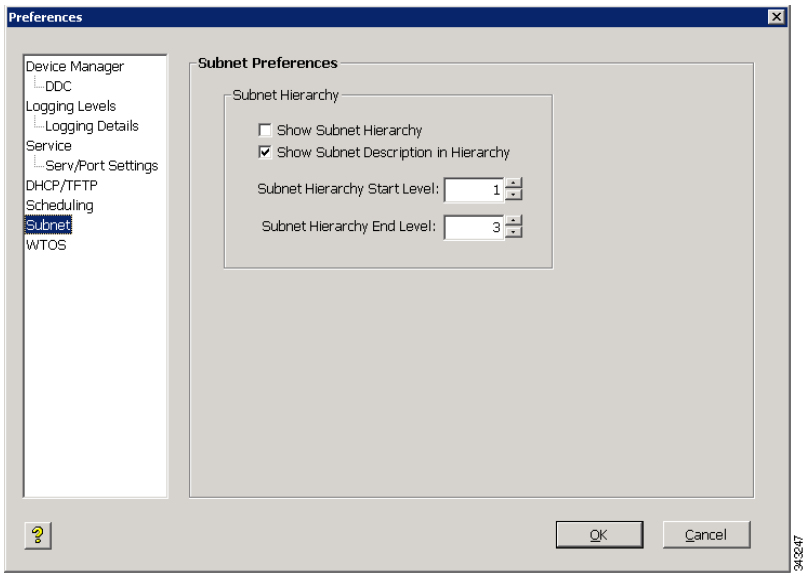
    - Client Response Time-out (Minutes)—Specify the time period for which the Cisco VXC Manager server will wait for the client to check in after Cisco VXC Manager has successfully sent the notification to the client.

- Auto-sync Remote Repositories—Check this check box to enable Cisco VXC Manager to determine whether Remote Software Repositories should be synchronized before performing an update to devices served by a Remote Software Repository.
- Rescheduling Failed Packages area:
  - Max. Retry Count—Specify the maximum number of retries you want if Cisco VXC Manager package distribution fails.
- Imaging Option area—Click one of two ways to image a device:
  - WISard—Not applicable to Cisco VXC. Legacy method for imaging devices which requires PXE for imaging.
  - Merlin—Enables FTP, HTTP or HTTPS-based imaging for the devices. Required for Cisco VXC.
- Network Card Speed—(Merlin Imaging Only) Possible values are Auto, 100M-F (100 Mb/s full duplex), 100M-H (100 Mb/s half duplex).

Subnet Preferences

Double-click **Subnet** in the list of preferences to open the Subnet Preferences dialog box.

Figure 7-22 Subnet Preferences



Use the following guidelines:

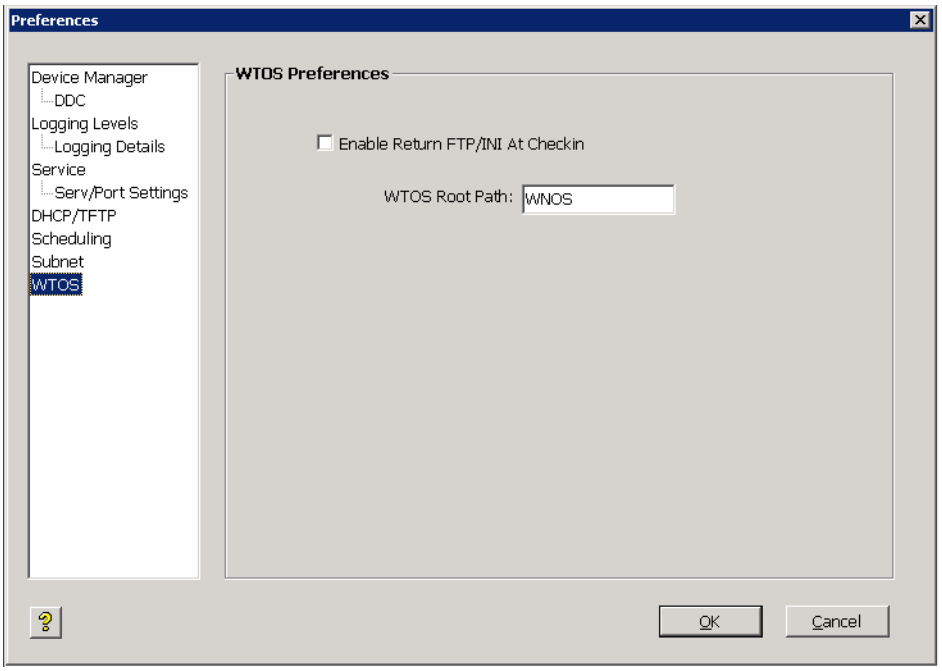
- Show Subnet Hierarchy—Check this check box to allow any subnet views to include the hierarchical view of the subnet.
- Show Subnet Description in Hierarchy—Check this check box to display hierarchical subnet views by the descriptions of the subnets rather than by their address. Note that the default description is always the subnet IP.
- Subnet Hierarchy Start Level—Specify the starting level for displaying subnet hierarchies. A level refers to one of the four octets in the subnet address.
- Subnet Hierarchy End Level—Specify the ending level for displaying subnet hierarchies. A level refers to one of the four octets in the subnet address.

WTOS Preferences

Caution This section is applicable only to Cisco VXC 2112/2212 clients running WTOS firmware for ICA.

Double-click **WTOS Preferences** in the list of preferences to open the WTOS Preferences dialog box.

Figure 7-23 WTOS Preferences



Use the following guidelines:

- Enable Return FTP/INI At Checkin—If you check this check box, Cisco VXC Manager provides the same INI file to every WTOS device that checks in.

Note Cisco recommends that you enable this option only for use in small scale environments where all clients require the identical configuration. For larger environments, use RSP files to assign different INI files to groups of clients, as doing so provides greater flexibility to customize your environment.

For the Enable Return FTP/INI At Checkin option to work properly, you must create a WNOS folder containing the desired common INI file at the following path on the Cisco VXC Manager server:

```
rapport/WNOS
```

Also note that this option is not specific to FTP as the transfer protocol. It applies with HTTP also.

- WTOS Root Path—Enter the WTOS root path.

Understanding Cisco VXC Manager Repositories

A Cisco VXC Manager Repository is a server which supports the FTP, HTTP, and HTTPS protocols for communication and contains Cisco VXC Manager packages. When you register a Cisco VXC Manager package using the Package Manager, Cisco VXC Manager copies the related folders and files to a Cisco VXC Manager Repository. There are two types of Cisco VXC Manager repositories, Master and Remote. By default, each Cisco VXC Manager installation has one Master Repository. The Master Repository is the central storage place for all Cisco VXC Manager package files.

When you distribute an update, devices connect to the Master Repository through FTP, HTTP, or HTTPS (depending on the configuration settings) and download the files that the script file (RSP file) of the package dictates. Cisco VXC Manager and the Cisco VXC Manager Agents use FTP, HTTP, or HTTPS to send and retrieve the appropriate Cisco VXC Manager packages from the Master Repository.

In addition, Cisco VXC Manager allows you to install remote repositories on multiple computers on different subnets throughout your network (see Managing Software Repositories, page 7-87). This scalability reduces network traffic when you need to send updates across subnets. By using their local Remote Software Repository, devices on a specific subnet do not need to access the Master Repository across a wide-area network (WAN) to retrieve files (Cisco VXC Manager synchronizes the Master and Remote software repositories prior to a Cisco VXC Manager package distribution).

If your Cisco VXC Manager installation contains Remote Software Repositories, Cisco VXC Manager must establish the relationship between a given set of devices and the Remote Software Repository that services those devices (thereby ensuring lower network loads). After establishing this relationship, Cisco VXC Manager is able to choose the appropriate repository when distributing packages to devices. Devices are associated to a Remote Software Repository by the subnet to which they belong. After you assign a subnet to a repository, all devices on that subnet will use the assigned repository.

Managing Software Repositories

Cisco VXC Manager allows you to install multiple repositories on your network (for repository installation procedures, see the *Installation Guide for Cisco Virtualization Experience Client Manager*). Remote Software Repositories help save network bandwidth because they store and distribute software updates locally to devices that reside in the same subnet as each repository.

Be aware that:

- Cisco VXC Manager always names the first repository you install Master. Any additional Remote Software Repositories that you install can be named anything other than Master. The user IDs and passwords for all repositories can be the same for FTP-based repositories, but must be different for HTTP-based repositories.
- If you do not install multiple Remote Software Repositories, then Cisco VXC Manager uses the Master Repository for all subnets.
- If you deploy Cisco VXC Manager components separately, then it is recommended that you install the Master Repository on a machine on the same subnet as where you installed the other Cisco VXC Manager components.
- There are two possible repository authentications:
  - Basic Authentication—This authentication mode requires you to enter a valid NT login and password to gain access to the system. When Basic Authentication is enabled, you will be prompted for your username and password when you attempt to access the virtual directory. The password is sent in Clear Text.
  - Integrated Windows Authentication—This is the most secure form of authentication in IIS. When you login, NT validates your login and only your username is transmitted over the network. No password is transmitted, so your password cannot be compromised.

This section contains information on:

Registering Remote Software Repositories

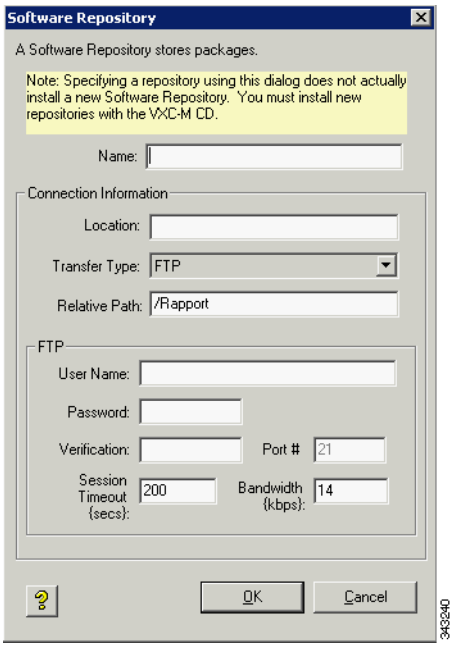
After installing an additional Remote Software Repository, you must register it in the Cisco VXC Manager Database and then assign the Remote Software Repository to a subnet.

Tip For information on assigning a Software Repository to a subnet, see Managing Subnets, page 7-90.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, right-click **Software Repositories** and choose **New > Software Repository** to open the Software Repository dialog box.

Figure 7-24 Software Repository



Step 2 Use the following guidelines:

- Name—Displays the descriptive name for the Remote Software Repository you entered during installation.
- Connection Information area:
  - Location—IP address to identify the Remote Software Repository.
  - Transfer Type—Type of transfer protocol that is in use (see Service Preferences, page 7-78). Options are FTP, HTTP, or both
  - Relative Path—Relative path from the FTP root folder.
- FTP area:
  - User/Group Name—User name for the FTP account as set up by IIS FTP or the FTP service that you use to connect to the repository.
  - Password—FTP password as set up by IIS FTP or the FTP service that you use to connect to the repository.

  - Verification—Retype the password to verify you entered it correctly.
  - Port Number—Port number for FTP communication. The default port number for FTP is 21.
  - Session Timeout—Time in seconds that the connection for each session should remain open.
  - Bandwidth—The amount of bandwidth in Kbps to utilize for data transfer to and from the Software Repository.
- HTTP area:
  - User/Group Name—Strongly recommended if Basic Authentication or Windows Integrated Authentication is used for the software repository, but this field is not mandatory.
  - Context—Virtual directory path for HTTP communication. This field is disabled if the selected transfer type is FTP only.
  - Password—Strongly recommended if Basic Authentication or Integrated Windows Authentication is used for the software repository; however, this field is not mandatory.
  - Port Number—Port number for HTTP communication. The default port number for HTTP is 80, and for HTTPS is 443.
  - Verification—Password verification for HTTP user.
  - Timeout—Time in seconds that the connection for each session should remain open.
  - Secure (HTTPS)—If checked, the HTTP communication for the repository is secure.
  - Validate Certificate with CA—If checked, the Certificate validation for HTTPS communication is enabled.

Step 3 Click OK. Cisco VXC Manager tests the connection to the Remote Software Repository that you registered to ensure that it is properly configured (you can test the connection to a Remote Software Repository at any time by right-clicking the Remote Software Repository name and selecting **Test Connection**). The new Remote Software Repository is then successfully set up and registered in the Cisco VXC Manager Database. You can now assign the Remote Software Repository to a subnet (see Managing Subnets, page 7-90).

Tip Cisco VXC Manager stores every package that you register in its Master Repository. You can synchronize Remote Software Repositories whenever you perform an update for a device on a subnet that has access to a local repository. Table 7-3 shows the protocol that are used for synchronization, based on the protocol settings for the Master Repository and Remote Software Repository. For more information on Remote Software Repository synchronizations, see Scheduling a Remote Repository Synchronization, page 5-38.

Table 7-3 Protocol Used for Remote Software Repository Synchronization

Master Repository Preference Setting	Remote Software Repository Preference Setting	Synchronization Protocol
HTTP	HTTP(S)	HTTP(S) only
HTTP	FTP	Error - no synchronization
HTTP	HTTP and FTP	HTTP only
FTP	HTTP(S)	Error - no synchronization
FTP	FTP only	FTP only
FTP	HTTP(S) and FTP	FTP only
HTTP and FTP	HTTP(S)	HTTP(S) only
HTTP and FTP	FTP	FTP only
HTTP and FTP	HTTP(S) and FTP	HTTP(S) is attempted and used if successful; if it fails, FTP is used

Editing Software Repositories

In the tree pane of the Administrator Console, expand **Configuration Manager**, click **Software Repositories**, right-click on the Software Repository you want to edit, and then choose **Properties** to open and use the Edit Software Repository dialog box.

Deleting Software Repositories

In the tree pane of the Administrator Console, expand **Configuration Manager**, click **Software Repositories**, right-click on the Software Repository you want to delete, choose **Delete**, and then click **Yes** to confirm.

Managing Networks

Managing Networks includes:

- Managing Subnets, page 7-90
- Managing IP Ranges, page 7-93

Managing Subnets

Cisco VXC Manager uses subnet information to discover and communicate with the devices on your network.

Tip Although you can add subnets to Cisco VXC Manager manually, you can also use a Cisco VXC Manager utility to import subnet data from comma-delimited and tab-delimited files into the Database (see Importing Subnet Data from Files, page 7-99).

This section contains information on:

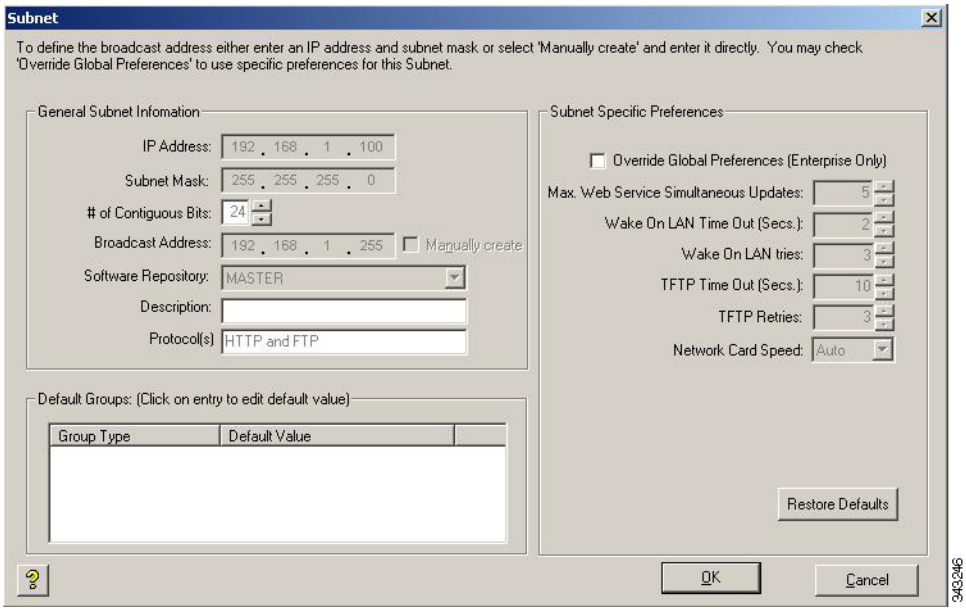
Adding Subnets to Cisco VXC Manager Manually

Use the following procedure to manually add subnets to Cisco VXC Manager.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, expand Networks, right-click **Subnets**, and then choose **New > Subnet** to open the Subnet dialog box.

Figure 7-25 Subnet



Step 2 Complete one of the following:

- If you want to provide a broadcast address for the subnet manually, check the **Manually create** check box and enter a value in the **Broadcast Address** field.
- If you do not want to provide a broadcast address for the subnet manually, complete the following fields: **IP Address** (enter a valid IP address from the subnet), **Subnet Mask** (enter the subnet mask for the subnet), and **# of Contiguous Bits** (if your network uses Classless Inter-Domain Routing or supernetting, type the number of contiguous bits to configure your subnet mask).

Step 3 Enter a **Description** to identify the subnet in the Cisco VXC Manager Database.

Step 4 Choose the Software Repository. If your Cisco VXC Manager configuration includes multiple Remote Software Repositories and you want to associate the subnet with one of them, choose it in the Software Repository list.

Tip When distributing Cisco VXC Manager packages to a group of devices, Cisco VXC Manager uses the subnet/repository association to determine the appropriate Remote Software Repository for the devices.

Step 5 (Optional) If you want to associate newly discovered devices on this subnet with a user-defined Group Type (Cisco VXC Manager always assigns devices to the predefined Group Types according to the values found on the devices), choose the row for the Group Type you want from the Default Groups pane to open and use the Default Group Value dialog box (choose the **Default Value** in the Default Group Value dialog box and click **OK** to return to the Subnet dialog box). Be aware that to associate devices in a subnet with a Group Type, you must have previously created the desired Group Types.

Step 6 Complete one of the following:

- If you do not want to override the global preferences for this subnet, click **OK**.
- If you want to override the global preferences for this subnet, check the **Override Global Preferences** check box, complete the subnet preferences using the following guidelines, and then click **OK**:
  - Maximum Simultaneous Updates—Maximum number of device updates you can perform at the same time in the subnet.
  - Wake On LAN Time Out (Secs.)—Length of time Cisco VXC Manager attempts to wake a device on the subnet before stopping.
  - Wake On LAN Retries—Number of times Cisco VXC Manager attempts to wake a device in the subnet before stopping.
  - TFTP Time Out (Secs.)—Length of time Cisco VXC Manager attempts to use the Trivial File Transfer Protocol (TFTP) to communicate with devices during PXE operations.
  - TFTP Retries—Number of times Cisco VXC Manager attempts to use TFTP before stopping.
  - Network Card Speed—This field is valid only for Merlin imaging. The possible values are Auto, 100M-F (100 MBPS Full duplex), 100M-H (100 MBPS Half duplex).

The information about the subnet and its preferences are now stored in the Cisco VXC Manager Database and Cisco VXC Manager can discover the devices on the subnet.

Editing Subnets

In the tree pane of the Administrator Console, expand **Configuration Manager**, expand **Networks**, click **Subnets**, right-click on the Subnet you want to edit, and then choose **Properties** to open and use the Edit Subnet dialog box.

Deleting Subnets

In the tree pane of the Administrator Console, expand **Configuration Manager**, expand **Networks**, click **Subnets**, right-click on the Subnet you want to delete, choose **Delete**, and then click **Yes** to confirm.

Managing IP Ranges

IP Ranges allow Cisco VXC Manager to discover devices with all supported versions of Cisco VXC Manager Agents through a Transmission Control Protocol (TCP) connection to each device in an IP Range rather than through a User Datagram Protocol (UDP) broadcast to an entire subnet level.

Tip Although you can add IP ranges to Cisco VXC Manager manually, you can also use a Cisco VXC Manager utility to import IP Range data from comma-delimited and tab-delimited files into the Database (see Importing IP Range Data from Files, page 7-98).

This section contains information on:

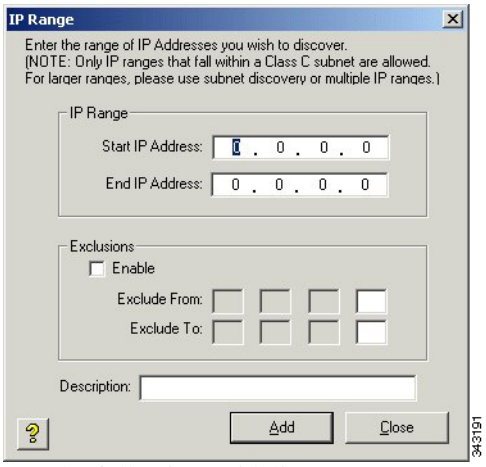
Adding IP Ranges to Cisco VXC Manager Manually

Use this procedure to manually add IP ranges to Cisco VXC Manager.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, expand **Networks**, right-click **IP Ranges**, and then choose **New > IP Range** to open the IP Range dialog box.

Figure 7-26 IP Range



Step 2 Use the following guidelines:

Start IP Address—Starting IP address for the IP Range.

End IP Address—Ending IP address for the IP Range.

Exclude From—Beginning IP address for the range of addresses to exclude from the range you are setting up (for example, if you wanted to exclude devices from 192.168.1.30 onward then you would enter 192.168.1.30).

Exclude To—Ending IP address for the range of addresses to exclude from the range you are setting up (for example, if you wanted to exclude devices up to 192.168.1.35 then you would enter 192.168.1.35).

Description—Type a brief description to identify the IP Range.

Step 3 Click **Add** to store information about the IP Range in the Cisco VXC Manager Database. Cisco VXC Manager can now selectively discover devices in a subnet through a TCP connection to each device.

Editing IP Ranges

In the tree pane of the Administrator Console, expand **Configuration Manager**, expand **Networks**, click **IP Ranges**, right-click on the IP Range you want to edit, and then choose **Properties** to open and use the Edit IP Range dialog box.

Deleting IP Ranges

In the tree pane of the Administrator Console, expand **Configuration Manager**, expand **Networks**, click **IP Ranges**, right-click on the IP Range you want to delete, choose **Delete**, and then click **Yes** to confirm.

Managing User Permissions

As an administrator you can add, edit and delete Cisco VXC Manager users. Cisco VXC Manager allows you to manage users from local computer accounts or from Active Directory.

This section contains information on:

Adding Users from Local Computer Accounts

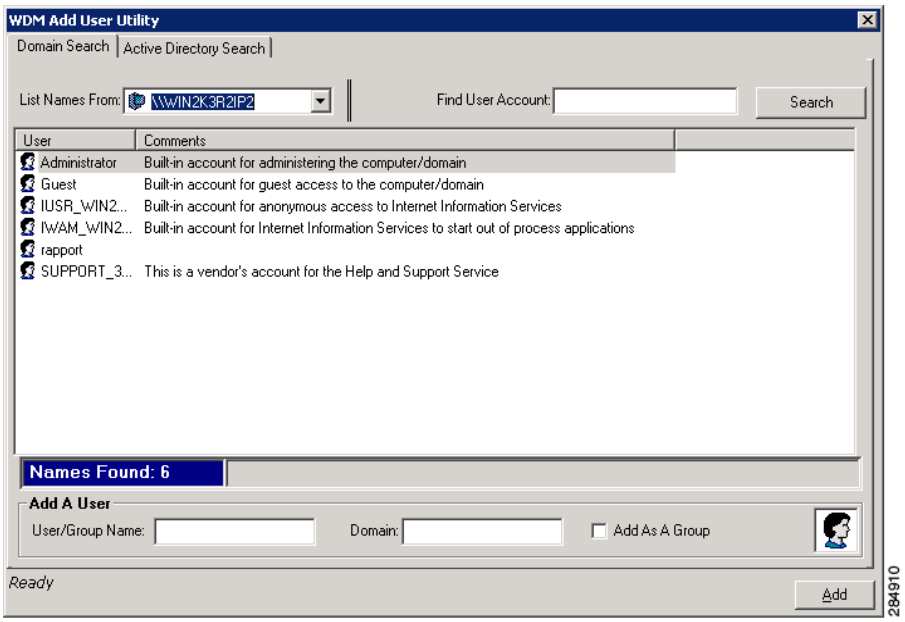
Use the following procedure to add users from local computer accounts.

Tip Before you can add a Cisco VXC Manager user, the user must already exist in the list of users for the Windows Domain where you installed Cisco VXC Manager.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, right-click **User Permissions**, and choose **New > User/Group** to open the Cisco VXC Manager Add User Utility dialog box.

Figure 7-27 Cisco VXC Manager Add User Utility – Domain Search Tab



Step 2 On the Domain Search tab, choose the name of the user you want to add as a Cisco VXC Manager user and click **Add**.

Step 3 Click **OK** to add the new user to the list of Cisco VXC Manager users.

Step 4 New users do not have permissions until you edit the user permissions. See Editing User Permissions, page 7-96 for more information.

Adding Users and Groups from Active Directory

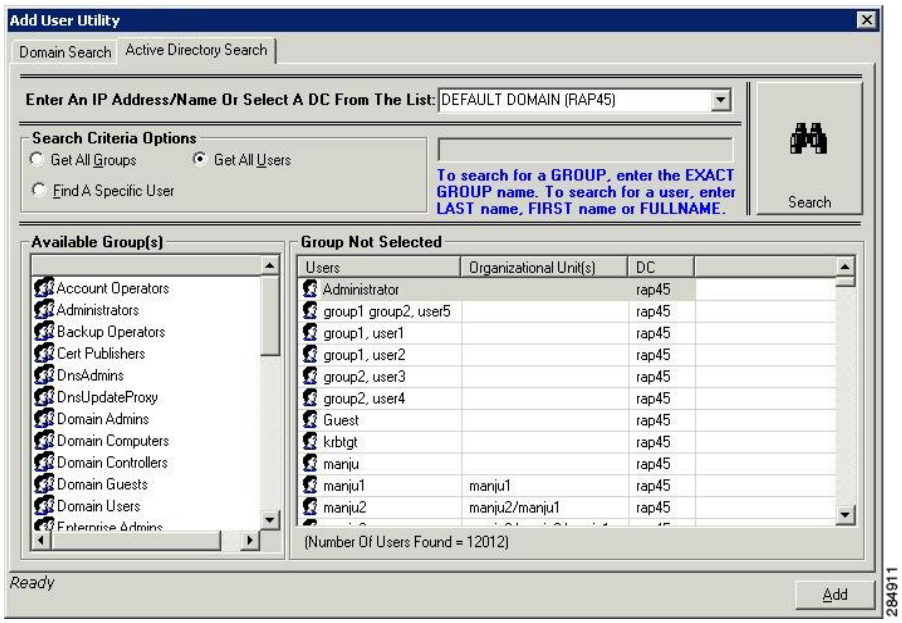
Use the following procedure to add users and groups from Active Directory.

Tip Before you can add a Cisco VXC Manager group, the group must already exist in Active Directory.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, right-click **User Permissions**, and choose **New > User/Group** to open the Cisco VXC Manager Add User Utility dialog box.

Figure 7-28 Cisco VXC Manager Add User Utility – Active Directory Search Tab



Step 2 On the Active Directory Search tab, enter an IP Address/name or choose a Domain Controller from the list (the server to which you installed Cisco VXC Manager must be a part of the Domain).

Step 3 Click the search criteria radio button you want (if you click **Find A Specific User**, be sure to enter the exact name of the user), and then click **Search** to view the search results.

Step 4 After making your selections, click **Add** to integrate the users and groups with Cisco VXC Manager.

Editing User Permissions

Use the following procedure to edit user permissions.

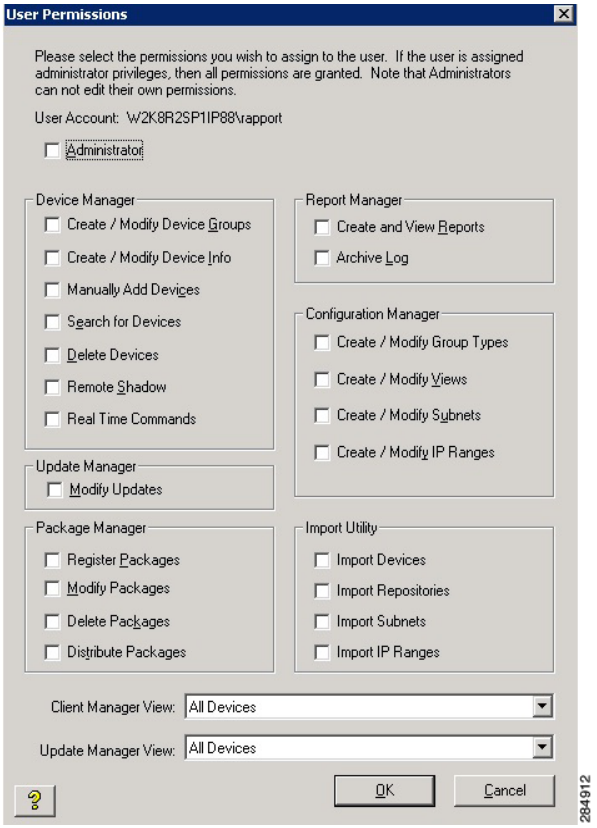
Tip You cannot edit your own user permissions.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, and click **User Permissions** to view the list of Cisco VXC Manager users.

Step 2 Right-click the user you want to edit, and choose **Properties** to open the User Permissions dialog box.

Figure 7-29 User Permissions



Step 3 Check the user permissions you want for the user and then click **OK**.

Tip If you check the **Administrator** check box, all permissions are selected.

Deleting Users

Tip You cannot delete your own account.

In the tree pane of the Administrator Console, expand **Configuration Manager**, click **User Permissions**, right-click on the user you want to delete, choose **Delete**, and then click **Yes** to confirm.

Tip When you delete a user, the private Views of the user are also deleted.

Using Cisco VXC Manager Utilities

Cisco VXC Manager includes various utilities to help you with administration tasks.

This section contains information on:

Importing IP Range Data from Files

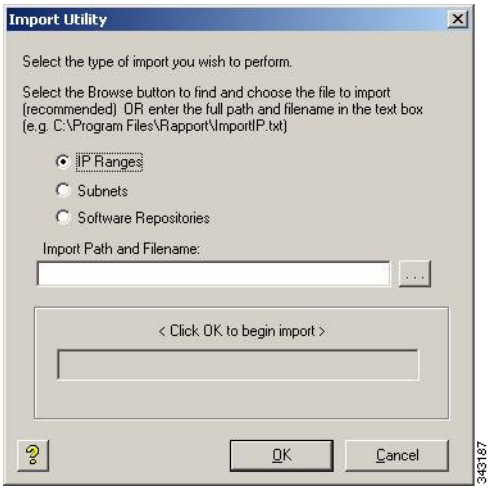
With Cisco VXC Manager, you can import IP Range data from comma-delimited and tab-delimited files into the Cisco VXC Manager Database.

Tip For the required format of Remote Software Repository flat files, see Required Format for Importing IP Range Data from Files, page 7-99.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, expand **Utilities**, right-click **Imports**, and then choose **New > Import** to open the Import Utility dialog box.

Figure 7-30 Import Utility – IP Ranges



Step 2 Click the **IP Ranges** radio button, and enter (or browse for) the location of the data file in the **Import Path and Filename** field.

Step 3 Click **OK** to import the IP Range data into the Cisco VXC Manager Database (in the tree pane of the Administrator Console, you can expand **Configuration Manager**, expand **Networks**, and then click **IP Ranges** to view the newly imported remote IP Range data).

Required Format for Importing IP Range Data from Files

The following example shows the required format for IP Range flat files:

StartIP, EndIP, ExclusionStartIP, ExclusionEndIP, Description

- StartIP—Beginning IP address for IP range
- EndIP—Ending IP address for IP range
- ExclusionStartIP—Beginning IP address for IP exclusion range
- ExclusionEndIP—Ending IP address for IP exclusion range
- Description—Name of IP range that will appear in the Administrator Console

Example: 10.10.10.10,10.10.10.200,10.10.10.20,10.10.10.30, My IP Range

This IP Range definition is added to the database to allow for IP Range walking discover on and discover all devices between the ranges of 10.10.10.10 to 10.10.10.19 and 10.10.10.31 to 10.10.10.200. This IP Range definition appears in the Administrator Console as My IP Range.

Importing Subnet Data from Files

With Cisco VXC Manager, you can import subnet data from comma-delimited and tab-delimited files into the Cisco VXC Manager Database.

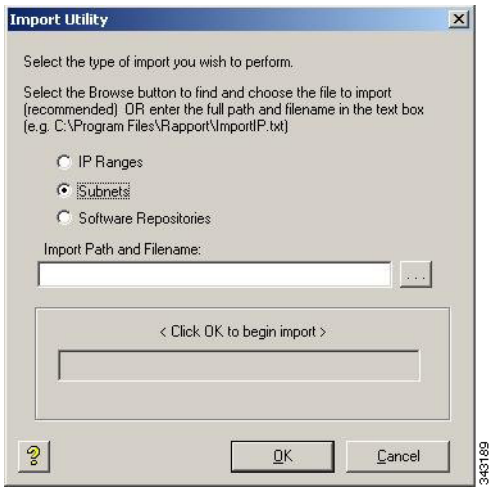
Tip For Remote Software Repositories, your Cisco VXC Manager Database must contain information about at least one Remote Software Repository before you can work with subnets (see Managing Software Repositories, page 7-87).

Tip For the required format of Remote Software Repository flat files, see Required Format for Importing Subnet Data from Files, page 7-100.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, expand **Utilities**, right-click **Imports**, and then choose **New > Import** to open the Import Utility dialog box.

Figure 7-31 Import Utility – Subnets



Step 2 Click the **Subnets** radio button, and enter (or browse for) the location of the data file in the **Import Path and Filename** field.

Step 3 Click **OK** to import the Subnet data into the Cisco VXC Manager Database (in the tree pane of the Administrator Console, you can expand **Configuration Manager**, expand **Networks**, and then choose **Subnets** to view the newly imported remote Subnet data).

Required Format for Importing Subnet Data from Files

The following example shows the required format for subnet flat files:

Broadcast Address, Description, SW Repository, Override Default Parameters, IP Address, Subnet Mask, Max. Web Service Simultaneous Updates, Wake On LAN Time Out(Secs.), Wake On LAN Tries, TFTP Time Out(Secs.), TFTP Retries, Network Card Speed

- Broadcast Address—Broadcast address; example: 10.10.10.255
- Description—Name of Subnet that will appear in the Administrator Console
- SW Rep—Name of a Software Repository. You can not add a Subnet without a Software Repository. The name of the master Repository ID is MASTER.
- Override Default Parameters—Override Global Preferences (Enterprise Only).
- IP Address—Valid IP address in subnet; example: 199.199.10.2.
- Subnet Mask—Subnet mask; example: 255.255.255.0
- Max. Web Service Simultaneous Updates—Maximum Simultaneous Updates; example: 5
- Wake On LAN Time Out(Secs.) -Time Out for Wake On LAN; example: 2
- Wake On LAN Tries—WOL Retry; example: 3
- TFTP Time Out(Secs.)—TFTP Timeout; example: 10
- TFTP Retries—TFTP Retries; example: 3
- Network Card Speed—Network Card Speed; example: 1 (for Auto), 2(for 100M-F), 3(for 100M-H)

Example: 10.10.10.255,Subnet1,MASTER,False,199.199.10.2,255.255.255.0,6,2,1,1,7,2

This example adds to the database a subnet definition that will discover and manage devices on a subnet with IP address assignments from 199.10.0.1 to 199.10.0.254. The column header either does not exist or exists in the above proper order.

Importing Software Repository Data

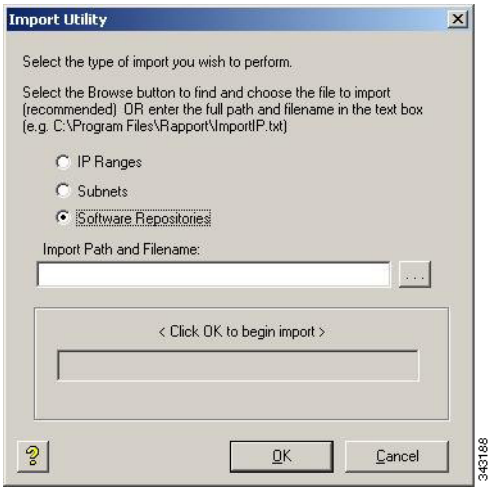
With Cisco VXC Manager, you can import Remote Software Repository data from comma-delimited and tab-delimited files into the Cisco VXC Manager Database.

Tip For the required format of Remote Software Repository flat files, see Required Format for Importing Subnet Data from Files, page 7-100.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, expand **Utilities**, right-click **Imports**, and then choose **New > Import** to open the Import Utility dialog box.

Figure 7-32 Import Utility – Software Repositories



Step 2 Click the **Software Repository** radio button, and enter (or browse for) the location of the data file in the **Import Path and Filename** field.

Step 3 Click **OK** to import the Software Repository data into the Cisco VXC Manager Database (in the tree pane of the Administrator Console, you can expand **Configuration Manager**, and then choose **Software Repository** to view the newly imported remote Software Repository data).

Tip When you register a new software repository, Cisco VXC Manager establishes a connection to ensure that it can communicate with the Remote Software Repository. When you import repository data, Cisco VXC Manager tests the connection to the repository automatically. Therefore, after you import data one or more Remote Software Repository, you do not need to test the connection.

Required Format for Importing Software Repository Data from Files

The following example shows the required format for Remote Software Repository flat files:

Name of Rep,IP Address of Repository,TransferType,RelPath,Context,FTPPortNumber, HTTPPortNumber,FTP UserName,FTP Password,HTTP UserName,HTTP Password, IsHTTPSecure,HTTPSValidateWithCA

- Name—Name of the Remote Software Repository as it appears in the Administrator Console
- Location—IP address of the FTP server
- Transfer Type—Type of transfer protocol in use. Options are: FTP, HTTP or both.
- Relative Path—Path to the software repository relative to the root directory. The default value for this is /rapport.
- Context—This is valid for HTTP communication and is the name of the virtual directory.
- FTP Port Number—Port number for FTP communication. The default port number is 21.
- HTTP Port Number—Port number for HTTP or HTTPS communication. The default port number for HTTP is 80. The default port for HTTPS communication is 443.
- FTP User Name—User name for the FTP account as set up by IIS FTP or the FTP service that you use to connect the repository
- FTP Password—Password for the FTP account as set up by IIS FTP or the FTP service that you use to connect the repository
- HTTP User Name—User name for the HTTP account as set up by IIS HTTP or the HTTP service that you use to connect the repository
- HTTP Password—Password for the HTTP account as set up by IIS HTTP or the HTTP service that you use to connect the repository
- Secure (HTTPS)—The value is -1 if Secure is checked (HTTPS supported) and 0 if Secure is unchecked (HTTP is supported, but not HTTPS).
- HTTPSValidateWithCA—It is -1 if "Validate Certificate with CA" is checked and 0 if unchecked
- Example: Transfer Type is FTP
- RemoteFTP,10.10.11.9,FTP,/rapport,,21,,FTPUserName,FTPPassword,,,0,0

The syntax in Example 4 specifies this software repository definition will be added to the Cisco VXC Manager database to define a repository on a server at the IP address 10.10.11.9, where the FTP service root directory is the default path of /rapport. It can be accessed using a username of user. It will use FTP as the transfer protocol and appear in the Administrator Console as Remote. The column header either does not exist or exists in the above proper order.

Importing Device Settings Data from Files

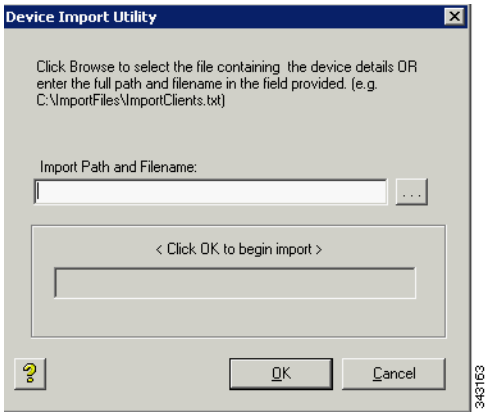
With Cisco VXC Manager, you can import Device Settings data from comma-delimited and tab-delimited files into the Cisco VXC Manager Database.

Tip For the required format of Remote Software Repository flat files, see Required Format for Importing Device Settings from Files, page 7-103.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, expand **Utilities**, right-click **Import Device Settings**, and then choose **New > Device Import** to open the Device Import Utility dialog box.

Figure 7-33 Device Import Utility



Step 2 Enter (or browse for) the location of the data file in the **Import Path and Filename** field.

Step 3 Click **OK** to import the Device Settings data into the Cisco VXC Manager Database (in the tree pane of the Administrator Console, you can click **Device Manager** to view the newly imported remote Device Settings data).

Required Format for Importing Device Settings from Files

The following example shows the required format for IP Range flat files:

- Client Name—Name of the client; example W1009341019
- Mac address—MAC address of the client; example 0080646A1144
- Platform—Platform of the device; example VX0
- Custom field 1—Custom field of the specific device
- Custom field 2—Custom field of the specific device
- Custom field 3—Custom field of the specific device
- Contact—Contact information of the device
- Location—Location of the device

The following example shows the required format for Client Import Files:

ClientName;MACAddress;Platform;Custom1;Custom2;Custom3;Contact;Location
W1009341019;0080646A1144;VX0;ABCD;EFGH;IJKL;Administrator;Saj Jose Office

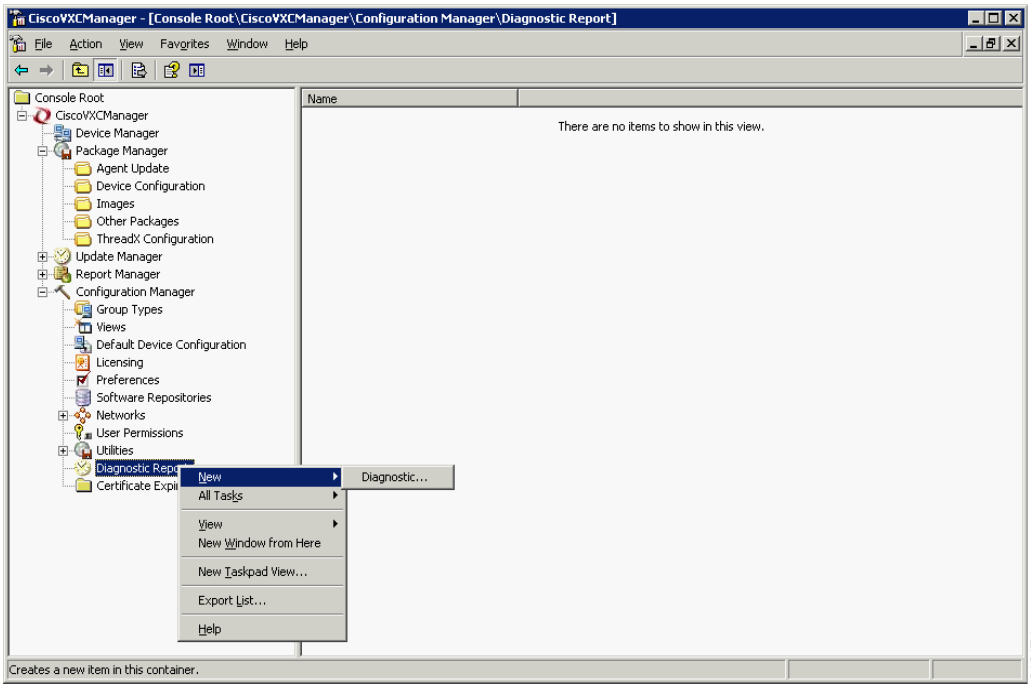
Generating Diagnostic Reports

Diagnostic Reports provide hardware and software summary information and a list of running processes.

In the tree pane of the Administrator Console, expand **Configuration Manager**, right-click **Diagnostic Report**, and then choose **New > Diagnostic Report** to generate a report.

Tip You can also right-click a device in the details pane of the Device Manager window and choose **Diagnostic Report** to generate a report.

Figure 7-34 Diagnostic Report



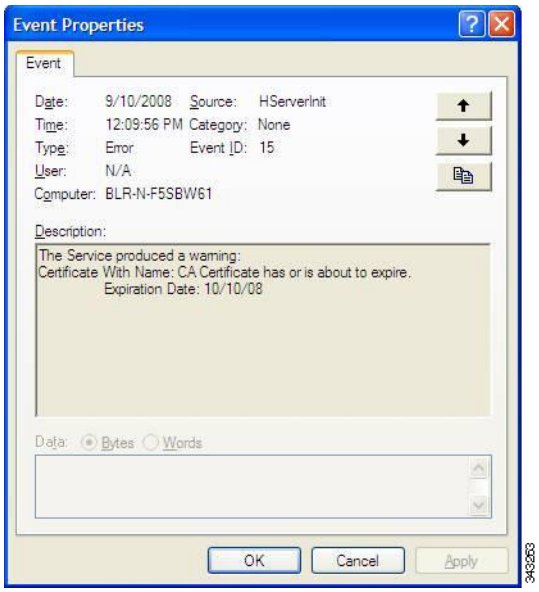
A Diagnostic Report of the Cisco VXC Manager system includes the following sections:

- Software Repository Information—Status of the Software Repository component.
- HServer Information—Status of the HServer component.
- Standard Service Information—Status of the Standard Service component.
- Basic System Information—Status of the currently running processes.
- Install Information—Installed component information.
- Database Information—Values of the preference settings.
- Logs—Log information.

Using the Certificate Expiration Tracker

The Certificate Expiration Tracker utility helps you keep track of the expiration dates of certificates you add to the system. It warns you about the expiration of the certificates according to your specifications, and logs expiration information to the Windows Event Viewer.

Figure 7-35 Warning Message

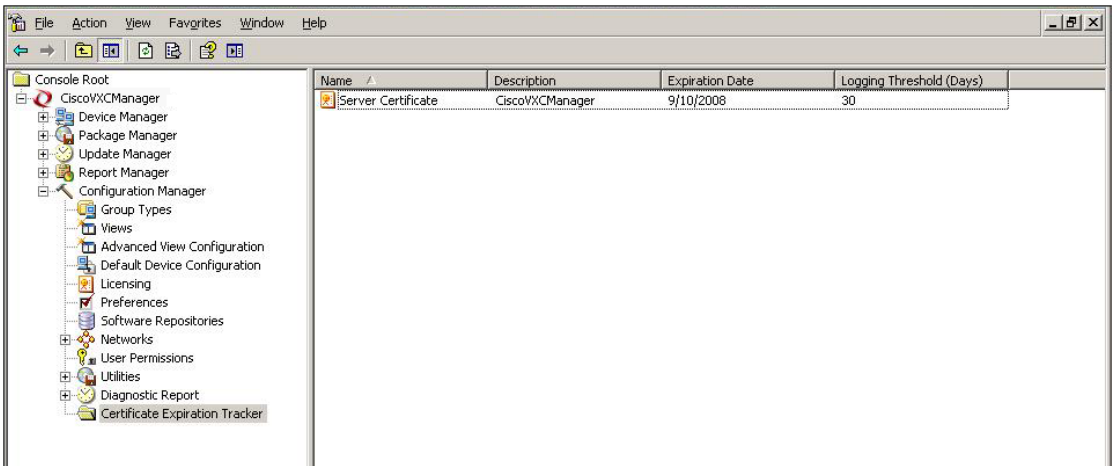


Tip For information on licensing and certificates, see Licensing and Sales Keys, page F-1.

Viewing Certificate Information in the Certificate Expiration Tracker

In the tree pane of the Administrator Console, expand **Configuration Manager**, and then click **Certificate Expiration Tracker** to display information on all certificates being tracked.

Figure 7-36 Certificate Expiration Tracker



Adding a Certificate to the Expiration Tracker

In the tree pane of the Administrator Console, expand **Configuration Manager**, right-click **Certificate Expiration Tracker**, and then choose **New > Certificate Authority** to open and use the Certificate Expiration Tracker dialog box.

Figure 7-37 Certificate Expiration Tracker

Use the following guidelines:

- Name—Enter the name of the certificate to be tracked.
- Description—Enter a description for the certificate.
- Expiration Date—Choose the expiration date for the certificate.
- Logging Threshold (Days)—Specify the number of days before the certificate expires that you want warnings to begin being displayed. For example, if you specify 30 days, the warning message will appear on Windows Event Viewer each day, beginning 30 days before the certificate expiration date (the warning message appears as an error message).

Editing a Certificate in the Expiration Tracker

In the tree pane of the Administrator Console, expand Configuration Manager, click **Certificate Expiration Tracker**, right-click on the Certificate you want to edit, and then choose **Properties** to open and use the Certificate Expiration Tracker dialog box.

APPENDIX A

Working with Groups and Views

This appendix includes advanced information on working with Groups and Views within Cisco VXC Manager.

It includes:

Understanding Group Types and Views

Tip For information on managing Group Types, see Managing Group Types, page 7-62. For information on managing Views, see Managing Views, page 7-63.

Groups can be defined as a Group Type (predefined or custom), a Group Instance (within a Group Type), or any combination of these items. Cisco VXC Manager allows you to use predefined Group Types (OS, Platform, Image/Firmware Image Number, Subnet, Location, TimeZone, VendorID, Custom1, Custom2, and Custom3) or create any number of custom Group Types and Group Instances to facilitate the organization of your devices into functional hierarchies. You can then use these groups to create custom Views of your devices.

Views offer a way to visually organize your devices functionally so that you can better manage them. Because Cisco VXC Manager provides predefined Group Types and allows you to create custom Group Types and Group Instances, you can easily organize your devices in ways that best suit your organizational needs. By combining predefined Group Types, custom Group Types, and Group Instances you can achieve high levels of granularity in your Views (for information on creating Views, see Managing Views, page 7-63).

In a simple View, you would have a single Group Type and any number of Group Instances to accommodate your devices. For example, assume that your company devices are spread among two buildings. You might want a View that organizes your devices by the building where the devices reside physically. In this example View:

- Every View is identified by a View name. In our example, the view name could be By Building.

- A single-level View uses one Group Type to organize the devices. In our example, the Group Type is Building.
- The Group Instances within the Group Type define specific instances of that Group Type. In our example, Cisco I Building and Cisco II Building could be the two Group Instances of the general Group Type Building.

Multi-level Views use more than a single hierarchical level. Each additional level is nested within the larger level. Just as you can create your own custom Group Type for a single-level View, you can continue creating custom Group Types for nested hierarchical levels. For example, assume that, in addition to organizing your devices by building, your company also wants to distinguish the devices in each building by the department in which each device operates. Such a View would assume a slightly more granular hierarchy than our simple View example. In this multi-level View case:

- The View name should match the hierarchy of your view for easy identification. In our example, the View could be named By Building => Departments.
- Each Group Type corresponds to a view level in the View. In our example, Building is the Group Type for the View Level-1, and Departments is the Group Type for View Level-2.
- The View Level-2 Groups are Group Instances of the Group Type for that level. In our example, groups such as Engineering, Sales, and Marketing are all Group Instances of the general Group Type Departments.

Understanding the Show Empty Custom Group Folders Option

Cisco VXC Manager Views consist of hierarchies of folder groups, whether the folders are for a Group Type (predefined and/or custom), a Group Instance (within a Group Type), or any combination of these items. Show Empty Custom Group Folders is a Device Manager preference option that lets you choose whether or not to include empty custom group folders in your Views (see Device Manager Preferences, page 7-73).

When you create Views, it is generally recommended that you enable Show Empty Custom Group Folders. Every new folder for a custom group that you create starts out empty. If Show Empty Custom Group Folders is disabled, you will not be able to see newly created folders (or existing folders that have no devices in them) in your Views. For this reason, if the option is disabled while you are creating custom groups, Cisco VXC Manager prompts you whether or not to enable Show Empty Custom Group Folders so you can see the folders that you are creating. After you have assigned devices among your custom groups, there may be some group folders to which you did not assign any devices. You can choose to disable the Show Empty Custom Group Folders option to remove the empty folders from the View so that the hierarchy reveals only folders with assigned devices.

Use the following guidelines when enabling or disabling the Show Empty Custom Group Folders option:

- Using Predefined Group Types—The Show Empty Custom Group Folders option has no effect on the Cisco VXC Manager predefined Group Types. Empty predefined group folders never display in the Administrator Console, regardless of whether or not the Show Empty Custom Group Folders option is enabled. This prevents you from seeing folders for predefined Group Types that do not match the characteristics of any devices in your network. For example, if the Operating Systems of all of your devices is WTOS, you would not want to show the empty folders for the ThreadX operating system when there are no such devices in your network. Note that you cannot move devices across the Cisco VXC Manager predefined Group Types (for example, you cannot move a device from a WTOS OS group to a ThreadX OS group).
- Using Custom Group Types and Custom Instances—The Show Empty Custom Group Folders option should be enabled if you want to move devices from one custom group within the View to another custom group, particularly when some of your folders are still empty.

- **Using Views with Folders of Predefined Group Types Only**—As mentioned earlier, the Show Empty Custom Group Folders option has no effect on folders for predefined Group Types. Folders for predefined Group types will not show on a View unless there are devices that meet the characteristics of the predefined Group Types. For example, if all of the devices in your network are either WTOS and you have a single-level View with the predefined Group Type of OS, the View would contain only groups for WTOS, but not groups for the ThreadX operating system. In a View that contains predefined Group Types, Cisco VXC Manager prevents you from moving devices across predefined Group Types. It would be illogical to move a device that has the ThreadX OS to a folder of devices that have the WTOS OS.
- **Using Views with Folders of Custom Groups Types and Group Instances Only**—If you have a View that uses only custom Group Types and Group Instances, and the Show Empty Custom Group Folders option is enabled, your View will show all of the group folders, regardless of whether or not the devices have been assigned to every folder. For example, in a single-level View there is only one custom Group Type, in this case Building. The Group Instances for this custom Group Type include the Cisco I Building and Cisco II Building. Because the Show Empty Custom Group Folders option is enabled, the View shows the folder for the Cisco I Building even though there are no devices in it (in a View such as this, you can move devices from the Cisco II Building to the Cisco I Building by dragging and dropping (see Moving Devices Across Custom Groups, page A-4). However, if the Show Empty Custom Group Folders option is disabled, the View would show only the Cisco II Building (containing devices).
- **Using Views with Folders of Predefined Group Types and Custom Group Types**—When you have a View with both predefined Group Types and custom Group Types, the standard rules for each Group Type still apply. However, because a folder for a predefined Group Type can be a parent to children folders of custom Group Types, some special circumstances can arise. For example, even with Show Empty Custom Group Folders enabled, folders for custom Group Types that are children of a predefined Group Type will not be shown as long as all of the custom Group Type folders are empty. However, if a one of these children folders has a device assigned, all of the other sibling folders under the same parent folder will be shown.

Assigning Devices to Groups

Cisco VXC Manager uses the following three methods to assign devices to groups (in the first two methods, Cisco VXC Manager performs the device assignment without your direct intervention):

- **By System values of each device**—When discovering a device, Cisco VXC Manager examines the system values of the device (Platform, Vendor ID, OS, and so on). It then automatically groups the devices into the corresponding predefined Group Types that are built-into Cisco VXC Manager (OS, Platform, Image/Firmware Image Number, Subnet, Location, and Contact).
- **By Custom Group Type and Group Instance within a Group Type associated with a subnet**—When you define a subnet, Cisco VXC Manager allows you to specify whether the devices in the subnet should be automatically assigned to a custom Group Type and Group Instance within that Group Type. For example, a custom Group Type named Department can serve to denote the various departments within an organization (Marketing, Sales, Engineering, and so on). In this example, each individual department is a Group Instance within the larger Group Type. To assign devices by subnet, you must create the Groups you want (Group Types and Group Instances) prior to assigning the subnet (see Managing Views, page 7-63).
- **By Manual assignment**—After you have created a View and assigned devices to specific Group Types and Group Instances within those Group Types, you can manually drag-and-drop (assign) a device from one custom group within the View to another custom group. For example, if a View

groups devices by department within buildings, you can easily drag-and-drop a device from the Engineering department in one building to the Marketing department in the same building or in another building (see Moving Devices Across Custom Groups, page A-4).

Moving Devices Across Custom Groups

After creating a View and then assigning the devices to specific custom Group Types and/or Group Instances, you can manually move devices from one custom group within the View to another custom group (for example, in cases where certain devices must be relocated to a new department or assigned to a different function).

Cisco VXC Manager allows certain device moves and prevents others. For example, it does not allow you to move a device from a group of WTOS devices to a group of ThreadX devices. Be aware of the following rules of device movement:

- You can move devices only across custom groups.
- You cannot move devices between the Cisco VXC Manager predefined Group Types. For example, you cannot move a device from a WTOS OS group to a ThreadX OS group.
- You can move a device from its source to a destination at a higher level in a different branch. However, the device will move down the target branch to the group that matches the device characteristics from the originating group. If there is not a matching group for its device characteristics, the device spawns another set of groups to match the device characteristics from the originating group.

Tip Ensure that the Device Manager preference Show Empty Custom Group Folders is enabled, so your View can display newly created/empty folders (see Understanding the Show Empty Custom Group Folders Option, page A-2).

To move devices across custom groups within a View:

Procedure

Step 1 Switch to the View in which you wish to move devices across groups.

Step 2 Click the folder for the group that has the device or devices that you want to move to open the details pane displaying the devices in that group folder.

Step 3 Drag and drop the desired devices from the details pane to the desired target folder.

Creating Views: A Working Example

The process of creating Views can be divided into three stages. When creating your Views, use the guidelines discussed in the following sections.

Stage I: Determine Logical Groups and a Hierarchy for your View

Step 1 Analyze your organizational structure along functional lines and determine how you can logically group your devices to better manage them. Then conceive the necessary categories (Group Types) that you can use to organize your devices. Cisco VXC Manager allows you to use these Group Types to build hierarchies of device groups (Views) with any level of granularity you want. When your devices are grouped into hierarchies of Views, you can then easily manage and control them.

Step 2 Determine ways of organizing the Group Types you conceived into functional hierarchies of devices (Views) for your organization. Just as Cisco VXC Manager allows you to have unlimited Group Types, it also allows you to have any number of Views. You can create as many Views as is necessary to organize your devices. For example, if your Group Types include Building and Department, you could have one View that groups devices by building within each department. Conversely you could use the same Group Types and create a View that groups devices by department within each building.

Step 3 Use the Configuration Manager of the Administrator Console to create the necessary Group Types to accommodate the organizational hierarchy you developed in the previous steps. To create a Group Type, use the Group Type node under Configuration Manager (see Managing Group Types, page 7-62).

Stage II: Create a View and Choose Its View Levels

Step 4 A View name can be any text you want. However, it makes sense to assign names that correspond to the levels in your View so that you can easily identify your Views. By using arrows (=>) between each level, you can clearly establish the hierarchy of your View with the View name. After deciding on your naming conventions, you can create a View Name by using the Views node under Configuration Manager (see Managing Views, page 7-63).

Step 5 Every View requires you to choose at least one view level. The number of view levels dictates the granularity of your device hierarchy. View levels equate to Group Types that you might have created earlier, in Stage I. Because our example includes Group Types for Building and Departments and our example View uses a two-level hierarchy of Building => Departments, you would choose the Group Type Building as the first view level and Departments as the second view level. This hierarchical arrangement would allow you to group your devices by building and then within each building (by the department to which the devices belong).

Stage III: Create Group Instances and Prepare to Assign Devices to Groups

Step 6 After creating a Group Type (in Stage I) and assigning it to a level view (in Stage II), you can create Group Instances for each Group Type. In our example, we created the Cisco I Building and Cisco II Building as Group Instances for the Group Type Building. Similarly, we created the groups Engineering, Sales, and Marketing as groups of the Group Type Departments. To create a Group Instance, use the Device Manager node at each view level.

Once you have created a View, you are ready to assign devices to groups. For example, you can drag-and-drop devices from the Unassigned folder into the appropriate folder for your View (the Unassigned folder serves as a container to hold devices until they are assigned to a Group Type or Group Instance). For information on assigning devices to groups, see Assigning Devices to Groups, page A-3.

APPENDIX B

About Cisco VXC Manager Security

This appendix contains advanced information about Cisco VXC Manager security.

Note For detailed information about setting up Cisco VXC Manager for HTTPS communications, see *Installation Guide for Cisco Virtualization Experience Client Manager.*

Cisco VXC Manager allows you to set a Device Manager preference that prevents unauthorized Cisco VXC Manager installations from managing your devices. When the Enable Device Security option is set, the Cisco VXC Manager Agent (HAgent) and the Cisco VXC Manager Web Service enter into a one-to-one relationship. In this relationship, both the device and the Web Service share a unique security certificate in common. Before processing any Cisco VXC Manager requests, the Cisco VXC Manager Agent on the device verifies the certificate. If the Web Service certificate matches its own, the Cisco VXC Manager Agent allows the device to perform the requested functions or instructions. If the certificates do not match, the Cisco VXC Manager Agent prevents the device from complying with any of the requests.

Note Cisco ThreadX devices do not support device security.

Caution When Enabling Device Security: If you decide to enable device security, be sure to write down your certificate number and keep it in a safe place. If your Cisco VXC Manager installation becomes corrupt for any reason, and you must reinstall Cisco VXC Manager, you will get a new certificate number. Without the original certificate number, however, you will not be able to manage your devices. Cisco VXC Manager gives you the option of either changing a security certificate to a new one, or restoring an older certificate.
When Disabling Device Security: If you decide to disable device security, existing devices will not release their security certificate until their next check-in. They cannot be refreshed or rediscovered because the server no longer presents a certificate. They must check-in on their interval (that is, pull not push).

To enable Cisco VXC Manager Security, perform the following procedures:

Importing Certificates on Devices

Before starting secure communication between the components of Cisco VXC Manager, import the certificate to the devices. There are two ways to import certificates. One is to create and deploy a package containing the certificate. The other is to create a DDC containing the certificate, and allow the DDC to automatically deploy the certificate to all devices. The import procedure depends upon the device OS.

Tip Certificate Authentication: After deploying the certificate package to the devices, you need to authenticate the certificate with the server. The criteria for authentication of the certificate between the server and clients are based on the Certificate Issuing Authority, certificate creation date and name of the certificate. Upon successful certificate authentication, the server and the clients begin secure communication with one another.

WTOS

To import the certificate on devices running WTOS, you need to register two packages (like any other package you register in Cisco VXC Manager). One package is for adding the certificate and the other package is for removing the certificate from the devices. When you want to add or delete a certificate, you need to change the wnos.ini file and register two separate packages.

The folder structure for the certificate package is VXC-M Package\CADeployment and the folder named CADeployment contains one folder named wnos. The folder named wnos contains a folder named cacerts and a file named wnos.ini. The folder named cacerts contains the actual certificate file.

A sample wnos.ini for adding the certificate is shown below:

```
# Bypass the user log in to the local device
signon=0
# Set the Privilege to high
Privilege=high
# Command to Import the certificate to WTOS devices
AddCertificate= CA certificate file name
```

A sample wnos.ini to delete a certificate is shown below:

```
# Bypass the user log in to the local device
signon=0
# Set the Privilege to high
Privilege=high
# Command to delete the certificate in WTOS devices
DelCertificate= CA certificate file name
```

A sample rsp file for adding the certificate to WTOS devices is shown below:

```
[Version]
Number=CADeployment
Description=CA Certificate Deployment
OS=BL
Category=Images
ImageSize=
[Script]
```

SUSE Linux

A sample wlx.ini configuration for adding a SUSE Linux certificate is shown below:

```
ImportCerts=yes
Certs=rootca_new.cer;vxcm_new.cer
```

A sample rsp file for adding the certificate to SUSE Linux devices is shown below:

```
[Version]
Number=Certs_Package
OS=SLX
Category=Other Packages
[Script]
RP= "<regroot>"
```

Using Secure Communication (HTTPS)

Cisco VXC Manager supports secure HTTPS communication between components of Cisco VXC Manager.

The secure communication can be initiated in two ways:

- HTTPS Communication Initiated by Cisco VXC Manager Agent
- HTTPS Communication Initiated by the Cisco VXC Manager Administrator Console

HTTPS Communication Initiated by Cisco VXC Manager Agent

The Cisco VXC Manager Agent can initiate communication with the HServer during client device startup. When the Cisco VXC Manager Agent on a client boots up, it requests the following information from the DHCP server or proxy server:

- Server IP address
- HTTPS port number used for communication

If the Cisco VXC Manager Agent can retrieve the HTTPS port number from the DHCP option tags, it uses the IP address and port number to communicate with the HServer via HTTPS.

If the Cisco VXC Manager Agent cannot retrieve the HTTPS Port number from the DHCP option tags, it follows the sequence below:

1. The Cisco VXC Manager Agent tries to communicate via HTTPS using ports 443 and 8443.
2. If the Cisco VXC Manager Agent cannot communicate via HTTPS, it tries to connect via HTTP using ports 80 and 280.
3. If the Cisco VXC Manager Agent successfully initiates communication with the HServer, it caches the communication mechanism, IP address, and port number used and uses that information for any subsequent requests.
4. If HTTPS communication fails during startup, the Cisco VXC Manager Agent will not try the HTTPS protocol again.

HTTPS Communication Initiated by the Cisco VXC Manager Administrator Console

You can configure your network to allow the Administrator Console to determine the port number and protocol to use for communication with the HServer.

Determining the Port Number

To allow the Administrator Console to determine the port number for communication:

Procedure

Step 1 Configure the IIS that hosts the HServer with the desired port number.

Step 2 Stop the IIS and WWW service.

Step 3 Start the HServerInit service.

When the Administrator Console starts, it queries the database to retrieve the port number and IP address to use for communication with the HServer.

Determining the Protocol

To allow the Administrator Console to determine the protocol for communication:

Procedure

Step 1 Bind the IIS that hosts the HServer with a TCP, SSL, or TCP and SSL port.

Tip For an SSL port, you must install a certificate.

Step 2 Stop the IIS and WWW service.

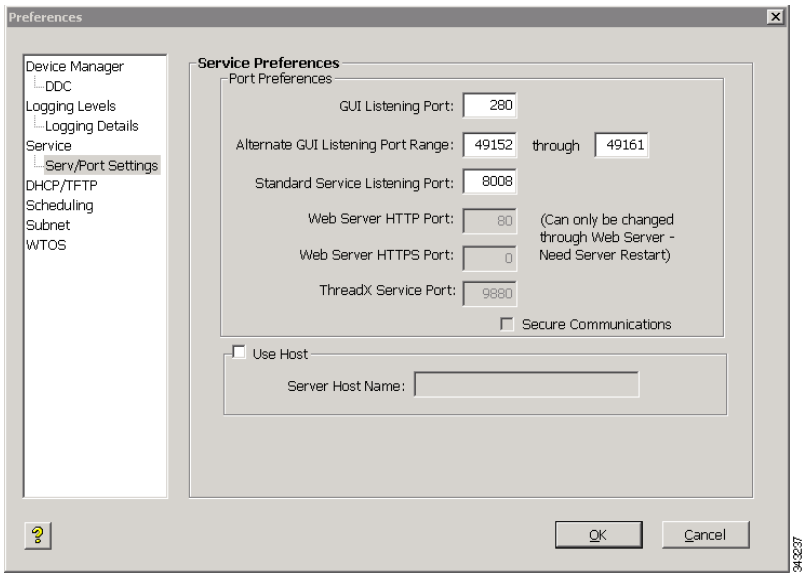
Step 3 Start the HServerInit Service.

The port number and IP address are stored in the Cisco VXC Manager Database.

If the request came via SSL, the entire Cisco VXC Manager configuration is set to secure.

No configuration is required in the Administrator Console, but the Secure Communications check box will appear in the Serv/Port Settings Preferences dialog box for information purposes.

Figure B-1 Serv/Port Settings Preferences



If an SSL port is configured on IIS, the Secure Communications check box is checked; otherwise it is unchecked.

Before starting secure communication, make sure all the following settings are configured:

- GUI Listening Port is 280.
- Alternate GUI Listening Port Range is 49152 through 49161.
- Standard Service Listening Port is 8008.
- Web Server HTTP Port is 80.
- Web Server HTTPS Port is 443.
- Secure Communications is checked.
- Check the **Use Host** check box to have the Cisco VXC Manager Agent use the Server Host Name you enter to connect to the server. Note that the Server Host Name will have a default value of the host machine and an administrator can change this value to a different host name (useful in cases of request forwarding through an HTTP Proxy).

Tip The secure communications flag applies to both remote and master repositories.

Enabling Cisco VXC Manager Device Security

Cisco VXC Manager allows you to set a Device Manager preference that prevents unauthorized Cisco VXC Manager installations from managing your devices.

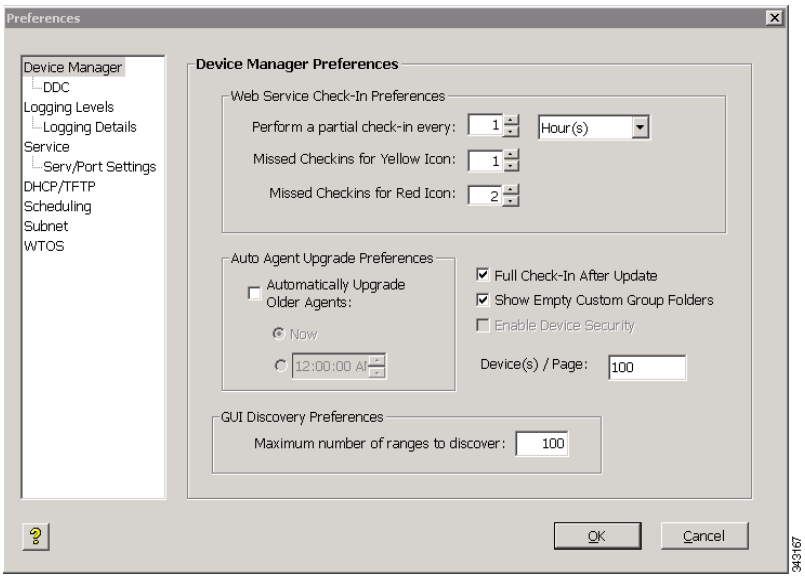
To enable device security:

Procedure

Step 1 In the tree pane of the Administrator Console, expand the Configuration Manager and choose **Preferences** to view the details pane displaying the categories for the Cisco VXC Manager Preferences.

Step 2 Double-click **Device Manager Preferences** to open the Device Manager Preferences dialog box.

Figure B-2 Device Manager Preferences



Step 3 Check the **Enable Device Security** check box, click **OK**, and then click **Yes** to confirm.

From this point forward, if a device does not already possess a security certificate, then the next time the device is discovered or checks-in, Cisco VXC Manager will establish the one-to-one relationship between the Cisco VXC Manager Agent of the device and the Cisco VXC Manager installation. This relationship prevents unauthorized Cisco VXC Manager installations from managing the devices.

Tip When you enforce device security, Cisco VXC Manager automatically encrypts all communications between the Web Service and the Cisco VXC Manager Agents. However, encryption can be turned on independently of device security (see Service Preferences, page 7-78).

Changing the Cisco VXC Manager Security Certificate

Before you change the Cisco VXC Manager security certificate, ensure that you have disabled device security. After changing the certificate number, you can re-enable device security (see Enabling Cisco VXC Manager Device Security, page B-5).

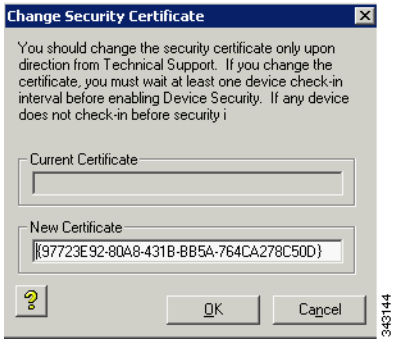
Use this procedure to change the Cisco VXC Manager certificate number (you can change the certificate to a new number or restore an older certificate).

To change the Cisco VXC Manager Security Certificate:

Procedure

Step 1 Expand the Configuration Manager, right-click the **Licensing** node, and choose **New > Certificate** to open the Change Security Certificate dialog box (note that Cisco VXC Manager creates a new certificate number in the New Certificate box).

Figure B-3 Change Security Certificate



Tip If you have not disabled device security, you will see a warning message.

Step 2 Depending on whether or not you want to accept the new certificate, complete one of the following:

- If yes, click **OK**. You are done with this procedure.
- If no, enter the security certificate to restore (presumably, your devices share this certificate from a previous Cisco VXC Manager installation; by restoring the security certificate, you will regain control of the devices), and then click **OK**.

Caution Before changing the security certificate, wait for a period of one check-in interval to allow all devices to check-in and release the current certificate. If a device that uses the current certificate does not check-in within this time, and you enable security for the new certificate, the device that did not check-in will be unmanageable (as it still has the old certificate).

APPENDIX C

Upgrading Cisco VXC Manager Agents

This appendix contains advanced information about upgrading Cisco VXC Manager Agents (HAgent). It also provides information on Cisco VXC Manager Agent error codes.

Note Because the Cisco VXC 2000 Series devices use a Cisco VXC Manager Agent that is integrated into the firmware, the upgrade procedures in this appendix do not apply to these devices. These procedures are only applicable to the Cisco VXC 6215, and only if an updated Cisco VXC Manager Agent is released for the device.

The Cisco VXC Manager Agent is a small Web agent that runs within the operating system of the device being managed. It has a very small footprint and is optimized for the thin client environment. The Cisco VXC Manager Agent works with the Cisco VXC Manager Services on the Cisco VXC Manager Server to perform the actions that are needed by you, the administrator. The Cisco VXC Manager Agent interprets the commands sent by the Cisco VXC Manager Server and makes the necessary changes to the device being managed. In addition, the Cisco VXC Manager Agent also provides status updates about the device to the Cisco VXC Manager Server.

t includes:

Using the Auto-Agent Upgrade Feature

The Auto-Agent Upgrade feature enables existing versions of the Cisco VXC Manager Agent on a device to be upgraded automatically. With this preference enabled, a device is automatically upgraded to the most current version of the Cisco VXC Manager Agent when the device is discovered (or checks-in).

Caution In cases where you have FTP or HTTP limitations, or have a large number of devices with older Cisco VXC Manager Agents on your network, this operation could take a significant amount of time. Therefore, it is recommended that you begin upgrading older Cisco VXC Manager Agents selectively. After upgrading a number of the devices selectively, you can turn on the Auto-Agent Upgrade feature to complete the upgrading process, and to continue upgrading any new devices that are added to the network as Cisco VXC Manager discovers them.

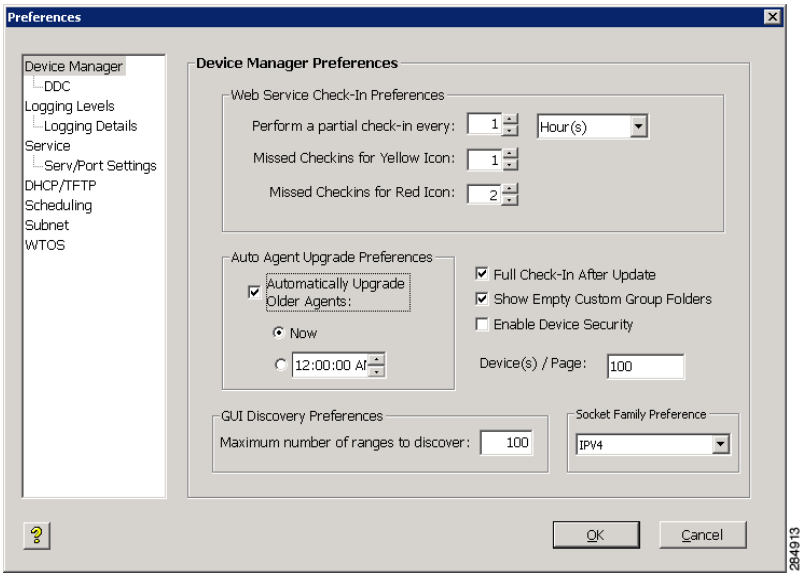
To enable automatic upgrading of Cisco VXC Manager Agents:

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager** and click **Preferences**.

Step 2 Double-click **Device Manager Preferences** to open the Preferences dialog box.

Figure C-1 Preferences—Device Manager



Step 3 Check the **Automatically Upgrade Older Agents** check box, and set the Auto-Agent Upgrade Preferences you want (selecting **Now** starts the upgrading process immediately; selecting the clock option allows you to set the desired time to start the upgrading process—a recommended time is during low network activity).

Tip By default, the time zone specified is the Database Update Server time zone (to specify a different the time zone, refer to Scheduling Preferences, page 7-83).

Be aware of the following:

- The new packages installed with Cisco VXC Manager are designed to upgrade existing Cisco VXC Manager Agent devices.
- Cisco VXC Manager Agent upgrades use the first 3 digits of the version number to determine if a newer Cisco VXC Manager Agent is available. The last digit is specific to Cisco VXC Manager for internal control and is not used by Auto-Agent Upgrade.
- If any Default Device Configuration (DDC) exists with Enforce Sequence enabled, Auto-Agent Upgrade will trigger the DDC to re-image devices, which will trigger Auto-Agent Upgrade in an infinite regression. Rebuild existing DDCs with an image containing the newest Cisco VXC Manager Agent.

Step 4 After you have finished your settings, click **OK**.

Tip For information on editing or deleting a scheduled update, see Managing the Schedules for Device Updates, page 5-29.

Understanding Cisco VXC Manager Agent Error Codes

This section contains information on the following errors:

- File Transfer Protocol Error Codes—The File Transfer Protocol (FTP) is a protocol that is able to transfer files between machines with different operating systems. The FTP utility issues an error, or reply, code to every user command. FTP errors are discussed in File Transfer Protocol (FTP) Error Codes, page C-3.
- Windows Sockets Error Codes—When using any TCP/IP application, it is possible for errors to occur in both configuration and networking. Many applications do not report these errors, but simply tell you that you have a network error. A list of possible errors (as reported by Microsoft) is shown in Windows Sockets Error Codes, page C-6.

File Transfer Protocol (FTP) Error Codes

The following are excerpts from RFC 959 for FTP.

An FTP reply consists of a three-digit number (transmitted as three alphanumeric characters) followed by some text. The number is intended for use by automata to determine what state to enter next; the text is intended for the human user.

The three digits of the reply each have a special significance. This is intended to allow a range of very simple to very sophisticated responses by the user-process. The first digit denotes whether the response is good, bad or incomplete. An unsophisticated user-process will be able to determine its next action (proceed as planned, redo, retrench, and so on) by simply examining this first digit. A user-process that wants to know approximately what kind of error occurred (for example, file system error, command syntax error) may examine the second digit, reserving the third digit for the finest gradation of information.

First Digit

There are five values for the first digit of the reply code:

- 1yz Positive Preliminary reply—The requested action is being initiated; expect another reply before proceeding with a new command (the user-process sending another command before the completion reply would be in violation of protocol; but server-FTP processes should queue any commands that arrive while a preceding command is in progress). This type of reply can be used to indicate that the command was accepted and the user-process can now pay attention to the data connections, for implementations where simultaneous monitoring is difficult. The server-FTP process can send at most, one 1yz reply per command.
- 2yz Positive Completion reply—The requested action has been successfully completed. A new request can be initiated.
- 3yz Positive Intermediate reply—The command has been accepted, but the requested action is being held in abeyance, pending receipt of further information. The user should send another command specifying this information. This reply is used in command sequence groups.

- 4yz Transient Negative Completion reply—The command was not accepted and the requested action did not take place, but the error condition is temporary and the action may be requested again. The user should return to the beginning of the command sequence, if any. It is difficult to assign a meaning to transient, particularly when two distinct sites (Server- and User-processes) have to agree on the interpretation. Each reply in the 4yz category might have a slightly different time value, but the intent is that the user-process is encouraged to try again. A rule of thumb in determining if a reply fits into the 4yz or the 5yz (Permanent Negative) category is that replies are 4yz if the commands can be repeated without any change in command form or in properties of the User or Server (for example, the command is spelled the same with the same arguments used; the user does not change his file access or user name; the server does not put up a new implementation).
- 5yz Permanent Negative Completion reply—The command was not accepted and the requested action did not take place. The User-process is discouraged from repeating the exact request (in the same sequence). Even some permanent error conditions can be corrected, so the human user may want to direct his User-process to re-initiate the command sequence by direct action at some point in the future (for example, after the spelling has been changed, or the user has altered his directory status).

Second digit (Function Groupings)

The following function groupings are encoded in the second digit:

- x0z Syntax—These replies refer to syntax errors, syntactically correct commands that do not fit any functional category, non-implemented or superfluous commands.
- x1z Information—These are replies to requests for information, such as status or help.
- x2z Connections—Replies referring to the control and data connections.
- x3z Authentication and accounting—Replies for the login process and accounting procedures.
- x4z—Unspecified as yet.
- x5z File system—These replies indicate the status of the Server file system through the requested transfer or other file system action.

Third Digit

The third digit gives a finer gradation of meaning in each of the function categories specified by the second digit, as shown in the following list:

Tip The text associated with each reply is recommended, rather than mandatory, and may even change according to the command with which it is associated. The reply codes, on the other hand, must strictly follow the specifications in the last section; that is, Server implementations should not invent new codes for situations that are only slightly different from the ones described here, but rather should adapt codes already defined.

- **100**
  - 110 Restart marker reply.
  - 120 Service ready in minutes.
  - 125 Data connection already open; transfer starting.
  - 150 File status okay; about to open data connection.
- **200**
  - 200 Command okay.

  - 202 Command not implemented, superfluous at this site.
  - 211 System status, or system help reply.
  - 212 Directory status.
  - 213 File status.
  - 214 Help message.
  - 215 NAME system type.
  - 220 Service ready for new user.
  - 221 Service closing control connection. Logged out if appropriate.
  - 225 Data connection open; no transfer in progress.
  - 226 Closing data connection. Requested file action successful (for example, file transfer or file abort).
  - 227 Entering Passive Mode (h1, h2, h3, h4, p1, p2).
  - 230 User logged in, proceed.
  - 250 Requested file action okay, completed.
  - 257 PATHNAME created.
- **300**
  - 331 User name okay, need password.
  - 332 Need account for login.
  - 350 Requested file action pending further information.
- **400**
  - 421 Service not available, closing control connection. This may be a reply to any command if the service knows it must shut down.
  - 425 Can't open data connection.
  - 426 Connection closed; transfer aborted.
  - 450 Requested file action not taken. File unavailable (for example, file busy).
  - 451 Requested action aborted: local error in processing.
  - 452 Requested action not taken. Insufficient storage space in system.
- **500**
  - 500 Syntax error, command unrecognized. This may include errors such as command line too long.
  - 501 Syntax error in parameters or arguments
  - 502 Command not implemented.
  - 503 Bad sequence of commands.
  - 504 Command not implemented for that parameter.
  - 530 Not logged in.
  - 532 Need account for storing files.
  - 550 Requested action not taken. File unavailable (for example, file not found, or no access).
  - 551 Requested action aborted: page type unknown.

- 552 Requested file action aborted. Exceeded storage allocation (for current directory or data set).
- 553 Requested action not taken. File name not allowed.

Windows Sockets Error Codes

WINSOCK Errors are generated when a script is running on a Cisco VXC Manager Agent. In such a case, the Cisco VXC Manager Agent either had trouble obtaining or sending a file as part of the script. The following is a list of possible errors (as reported by Microsoft):

Tip Errors are listed in alphabetical order by error macro. Some error codes defined in Winsock2.h are not returned from any function—these are not included in this list:

- WSAEINTR 10004—Interrupted function call. A blocking operation was interrupted by a call.
- WSAEACCES 10013—Permission denied. An attempt was made to access a socket in a forbidden way.
- WSAEFAULT 10014—Bad address. The system detected an invalid pointer address.
- WSAEINVAL 10022—Invalid argument. Some invalid argument was supplied.
- WSAEMFILE 10024—Too many open files. Too many open sockets.
- WSAEWOULDBLOCK 10035—Resource temporarily unavailable. Socket operation not available at this time.
- WSAEINPROGRESS 10036—Operation now in progress. A blocking operation is currently executing.
- WSAEALREADY 10037—Operation already in progress. An operation was attempted on a non-blocking socket with an operation already in progress.
- WSAENOTSOCK 10038—Socket operation on non-socket. An operation was attempted on something that is not a socket.
- WSAEDESTADDRREQ 10039—Destination address required. A required address was omitted from an operation.
- WSAEMSGSIZE 10040—Message too long. A message sent on a datagram socket was larger than the internal message buffer.
- WSAEPROTOTYPE 10041—Protocol wrong type for socket. A protocol was specified in the socket function call that is not supported.
- WSAENOPROTOOPT 10042—Bad protocol option. An unknown, invalid or unsupported call was made.
- WSAEPROTONOSUPPORT 10043—Protocol not supported. The requested protocol has not been configured into the system.
- WSAESOCKTNOSUPPORT 10044—Socket type not supported. The support for the specified socket type does not exist.
- WSAEOPNOTSUPP 10045—Operation not supported. The attempted operation is not supported.
- WSAEPFNOSUPPORT 10046—Protocol family not supported. The protocol family has not been configured into the system or no implementation for it exists.

- WSAEAFNOSUPPORT 10047—Address family not supported. An address incompatible with the requested protocol was used.
- WSAEADDRINUSE 10048—Address already in use. An application attempts to bind a socket to an IP address/port that has already been used for an existing socket.
- WSAEADDRNOTAVAIL 10049—Cannot assign requested address. The requested address is not valid.
- WSAENETDOWN 10050—Network is down. A socket operation encountered a dead network.
- WSAENETUNREACH 10051—Network is unreachable. A socket operation was attempted to an unreachable network.
- WSAENETRESET 10052—Network dropped connection. The connection has been broken due to keep-alive activity detecting a failure while the operation was in progress.
- WSAECONNABORTED 10053—Software caused connection abort. A connection was aborted by the software in your machine, possibly due to a TCP/IP configuration error, data transmission time-out or protocol error.
- WSAECONNRESET 10054—Connection reset by peer. An existing connection was forcibly closed by the remote host.
- WSAENOBUFS 10055—No buffer space available. An operation on a socket could not be performed because the system lacked sufficient buffer space or because a queue was full.
- WSAEISCONN 10056—Socket is already connected. A connect request was made on an already-connected socket.
- WSAENOTCONN 10057—Socket is not connected. A request to send or receive data was disallowed because the socket is not connected.
- WSAESHUTDOWN 10058—Cannot send after socket shutdown. A request to send or receive data was disallowed because the socket had already been shut down.
- WSAETIMEDOUT 10060—Connection timed out. A connection did not properly respond after a period of time.
- WSAECONNREFUSED 10061—Connection refused. No connection could be made because the target machine actively refused it.
- WSAEHOSTDOWN 10064—Host is down. A socket operation failed because the destination host is down.
- WSAEHOSTUNREACH 10065—No route to host. A socket operation was attempted to an unreachable host.
- WSAEPROCLIM 10067—Too many processes. A Windows Sockets implementation may have a limit on the number of applications that can use it simultaneously.
- WSASYSNOTREADY 10091—Network subsystem is unavailable. This error is returned if the sockets implementation cannot function because the system is currently unavailable.
- WSAVERNOTSUPPORTED 10092—Winsock.dll version out of range. The current Windows Sockets implementation does not support the Windows Sockets specification version requested.
- WSANOTINITIALISED 10093—Startup failed. The application socket startup failed.
- WSAEDISCON 10101—Graceful shutdown in progress. Returned to indicate that the remote party has initiated a graceful shutdown.
- WSATYPE_NOT_FOUND 10109—Class type not found. The specified class was not found.
- WSAHOST_NOT_FOUND 11001—Host not found. No such host is known.

- WSATRY_AGAIN 11002—Non-authoritative host not found. A temporary error during host name resolution and means that the local server did not receive a response from an authoritative server.
- WSANO_RECOVERY 11003—This is a nonrecoverable error. A nonrecoverable error occurred during a database lookup.
- WSANO_DATA 11004—Valid name, no data record of requested type. The requested name is valid and was found in the database, but does not have the correct associated data being resolved for it.
- ERROR_INTERNET_TIMEOUT 12002—Internet time-out. The request has timed out.

APPENDIX D

Device Discovery, Device Imaging, and Mass Imaging Tool

This appendix contains information about device discovery and advanced information about using the Cisco VXC Manager Mass Imaging Tool and using device imaging in Cisco VXC Manager.

It includes:

Device Discovery

This section contains information about the methods you can use to allow Cisco VXC Manager to discover Cisco VXC devices in your network, including the following:

Configuring the DHCP Server

Configure the following option tag values on your DHCP server:

- Option tag 186—IP address of your Cisco VXC Manager server (for example, 192.168.1.10). The value should be in 4-byte IP address format.
- Option tag 190—Secure port number to which Cisco VXC Manager server listens (for example, port 443). The value should be in word format (value = 0x01bb) or 2-byte array format (value = 0x01 0xbb).
- Option tag 192—Non-secure port number to which Cisco VXC Manager server listens (for example, 80). The value should be in either word format (value = 0x0050), or 2-byte array format (value= 0x00 0x50).

Tip The Cisco VXC Manager server and the DHCP server should not be running on the same machine. Some older agents use option tag 187 for the Cisco VXC Manager non-secure port number. The value of this option tag, when embedded within vendor class-specific information (option 43), was interpreted the same way as option tag 192. If option tag 192 is not supplied, the new Cisco VXC Manager Agent will accept option tag 187 for legacy support only. It is recommended that the DHCP server use option tag 192. Consult your DHCP server manual for DHCP option value configuration details.

To configure the Cisco VXC Manager server IP address and port option values on a Windows DHCP server:

Procedure

Step 1 Open the DHCP management wizard, choose the DHCP server to be configured, right-click the server name, and choose Set Predefined Options to open the Select Predefined Options and Values window.

Figure D-1 DHCP Window

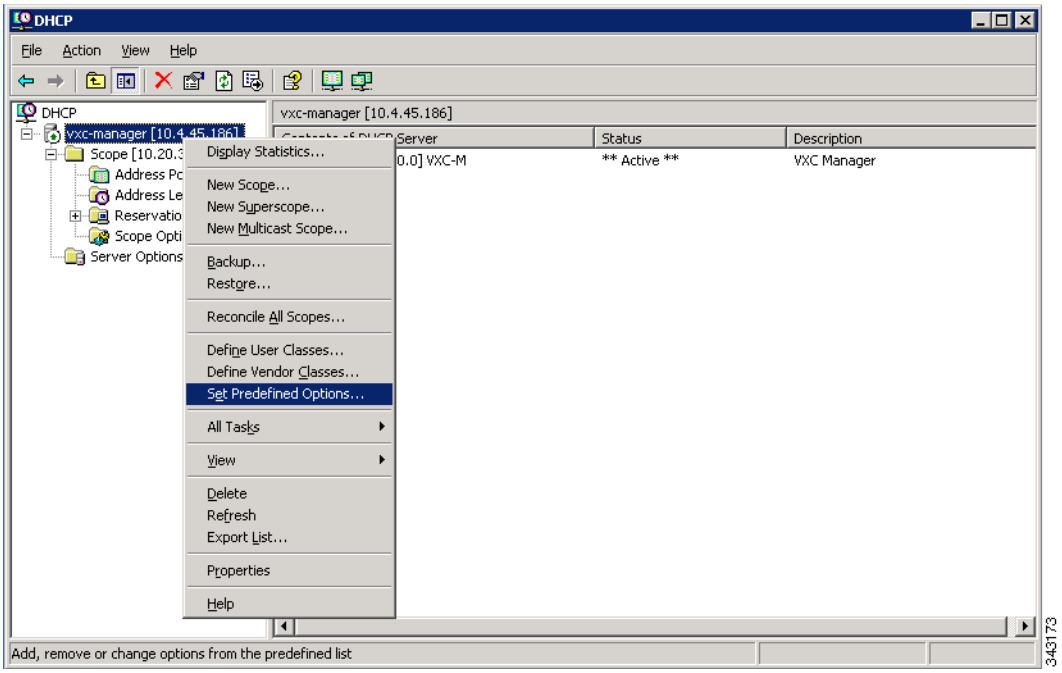
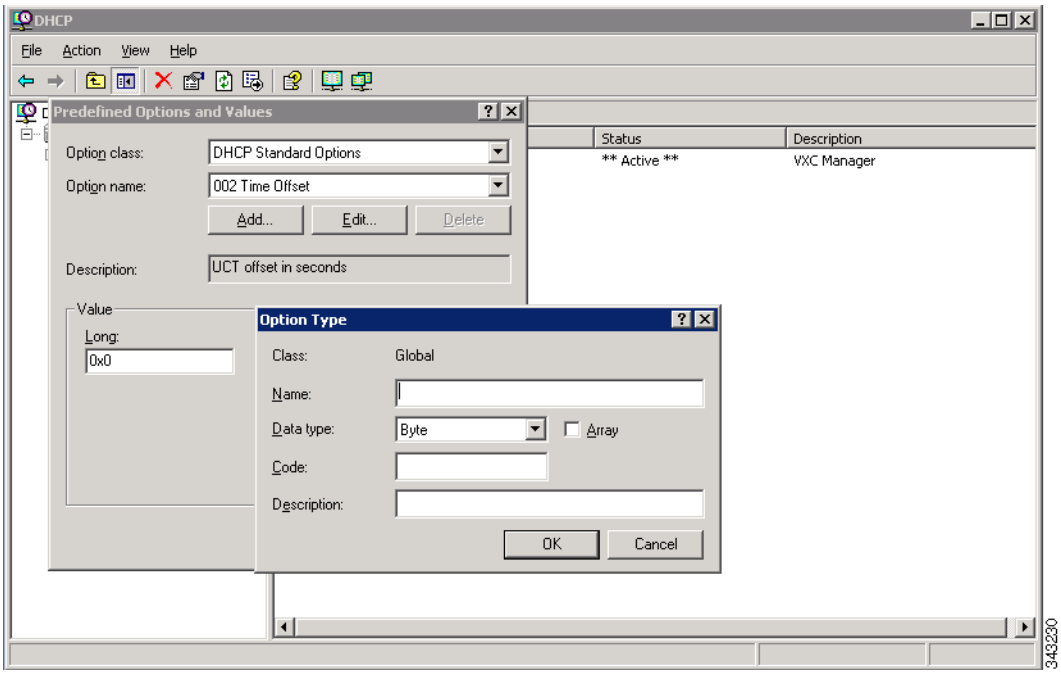


Figure D-2 Select Predefined Options and Values

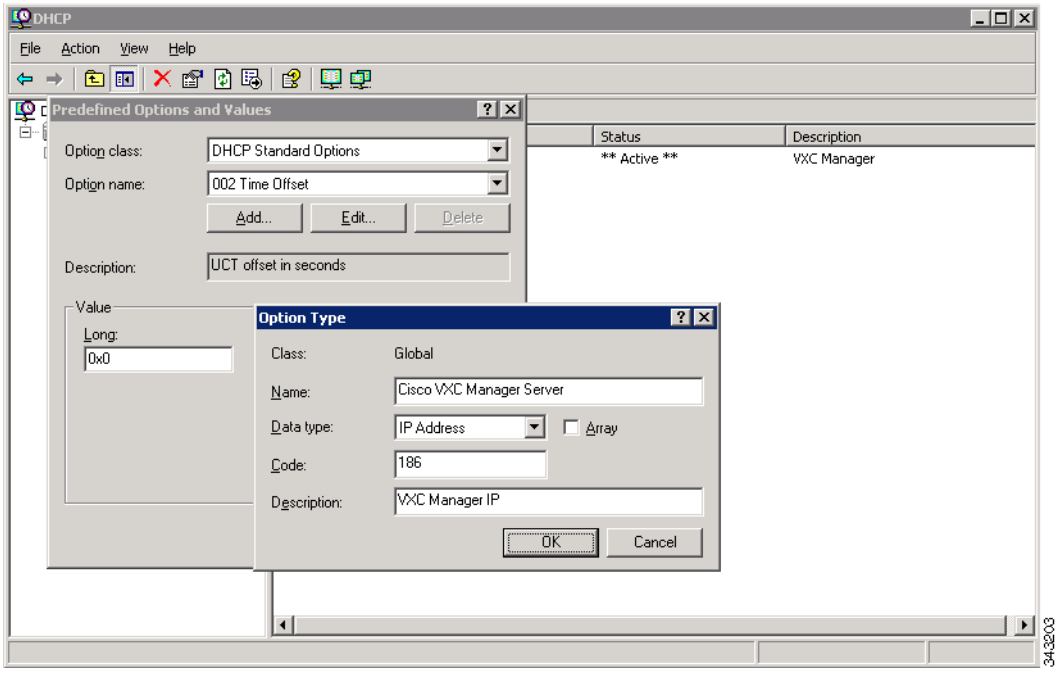


Step 2 On the Predefined Options and Values screen, click the **Add** button. The Option Type window appears.

Step 3 In the Option Type window, enter the required information:

- Name—Cisco VXC Manager Server
- Code—186
- Data Type—IP Address
- Description (optional)—Enter desired information, or nothing

Figure D-3 Option Type: Server IP



Step 4 Click **OK**.

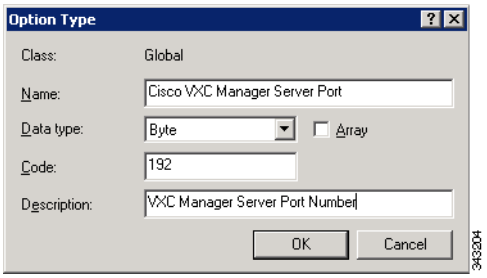
Step 5 Repeat Steps 2 and 3 for the Cisco VXC Manager Server port, with these changes:

- Name—Cisco VXC Manager Server Secure Port
- Code—190
- Data Type—Word

Step 6 Repeat Steps 2 and 3 for the Cisco VXC Manager Server port, with these changes:

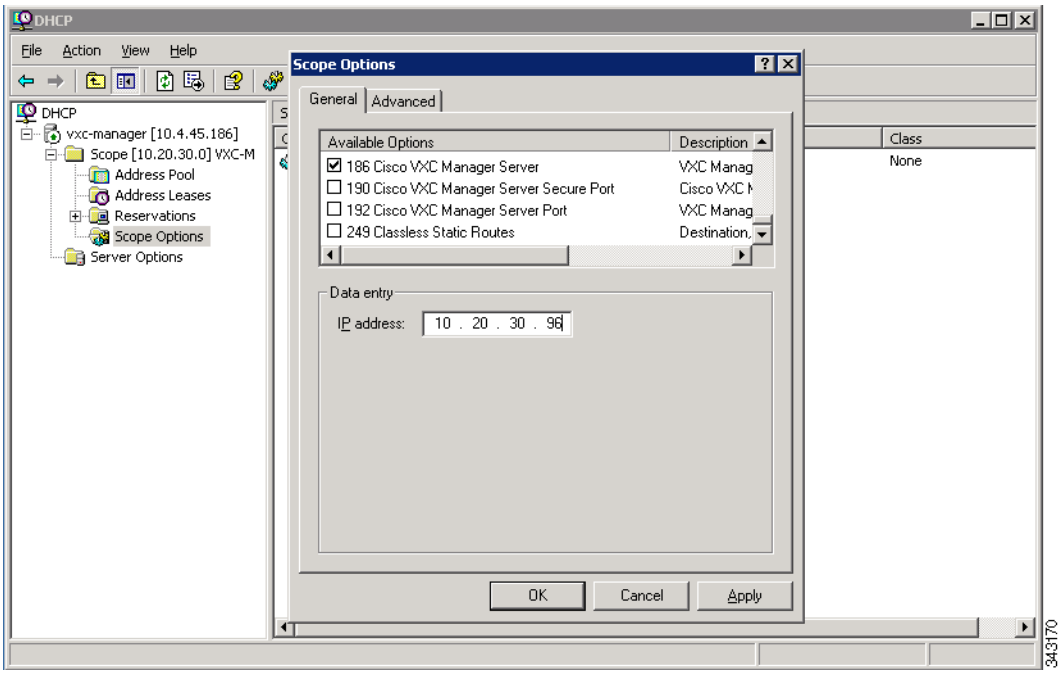
- Name—Cisco VXC Manager Server Port
- Code—192
- Data Type—Byte or Word

Figure D-4 Option Type: Cisco VXC Manager Server Port



Step 7 Click **OK**.

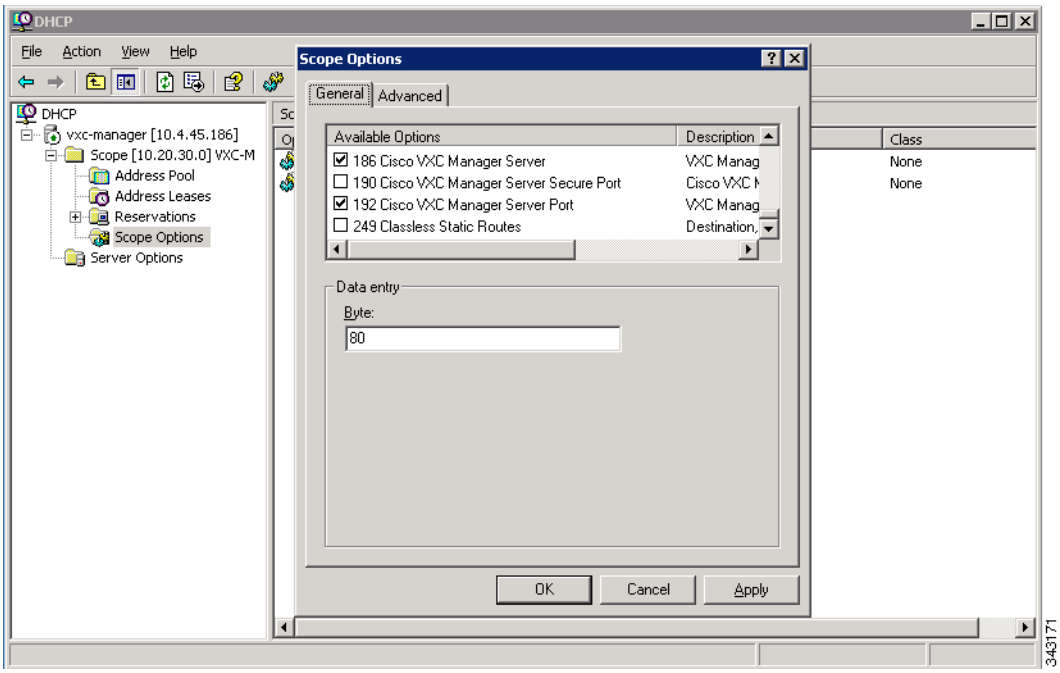
Figure D-5 DHCP Scope Options: Cisco VXC Manager Server



Step 8 From the DHCP management wizard, choose **Scope Options** (from the target DHCP Server Scope, as shown in Figure D-5), right-click, and choose **Configure Options**.

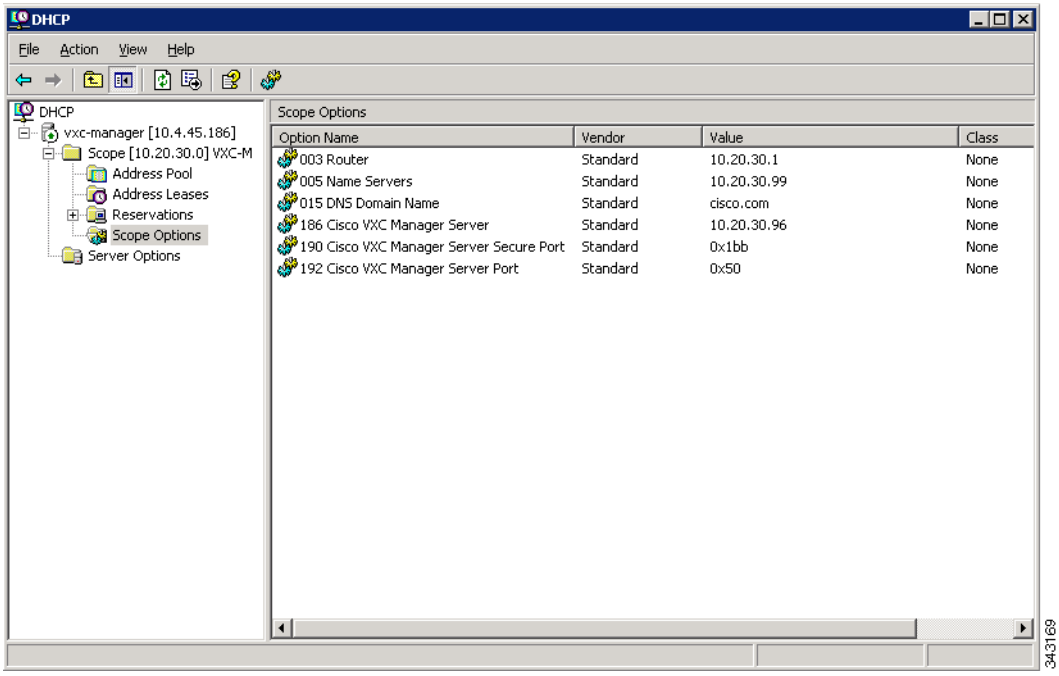
- In the list of Available Options, check option number 186, and enter the IP address of the Cisco VXC Manager server.
- In the list of Available Options, check option number 190, and enter the port number at which your Cisco VXC Manager server listens for secure communication.
- In the list of Available Options, check option number 192, and enter the port number at which your Cisco VXC Manager server listens (Port 80 is shown in Figure D-6).

Figure D-6 DHCP Scope Options: Cisco VXC Manager Server Port



Step 9 Click **OK**.

Figure D-7 DHCP Scope Options List



Step 10 Confirm that options 186, 190 and 192 are listed with proper values under the target DHCP server and scope.

Configuring a DNS Service Location (SRV) Resource Record for ThreadX Devices

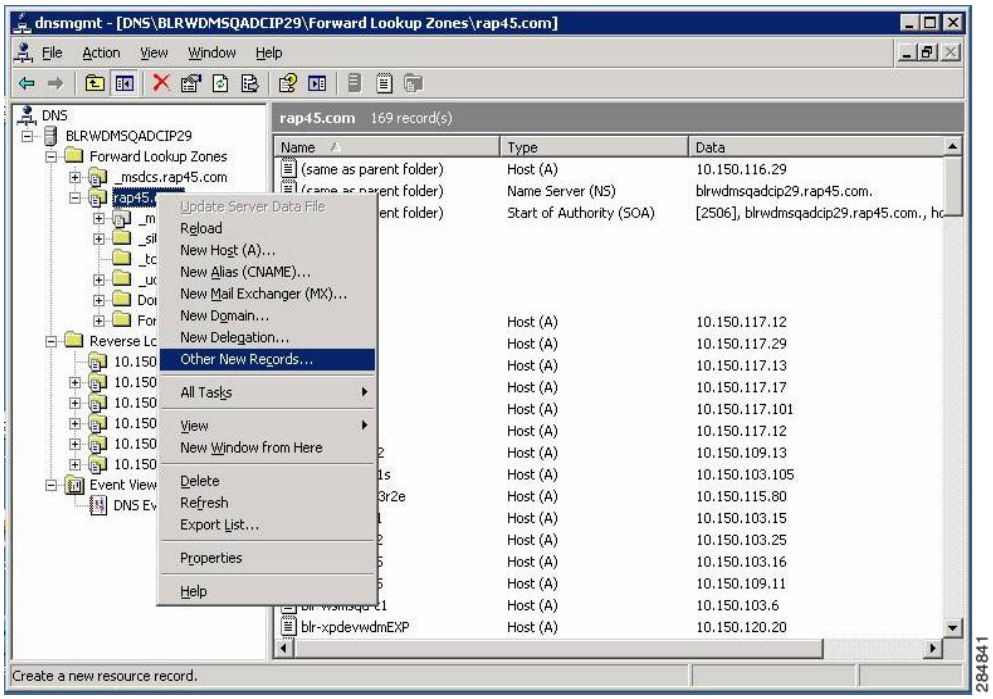
If you plan to use ThreadX devices, you can greatly improve the ThreadX client discovery process by creating a DNS Service Location (SRV) resource record.

Use the following procedure to create a DNS Service Location (SRV) resource record.

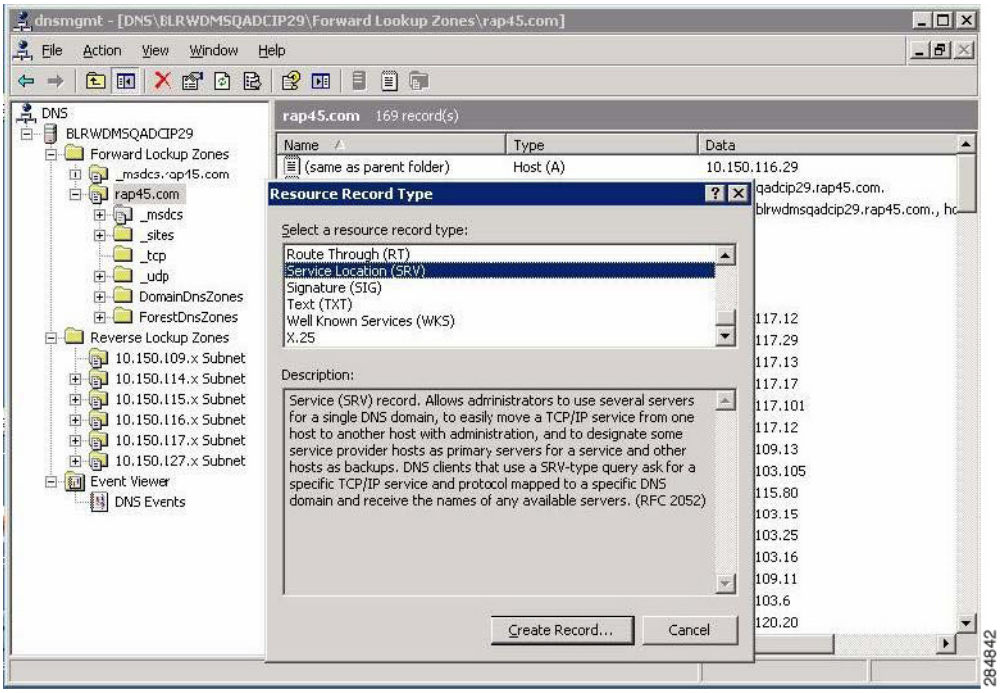
Procedure

Step 1 Open the DNS management console.

Step 2 Choose the domain where the server is configured, right-click it, and then choose **Other New Records** to open the Resource Record Type dialog box.

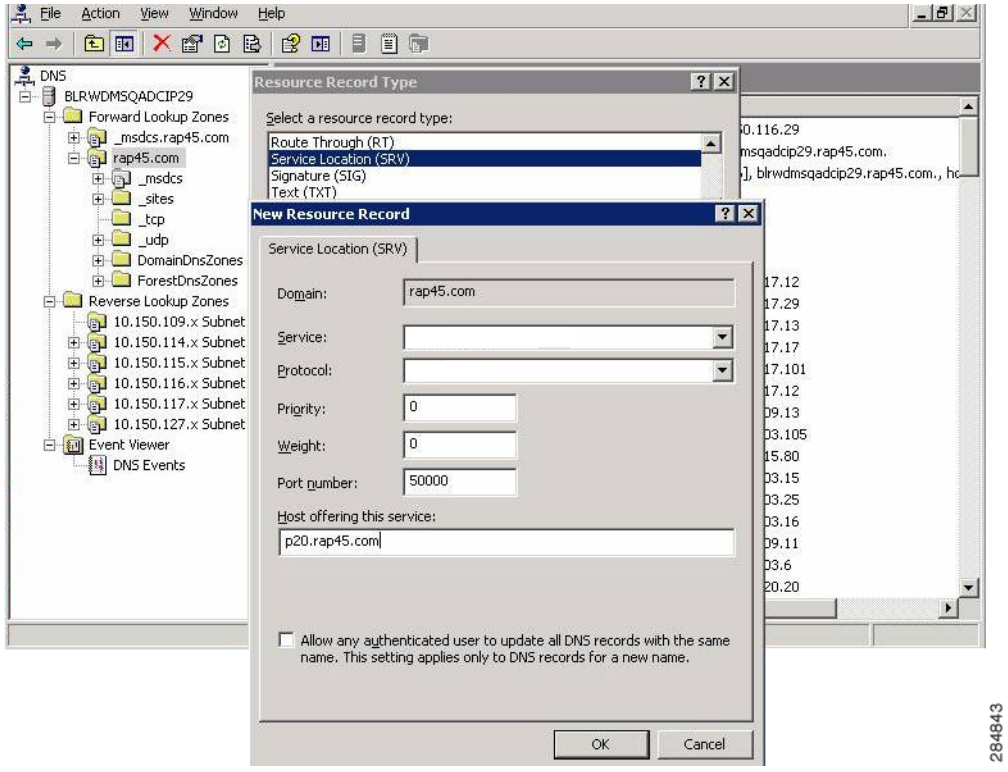


Step 3 Choose the Service Location (SRV) resource record type and then click **Create Record** to open the New Resource Record dialog box.



Step 4 Use the following guidelines (Domain is automatically shown):

- Enter **_Pcoip-tool** in the Service field.
- Enter **_tcp** in the Protocol field.
- (Optional) Enter the value you want for this Cisco VXC Manager server in the Priority field (the lower the priority value, the higher the priority).
- (Optional) Enter the value you want for this Cisco VXC Manager server in the Weight field (within the same priority class the higher the weight value, the higher the priority).
- Enter **50000** in the Port Number field.
- Enter the <FQDN of the Cisco VXC Manager server> (for example, p20.rap45.com) in the Host offering this service field.



Step 5 Click **OK**.

Configuring a Cisco VXC Manager Server Host Name in the DNS Server

This procedure describes how to register the server on which you installed Cisco VXC Manager with your DNS server (if not already registered).

On the DNS server, configure a host name record specifying the name and IP address of the server on which you have installed Cisco VXC Manager. Since no port number is provided, the Cisco VXC Manager Agent uses HTTP and the default port number 80.

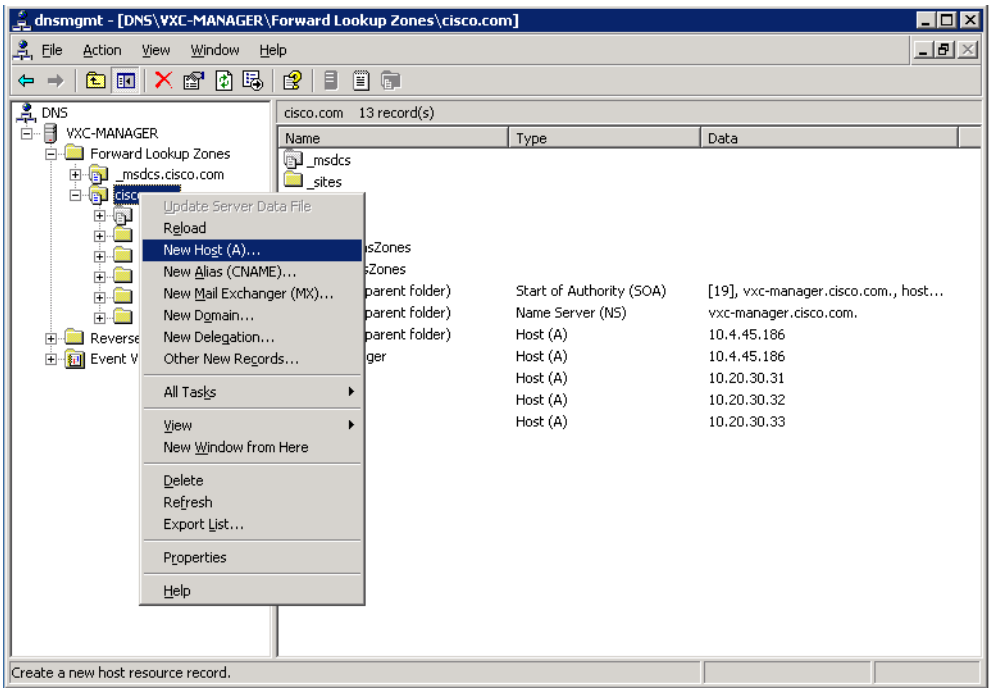
Tip The DHCP server must provide a proper DNS server and domain name in its offer before the Cisco VXC Manager Agent can query the DNS server. Consult your DNS server manual for host name configuration details.

To configure a Cisco VXC Manager server host name on a Windows DNS server:

Procedure

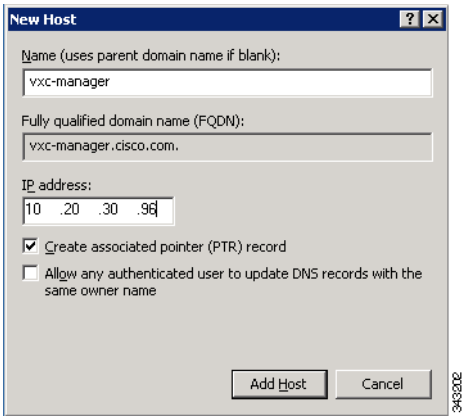
Step 1 Open the DNS management window.

Figure D-8 DNS Management: New Host



Step 2 Choose the domain to which the Cisco VXC Manager server belongs, right-click the domain, and choose **New Host**.

Figure D-9 New Host



Step 3 In the New Host window, enter the required information:

- Name—<Cisco VXC Manager Server name>
- IP address—<Cisco VXC Manager Server IP address>

Step 4 Click **Add Host**.

Step 5 Confirm that the Cisco VXC Manager Server host name is displayed with the proper IP address under the appropriate domain on the DNS management screen.

Configuring a Cisco VXC Manager Alias Record in the DNS Server

As an alternative to configuring the Cisco VXC Manager host name on the DNS server, you can configure an alias record using the name WDMServer and include the FQDN or IP address of the Cisco VXC Manager server. Since no port number is provided, the Cisco VXC Manager uses HTTP and the default port number 80.

Tip The DHCP server must provide a proper DNS server and domain name in its offer before the Cisco VXC Manager Agent can query the DNS server. Consult your DNS server manual for host name configuration details.

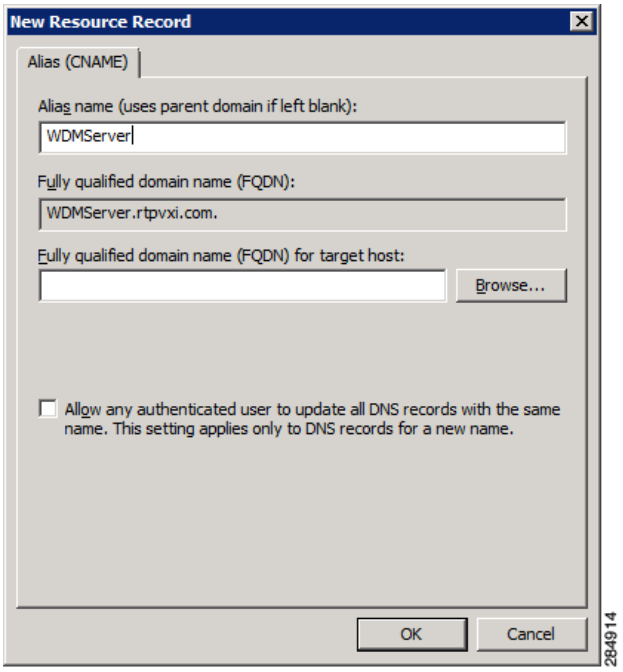
To configure a Cisco VXC Manager server alias record on a Windows DNS server:

Procedure

Step 1 Open the DNS management window.

Step 2 Choose the domain to which the Cisco VXC Manager server belongs, right-click the domain, and choose **New Alias (CNAME)**.

Figure D-10 New Resource Record

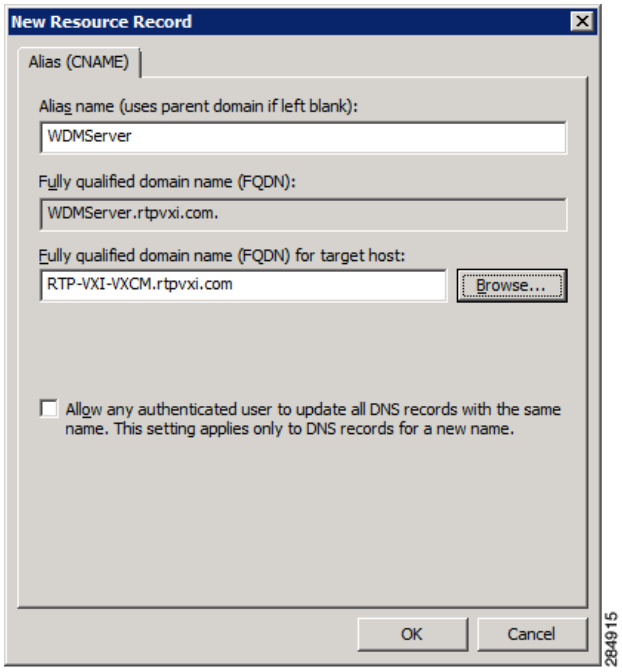


Step 3 In the New Resource Record window, enter **WDMServer** in the Alias name field.

Note The value in the Alias name field must be WDMServer. No other value is supported.

Step 4 Click **Browse** and choose the FQDN of the Cisco VXC Manager as the target host.

Figure D-11 New Resource Record—FQDN



Step 5 Click **OK**.

Step 6 Confirm that the WDMServer alias name is displayed with the proper FQDN (or IP address) under the appropriate domain on the DNS management screen.

Using Device Imaging in Cisco VXC Manager

Cisco VXC Manager can perform work on devices before the operating system loads on the device. To do this, the device is booted into an environment where it can communicate with the Cisco VXC Manager Server to perform imaging tasks. In order to perform image capture and deployment, scripted installs, registry backups, or execute certain scripts, you must implement a way to boot devices into this environment.

There are three ways to image devices:

- PXE Based Imaging, page D-12 (not applicable to Cisco VXC clients)
- Non-PXE Based Imaging (WTOS Boot Agent), page D-15 (not applicable to Cisco VXC clients)
- Non-PXE Based Imaging (Merlin Boot Agent), page D-15 (not applicable to Cisco VXC clients)

PXE Based Imaging

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

Pre-boot Execution Environment (PXE) is an industry standard developed to boot devices using the network. PXE can boot devices regardless of the disk configuration or operating system installed, and does not require any files or configuration settings on a device. After PXE boot is turned on in the BIOS, a device can communicate with your network PXE Server to receive imaging jobs. PXE provides a number of advantages, and enables you to remotely deploy an image to a device.

Note With PXE based imaging, the Cisco VXC Manager TFTP transfer is restricted to a 1500-byte packet size, and the Don't Fragment bit is set.

PXE Request Routing

PXE clients use broadcast packets to find DHCP and PXE services on a network to transfer files. These packet types can present challenges when planning a PXE deployment because most default router configurations do not forward broadcast traffic. To resolve this, you must either configure your routers to forward these broadcast packets to the correct server(s), or install a PXE Server on each subnet. Routers are generally configured to forward broadcast traffic to specific machines. The source subnet experiences the broadcast, but any forwarded broadcast traffic targets specific machines. Enabling a router to support DHCP is common. If both PXE and DHCP services are located on the same machine, and DHCP packet forwarding is enabled, you should have no problem transferring broadcast packets. If these services are located on different machines, additional configuration might be required. If you are going to forward packets, be sure your router configuration allows DHCP traffic to access the proper ports and IP addresses for both DHCP and PXE servers.

Installing and Configuring DHCP

DHCP is an integral part of the PXE process, and must be installed and configured in order to use PXE. You must obtain, install, and configure a DHCP server component separately (a DHCP server is not provided with Cisco VXC Manager). After DHCP is set up and your PXE servers are installed, you must configure how your PXE servers will interact with the DHCP server.

Deploying an Image Package

Prior to deploying an image package, complete the following:

Procedure

Step 1 Register the image package within Cisco VXC Manager. The image package can be either a custom image, or an image which has been registered from an existing reference device.

Step 2 Enable the image package so that it can be deployed.

Step 3 Ensure that the device to be imaged is part of the Cisco VXC Manager system (the device must either be previously discovered or manually added using the Administrator Console as described in Adding and Automatically Discovering Devices, page 2-13).

Step 4 To register an image, see Register a Package from a Script File (.RSP), page 3-35.

To image a device you can:

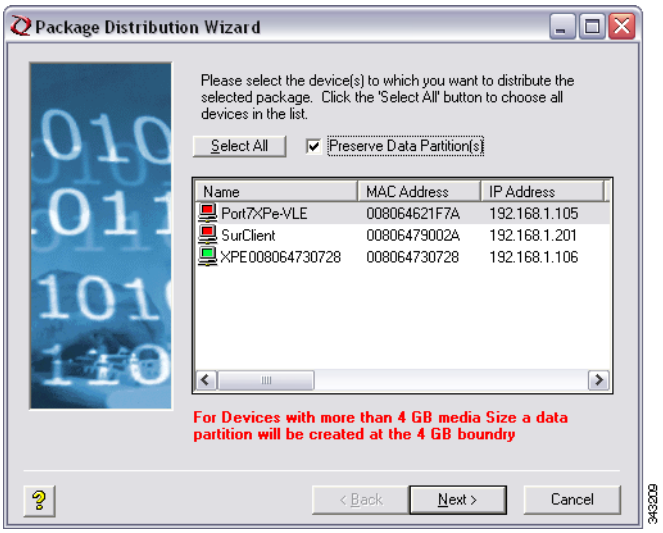
- **Image a Group of Devices**:

a. In the tree pane of the Administrator Console, expand the **Package Manager** until you find the image you need to deploy, and then choose the image.

b. In the same tree pane, expand the **Device Manager** node, and open the folder that contains the list of devices to be imaged.

c. Drag and drop the Cisco VXC Manager package to the group where the image needs to be deployed. (For example, if you created a default View to display all the devices in your finance department and placed it in a folder named Finance, you can open the folder and drag and drop the image to the folder. Note that the list of devices will automatically be filtered to include only the devices which have the same operating system as the image being deployed.) The Package Distribution Wizard appears.

Figure D-12 Package Distribution Wizard



d. Choose the devices to which the image package needs to be scheduled (if a data partition needs to be preserved, check the **Preserve Data Partition(s)** check box), click **Next**, and then schedule the Cisco VXC Manager package for deployment.

- **Image from the Update Manager**:

a. In the tree pane of the Administrator Console, right-click **Update Manager** and choose **New > Update** to open the Software Package Wizard.

b. Choose the folder that contains the image you want to distribute and click **Next**.

c. Choose the image you want to be deployed and click **Next** (note that the list of devices will automatically be filtered to include only the devices which have the same operating system as that of the image being deployed).

d. Schedule the Cisco VXC Manager package for deployment.

About the Imaging Process

After you schedule the Cisco VXC Manager package for deployment and the device checks in with the Cisco VXC Manager Server, the following imaging process occurs:

1. The Cisco VXC Manager server checks if there is an update for the device.
2. If an imaging job is scheduled, the device is notified.
3. The device will then re-boot and go through a network boot process.
4. The Cisco VXC Manager Agent will be downloaded to the device and will contact the Cisco VXC Manager server to get the appropriate image that has been specified from the Cisco VXC Manager Repository.
5. The Cisco VXC Manager Agent will then apply the image to the flash file system of the device.
6. The device will then re-boot to the new image.

Non-PXE Based Imaging (WTOS Boot Agent)

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

Non-PXE based imaging relies on a Boot Agent that resides in the client device flash memory. The Boot Agent currently supports downloading of Merlin boot floppy only. The Boot Agent communicates with the Cisco VXC Manager server to determine whether the target device needs imaging. Since the Boot Agent does not boot via the PXE protocol, it does not receive the Cisco VXC Manager server IP address and port number from the Cisco VXC Manager proxy DHCP service. In this release, the Boot Agent can discover the Cisco VXC Manager server IP address and port number from any one of the following sources (listed in priority order):

1. DHCP option tag values received from the standard DHCP server.
2. Cisco VXC Manager server URLs configured from the Boot Agent desktop.
3. DHCP option tag values received from standard or Cisco VXC Manager proxy DHCP service for vendor class RTIAgent.
4. DNS service location record.
5. DNS host name lookup.

Non-PXE Based Imaging (Merlin Boot Agent)

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

When configuring the Merlin Boot Agent statically, use the following guidelines:

Procedure

Step 1 Image the Non-PXE client with the latest initrd.pxe and vmlinuz.pxe so that the device has the latest initrd.pxe.

Step 2 Disable the DHCP Server and Standard Service.

Step 3 Schedule a Non-PXE imaging job.

Step 4 During Merlin boot up after the beep, press the Esc Key to clear the previous static configuration. This is required only when you need to enter the configuration once again. If you do not press the Esc key press and if the configuration is not present (for the first time) you will be prompted to enter the following inputs (otherwise, if you already entered configuration values you will not be prompted to enter the following inputs and it will go to the imaging mode directly):

- Client IP Address
- Subnet Mask
- Default Gateway
- Cisco VXC Manager IP address
- Protocol (http/https) default http
- Port number (default port 80)

Deploying the Image Using Merlin in Non-PXE Based imaging

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

To deploy a Merlin Image complete the following steps:

Procedure

Step 1 In the Administrator Console, expand **Device Manager** to display the list of devices. Drag and drop the Merlin image (for example, push_9V92_S550_512) onto the desired device.

Step 2 To verify the Merlin imaging process, check to see that the Boot Agent boots first on the device and then boots the guest OS after contacting the Cisco VXC Manager server.

Step 3 Pull or push the image of the devices which you have already programmed with the Boot Agent image, using Merlin.

Step 4 To verify image deployment, observe the following sequence of events:

- The device boots up through the Boot Agent.
- The device contacts the Cisco VXC Manager and downloads Merlin through HTTP.
- Merlin contacts the Cisco VXC Manager server and starts the imaging process.

Using the Cisco VXC Manager Mass Imaging Tool

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

The Cisco VXC Manager Mass Imaging Tool is designed to help you manage (Register, Unregister, Add Schedule, Remove Schedule, and Delete Records) Cisco VXC Manager packages for all of the devices in your Cisco VXC Manager system at the same time. While you can perform Cisco VXC Manager package registration and scheduling using the Cisco VXC Manager Administrator Console (see Package Manager, page 3-31 and Update Manager, page 5-29 respectively), the Cisco VXC Manager Mass Imaging Tool allows you to easily perform these tasks when you intend to perform them for all of the devices in your Cisco VXC Manager system.

Prerequisites

Caution Before opening and using the Cisco VXC Manager Imaging Tool, be sure that the following prerequisites are satisfied.

- The devices you want to update belong to subnets that have been added to the Cisco VXC Manager system (the subnets are recognized by the Cisco VXC Manager system).

Tip If you manually add a single device to the Cisco VXC Manager system, you will add the subnet needed for all devices in that subnet (see Adding Devices Manually, page 2-15).

- Only the devices you want to image are connected to the Cisco VXC Manager system. Distribution of the image occurs for all connected devices upon device boot/reboot until you use the Remove Schedule command button on the Cisco VXC Manager Imaging Tool to remove the scheduled update appearing in the Current Scheduled Package field. Be sure that any device you do not want to image is disconnected from the Cisco VXC Manager system until after you use the Remove Schedule command button on the Cisco VXC Manager Imaging Tool to remove the scheduled update appearing in the Current Scheduled Package field.
- The Cisco VXC Manager Administrator Console (GUI) is closed.

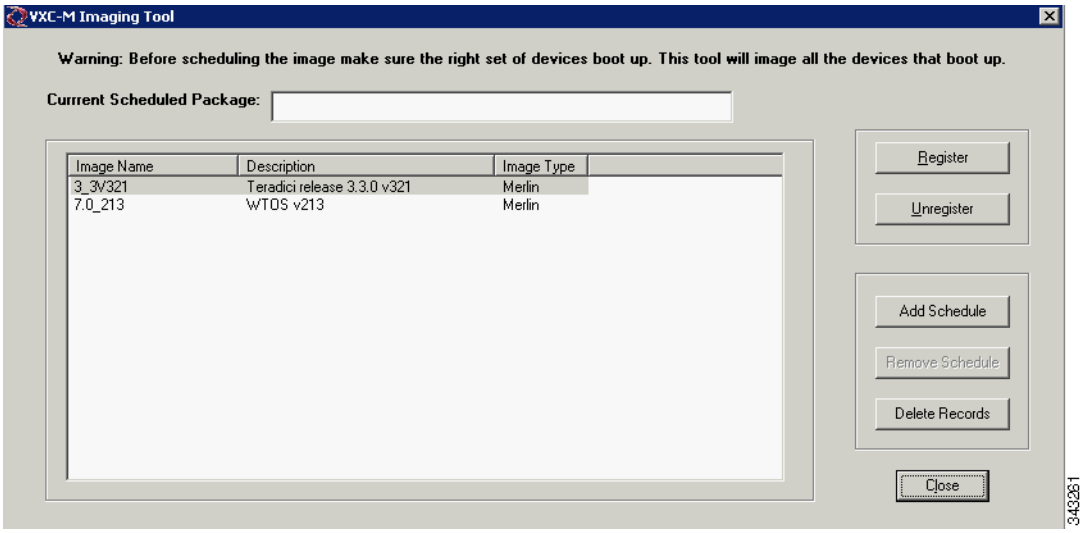
Procedure

Use the following procedure to use the Cisco VXC Manager Mass Imaging Tool.

Procedure

Step 1 Click **Start > All Programs > Cisco VXC Manager > VXC-MImaging** to open the Cisco VXC Manager Imaging Tool.

Figure D-13 Cisco VXC Manager Imaging Tool



Step 2 Use the following guidelines for the command buttons available:

- Register—allows you to register a Cisco VXC Manager package using the Cisco VXC Manager Package Registration wizard (click **Register**, browse and choose the RSP file you want, click **Next**, click **Register**, and then click **OK**—all packages you register appear in the main pane of the tool and are ready to be scheduled by clicking **Add Schedule**).
- Unregister—allows you to remove the registration of Cisco VXC Manager packages from the system (choose a package in the main pane, click **Unregister**, and then confirm).
- Add Schedule—allows you to schedule a Cisco VXC Manager package for distribution (choose a package in the main pane, click **Add Schedule**, and then confirm—the Cisco VXC Manager package appears in the Current Scheduled Package field, and the distribution will occur on the next device boot up).

Caution If you are rescheduling an image that has been successfully distributed to the same devices, you must first click **Delete Records** to clear the entries from the database.

- **Remove Schedule**—allows you to remove the scheduled update appearing in the Current Scheduled Package field. For example, after successfully imaging all connected devices upon device boot/reboot, click **Remove Schedule** before you connect any device you do not want to image.
- **Delete Records**—allows you to reset the imaging status for the devices in the Cisco VXC Manager database. For example, after imaging is done successfully (and the Cisco VXC Manager database table is updated for those particular MAC addresses) and you want to reschedule the image to the same devices, you must first click **Delete Records** to clear the entries from the database.

Step 3 When you are finished using the Cisco VXC Manager Imaging Tool, click **Close**.

APPENDIX E

Troubleshooting

This appendix contains provides general troubleshooting information.

It includes:

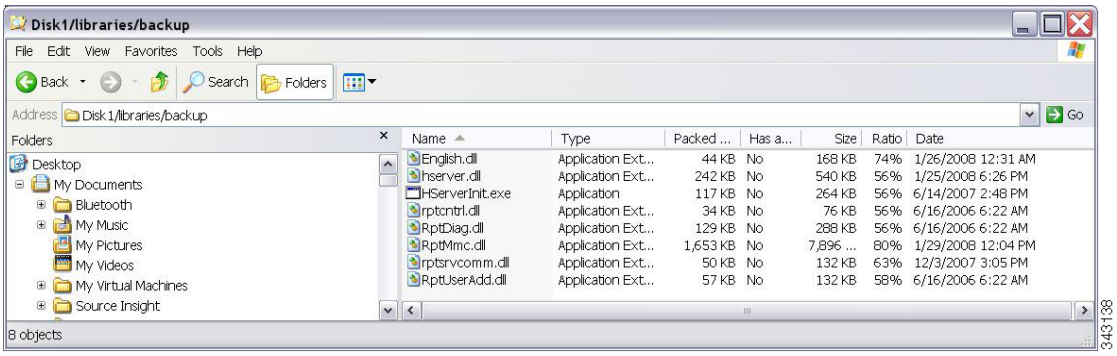
Problem with Cisco VXC Manager Upgrade Installation

Problem: Files that were in use during the upgrade process were not overwritten.

Solution: Do the following:

- Navigate to the folder VXC-Mv<ReleaseNumber>\Disk1\libraries\backup

Figure E-1 Backup Folder Contents



- For each file listed in the backup folder (see Figure E-1), check the modification date and file size properties
- Compare the file properties shown in the backup folder to the properties for the same file in its destination folder. Table E-1 shows the paths to the destination folders for each file in the backup folder

Table E-1 .Destination Folder Paths

File Name	Path to Destination Folder
English.dll	~\Program Files\Cisco\VXC-M
HServer.dll	~\Inetpub\wwwroot
HServerInit.exe	~\Program Files\Cisco\VXC-M
rptcntrl.dll	~\WINDOWS\system32
rptdiag.dll	~\Program Files\Cisco\VXC-M\Utilities
RptMmc.dll	~\Program Files\Cisco\VXC-M
RptSrvComm.dll	~\WINDOWS\system32
RptUserAdd.dll	~\WINDOWS\system32

- If the properties shown for a file in the backup folder do not match the properties for that file in its destination folder, make a copy of the file in the backup folder and put it in the appropriate destination folder.

License Error

Problem: If Cisco VXC Manager discovers non-Cisco devices, this results in a pop-up license error that automatically appears every time such devices check in or if the administrator tries to manage these non-Cisco devices.

Solution: Upload a valid license for the non-Cisco devices. If a valid license is not available, delete the non-Cisco devices from the Device Manager and disconnect the devices from the network.

PCoIP clients unable to connect following firmware upgrade

Problem: If Cisco VXC Manager is used to upgrade the firmware for Cisco VXC 2111/2211 PCoIP clients, the client may be unable to connect to the virtual machine following the upgrade.

Solution: The local user must access the On Screen Display menu for the client and do the following:

Procedure

Step 1 Choose **Options > Config > Unlock**.

Step 2 Leave the password field blank, and click **OK.**

Step 3 Click the **Connection Management** tab and uncheck **Enable Connection Management**.

Step 4 Click the **VMware View** tab and check **Enable VMware View** and **FQDN**.

Step 5 In the FQDN field, enter the FQDN of the broker server hosting the virtual machine.

Step 6 In the Port field, delete the port value of zero (**0**) and leave the field blank.

Step 7 Click **OK**.

Step 8 When asked to reset the client for the changes to take effect, click **Yes**.

Remote Shadowing Problems

Problem: You are having problems with Remote Shadowing.

Solution: Ensure that you set the appropriate preferences in Remote Shadow to **Viewer** or **Browser**.

Setting the Correct Logging Levels

Problem: You want to set the logging levels appropriately.

Solution: Set logging levels to Debug only for isolating problems. During normal Cisco VXC Manager functioning, set the logging levels to either Warning or Error.

Viewing Service Logs—Example

Use these procedures to view the logged activity for the Cisco VXC Manager service logs including:

- Web Services Log—Details the activity of the Cisco VXC Manager Web Services for device management.
- TFTP Log—Details the Trivial File Transfer Protocol activity for distributing software packages to devices.
- Standard Services Log—Details the activity of the Cisco VXC Manager Standard Services.
- DHCP Log—Details the activity of the Cisco VXC Manager Dynamic Host Configuration Protocol as it assigns IP addresses to devices.

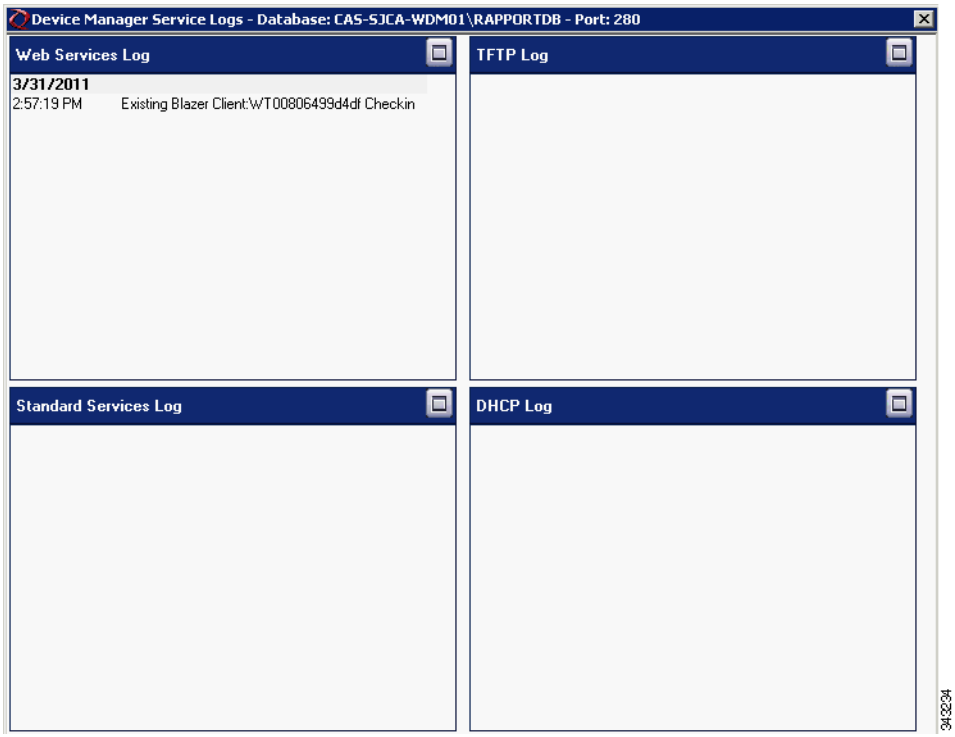
Tip For information on setting the level of logging activity for the Cisco VXC Manager service logs, refer to Logging Preferences, page 7-75.

To view the Cisco VXC Manager service logs:

Procedure

Step 1 Double-click the **Service Logs** icon in the Cisco VXC Manager system tray to open the Cisco VXC Manager Service Logs window.

Figure E-2 Service Logs



Step 2 Review the information for the log you want.

Tip To expand a window for any of the logs, click its maximize button.

Changing the IP Address of the Cisco VXC Manager Server

Problem: You want to change the IP address of the Cisco VXC Manager Server, where the HServer is running.

Solution: Change the IP address of the Cisco VXC Manager Server by completing the following:

Procedure

Step 1 Change the following registry settings:

- Configuration Manager\Software Repositories\Master = new IP address
- HKLM\Software\Rapport\SWRep\FTPUserDomain = new IP address

Step 2 Restart IIS.

Step 3 Restart Cisco VXC Manager services (use the Services tab).

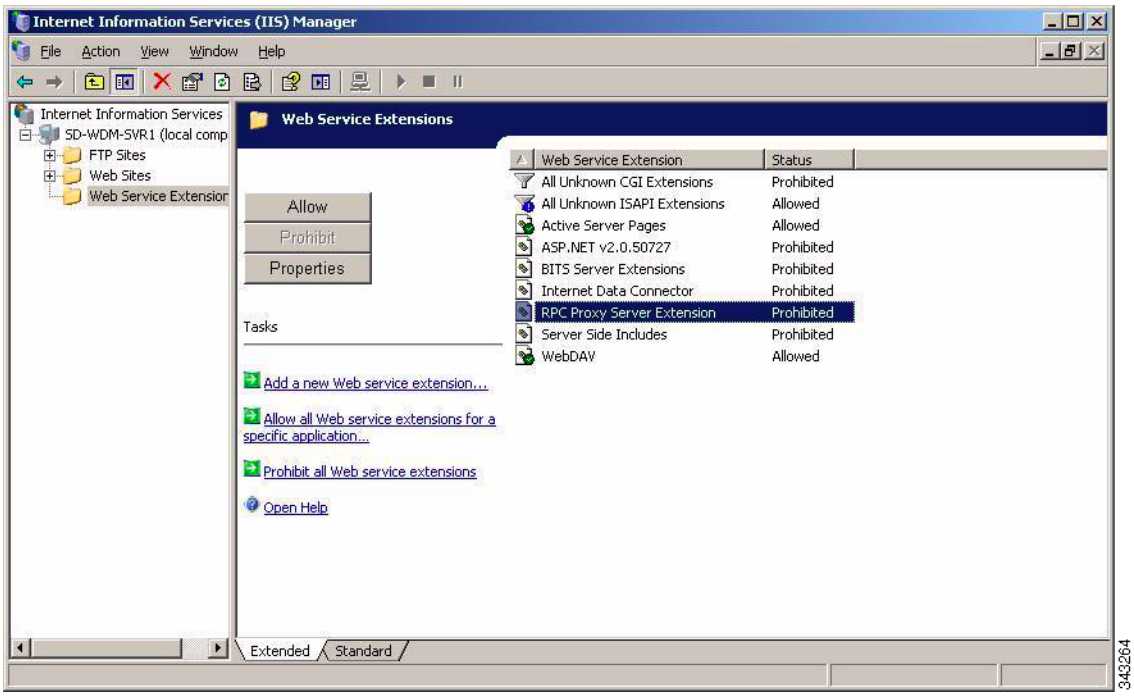
Problems with Repository Test Connection in IIS 6.0

If a test connection with the Master or Remote Repository fails, please verify the following:

Procedure

Step 1 Navigate to **IIS**, choose **World Wide Web Service** and click the **Details** button.

Figure E-3 Web Service Extensions



Step 2 Look at the Web Service Extensions and verify that the status is Allowed for both WebDAV and All Unknown ISAPI Extensions.

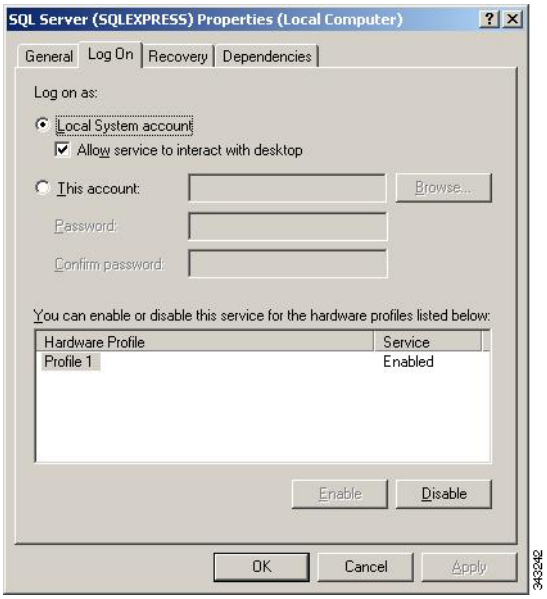
Step 3 For an FTP repository, make sure the Password (for the default user named rapport) is correct.

Step 4 For Linux repositories, make sure the “rapport” folder in WebDAV has all rights enabled. (Please refer to the *Installation Guide for Cisco Virtualization Experience Client Manager*).

Problems with Attaching Database

During the installation, if you encounter a problem attaching a SQL Server 2005 Express Edition database, make sure the “Log on as" setting for the SqlExpress service is set to "Local System account,” and restart the service. (See Figure E-4.)

Figure E-4 SQL Server Properties



Problems with Discovering Devices

Problem: You are having problems with discovering devices.

Solution: Ensure that the:

- Device service is running correctly
- Server service is running correctly
- Path between the device service and the server service is running correctly (use ping)
- Subnet and IP ranges are defined correctly (when you are attempting to discover devices by subnet or IP range)

Problems with Discovering PXE Devices

Problem: You are having problems with discovering PXE devices.

Solution: Ensure that:

- port 4011 is open in all routers
- IP-Helper addresses are defined and pointing to the Cisco VXC Manager-Server
- the PXE devices have re-booted at least one time after being discovered by Cisco VXC Manager (before Cisco VXC Manager recognizes them as PXE devices, the PXE devices must be re-booted at least one time after being discovered)

Package Errors

Problem: You are receiving package errors.

Solution: Try the following:

- Verify the scripting syntax
- Edit the script (*.rsp) and re-mark out LU command (have target device available)
- Make use of Network Sniffer
- Ensure that the Cisco VXC Manager Server IP address has not changed
- Ensure that the Repository information is correct
- Ensure that you can manually FTP a file to the Repository
- Ensure that you can run an unattended install
- Ensure that the package structure is correct (Folder = *.rsp name = scripts'NUMBER'value)

Problem With HServer Init Requests in IIS 6.0

Problem: You are not able to see the ports in the Preferences window.

Solution: Restart HServerInit and verify the preferences again.

If the ports are still not visible in the Preferences window, an IIS Lockout tool might be running in your server and using the URLScan security tool which stops the request for HServer. To resolve the problem, you need to configure the urlscan.ini file and after configuring, restart the WWW service.

The urlscan.ini file contains the following sections:

- [Options]—This section describes general URLScan options.
- [AllowExtensions] and [DenyExtensions]—This section defines the file name extensions that URLScan permits. • [AllowVerbs] and [DenyVerbs]—This section defines the verbs (also known as HTTP methods) that URLScan permits.
- [DenyHeaders]—This section lists HTTP headers that are not permitted in an HTTP request. If an HTTP request contains one of the HTTP headers that are listed in this section, URLScan rejects the request.
- [DenyURLSequences]—This section lists strings that are not permitted in an HTTP request. URLScan rejects HTTP requests that contain a string that appears in this section.
- [RequestLimits] section—This section enforces limits on the size, in bytes, of separate parts of requests reaching the server.

Configure the urlscan.ini file as follows:

Procedure

Step 1 In the [Options] section configure the following settings:

- [Options]
- AllowDotInPath = 1
- UseAllowVerbs=1
- UseAllowExtensions=1

Step 2 In the [AllowExtensions] and [DenyExtensions] section configure the following settings:

- [AllowExtensions]
- .bat
- .cmd
- .com
- .exe

Step 3 In the [AllowVerbs] and [DenyVerbs] section configure the following settings:

- [Allowed Verbs]
- GET
- HEAD
- POST
- PROPFIND
- MKCOL
- DELETE
- PUT
- MOVE

Step 4 In the [DenyHeaders] section configure the following settings:

- [DenyHeaders]
- Allow “Translate” header

Step 5 In the [RequestLimits] section configure the following settings:

- [RequestLimits]
- MaxAllowedContentLength=4294967296

Wake on LAN Command Does Not Reach Remote Devices

Problem: The HServer is unable to send the WOL command to the remote devices.

Solution: Enable port forwarding for UDP port 16962.

Wake on LAN Does Not Reach Devices in Remote Subnet

Problem: Wake on LAN does not reach devices in a remote subnet.

Solution: To use the Wake On LAN feature when the Cisco VXC Manager and the Cisco VXC clients are in different subnets, you must configure the router to allow directed broadcasts on all subnets where clients are present. For a sample router configuration, see:

Catalyst Layer 3 Switch for Wake-On-LAN Support Across VLANs Configuration Example

Wake on LAN Delayed Response

Problem: Wake on LAN response on the client is delayed (30 to 50 seconds).

Solution: If the Cisco VXC 2112/2212 client is connected to a switch that has spanning tree enabled, you must enable STP PortFast on the connected switch port for Wake on LAN to function as normal. Otherwise, the client must wait for the port to transition to STP forwarding mode (about 30 to 50 seconds) before Wake on LAN takes effect.

Problem in Repository Installation in IIS 7.0 in HTTP Mode

Problem: Repository installation fails in HTTP mode.

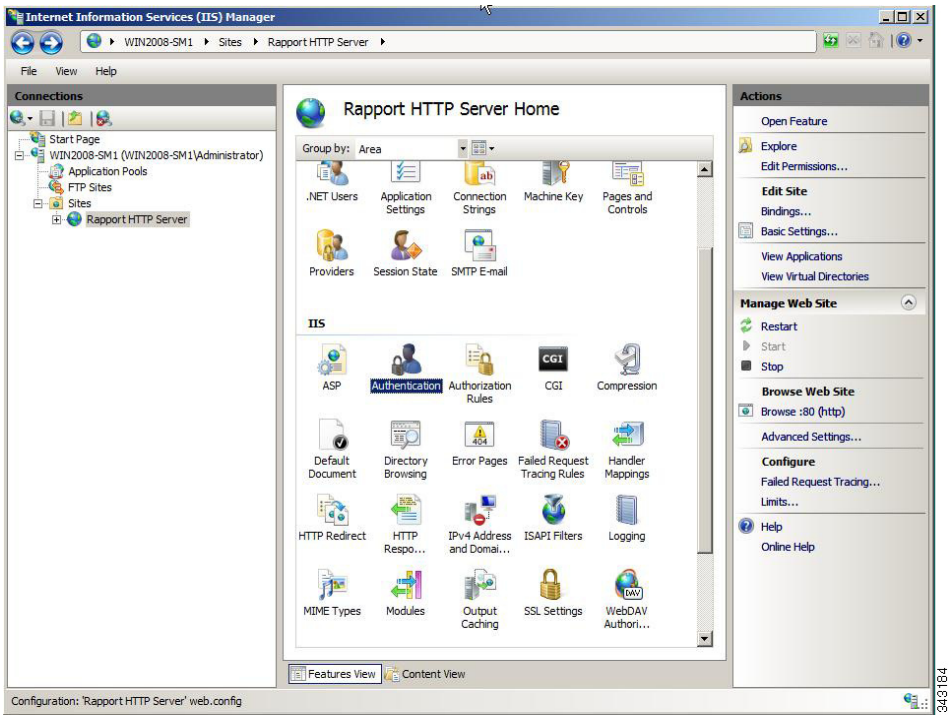
Solution:

Procedure

Step 1 Ensure that WebDAV is enabled. To verify WebDAV status:

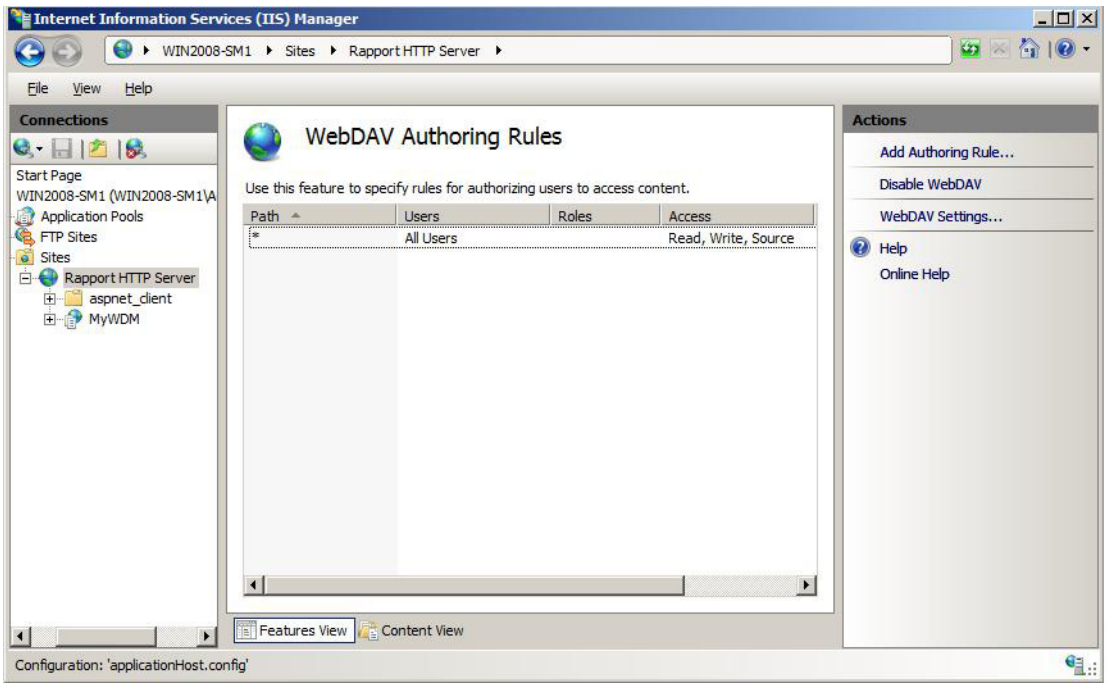
- Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager** to open the IIS Manager window.
- Expand the server node (shown with the name of the server).
- Expand the **Sites** node and choose **Rapport HTTP Server**.

Figure E-5 IIS Manager



- Choose WebDAV Authoring Rules for the Rapport HTTP Server in the far right pane.
- Verify that WebDAV is enabled.

Figure E-6 Enable and Disable WebDAV



Step 2 Ensure that the Rapport user is part of the Administrator group.

Step 3 Ensure that WebClient service is running on your system.

Problem with Merlin Imaging in Windows Server 2008

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

Problem: Merlin imaging fails in Windows Server 2008 because either:

- The size of the file being uploaded is greater than 30 MB.
- The URL and query string size is not adequate.

Solution: Modify the web.config file located in the inetpub\wwwroot folder by adding the following contents:

```
<security>
    <requestFiltering>
        <requestLimitsmaxAllowedContentLength="4294967296"
        maxUrl="8000"maxQueryString="8000" />
    </requestFiltering>
</security>
```

Recovering Dead Devices

Problem: How do I recover a dead device?

Solution: You can re-image a dead device to recover it.

Use the following guidelines:

- Prepare an image to use by doing one of the following:
  - Obtain the image firmware and register this image in Cisco VXC Manager as described in Managing Cisco VXC Manager Packages, page 3-31.
  - Use an existing image which has already been registered from a device in your installation.
- Add a new Device (as described in Adding and Automatically Discovering Devices, page 2-13) or choose an existing device, and then assign the image you prepared to the device using the Package Manager as described in Managing Cisco VXC Manager Packages, page 3-31.
- Schedule the Cisco VXC Manager package deployment for the Next Time Device Boots (this requires PXE).
- Expand **Update Manager** in the tree pane to find the scheduled device.
- Right-click the scheduled Cisco VXC Manager package entry and choose **Roll to boot**.
- Power on the dead device to allow the device to be re-imaged.

Converting a WISard Image to Merlin

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

Problem: How do I convert a WISard image to a Merlin image?

Solution: Merlin enables FTP/ HTTP/and HTTPS-based imaging, as well as better performance when deploying large images. If a WISard image is registered in Cisco VXC Manager, it can be converted into the Merlin format (if you do not want to convert an already registered WISard Image in Cisco VXC Manager, you can convert the WISard Image directly using the conversion utility, and then after converting the image, you can register it in Cisco VXC Manager for distribution).

Cisco VXC Manager provides a conversion utility that converts existing i2d images (WISard images) to the Merlin image format when the image package is registered in WISard mode using the Administrator Console.

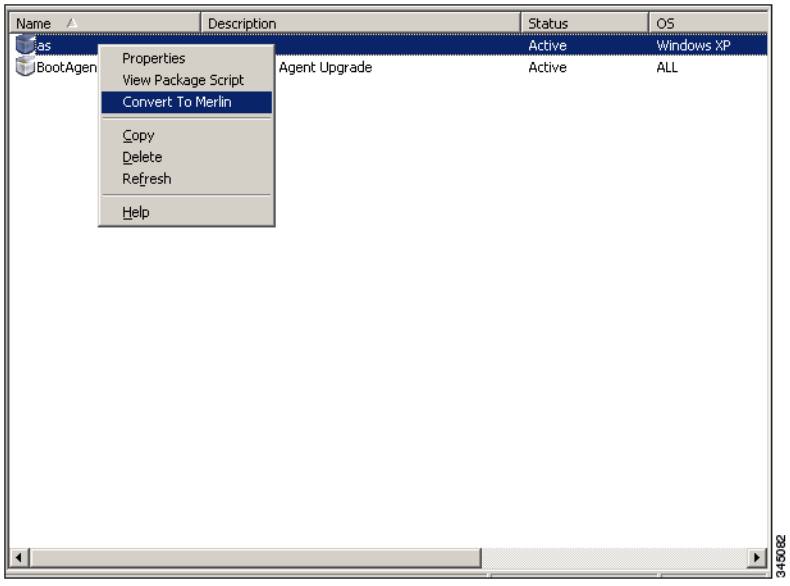
To convert an existing WIsard Image to Merlin:

Procedure

Step 1 In the Administrator Console, navigate to **Package Manager > Images** and choose a registered WISard image.

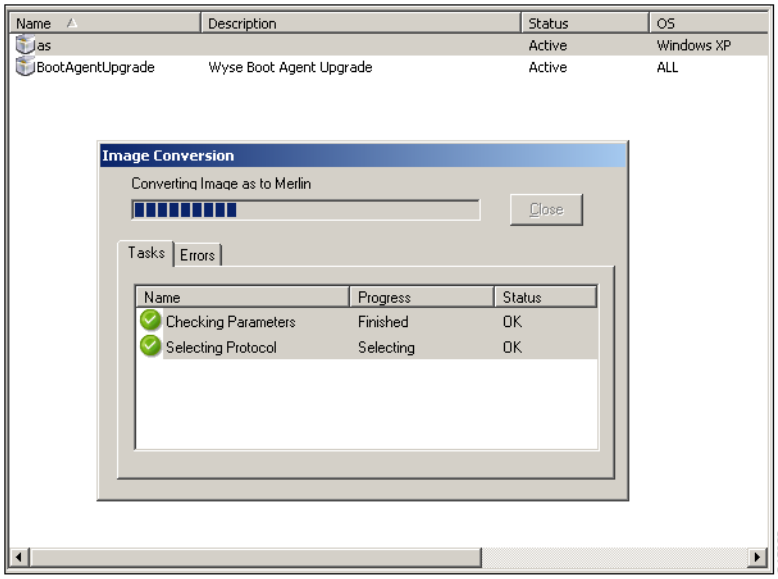
Step 2 Right-click the WISard Image and choose **Convert to Merlin**.

Figure E-7 Convert to Merlin



Step 3 The Image Conversion window appears and shows the progress of the conversion.

Figure E-8 Image Conversion Progress



Step 4 After the conversion is successfully completed, the progress window closes.

Step 5 If any of the tasks in the progress window fails, click the **Errors** tab to see the problem. Click **Close** to close the window.

APPENDIX F

Licensing and Sales Keys

This appendix provides information on Cisco VXC Manager licensing. It includes the detailed steps to activate Sales Keys.

Note Cisco VXC Manager does not require license keys to manage Cisco VXC clients. This section applies only to third-party products that may require licenses to interoperate with Cisco VXC Manager.

Managing Licenses and Certificates

Cisco VXC Manager allows you to manage licenses and certificates.

For information on tracking certificate expirations, see Using the Certificate Expiration Tracker, page 7-104.

Managing Cisco VXC Manager Sales Keys

Cisco VXC Manager allows you to view, add, upgrade, and delete Sales Keys as needed.

Viewing Sales Key Details

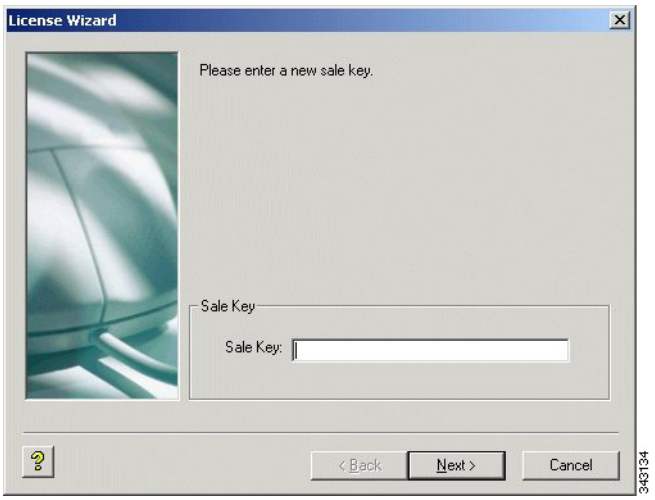
In the tree pane of the Administrator Console, expand Configuration Manager, click **Licensing**, right-click on the Sales Key you want to view, and then choose **Properties** to display the license details.

Adding Sales Keys

Procedure

Step 1 In the tree pane of the Administrator Console, expand Configuration Manager, right-click **Licensing**, and choose **New > License** to open the License Wizard.

Figure F-1 Add License Wizard



Step 2 Enter (or copy-and-paste) the Sales Key for the license you want to add, and click **Next** to open the success page.

Step 3 Click **Finish** to open the Licensing details pane displaying your new Non-activated Cisco VXC Manager Sales Key.

Step 4 Activate this Sales Key by completing the procedures in Activating Your Sales Key.

Activating Your Sales Key

Caution Be sure to perform the activation (enter an Activation Code) on the server to which you installed the Administrator Console (MMC Snap-in).

Use the following guidelines:

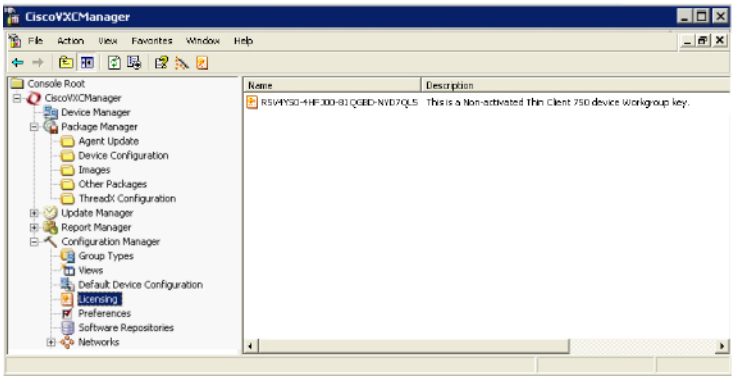
Procedure

Step 1 On the desktop of the server on which you installed the Administrator Console (MMC Snap-in), double-click the Cisco VXC Manager icon to open the Cisco VXC Manager Administrator Console.

Step 2 In the tree pane, expand Configuration Manager and choose **Licensing** to show the Non-activated Cisco VXC Manager Sales Key in the details pane.

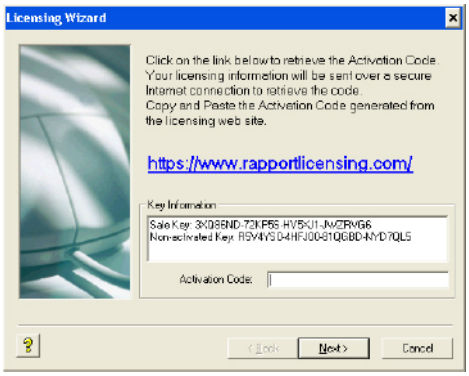
Tip If your Sales Key is already activated (displays as Activated), you can stop at this step.

Figure F-2 Cisco VXC Manager Administrator Console – Licensing



Step 3 Right-click the Non-activated Cisco VXC Manager Sales Key and choose **Activate** to open the Licensing Wizard.

Figure F-3 Licensing Wizard

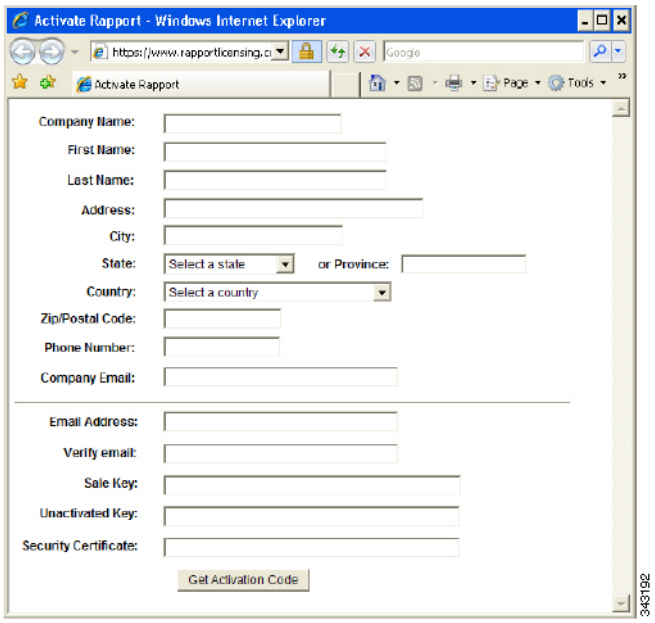


Step 4 Note your Sales Key and Non-activated Key numbers as you will use them in the online Cisco VXC Manager licensing form.

Tip If the server on which you installed the Administrator Console (MMC Snap-in) has internet access, you can copy-and-paste the Sales Key and Non-activated Key numbers from the Key Information area of the Licensing Wizard into the online Cisco VXC Manager licensing form.

Step 5 On a server which has internet access, use your browser to open the online Cisco VXC Manager licensing form at: https://www.rapportlicensing.com/clientframe/rapport.aspx.

Figure F-4 Licensing form



Step 6 Enter the information to complete the form (be sure to use the correct Sales Key and Non-activated Key numbers, and enter uppercase B for Security Certificate).

Step 7 After completing the form, click **Get Activation Code** to display the Activation Code (an e-mail containing the Activation Code is also sent to the Email Address you provided).

Step 8 In the Licensing Wizard on the server to which you installed the Administrator Console (MMC Snap-in), enter (or copy-and-paste) the Activation Code into the Activation Code field, and then click **Next** to open the details pane displaying your Sales Key as Activated.

Deleting Cisco VXC Manager Sales Keys

In the tree pane of the Administrator Console, expand Configuration Manager, click **Licensing**, right-click on the Sales Key you want to delete, choose **Delete**, and then click **Yes** to confirm.

APPENDIX G

Additional Package Manager Procedures

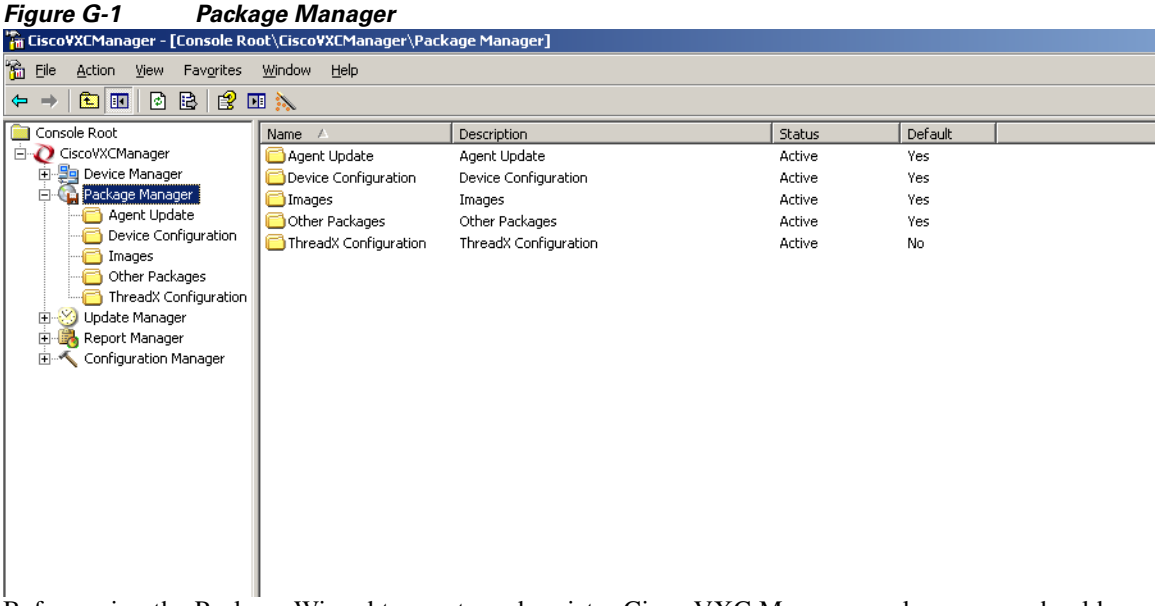
This appendix describes how to perform additional routine Cisco VXC Manager package management tasks for third-party clients.

Note This appendix contains additional Package Manager procedures that are applicable only to third-party clients. This appendix is not applicable to Cisco VXC clients.

Managing Cisco VXC Manager Packages

Clicking **Package Manager** in the tree pane of the Cisco VXC Manager Administrator Console opens the Package Manager. The Package Manager allows you to quickly view and manage the Cisco VXC Manager packages that can be distributed to the devices within your Cisco VXC Manager environment (see Table G-1). It also allows you to easily display the Cisco VXC Manager packages you want by using the filtering and customizing features available.

Figure G-1 Package Manager



Before using the Package Wizard to create and register Cisco VXC Manager packages, you should understand the update distribution process and the contents of Cisco VXC Manager packages, know the location of the existing Cisco VXC Manager packages that you want to register, know the location of

the base image and the add-ons you want to add to it when creating CE bundled images, and ensure that the devices from which you will be getting images or configurations already have the Cisco VXC Manager Agent (HAgent) installed. After Cisco VXC Manager packages are registered, you can distribute them as updates to the devices within your Cisco VXC Manager network (see Update Manager, page 5-29).

Tip If you intend to perform Cisco VXC Manager package registration and scheduling for all of the devices in your Cisco VXC Manager system at the same time, the Cisco VXC Manager Mass Imaging Tool can be a convenient way for you to easily perform these tasks (see Using the Cisco VXC Manager Mass Imaging Tool, page D-17).

Table G-1 provides a quick overview of what you can do using the Package Manager.

Table G-1 Routine Package Manager Tasks

Tasks You Can Do	How	Details
Create and register an image from a device (for example, from a device running XPE or CE) so it is ready to be distributed.	In the tree pane of the Administrator Console, right-click **Package Manager**, choose **New > Package** to open the Package Wizard, choose the **Register an Image from a Device (Requires PXE)** option, and then follow the wizard. **Tip** You can also right-click the Reference Device and choose **Get Device Image** to open and use the Package Wizard.	Register an Image from a Device (Requires PXE), page G-5
Create and register a Windows configuration from a device (for example, from a device running WES 2009 or WES 7) so it is ready to be distributed.	In the tree pane of the Administrator Console, right-click **Package Manager**, choose **New > Package** to open the Package Wizard, choose the **Register a Windows Configuration** option, and then follow the wizard.	Registering a Windows Configuration, page G-12
Create and register a configuration from a third-party device running Wyse Enhanced SUSE Linux Enterprise or Linux v6.x so it is ready to be distributed.	In the tree pane of the Administrator Console, right-click **Package Manager**, choose **New > Package** to open the Package Wizard, choose the **Register a Configuration from a Device** option, and then follow the wizard. **Tip** You can also right-click the Reference Device and choose **Get Device Configuration** to open and use the Package Wizard.	Register a Configuration from a Device, page G-7 and Registering a Configuration from Third-party Devices Running Wyse Enhanced SUSE Linux Enterprise or Linux v6.x, page G-7

Table G-1 Routine Package Manager Tasks (continued)

Tasks You Can Do	How	Details
Create and register a configuration from a device running Windows CE so it is ready to be distributed.	In the tree pane of the Administrator Console, right-click **Package Manager**, choose **New > Package** to open the Package Wizard, choose the **Register a Configuration from a Device** option, and then follow the wizard. **Tip** You can also right-click the Reference Device and choose **Get Device Configuration** to open and use the Package Wizard.	Register a Configuration from a Device, page G-7 and Registering a Configuration from Third-party Devices Running Windows CE, page G-8
Create and register a CE image plus add-ons so it is ready to be distributed.	In the tree pane of the Administrator Console, right-click **Package Manager**, choose **New > Package** to open the Package Wizard, choose the **Build and register a CE image plus add-ons ("CE bundled image")** option, and then follow the wizard.	Build and Register a CE Image Plus Add-Ons (CE Bundled Image), page G-10
Use WISard to create and register an image from a device so it is ready to be distributed.	For first-time use, complete the instructions in Registering an Image from a Device Using WISard, page G-13 **Tip** After you have already set up the required preferences, you can expand the **Device Manager** (in the tree pane of the Administrator Console), right-click the device you want, and then choose **Get Device Image** to open and use the Package Wizard.	Registering an Image from a Device Using WISard: Initial Setup and Use, page G-13 and Registering an Image from a Device Using WISard: After Initial Setup, page G-16

Table G-1 Routine Package Manager Tasks (continued)

Tasks You Can Do	How	Details
Use Merlin to create and register an image from a device so it is ready to be distributed.	For first-time use, complete the instructions in Registering an Image from a Device Using Merlin, page G-16 **Tip** After you have already set up the required preferences, you can expand the **Device Manager** (in the tree pane of the Administrator Console), right-click the device you want, and then choose **Get Device Image** to open and use the Package Wizard.	Registering an Image from a Device Using Merlin: Initial Setup and Use, page G-17 and Registering an Image from a Device Using Merlin: After Initial Setup, page G-20

Table G-1 Routine Package Manager Tasks (continued)

Tasks You Can Do	How	Details
Delete a registered Cisco VXC Manager package from the system.	In the tree pane of the Administrator Console, expand **Package Manager** and choose the folder that contains the Cisco VXC Manager package. In the details pane, right-click the Cisco VXC Manager package, choose **Delete**, and then confirm the deletion.	You cannot delete default Cisco VXC Manager packages. You cannot delete a registered Cisco VXC Manager package that is scheduled for distribution; you must first delete the scheduled update as described in Managing the Schedules for Device Updates, page 5-29 before you can delete a registered Cisco VXC Manager package. **Caution** When you delete a registered Cisco VXC Manager package that has never been distributed, Cisco VXC Manager also deletes it from the Cisco VXC Manager Repository. The Cisco VXC Manager package is recoverable only if you have a copy of it outside of Cisco VXC Manager. In such a case, you can re-register the Cisco VXC Manager package. **Tip** If you delete a Cisco VXC Manager package that has already been distributed, you can recover it from the Backup folder of the Cisco VXC Manager Repository and re-register it. When archived, a Cisco VXC Manager package receives a date-stamped name, therefore, before re-registering an archived Cisco VXC Manager package, you must rename it to its original name.

Register an Image from a Device (Requires PXE)

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

This Package Wizard option requires that an Imaging Scripting Template exists for the Device Type. If no Imaging Scripting Template is available, a warning message will display (contact the manufacturer of the device to obtain an Imaging Scripting Template).

Procedure

Step 1 In the tree pane of the Administrator Console, right-click **Package Manager** and choose **New > Package** to open the Package Wizard.

Tip You can also right-click the Reference Device in the details pane of the Device Manager and choose **Get Device Image** to open the Package Wizard.

Figure G-2 Package Wizard

Step 2 Click the **Register an Image from a Device (Requires PXE)** radio button and click **Next**.

Step 3 Enter a name and description for the Read Image Cisco VXC Manager package that will read the image from a device (such as a Reference Device), and click **Next** (when you create the Read Image Cisco VXC Manager package, ensure that the RSP file contains values for the imagesize parameter and for the image number of the device upon which the image is based; proper RSP files will have a well-formed header).

Step 4 When the Package Wizard prompts you to choose the group from which to read the image, choose the group where the Reference Device is found and click **Next**.

Step 5 When the Package Wizard prompts you to choose the desired device, choose the device whose image you want to read with the Get Cisco VXC Manager package (be sure to choose a Reference Device that supports PXE) and click **Next**.

Step 6 Depending on your preferences, do one of the following:

- (WISard Only) If you are using WISard, continue with step 7.
- (Merlin Only) If you are using Merlin the Merlin Pulling Options dialog box appears; choose the options you want and then continue with step 7.

Step 7 Click **Next**. The wizard notifies you that is ready to create and register the new Cisco VXC Manager package.

Step 8 Click **Next** to create and register the Cisco VXC Manager package.

Step 9 After the Cisco VXC Manager package has been created and registered, click **Finish**. The image pull operation will appear in the details pane of the Update Manager. Cisco VXC Manager will send the imaging job to the Reference Device. After completion of the pull operation, the pulled image will appear in the Images folder of the Package Manager (depending on the flash size of the device, the process to pull the image from the device may take some time). The Cisco VXC Manager package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

Register a Configuration from a Device

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

This Package Wizard option pulls a configuration from a device (such as a Reference Device) to easily configure (clone) similar devices within your Cisco VXC Manager installation.

Tip Supported devices for this functionality include third-party devices running Wyse Enhanced SUSE Linux Enterprise, Linux v6.x, or Windows CE.

Prior to using the Package Wizard to pull and register the configuration from a Reference Device, ensure that:

- The Reference Device supports Pre-boot Execute Environment (PXE).
- You have configured the Reference Device to fulfill your specifications.
- Tested the Reference Device and resolved any issues.

After you ensure your Reference Device is ready, you can continue using the Package Wizard to pull and register the configuration from the device according to your OS:

- Third-party Devices Running Wyse Enhanced SUSE Linux Enterprise or Linux v6.x—See Registering a Configuration from Third-party Devices Running Wyse Enhanced SUSE Linux Enterprise or Linux v6.x, page G-7
- Third-party Devices Running Windows CE—See Registering a Configuration from Third-party Devices Running Windows CE, page G-8

Registering a Configuration from Third-party Devices Running Wyse Enhanced SUSE Linux Enterprise or Linux v6.x

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

Procedure

Step 1 In the tree pane of the Administrator Console, right-click **Package Manager** and choose **New > Package** to open the Package Wizard.

Tip You can also right-click the Reference Device in the details pane of the Device Manager and choose **Get Device Configuration** to open the Package Wizard.

Step 2 Click the **Register a Configuration from a Device** radio button and click **Next**.

Step 3 Enter a name and description for the Cisco VXC Manager package (the new Cisco VXC Manager package will remain inactive until Cisco VXC Manager successfully retrieves the configuration from the Reference Device).

Step 4 Click **Next**. The wizard notifies you that is ready to create and register the new Cisco VXC Manager package.

Step 5 Click **Next** to create and register the Cisco VXC Manager package.

Step 6 After the Cisco VXC Manager package has been created and registered, click **Finish**. The Cisco VXC Manager package is copied to the Master Repository and is displayed under the appropriate category. The Cisco VXC Manager package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

Registering a Configuration from Third-party Devices Running Windows CE

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

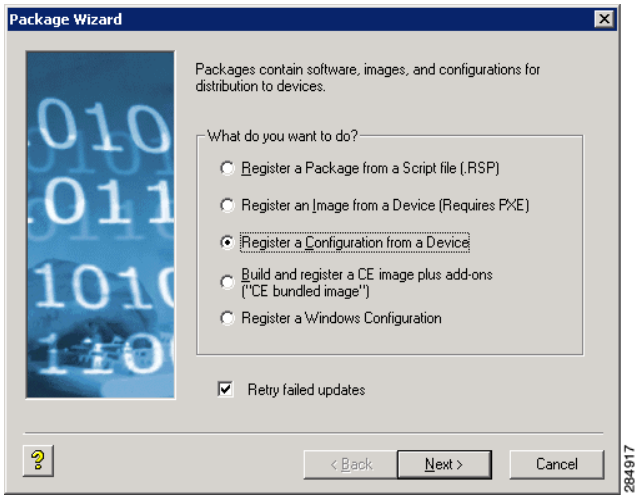
Tip With devices running Windows CE you can also control the action (replace, append, or exclude) of specific registry entries when later distributing the image.

Procedure

Step 1 In the tree pane of the Administrator Console, right-click **Package Manager** and choose **New > Package** to open the Package Wizard.

Tip You can also right-click the Reference Device in the details pane of the Device Manager and choose Get Device Configuration to open the Package Wizard.

Figure G-3 Package Wizard

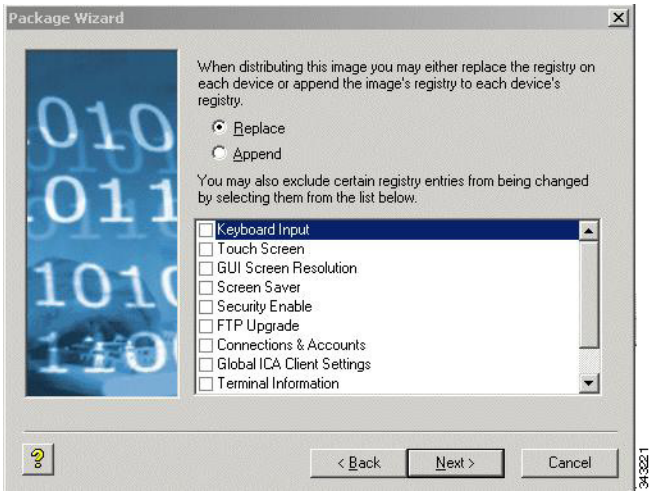


Step 2 Click the **Register a Configuration from a Device** radio button and click **Next**.

Step 3 Enter a name and description for the Cisco VXC Manager package (the new Cisco VXC Manager package will remain inactive until Cisco VXC Manager successfully retrieves the configuration from the Reference Device).

Step 4 Click **Next**.

Figure G-4 Replace or Append Registry Entries



Step 5 To replace or append registry entries, use the following guidelines:

The entire configuration can either be replaced or appended to your Reference Device configuration when this Cisco VXC Manager package is later distributed.

- **Replace**—Replacing the registry resets the registry to factory defaults and then applies the registry settings contained in the configuration (settings.reg) file of the Cisco VXC Manager package (these are the registry settings you configured when preparing your Reference Device).
- **Append**—Appending the registry applies registry settings from the configuration (settings.reg) files of both devices (the existing registry settings of the existing device and the registry settings of your Reference Device). Note that duplicate registry settings are not affected.

- **Exclude List**—You can also exclude specific registry entries from being changed during distribution by selecting it in the list (selecting the check box next to the configuration setting).

Step 6 Click **Next**. The wizard notifies you that it is ready to create and register the new Cisco VXC Manager package.

Step 7 Click **Next** to create and register the Cisco VXC Manager package.

Step 8 After the Cisco VXC Manager package has been created and registered, click **Finish**. The Cisco VXC Manager package is copied to the Master Repository and is displayed under the appropriate category. The Cisco VXC Manager package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

Build and Register a CE Image Plus Add-Ons (CE Bundled Image)

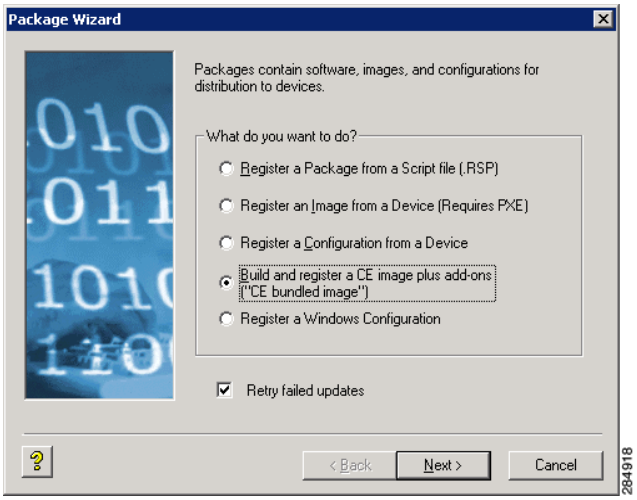
Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

This Package Wizard option creates and registers a CE bundled image comprised of a CE OS image and add-ons.

Procedure

Step 1 In the tree pane of the Administrator Console, right-click **Package Manager** and choose **New > Package** to open the Package Wizard.

Figure G-5 Package Wizard



Step 2 Click the **Build and register a CE image plus add-ons (“CE bundled image”)** radio button and click **Next**.

Step 3 Enter a name and description for the CE bundled image and click **Next**. Notice that the Category field is read-only and displays Images as the category in which to store the CE bundled image.

Step 4 Depending on whether or not you want to have the Cisco VXC Manager package distributed (active for distribution), choose or clear the **Active** check box.

Step 5 Click **Next**.

Step 6 Enter the CE version number and Base Image for the CE bundled image.

Step 7 Browse to find and choose the location of the Base CE Image, and optionally, for the location of the Registry Image in the CE Base field, and then click **Next**.

Caution The CE Base image (or Primer) is generally a binary or executable file (most often the CE operating system). The CE bundled image creation process requires a params.ini file. This file should reside in the same directory from which you obtain the CE base image. The wizard obtains the build version information from the params.ini file. If the file is not available, the CE bundled image creation process will stop.

Step 8 The wizard prompts you to choose add-ons for the CE bundled image. Click **Select File** to navigate and choose the location where known add-ons reside, and then choose the add-ons you want.

Tip The Add-on and Build fields display the name and build for each add-on you want. The Add-On selection dialog box will display your selected add-ons and allow you to continue making additional add-on selections. To remove add-ons from your selections, choose them (you can use Ctrl-click or Shift-click to choose multiple items), and then click **Remove** (you can click **Remove All** to delete all the add-ons).

Caution The add-on is generally a binary, executable, or registry file. The CE bundled image creation process requires a params.ini file for each add-on that you choose. This file should reside in the same directory from which you obtain the add-on. The wizard obtains the add-on build version information from the params.ini file. If the file is not available, the CE bundled image creation process will stop.

Step 9 When you have finished selecting the add-ons you want, click **Next**. The wizard informs you that it is ready to create the Cisco VXC Manager package for your CE Bundled image.

Step 10 Click **Next**. The wizard notifies you that is ready to create and register the new Cisco VXC Manager package.

Step 11 Click **Next** to create and register the Cisco VXC Manager package.

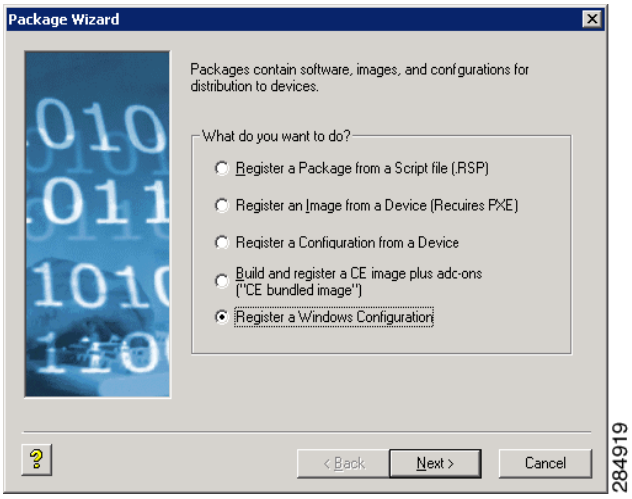
Step 12 After the Cisco VXC Manager package has been created and registered, click **Finish**. The Cisco VXC Manager package is copied to the Master Repository and is displayed under the appropriate category. The Cisco VXC Manager package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

Registering a Windows Configuration

Procedure

Step 1 In the tree pane of the Administrator Console, right-click **Package Manager** and choose **New > Package** to open the Package Wizard.

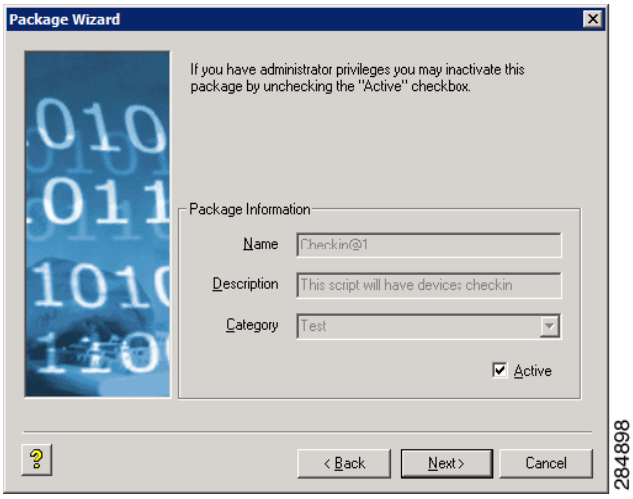
Figure G-6 Package Wizard



Step 2 Choose the **Register a Windows Configuration** option and click **Next**.

Step 3 Enter the File Path to the Cisco VXC Manager script file (.xml) file for the package (for example, commandsXML.xml) you want to register (you can click **Browse** to find and choose a file), and then click **Next** to open the Software Package Information dialog box.

Figure G-7 Software Package Information



The Name, Description, and Category of the package is obtained from the .xml file and displayed.

Step 4 Depending on whether or not you want to have the package distributed (active for distribution), check or uncheck the **Active** check box.

Step 5 Click **Next**. The wizard notifies you that is ready to create and register the new package.

Step 6 Click **Next** to create and register the package.

Step 7 After the package is created and registered, click **Finish**. The package is copied to the Master Repository and is displayed under the appropriate category. The package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

Registering an Image from a Device Using WISard

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

Depending on whether or not you have set up the required preferences so that the Package Wizard automatically uses WISard to create and register an image, complete one of the following:

- If you have not set up the required preferences (for example, if this is the first time you are using WISard to create and register an image), complete the procedures in Registering an Image from a Device Using WISard: Initial Setup and Use, page G-13 (this will take you through the entire process to set up the preferences and use WISard to create and register an image).
- If you have already set up the required preferences (for example, if you have already used WISard to create and register an image), complete the procedures in Registering an Image from a Device Using WISard: After Initial Setup, page G-16 (this will take you through the shortened process to use WISard to create and register an image).

Caution WISard requires that PXE is enabled in the BIOS of the device. For more information on PXE usage, see PXE Based Imaging, page D-12.

Registering an Image from a Device Using WISard: Initial Setup and Use

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

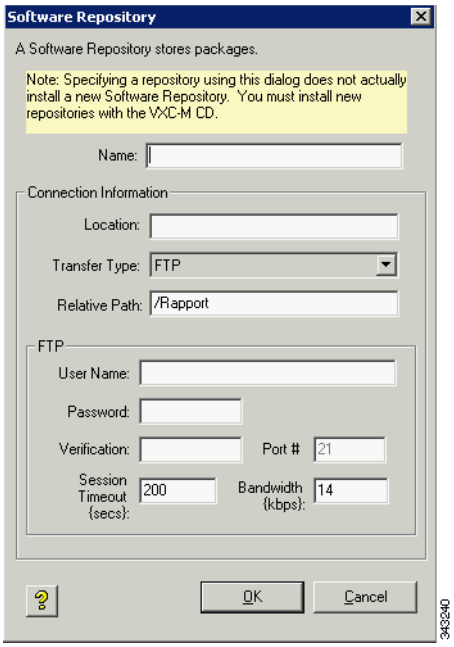
After completing this section, you can use the shortened process (Registering an Image from a Device Using WISard: After Initial Setup, page G-16) to use WISard to create and register an image in the future.

Procedure

Step 1 In the tree pane of the Administrator Console, navigate to **CiscoVXCManager > Configuration Manager > Software Repositories**.

Step 2 In the details pane, right-click **Master** and choose **Properties**.

Figure G-8 Software Repository



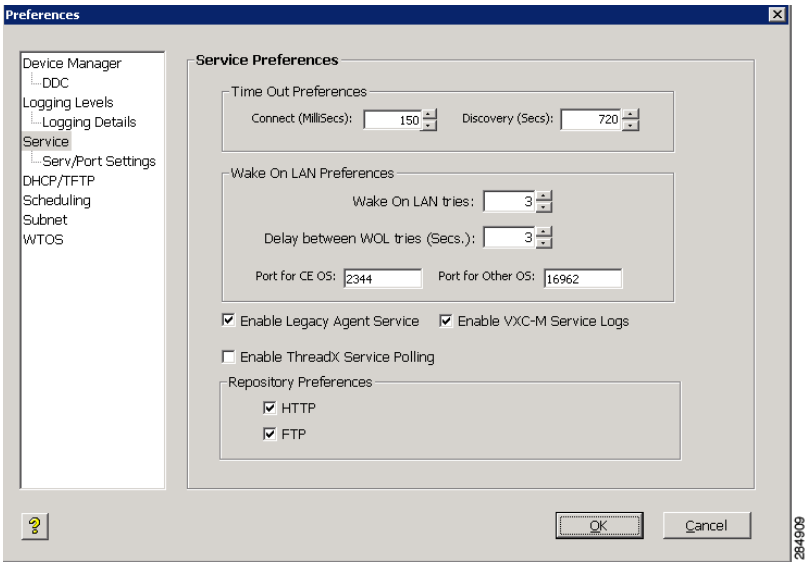
Step 3 In the Software Repository dialog box, choose **FTP** in the Transfer Type list for the Master Repository and click **OK**.

Step 4 In the tree pane of the Administrator Console, navigate to **CiscoVXCManager > Configuration Manager > Preferences**.

Step 5 In the results pane, double-click **Service Preferences** to open the Preferences window.

Step 6 In the tree pane of the Preferences window, choose **Service**.

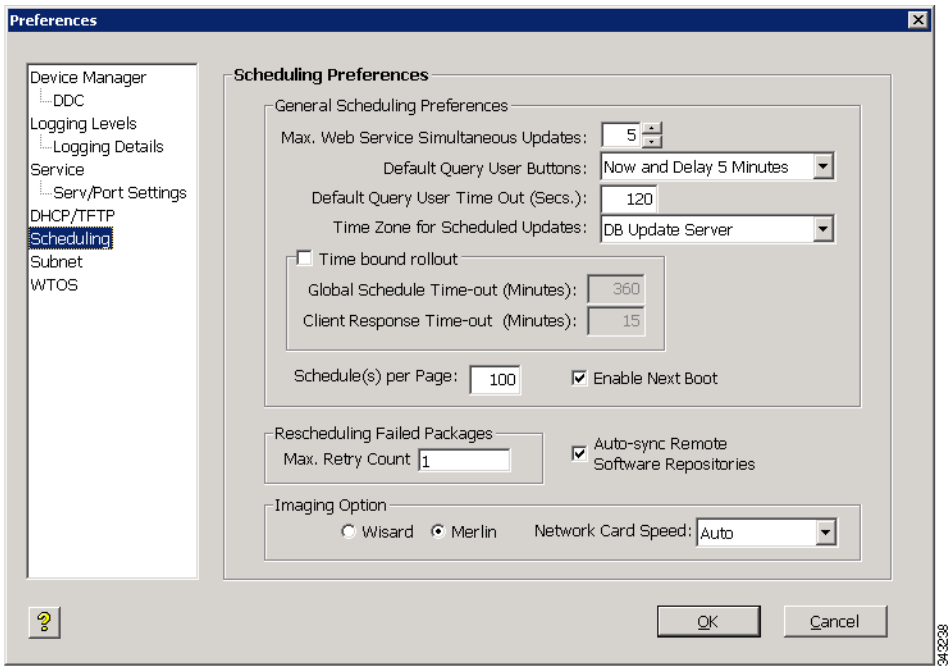
Figure G-9 Preferences: Service Preferences



Step 7 In the **Repository Preferences** area, choose the **FTP** check box.

Step 8 In the tree pane of the Preferences window, choose **Scheduling**.

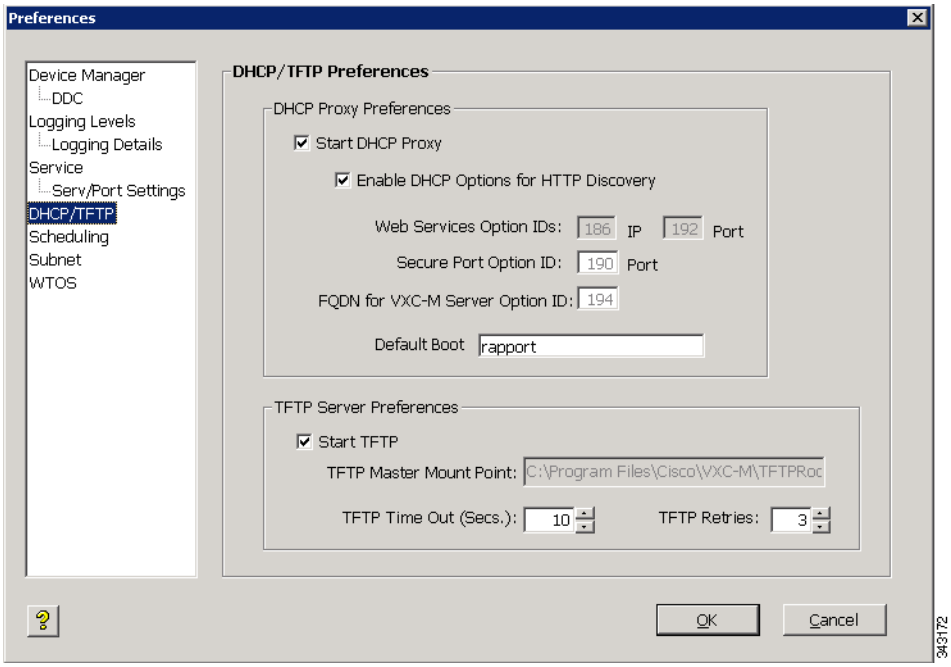
Figure G-10 Preferences: Scheduling Preferences



Step 9 In the **Imaging Option** area, choose the **WISard** option.

Step 10 In the tree pane of the Preferences window, choose **DHCP/TFTP**.

Figure G-11 Preferences: DHCP/TFTP Preferences



Step 11 In the **TFTP Server Preferences** area, check the **Start TFTP** check box.

Step 12 Click **OK**.

Step 13 Now that you have set up the required preferences, continue with Registering an Image from a Device Using WISard: After Initial Setup, page G-16.

Registering an Image from a Device Using WISard: After Initial Setup

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

Caution Before using this section, be sure you have completed the procedures in Registering an Image from a Device Using WISard: Initial Setup and Use, page G-13.

Procedure

Step 1 In the tree pane of the Administrator Console, expand the **Device Manager**.

Step 2 Right-click the device you want and then choose **Get Device Image** to open the Package Wizard.

Step 3 Enter the name and description of the Cisco VXC Manager package.

Step 4 Click **Next**. The wizard notifies you that is ready to create and register the new Cisco VXC Manager package.

Step 5 Click **Next** to create and register the Cisco VXC Manager package.

Step 6 After the Cisco VXC Manager package has been created and registered, click **Finish**. Cisco VXC Manager starts the image pull operation from the device (the device goes through a PXE boot and WISard imaging process) and creates the image. The Cisco VXC Manager package is copied to the Master Repository and is displayed under the appropriate category. The Cisco VXC Manager package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

Registering an Image from a Device Using Merlin

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

Depending on whether or not you have set up the required preferences so that the Package Wizard automatically uses Merlin to create and register an image, complete one of the following:

- If you have not set up the required preferences (for example, if this is the first time you are using Merlin to create and register an image), complete the procedures in Registering an Image from a Device Using Merlin: Initial Setup and Use, page G-17 (this will take you through the entire process to set up the preferences and use Merlin to create and register an image).

- If you have already set up the required preferences (for example, if you have already used Merlin to create and register an image), complete the procedures in Registering an Image from a Device Using Merlin: After Initial Setup, page G-20 (this will take you through the shortened process to use Merlin to create and register an image).

Caution Merlin can be used with a PXE or Non-PXE option for devices running XPe, WES, or WES 7. For other devices, Merlin requires that PXE is enabled in the BIOS of the device. For more information on PXE and Non-PXE usage, see PXE Based Imaging, page D-12.

Registering an Image from a Device Using Merlin: Initial Setup and Use

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

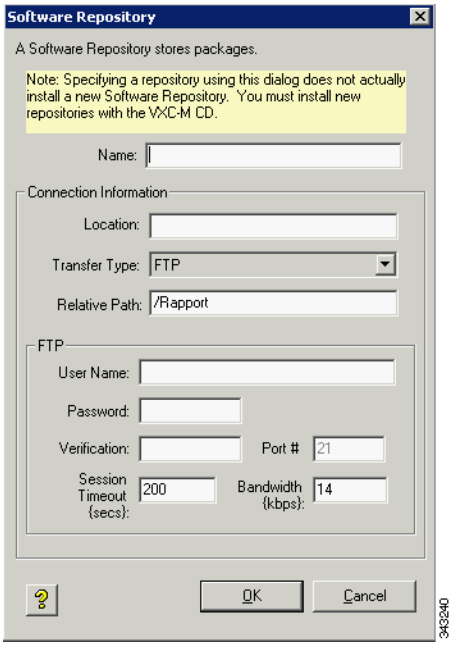
Tip After completing this section, you can use the shortened process (Registering an Image from a Device Using Merlin: After Initial Setup, page G-20) to use Merlin to create and register an image in the future.

Procedure

Step 1 In the tree pane of the Administrator Console, navigate to **CiscoVXCManager > Configuration Manager > Software Repositories**.

Step 2 In the details pane, right-click **Master** and choose **Properties**.

Figure G-12 Software Repository



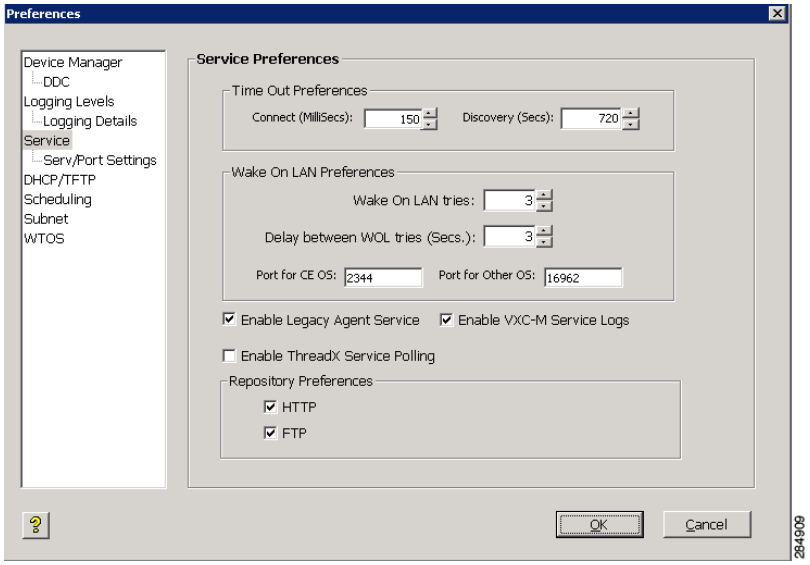
Step 3 In the Software Repository dialog box, choose the Transfer Type (Merlin supports both HTTP and FTP) for the Master Repository.

Step 4 In the tree pane of the Administrator Console, navigate to **CiscoVXCManager > Configuration Manager > Preferences**.

Step 5 In the results pane, double-click **Service Preferences** to open the Preferences window.

Step 6 In the tree pane of the Preferences window, choose **Service**.

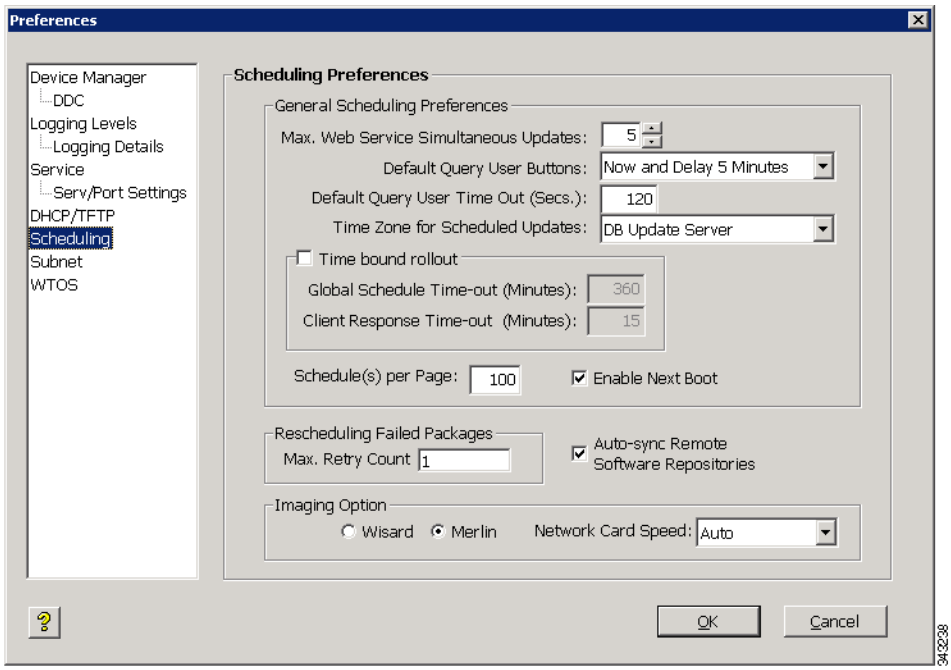
Figure G-13 Preferences: Service Preferences



Step 7 In the Repository Preferences area, choose the Repository Preferences option you want (Merlin supports both HTTP and FTP).

Step 8 In the tree pane of the Preferences window, choose **Scheduling**.

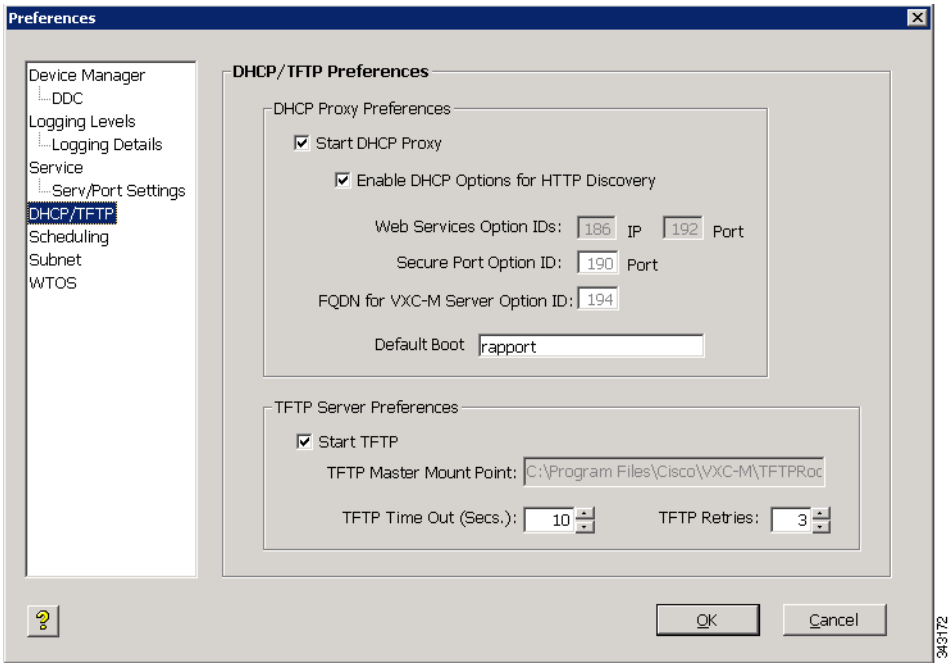
Figure G-14 Preferences: Scheduling Preferences



Step 9 In the Imaging Option area, choose the **Merlin** option, and then choose the **Network Card Speed** that matches the network speed of the subnet in which the device exists.

Step 10 In the tree pane of the Preferences window, choose **DHCP/TFTP**.

Figure G-15 Preferences: DHCP/TFTP Preferences



Step 11 In the **TFTP Server Preferences** area, click the **Start TFTP** check box.

Step 12 Click **OK**.

Step 13 Now that you have set up the required preferences, continue with Registering an Image from a Device Using WISard: After Initial Setup, page G-16.

Registering an Image from a Device Using Merlin: After Initial Setup

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

Caution Before using this section, be sure you have completed the procedures in Registering an Image from a Device Using Merlin: Initial Setup and Use, page G-17.

Procedure

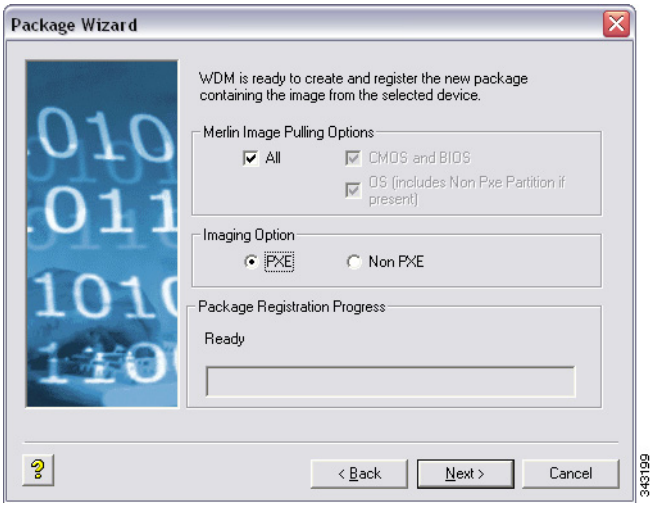
Step 1 In the tree pane of the Administrator Console, expand the **Device Manager**.

Step 2 Right-click the device you want and then choose **Get Device Image** to open the Package Wizard.

Step 3 Enter the name and description of the Cisco VXC Manager package.

Step 4 Click **Next**.

Figure G-16 Merlin Options



Step 5 Use the following guidelines to choose the options you want:

- **Merlin Pulling Options**
  - **All**—Pulls CMOS, BIOS, and OS (including any Non-PXE partitions if any exist)
  - **CMOS and BIOS**—Pulls CMOS and BIOS only
  - **OS**—Pulls OS only (including any Non-PXE partitions if any exist)

- **Imaging Option** (available only for devices running XPe, WES, or WES 7)
  - **PXE**—If selected, imaging occurs in PXE mode.
  - **Non PXE**—If selected, imaging occurs in Non-PXE mode.

Step 6 Click **Next**. The wizard notifies you that is ready to create and register the new Cisco VXC Manager package.

Step 7 Click **Next** to create and register the Cisco VXC Manager package.

Step 8 After the Cisco VXC Manager package has been created and registered, click **Finish**. Cisco VXC Manager starts the image pull operation from the device (if PXE is selected, the device goes through a PXE boot and Merlin imaging process) and creates the image. The Cisco VXC Manager package is copied to the Master Repository and is displayed under the appropriate category. The Cisco VXC Manager package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

APPENDIX H

Cisco VXC Manager ScriptBuilder Tool and Scripting Language

Note This section is not applicable to Cisco VXC clients. It is applicable only for the management of third-party clients.

This appendix contains advanced information about using the Cisco VXC Manager ScriptBuilder and using the Cisco VXC Manager scripting language to create Cisco VXC Manager Packages.

It includes:

Using Cisco VXC Manager Scripting Language

The Cisco VXC Manager scripting language was designed to allow you to create your own software packages (with or without the Cisco VXC Manager ScriptBuilder Tool). A software package consists of a script (RSP) file and any required application or image files. You can create a software package, and then register and distribute it to one or more devices using Cisco VXC Manager.

Distributing software packages to one or more devices on the network saves time but requires caution and planning. It is very important that you test your software package on a separate test device to ensure validity and reliability.

Caution It is imperative that all software packages be thoroughly tested before mass distribution occurs. This is the responsibility of the Cisco VXC Manager administrator with package distribution permissions.

Using the Cisco VXC Manager ScriptBuilder Tool

The Cisco VXC Manager ScriptBuilder Tool is designed to help you manage (create, edit, and view) Cisco VXC Manager scripting packages. For details on the script commands available for you to use with Cisco VXC Manager ScriptBuilder, see Script, page H-8.

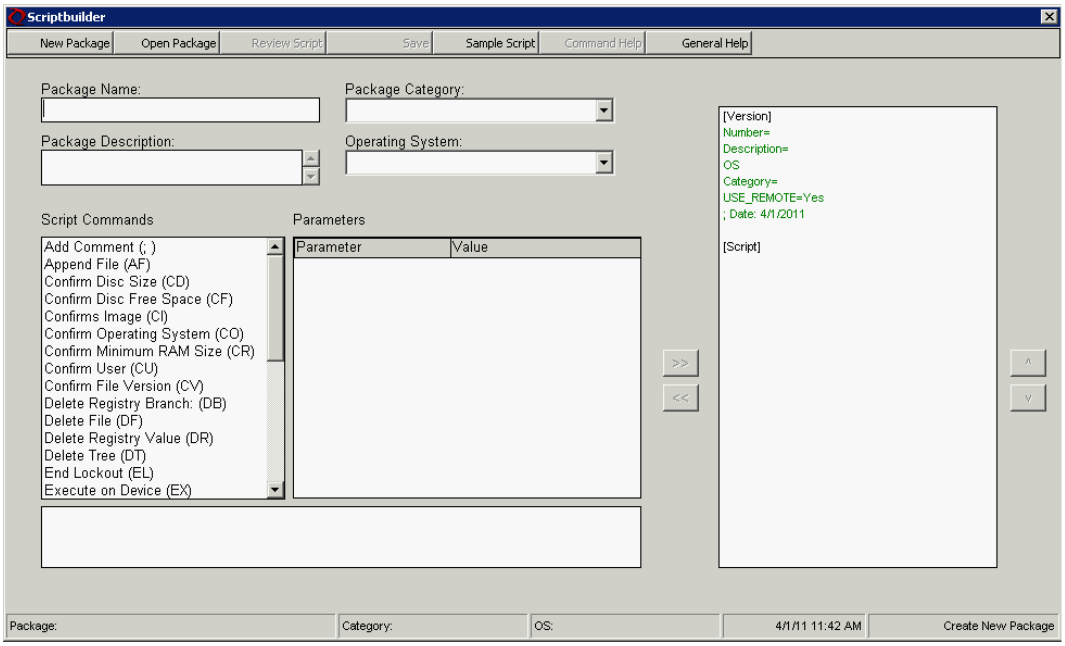
Creating a New Cisco VXC Manager Script Package

Use the following procedure to create a new Cisco VXC Manager script package.

Procedure

Step 1 Click **Start > All Programs > Cisco VXC Manager > ScriptBuilder** to open the ScriptBuilder Tool.

Figure H-1 Cisco VXC Manager ScriptBuilder



Step 2 Click **New Package** and then use the following guidelines:

- Enter the Package Name and Package Name Description (so you can easily recognize it later).
- Choose a Package Category.
- Choose an Operating System.
- Choose the script command you want to add to the from the Script Commands list.
- Enter the Value of the command you want (some Parameters will automatically enter a default Value). For details on the values available for you to use, see Script, page H-8.
- Click **>>** to add the script command to the script package pane.
- You can continue to choose the script commands in the Script Commands list you want to add to the script package pane.

- When adding script commands to the script package pane, you can choose an item in the script package pane and use the add, remove, move up, and move down command button arrows (which are automatically enabled and disabled according to possible or logical operations) as needed to build the script package you want.
- You can also edit existing script in the script package pane directly by double clicking the entry and making your modifications in the selected row, however, no command syntax or parameter validation is performed in this mode.
- Use **Sample Script** (opens a form with a typical sample script), **Command Help** (detailed help for commands selected in the Script Commands list), and **General Help** (general help with scripting) as needed for information.

Step 3 After configuring the Cisco VXC Manager scripting package you want, click **Save**.

Editing a New Cisco VXC Manager Script Package

Click **Start > All Programs > Cisco VXC Manager > ScriptBuilder** to open the ScriptBuilder dialog box, click **Open Package**, choose the package you want to edit, and then use the guidelines in Creating a New Cisco VXC Manager Script Package, page H-2.

Tip Modifications you make to an existing script package are shown in blue within the script package pane to indicate a change from the original package script.

Reviewing a New Cisco VXC Manager Script Package

Click **Start > All Programs > Cisco VXC Manager > ScriptBuilder** to open the ScriptBuilder dialog box, click **Review Script**, and then choose the package you want to open a read only version of the script for review.

Understanding the Cisco VXC Manager Package Structure

A Cisco VXC Manager Package structure consists of two components:

- The Package script (RSP) file (ImgXL24.rsp)
- The Package folder that contains the required application or image files (ImgXL24)

In order for a Package to function properly, these two components must adhere to the following structural rules:

- The Package script file must have an .rsp extension. You can create and edit an RSP file using Notepad.
- The Package folder must have the same name as the Package script file.
- The Number= parameter in the [Version] section of the Package script file should match the value reported by the device to the Client Manager. This becomes extremely important when using the Default Device Configuration feature.
- All the files referenced by the Package script file must be within the Package folder or a subfolder within.

- All command arguments should be enclosed in double-quotes and are separated by spaces ONLY.
- All registry paths are delimited with backslashes (‘\’) and are within quotes.
- Do not use abbreviations for the root registry keys (e.g. use HKEY_LOCAL_MACHINE, not HKLM).
- All filenames are delimited with backslashes (‘\’) and are within quotes.
- Neither path names nor registry branches should ever end with a backslash.
- In general, a script is aborted if a command fails. If you do not want the script to abort if a command fails, then appended the command with and asterisk (*). (Note not all commands support this).
- <REGROOT> (e.g. <regroot>\sourcefile.txt) points to the root directory of the registered package (e.g. c:\inetpub\ftproot\rapport\<packagename>).

Tip <regroot> is a pointer that tells the Cisco VXC Manager Service to look in a specific location on the Cisco VXC Manager server (not the device) for Package application files. <regroot> finds the Cisco VXC Manager Master Repository and identifies the folder contained within that is holding the needed Package files.

Optional Arguments and HKEY_CURRENT_USER

Four commands have optional arguments related to operations on the HKEY_CURRENT_USER registry branch.

The Cisco VXC Manager service HKEY_CURRENT_USER registry branch is not related to any user HKEY_CURRENT_USER branch, so changes made directly to HKEY_CURRENT_USER typically do not have the desired effect. When called with their optional UserName arguments these four commands translate all references to HKEY_CURRENT_USER to HKEY_USERS\<username’s SID>.

Tip These commands will fail if the given user is not logged-on at the time of distribution.

Understanding the Script File Structure

A Cisco VXC Manager script (RSP) file is one of two components that make up a Cisco VXC Manager Package:

- The Package script (RSP) file (ImgXL24.rsp)
- The Package folder that contains the required application or image files (ImgXL24)

The Package script (RSP) file must conform to a specific structure and should contain two sections:

- Version
- Script

Version

The Version section contains information required for package registration and distribution purposes. The following describes each of the elements of the Version section:

[Version] - Required section header

Number= - Must be the same as the Package Script File name

Description= - A brief description of what the Package is to achieve

OS= -The Operating System the Package is intended for

USE_REMOTE= - YES/NO, specifies whether or not a Remote Repository (if it exists) should be used. Default is YES. (OPTIONAL)

DEPLOYEDSW= - YES/NO defines whether package should be added to the Cisco VXC Manager deployed package table for device. Default is YES. (OPTIONAL)

Category= - The Cisco VXC Manager Package Manager category in the Administrator Console where the package will reside. Note if the category does not exist it will be created.

Image Category Special Tags

[Version] - Required section header

ImageSize= - size of image in Megabytes

BootFloppy= - name of bootfloppy; default is RAPPORT

Use_PXE= - YES/NO default value is YES for all scripts with Category=IMAGES

IMAGE= - name of image file to be used; by default Cisco VXC Manager uses the first file in file found in the package folder (excluding CRC.text)

Command= - the image operation to be performed

Script

The Script section contains the commands that are carried out when the script is distributed. Each command is executed in order as they appear within the [Script] section.

Recommended Scripting Template

```
[Version]
Number=Script name (matching the RSP_ file name and Package folder name)
Description=Detailed description with version number and valid images
OS=XX
Category=Other Packages
[Script]
Written by: Your Name and Company
; ..............................................................................
; >Check the Operating System
; >Check the Image Version
; ..............................................................................
CO "NT"
CI “XXXX”
; ..............................................................................
; >Check Free Space
; >Check Minimum Memory, if necessary
; >Check User, if necessary
; ..............................................................................
CF “X” “XXX”
CR “XXXX”
CU “XXXXXXXX”
; ..............................................................................
; > Query User then lock Workstation
; ..............................................................................
QU
LU*
; ..............................................................................
; >Add Commands Here
; ..............................................................................
;SF “<regroot>\files\x.xxx” “c:\yyyy\zzzz”
```

```
;EX "c:\yyyy\zzzz"
;DF "c:\yyyy\zzzz"
;MR "<regroot>\xxxx.reg"
;SP "c:\windows\system.ini" "DISPLAY" "screen-size" "640"
; ..............................................................................
; >End Lockout
; ..............................................................................
EL*
; ..............................................................................
; >Reboot, if necessary
; ..............................................................................
RB
--------------------------------------------------------------------------------
```

Version

The Version section contains information required for package registration and distribution purposes.

BootFloppy=

Specifies the boot floppy Cisco VXC Manager uses during the imaging process:

- Rapportitf.0 (Cisco VXC Manager Imaging agent for WISard imaging)
- pxelinux.0 (for Merlin imaging).

Category=

Defines the category for the Package. If you type a different category name in Category=, and then register the Package using Cisco VXC Manager, a folder is created under the Package Manager with that name.

Tip A package can be moved from one category to another by changing Category= and re-registering the package.

Command=

The image operation to be performed.

Example: Command=%ImageWrite%

Possible Values:

- %ImageWrite% (This value writes to the DiskOnChip)
- %ImageRead% (This value reads from the DiskOnChip)

DeployedSW=

This defines whether the package should be added to the Cisco VXC Manager deployed package table for the device.

DEPLOYEDSW=Yes or No - Default is Yes if not specified or specified incorrectly. This option is used primarily in conjunction with DDC. If a DDC has Enforce Sequence enabled any package sent to the device will trigger the DDC to re-image the device (thereby removing all packages). Using DeployedSW=No allows the user to send packages to devices without logging their distribution, thereby not triggering a DDC operation.

Description=

Allows the script developer to add a short description about the Package. The description is a comment line and is not parsed by Cisco VXC Manager when the script is executed.

Image=

This defines the file name to be used when reading or writing an image for PXE operation.

Image=filename - The default is the first file found in <regroot> excluding CRC.txt.

ImageSize=

Identifies for Cisco VXC Manager the size of image being sent to a client.

Values: 8, 16, 24, 32, 48, 64, 72, 80, 96, 128, 144, 192, 256, 512, 1024

Number=

Identifies for Cisco VXC Manager the name of the Package. The name of the Package script (RSP) file must match the Number= parameter. For example, if the Package script name is ImgXL24.rsp, you must have Number=ImgXL24 in the [Version] section of ImgXL24.rsp.

Example:

```
[Version]
Number=[Number reported by device in Device Manager under Image]
Description=Image to Write to Device
OS=NT
Category=Images
USE_PXE=YES
USE_REMOTE=NO
DEPLOYEDSW=YES
IMAGE=[xyz24xl.img]
IMAGESIZE=24
```

OS=

Defines the Operating System the device is running.

Values:

- XPe Windows XPe
- CE Windows CE 2.12
- CEN Windows CE .NET
- CE Windows CE 3.0
- WES Windows Embedded Standard
- LX Tuxia Linux
- BL WTOS

- RLX Red Hat Linux
- SLX SUSE Linux
- LVE Viance OS
- TDC ThreadX

Use_PXE=

Cisco VXC Manager utilizes Intel's® Wired for Management standard Preboot eXecution Environment (PXE) to load images to devices. The default is Yes if Category=Images and No for all other Categories (Categories<>Images) if not specified or specified incorrectly.

If Boot from LAN is enabled in the BIOS, then Use_PXE=. If you want the Package to be recognized by Cisco VXC Manager as a non-imaging package, or you are working with systems that are not PXE enabled, then type No as the value.

Values: Yes and No

Use_Remote=

This defines whether the package (script verbs and PXE) should use a Remote Repository assigned to its subnet or if it should always use the Master.

Use_Remote=Yes or No - Default is Yes, if not specified or specified incorrectly.

Script

The Script section contains the Cisco VXC Manager commands that are carried out when the script is distributed. Each command is executed in order as they appear within the [Script] section.

Append File

Verb: AF

Description: Adds the specified text as a new line at the end of specified device filename.

Support: XPe, Linux

Arguments:

- Path and filename
- New text line

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  - · AF "c:\temp\example.txt" "new line text" (This will add the line "new line text" to the end of example.txt located at c:\temp\)
- Linux Usage

  Continue if Script Command Fails: No

  Examples:

- AF "/wfs/Append.txt" "new line text" (This will add the line "new line text" to the end of Append.txt located at /wfs)

General Rules:

- This command will append a new line of text to the end of a text file. If the file does not already exist it will be created. This can be very useful in adding additional commands to batch and script files.

Tip The destination directory must exist for this command to work.

Confirm Disk Free Space

Verb: CF

Description: Confirms the free space is greater than the specified amount on the specified device drive.

Support: XPe, CE 2.12, CE.Net, CE 3.0, Linux

Arguments:

- Device drive letter (no colon required; for CE and Linux, it must be blank)
- Kilobytes free

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  - CF "C" "2048" (Confirms there is at least 2MB of free space on the C:\ drive)
- CE Usage

  Continue if Script Command Fails: No

  Examples:

  - CF "" "2048" (Confirms there is at least 2MB of free space on the storage device)
- Linux Usage

  Continue if Script Command Fails: No

  Examples:

  - CF "" "512" (Confirms there is at least 2MB of free space on the storage device)

General Rules:

- This command should be included on all scripts.
- Do not include a colon with the device drive letter.

Confirm File Version

Verb: CV

Description: Confirms the device filename against the operand and value specified.

Support: XPe, CE.Net, CE 3.0

Arguments:

- Device filename (CE add-on name)
- Test (<, =, >, <=, >=, or !=)
- Value (decimal #)

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  - CV "c:\Program Files\Rapport\HAgent.exe" ">=" "4.0.0.73" (Verifies HAgent.exe is version 4.0.0.73 or higher)
  - · CV "c:\windows\system32\mfc42.dll" "!=" "6.0.9586.0" (Verifies mfc42.dll is notversion 6.0.9586.0)

- CE Usage

  Continue if Script Command Fails: No

  Examples:

  - CV "ICA" ">=" "0019" (Verifies ICA addon is version 019 or higher)
  - CV "ICA" "=" "0023" (Verifies ICA addon is version 0023)
  - CV "ICA" "<" "0031" (Verifies ICA addon is less than version 0031)

Tip CV command is NOT supported on CE.212

General Rules:

- For a CE add-on name, use the add-on name as reported in the Administrator Console.

Confirm Image

Verb: CI

Description: Confirms the device operating image. This command uses the first characters (same number of characters specified in parameter) of the image number in image.ver on the device.

Support: XPe, CE 2.12, CE.Net, CE 3.0, Linux

Arguments:

- Image version substring

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  - CI "1.2" (Verifies device Image Number begins with 1.2. Thus 1.21, 1.256, 1.295.45 will all report success)
  - CI "2.00297.192" (Verifies device Image Number begins with 2.00297.192)

- CE Usage

  Continue if Script Command Fails: No

Examples:

- CI "441" (Verifies device Image Number begins with 441. Thus 441.6, 441.22 and 441.39.7 will all report success)
- · CI "486.7.1" (Verifies device Image Number begins with 486.7.1)

- Linux Usage

  Continue if Script Command Fails: No

  Examples:

  - CI "3.6.3.00.5" (Verifies the device Image Number)
  - CI "3.6.3." (Verifies the device Image Number)
  - CI "3." (Verifies the device Image Number)

General Rules:

- This command should be included on all scripts.
- The Image version substring behaves as if a wildcard were present at the end of the image number. For example, if command was CI=“441”, image numbers 441.22 and 441.23 would pass. Images 440 and 442 would fail.

Confirm Minimum RAM Size

Verb: CR

Description: Confirms the device has at least the specified amount of memory.

Support: XPe, CE 2.12, CE.Net, CE 3.0, Linux

Arguments:

- The minimum amount of RAM in Kilobytes

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  - CR "16000" (Verifies that device has a minimum of 16MB of RAM)

- CE Usage

  Continue if Script Command Fails: No

  Examples:

  - CR "16000" (Verifies that device has a minimum of 16MB of RAM)

- Linux Usage

  Continue if Script Command Fails: No

  Examples:

  - CR "32000" (Verifies that device has a minimum of 32000MB of RAM)

General Rules:

- This command should be included on all scripts where software is being deployed that requires a certain amount of memory.

Confirm Operating System

Verb: CO

Description: Confirms the device operating system. This command uses a character string representation for OS type (that is, CO “XPe”).

Support: XPe, CE 2.12, CE.Net, CE 3.0, Linux

Arguments:

- Device operating system
- Optional CE version arguments (valid only for CE)

Usage

- XPe Usage

  Continue if Script Command Fails: No

  - XP=Windows XP

  Example:

  - CO "XP" (Verifies that Operating System is XP)
- CE Usage

  Continue if Script Command Fails: No

  CE=CE 2.12, or

  CEN=CE.Net, or

  TPC=CE 3.0

  Examples:

  - CO "CE" (Verifies OS is CE 2.12)
  - CO "CEN" (Verifies OS is CE.Net. Returns true if OS is CE.Net version 4.0 or 4.10)
  - CO "CEN" "4.10" (Verifies OS is CE.Net version 4.10; Returns true if OS is CE.Net 4.10; Returns false if OS is CE.Net version 4.0)
- Linux Usage

  Continue if Script Command Fails: No

  LX=Tuxia Linux

  Example:

  - CO "LX" (Verifies that Operating System is LX)

General Rules:

- This command should be included on all scripts.

Confirm User

Verb: CU

Description: Confirms that the specified user is logged into the device.

Support: XPe

Arguments:

- Username

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  - CU "Administrator" (Verifies 'Administrator' is currently logged on)

General Rules:

- This command should be included on all scripts that have user-specific registry commands.

Delete File

Verb: DF

Description: Deletes the specified device filename (analogous to DEL or rm).

Support: XPe, CE 2.12 (limited support), CE.Net (limited support), CE 3.0, Linux

Arguments:

- Path and Filename

Usage:

- XPe Usage

  Continue if Script Command Fails: Yes

  Examples:

  - DF “c:\winnt\filetodelete.txt” (Deletes specific file from device)

- CE Usage

  Continue if Script Command Fails: Yes

  Examples:

  - DF“\Windows\filetodelete.txt” (Deletes specific file from device)

  Cisco VXC devices support limited DF commands:

  - DF "Gkeyreset" (Resets device to factory defaults)
  - DF "CEAddon" "<addon name>" (Removes add-on named in 3rd argument)

- Linux Usage

  Continue if Script Command Fails: Yes

  Examples:

  - DF "/wfs/SendTest/filetodelete.txt" (Deletes specific file from device)

General Rules:

- Device filename should include the path.

Delete Registry Branch

Verb: DB

Description: Deletes the specified registry branch.

Warning **Use this command carefully. Once executed, it cannot be undone.**

Support: XPe

Arguments:

- Device key string
- User profile (not used with CE) [Optional]

Usage:

- XPe Usage

  Continue if Script Command Fails: Yes

  Examples:

  - DB "HKEY_LOCAL_USER\Printers" "user" (Deletes specified registry branch fromuser profile)

General Rules:

- The name of the registry hive should not be abbreviated.
- The Cisco VXC Manager Agent runs in the system security context. Because of this, HKEY_CURRENT_USER for Cisco VXC Manager is the system user, not the currently logged in user. To overcome this, a special username argument must exist that tells the agent to apply the changes to the specified user rather than the system user. The specified user must be logged into the device for this command to succeed. Note that the user profile name is used to resolve the hive location. The profile name and username can be different.

Delete Registry Value

Verb: DR

Description: Deletes the specified device registry key. The option username is used to change user specific registry values. The REDEDIT file must use HKEY_CURRENT_USER. Cisco VXC Manager will change this to HKEY_USERS_USERSID

Warning **Use this command carefully. Once executed, it cannot be undone.**

Support: XPe

Arguments:

- Device key string
- User profile [Optional]

Usage:

- XPe Usage

  Continue if Script Command Fails: Yes

  Examples:

  - DR “HKEY_CURRENT_USER\CONTROL PANEL\COLORS\background” “user” (Deletes specified registry key from 'user's' profile)

General Rules:

- The name of the registry hive should not be abbreviated.

- The Cisco VXC Manager Agent runs in the system security context. Because of this, HKEY_CURRENT_USER for Cisco VXC Manager is the system user, not the currently logged in user. To overcome this, a special username argument must exist that tells the agent to apply the changes to the specified user rather than the system user. The specified user must be logged into the device for this command to succeed. Note that the user's profile name is used to resolve the hive location. The profile name and username can be different.
- DR must be followed by the Reboot command (RB) for the changes to take effect.

Delete Tree

Verb: DT

Description: Deletes the specified device directory and its contents (analogous to DELTREE or rm –R).

Warning **Use this command carefully. Once executed, it cannot be undone.**

Support: XPe, Linux

Arguments:

- Device directory

Usage:

- XPe Usage

  Continue if Script Command Fails: Yes

  Examples:

  - DT "C:\Test" (Deletes the 'Test' folder and all files within it)
- Linux Usage

  Continue if Script Command Fails: Yes

  Examples:

  - DT "/wfs/Test" (Deletes the 'Test' folder and all files within it)

General Rules:

- None

End Lockout

Verb: EL

Description: Removes the splash screen displayed by the LU command on the client device.

Support: XPe, CE 2.12, CE.Net

Arguments:

- None

Usage:

- XPe Usage

  Continue if Script Command Fails: Yes

  Examples:

  - EL

- CE Usage

  Continue if Script Command Fails: Yes

  Examples:

  - EL

General Rules:

- This command should always be used in conjunction with a LU. It is recommended that all non-image scripts use this command.

Execute on Device

Verb: EX

Description: Executes the specified client filename (assumes the specified file is executable).

Support: XPe

Arguments:

- Path and filename
- Synchronous execute [Optional]

Usage:

- XPe Usage

  Continue if Script Command Fails: Yes

  Examples:

  - EX "c:\test.exe" (Launches c:\test.exe on the device and continues to next command in script)
  - EX "c:\test.exe" "+" (Launches c:\test.exe on the device and pauses until the executable is finished before continuing with next command in script)
  - EX "c:\test.exe" "+30" (Launches c:\test.exe on the device and pauses until the executable is finished or 30 seconds have elapsed, whichever occurs first, before continuing with the next command in script)

General Rules:

- The command may be issued exactly as it would be from a command prompt on the device.
- In Windows, the path may be omitted if the executable is a registered Windows application
- The optional synchronous argument stops script processing until the executable is finished. This option can be expressed as "+" with no timeout or "+n" where n indicates the maximum time in seconds to wait before continuing script processing.

Tip Because of differences between process and system speeds, it is HIGHLY recommended that this option be used.

Get File

Verb: GF

Description: Copies the specified device filename to the specified master repository filename (analogous to COPY or cp).

Support: XPe, CE 2.12, CE.Net, CE 3.0, Linux

Arguments:

- Device filename (source)
- Master repository filename (destination)

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  - GF "c:\temp\temp.txt" "<regroot>\temp.txt" (Pulls temp.txt from the device to the Master repository)

- CE Usage

  Continue if Script Command Fails: No

  Examples:

  - GF "\Windows\temp.txt" "<regroot>\temp.txt" (Pulls temp.txt from the device to the Master repository)

  Cisco VXC devices have limited GF support:

  - GF "CEConfig" "<regroot>\Settings.reg" (Exports device registry to Settings.reg on the Master repository)

- Linux Usage

  Continue if Script Command Fails: No

  Examples:

  - GF "/wfs/SendTest/zero1.txt" "<regroot>\zero.txt" (Pulls zero1.txt from the device to zero.txt in the Master repository)

General Rules:

- Get operations always pull to the Master repository.
- Source and target filenames should include the complete path.
- The destination path should be defined with <regroot>.

Get Registry

Verb: GR

Description: Exports the specified device registry branch. The resulting local filename will be in REGEDIT4 format.

Support: XPe

Arguments:

- Device registry branch
- Master repository filename (destination)

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

- GR “HKEY_LOCAL_MACHINE\SOFTWARE\Rappport” "<regroot>\Rapport.reg" (Exports Cisco VXC Manager registry settings to Rapport.reg in the script folder)

General Rules:

- Get operations always pull to the Master repository.
- The name of the registry hive should not be abbreviated.
- The resulting local filename will be in REGEDIT format.
- The destination should include the complete path, defined with <regroot>.

Get Registry Value

Verb: GV

Description: Gets a single registry value to a file. The following types are supported:

- REG_SZ
- REG_MULTI_SZ
- REG_EXPAND_SZ
- REG_DWORD
- REG_BINARY

The output file types are:

- Windows NT 4.0: REGEDIT4 format, PC/ANSI
- Windows 2K/XP: Regedit v5.00, PC/UNICODE

Tip Certain registry keys may be locked by the OS and interfere with GV operations. Verify with the device manufacture that the registry value is not locked.

Registry value changes will not be persistent unless the device is rebooted using one of the following:

- Via the RB (reboot) command
- Right-click reboot
- Manual operation

Support: XPe, CE 2.12, CE.Net, CE 3.0

Arguments:

- The full path of the registry key, including the registry entry name
- Master repository filename (destination)

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  - GV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestValue1" "<regroot>\TestValue1.reg" (Pulls TestValue1 to TestValue1.reg in the script folder)

- CE Usage

  Continue if Script Command Fails: No

Examples:

- GV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestValue1" "<regroot>\TestValue1.reg" (Pulls TestValue1 to TestValue1.reg in the script folder)

General Rules:

- Get operations always pull to the Master repository.
- The name of the registry hive should not be abbreviated.
- The resulting local filename will be in REGEDIT format.
- The destination should include the complete path, defined with <regroot>.

Local Pause

Verb: LP

Description: Pauses the server for a number of seconds. This allows the server to pause after commands that may take a while.

Support: XPe, CE 2.12, CE.Net, CE 3.0

Arguments:

- Number of seconds to pause

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  - LP "30" (Pauses script processing for 30 seconds)
- CE Usage

  Continue if Script Command Fails: No

  Examples:

  - LP "30" (Pauses script processing for 30 seconds)

General Rules:

- None

Lockout User

Verb: LU

Description: Display a splash screen on the device explaining an update is occurring.

Support: XPe, CE 2.12, CE.Net, CE 3.0

Arguments:

- Yes or No (Optional)

Usage:

- XPe Usage

  Continue if Script Command Fails: Yes

  Examples:

  - LU (Displays splash screen on device, splash is not removed if package fails or ends)

  - LU "Yes" (Displays splash screen on device, splash automatically removed if package fails or ends)
  - LU "No" (Displays splash screen on device, splash is not removed if package fails or ends)
- CE Usage

  Continue if Script Command Fails: Yes

  Examples:
  - LU (Displays splash screen on device, splash is not removed if package fails or ends)
  - LU "Yes" (Displays splash screen on device, splash automatically removed if package fails or ends)
  - LU "No" (Displays splash screen on device, splash is not removed if package fails or ends)

General Rules:

- This command should always be used in conjunction with an EL. It is recommended that all non-image scripts use this command.

Merge Registry

Verb: MR

Description: Merges the specified device filename. The device filename must be in REGEDIT format (analogous to regedit –s). The option username is used to change user specific registry values. The REDEDIT4 file must use HKEY_CURRENT_USER. Cisco VXC Manager will change this to HKEY_USERS_USERSID.

Support: XPe

Arguments:

- Local filename
- User profile [Optional]

Usage:

- XPe Usage

  Continue if Script Command Fails: Yes

  Examples:
  - MR "<regroot>\control_panel.reg" "user" (Merges control_panel.reg into 'user's' profile)

General Rules:

- The filename should include the complete path, defined with <regroot>.
- The filename specified must be a REGEDIT file.
- MR must be followed by the Reboot command (RB) for the changes to take effect.
- The optional username argument is used to change user specific registry values.

Tip The REDEDIT file must specify HKEY_CURRENT_USER. Cisco VXC Manager will change this to HKEY_USERS_USERSID at runtime. The Cisco VXC Manager Agent runs in the system security context. Because of this, HKEY_CURRENT_USER for Cisco VXC Manager is the system user, not the currently logged in user. To overcome this, a special username argument must exist that tells the

agent to apply the changes to the specified user rather than the system user. The specified user must be logged into the device for this command to succeed. Note that the user profile name is used to resolve the hive location. The profile name and username can be different.

Query User

Verb: QU

Description: Query the user regarding the pending update. Allows the user to accept the update now, postpone the update 5 minutes or until next Logon to NT Server (NT/XP only).

Support: XPe, CE 2.12, CE.Net, CE 3.0, Linux

Arguments:

- Buttons (Optional)
  - 1=Now only
  - 2=Delay 5 Minutes only
  - 3=Now and Delay 5 Minutes
  - 4=Update on Log in only
  - 5=Now and Update on Log in
  - 6=Delay 5 minutes and Update on Log in
  - 7=Now, Delay 5 minutes and Update on Log in
- Timeout in seconds (Optional)

Tip If one argument is used, both must be specified.

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:
  - QU (Displays query user dialog with buttons and timeout as set by preferences on the Cisco VXC Manager server)
  - QU "2" "5" (Displays query user dialog with 'Delay 5 Minutes' button for 5 seconds)
  - QU "3" "120" (Displays query user dialog with 'Update Now' and 'Delay 5 Minutes' buttons for 120 seconds)
- CE Usage

  Continue if Script Command Fails: No

  Examples:
  - QU (Displays query user dialog with buttons and timeout as set by preferences on the Cisco VXC Manager server)
  - QU "2" "5" (Displays query user dialog with 'Delay 5 Minutes' button for 5 seconds)
  - QU "3" "120" (Displays query user dialog with 'Update Now' and 'Delay 5 Minutes buttons for 120 seconds)
- Linux Usage

Continue if Script Command Fails: No

Examples:

- QU "1" "5" (Displays query user dialog with 'Update Now' and '5 Minute Delay' buttons for 5 seconds)

General Rules:

- Check your company's policies concerning updating a computer without user confirmation.
- If no arguments are defined, global values from Cisco VXC Manager Preferences are used.
- If the user does not make a selection within the allotted timeout, the update automatically occurs.

Reboot

Verb: RB

Description: Reboots the device.

Support: XPe, CE 2.12, CE.Net, CE 3.0, Linux

Arguments:

• None

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  - RB (Reboots device)

- CE Usage

  Continue if Script Command Fails: No

  Examples:

  - RB (Reboots device)

- Linux Usage

  Continue if Script Command Fails: No

  Examples:

  - RB (Reboots device)

General Rules:

- None

Send File

Verb: SF

Description: Copies the specified local filename to the specified device filename (analogous to the COPY or CP DOS command).

Support: XPe, CE 2.12, CE.Net, CE 3.0, Linux

Arguments:

- Repository path and filename (source)
- Device path and filename (destination)

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  - SF “<regroot>\logos.bmp” “c:\winnt\logos.bmp” (Copies logos.bmp from the repository to c:\winnt\logos.bmp on the device)

- CE Usage

  Continue if Script Command Fails: No

  Examples:

  - SF "<regroot>\sol.exe" "\Windows\sol.exe" (Copies sol.exe from the repository to \Windows\sol.exe on the device)

  Cisco VXC devices have limited SF support:

  - SF "CEFirmware" "<regroot>\image.bin" (Loads image.bin (either an add-on or entire CE image) to the device)
  - SF "CEConfig" "<regroot>\setting.reg" (Applies settings.reg to the device; Note that the .reg file will be filtered before it is applied)

- Linux Usage

  Continue if Script Command Fails: No

  Examples:

  - SF "<regroot>\SendTest\zero.txt" "/wfs/SendTest/zero1.txt" (Copies zero.txt from the repository to /wfs/SendTest/zero1.txt on the device)

General Rules:

- Both source and destination should include the full path, and the source path should be defined with <regroot>.
- The destination filename does not have to be the same as the source filename.

Set Device Information

Verb: SC

Description: This command allows easy configuration of the device information.

Support: XPe, CE 2.12, CE.Net, CE 3.0, Linux

Arguments:

- CN=Computer Name
- CO=Contact
- LO=Location
- C1=Custom1
- C2=Custom2
- C3=Custom3

Usage:

- XPe Usage

Continue if Script Command Fails: No

Examples:

- SC "CN=DeviceName" "LO=location" "CO=contact" "C1=custom1" "C2=custom2" "C3=custom3" (Renames device and sets all custom information)

- CE Usage

  Continue if Script Command Fails: No

  Examples:

  - SC "CN=DeviceName" "LO=location" "CO=contact" "C1=custom1" "C2=custom2" "C3=custom3" (Renames device and sets all custom information)
  - SC "LO=Here" "CO=Admin" (Sets Location and Contact without altering computer name or Custom 1-3)

- Linux Usage

  Continue if Script Command Fails: No

  Examples:

  - SC "CN=DeviceName" "LO=location" "CO=contact" "C1=custom1" "C2=custom2" "C3=custom3" (Renames device and sets all custom information)

General Rules:

- Each argument is optional; as many or as few as desired can be set (however, you must set at least one).
- Do not set multiple devices with the same computer name (CN=).

Set Network Information

Verb: SN

Description: This new command will allow easy configuration of the network information.

Support: XPe, CE 2.12, CE.Net, CE 3.0, Linux

Arguments:

- IP=IP Address
- ED=DHCP on/off
- SM=Subnet Mask
- GW=Gateway Address
- 0D=DNS manual (0) or auto (1)
- 1D=DNS manual entry 1
- 2D=DNS manual entry 2
- 0W=WINS manual (0) or auto (1)
- 1W=WINS manual entry 1
- 2W=WINS manual entry 2
- DM=Domain suffix

Usage:

- XPe Usage

Continue if Script Command Fails: No

Examples:

– · SN

"IP=192.168.1.10" "ED=0" "SM=255.255.255.0"

"GW=192.168.1.1" "0D=0" "1D=192.168.3.21"

"2D=192.168.3.22" "0W=0" "1W=192.168.1.2"

"2W=192.168.1.3" "DM=MyDomain"

The above example will set the following:

Disable DHCP

Assign Static IP of 192.168.1.10

Subnet Mask 255.255.255.0

Gateway 192.168.1.1

Set manual entry of DNS

Assign primary DNS as 192.168.3.21

Assign secondary DNS as 192.168.3.22

Assign the DNS domain to MyDomain

Set manual entry of WINS

Assign primary WINS as 192.168.1.2

Assign secondary WINS as 192.168.1.3

- CE Usage

Continue if Script Command Fails: No

Examples:

– SN

"IP=192.168.1.10" "ED=0" "SM=255.255.255.0"

"GW=192.168.1.1" "0D=0" "1D=192.168.3.21"

"2D=192.168.3.22" "0W=0" "1W=192.168.1.2"

"2W=192.168.1.3" "DM=MyDomain"

The above example will set the following:

Disable DHCP

Assign Static IP of 192.168.1.10

Subnet Mask 255.255.255.0

Gateway 192.168.1.1

Set manual entry of DNS

Assign primary DNS as 192.168.3.21

Assign secondary DNS as 192.168.3.22

Assign the DNS domain to MyDomain

Set manual entry of WINS

Assign primary WINS as 192.168.1.2

Assign secondary WINS as 192.168.1.3

- Linux Usage

  Continue if Script Command Fails: No

  Examples:

  - SN

    "IP=192.168.1.10" "ED=0" "SM=255.255.255.0"

    "GW=192.168.1.1" "0D=0" "1D=192.168.3.21"

    "2D=192.168.3.22" "0W=0" "1W=192.168.1.2"

    "2W=192.168.1.3" "DM=MyDomain"

  The above example will set the following:

  Disable DHCP

  Assign Static IP of 192.168.1.10

  Subnet Mask 255.255.255.0

  Gateway 192.168.1.1

  Set manual entry of DNS

  Assign primary DNS as 192.168.3.21

  Assign secondary DNS as 192.168.3.22

  Assign the DNS domain to MyDomain

  Set manual entry of WINS

  Assign primary WINS as 192.168.1.2

  Assign secondary WINS as 192.168.1.3

General Rules:

- Do not set multiple devices with the same IP address (IP=).
- Sending ED=1 (DHCP on) will overrule the other entries
- 1D & 2D are only processed if 0D=0
- 1W & 2W are only processed if 0W=0

Set Profile

Verb: SP

Description: This command is used to update ini files. The device filename specifies the name of the ini file to update. The section, key, and value determine what to update in the ini file.

Support: XPe, CE 3.0, Linux

Arguments:

- Device path and filename
- Section
- Key
- Value

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  - SP "c:\winnt\system.ini" "drivers" "timer" "timer.drv" (Edits System.ini to:
    [drivers]
    timer=timer.drv)

- CE Usage

  Continue if Script Command Fails: No

  Examples:

  - SP "\Windows\SetProfile.txt" "SetProfile" "Test" "Worked" (Edits SetProfile.txt to:
    [SetProfile]
    test=worked

- Linux Usage

  Continue if Script Command Fails: No

  Examples:

  - SP "/wfs/SetProfile.txt" "SetProfile" "Test" "Worked" (Edits SetProfile.txt to:
    [SetProfile]
    Test=Worked

General Rules:

- If the file does not exist it will be created.
- Most INI files are organized by Section and Key. A section will be defined by a line that contains bracketed text ([Example]). A Key will be followed by an equal sign and a value (Key=value).
- Keys must be located on a line by themselves.

Set Registry Value

Verb: SV

Description: Sets a single registry value.

Tip Certain registry keys may be locked by the OS and interfere with SV operations. Please verify with the device manufacture that the registry value is not locked.

Registry value changes will not be persistent unless the device is rebooted using one of the following:

RB (reboot) command

Right-click reboot

Manual operation

Support: XPe, CE 2.12, CE.Net

Arguments:

- The full path of the registry key, including the registry entry name
- The value to set the registry entry to
- The registry type to use for argument #2. Currently only REG_SZ (string) and REG_DWORD (number) are supported. [Optional] <![endif]>

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  - SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestValue1" "5551234"
    Possible scenarios:
    - TestValue1 already exists as a REG_SZ and will be set to string "5551234"
    - TestValue1 already exists as a REG_DWORD and will be set to the number 5551234
    - TestValue1 already exists as another type and the agent will return an error
    - TestValue1 doesn't exist and will be set to string "5551234"
  - SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestValue2" "StringValue"

    Possible scenarios:
    - TestValue2 already exists as a REG_SZ and will be set to string "StringValue"
    - TestValue2 already exists as another type and the agent will return an error
    - TestValue2 doesn't exist and will be set to string "StringValue"
  - SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestDWORD" "2833" "REG_DWORD"

    Possible scenarios:
    - TestDWORD already exists as a REG_DWORD and will be set to the number 2833
    - TestDWORD already exists as another type and the agent will return an error
    - TestDWORD doesn't exist and will be set to the number 2833
  - SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestString" "MyString" "REG_SZ"

    Possible scenarios:
    - TestString already exists as a REG_SZ and will be set to string "MyString"
    - TestString already exists as another type and the agent will return an error
    - TestString doesn't exist and will be set to string "MyString"
- CE Usage

  Continue if Script Command Fails: No

  Examples:

  - SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestValue1" "5551234"

    Possible scenarios:
    - TestValue1 already exists as a REG_SZ and will be set to string "5551234"
    - TestValue1 already exists as a REG_DWORD and will be set to the number 5551234
    - TestValue1 already exists as another type and the agent will return an error
    - TestValue1 doesn't exist and will be set to string "5551234"
  - SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestValue2" "StringValue"

Possible scenarios:

- TestValue2 already exists as a REG_SZ and will be set to string "StringValue"
- TestValue2 already exists as another type and the agent will return an error
- TestValue2 doesn't exist and will be set to string "StringValue"

– SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestDWORD" "2833" "REG_DWORD"

Possible scenarios:

- TestDWORD already exists as a REG_DWORD and will be set to the number 2833
- TestDWORD already exists as another type and the agent will return an error
- TestDWORD doesn't exist and will be set to the number 2833

– · SV "HKEY_LOCAL_MACHINE\SOFTWARE\Rapport\hAgent\TestString" "MyString" "REG_SZ"

Possible scenarios:

- TestString already exists as a REG_SZ and will be set to string "MyString"
- TestString already exists as another type and the agent will return an error
- TestString doesn't exist and will be set to string "MyString"

General Rules:

- The name of the registry hive should not be abbreviated.
- If three arguments are supplied then the agent will either create non-existing keys of the supplied type, or error out if the type does not match an existing key's type.
- If only two arguments are supplied and the key does not already exist then the type REG_SZ (string) is assumed.
- If only two arguments are supplied and the key does exist and it is of type REG_DWORD then the agent will confirm the value is a number and set it as a DWORD.

Shutdown

Verb: SD

Description: Shuts down the device and sets the power state.

Support: XPe, CE 2.12, CE.Net, CE 3.0, Linux

Arguments:

- None

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  – SD (Shut down device)

- CE Usage

  Continue if Script Command Fails: No

  Examples:

  – SD (Shut down device)

- Linux Usage

  Continue if Script Command Fails: No

  Examples:

  - SD (Shut down device)

General Rules:

• None

Synch Time

Verb:ST

Description: Changes the device time to match the update server time.

Support: XPe, CE 2.12, CE.Net, CE 3.0, Linux

Arguments:

- None

Usage:

- XPe Usage

  Continue if Script Command Fails: Yes

  Examples:

  - ST (Synchronizes the device time to the Cisco VXC Manager server time)
- CE Usage

  Continue if Script Command Fails: Yes

  Examples:

  - ST (Synchronizes the device time to the Cisco VXC Manager server time)
- Linux Usage

  Continue if Script Command Fails: Yes

  Examples:

  - ST (Synchronizes the device time to the Cisco VXC Manager server time)

General Rules:

- There may be a slight time difference between server and device due to network latency.
- Time Zone offset is taken into account, please ensure that the proper time zone is set on the device.

Wake On LAN

Verb: WL

Description: Boots a device that is shutdown (the device must have Wake On LAN enabled in its BIOS).

Support: Hardware dependent, not agent dependent

X Copy

Verb: XC

Description: Copies the specified device directory and its contents to the specified local directory (analogous to XCOPY or cp –R).

Support: XPe, CE 3.0, Linux

Arguments:

- Repository directory (source)
- Device directory (destination)

Usage:

- XPe Usage

  Continue if Script Command Fails: No

  Examples:

  - XC "<regroot>\Files\winnt\system32*" "C:\winnt\system32" (Copies all files in the system32 folder of the package to the device's system32 folder)

- CE Usage

  Continue if Script Command Fails: No

  Examples:

  - XC "<regroot>\system*" "\system" (Copies all files in the system folder of the package to the device's system folder)

- Linux Usage

  Continue if Script Command Fails: No

  Examples:

  - XC "<regroot>\XCTest*" "/wfs/" (Copies all files in the XCTest folder of the package to the device's wfs folder)

General Rules:

- The source path should be defined with <regroot>.
- The source path should end in * (* is a wildcard to indicate all files and directories)..

APPENDIX I

Autogenic Imaging

Note This appendix is not applicable to Cisco VXC devices. It is applicable only for the management of third-party clients.

This appendix contains advanced information about Autogenic Imaging.

Overview

The purpose of Autogenic Imaging (image backup mechanism scheme) is to image a device with the image residing on the flash or hard drive of the device. This document describes the following steps you must complete prior to the actual imaging process/scheme:

Procedure

Step 1 Prepare an Image to be Autogenic Capable.

Step 2 Register the Prepared Image in Cisco VXC Manager.

Step 3 Convert the Registered Image to an Autogenic Capable Image.

Step 4 Convert a Device to an Autogenic Capable Device.

Step 5 Schedule an Autogenic Capable Image to an Autogenic Capable Device.

Caution To allow Autogenic Imaging to work correctly, Cisco VXC Manager expects the flash to be twice the size of the active OS partition. If you are using WES7, Autogenic Imaging requires 8 GB.

Autogenic Imaging means to image a device with the image residing on the backup partition of the device flash/hard drive. The backup OS partition is a FAT32 partition where the backup image resides. The disk layout of the device is as follows.

For XPe:

WFS | Active OS partition (NTFS) | Non-PXE boot agent (Fat32) | Back up OS partition (Fat32)

For WES 2009:

WFS | Non-PXE boot agent (Fat32) | Active OS partition (NTFS) | Back up OS partition (Fat32)

For WES 7:

Non-PXE boot agent (Fat32) | Active OS partition (NTFS) | Back up OS partition (Fat32)

The Autogenic Image contains the standard image files with one extra script file named image.rsp inside the package. In the package script you can verify the Autogenic Image by looking for the <BackupImage> tag. If this tag is present in the registered image package script, then the image is autogenic. Upon scheduling the image, the image script (RSP file) will have instructions for the agent to download the image from the Master (or remote) repository to the back-up partition.

Procedures

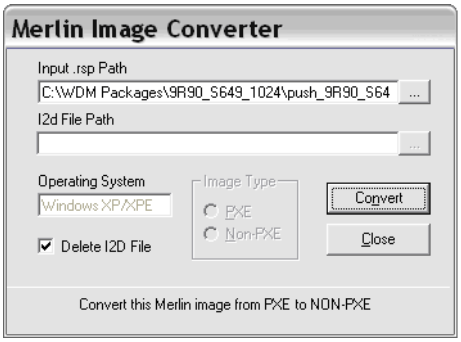
Step 1: Prepare an Image to be Autogenic Capable

Convert a normal WISard Image or Merlin Image to a non-PXE Merlin Image by using a converter utility.

Note If it is a WISard Image, be sure that you have checked the Delete I2D file check box in the converter utility.

Caution Before converting the image, be sure the initrd.pxe and vmlinuz files are residing in the same folder as ConverterUtility.exe.

Figure I-1 Merlin Image Converter



Step 2: Register the Prepared Image in Cisco VXC Manager

Note Only non-PXE Merlin image can be converted to an Autogenic Capable Image. Therefore, before registering an image in Cisco VXC Manager, be sure that you will register a non-PXE Merlin image (the package should not contain an i2d file).

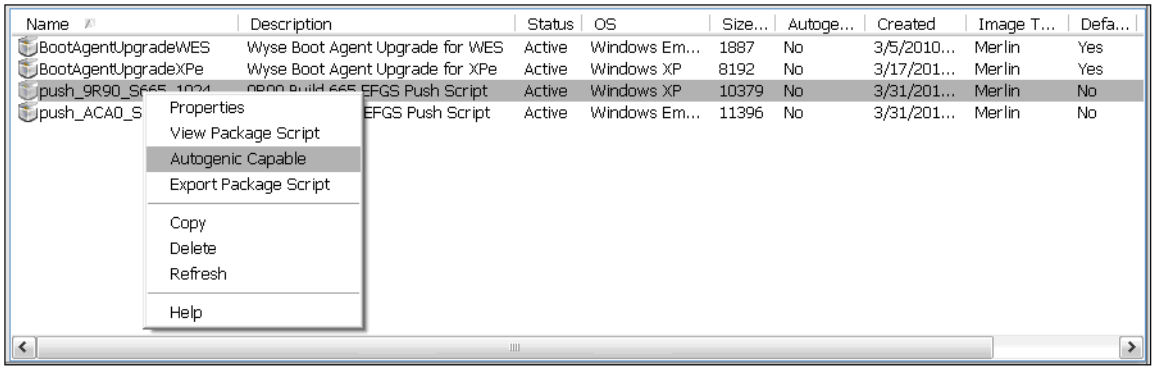
To register the prepared image in Cisco VXC Manager, perform the same steps as you would to register a normal package in Cisco VXC Manager (see Cisco VXC Manager documentation). After registering the image in Cisco VXC Manager, be sure that image type appears as Merlin in the Package Manager View.

Step 3: Convert the Registered Image to an Autogenic Capable Image

After registering the image in Cisco VXC Manager, right-click on the registered image and choose the Autogenic Capable option from the available options. The image will be converted to an Autogenic Capable Image.

After converting the image to an Autogenic Capable Image in Cisco VXC Manager, be sure that Yes appears in the Autogenic column for the image in the Package Manager View.

Figure I-2 Package Manager View



Step 4: Convert a Device to an Autogenic Capable Device

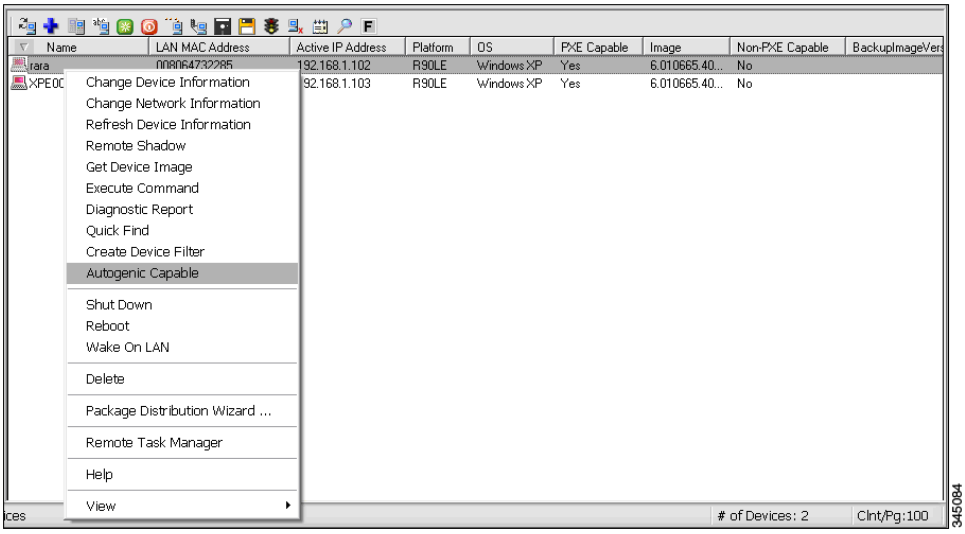
If there is no registered Autogenic Capable Image in the Cisco VXC Manager Package Manager, the device cannot be converted to an Autogenic Capable Device. Thus, before attempting to convert a device to an Autogenic Capable Device, be sure that an Autogenic Capable Image exists in the Cisco VXC Manager Package Manager.

Procedure

Step 1 In the Cisco VXC Manager MMC Snap-in tree panel, expand the Device Manager node.

Step 2 Choose the devices you want and right-click them.

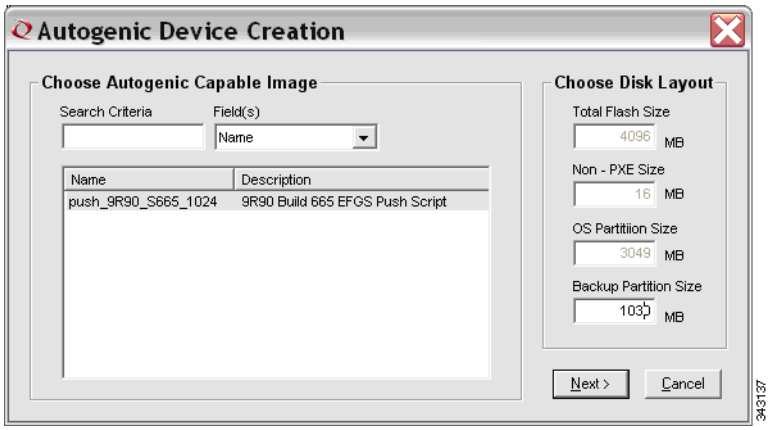
Figure I-3 Device Manager



Step 3 Choose the Autogenic Capable option from the available options. The Autogenic Device Creation window appears.

Note The Autogenic Capable option will appear only if all selected devices are Windows XP/WES Non-PXE capable devices with the same flash size.

Figure I-4 Autogenic Device Creation



Step 4 Choose the disk layout as per the requirement. The size of backup partition should be large enough to fit the backup image in it. The device should have enough space to fit backup image as well as the running OS partition.

Note You can use the Search Criteria and Field(s) fields to create a filter that narrows down the selection of available images. Only images that have a name or description that contains the text entered into the Search Criteria field will be displayed. If no text is entered in the Search Criteria field, then all appropriate images will appear in the list.

Step 5 The four Disk Layout values are pre-populated with the following values whenever an image is selected:

- Total Flash Size—This is the total size in MB of the Flash on the selected devices.
- Non - PXE Size—This is always 16 MB.
- OS Partition Size—This is dependant on the Backup Partition Size and is set to be (Total Flash Size, Non - PXE Size, and Backup Partition Size) for devices with flash size of 4096 MB or less, and to (4096, Non - PXE Size, and Backup Partition Size) for devices with flash greater than 4096 MB.
- Backup Partition Size—Initially this is set to be 100 MB plus the size of the selected image. If the Total Flash Size for the device(s) is greater than 4096 MB, this value cannot be changed. However, if the Total Flash Size is not greater than 4096 MB, you can increase up to any value that still provides room for the OS partition.

Step 6 After selecting the Disk Layout values, click Next. The Package Distribution Wizard window appears with default values.

Step 7 Leave the default values and click Next.

Step 8 Choose the PXE or Non-PXE option based on the device configuration, and then click Next.

Step 9 Click Finish to schedule the image package to the device. The scheduled image package will appear on the Update Manager View. After finishing the imaging task, the device will recreate the disk layout of the device and will create the backup partition of specified size on the device flash/disk.

Step 5: Schedule an Autogenic Capable Image to an Autogenic Capable Device

Procedure

Step 1 Drag and drop the Autogenic Capable Image to the Cisco VXC Manager Device Manager. It will list all the devices that fulfill the criteria for the scheduled Autogenic Capable Image (this can also be done by right-clicking on the device in the Device Manager).

Step 2 Choose the Autogenic Capable Device from the list of devices to which the Autogenic Capable Image will be scheduled.

Step 3 Continue with one of the following:

- If you want to complete the downloading and imaging processes separately (you want to download the image to the backup partition now, but want to schedule imaging the device from the backup partition later), continue with Case 1: Performing the Downloading and Imaging Processes Separately, page I-5.
- If you want to complete the downloading and imaging processes together (you want to download the image to the backup partition and schedule imaging the device from the backup partition now), continue with Case 2: Performing the Downloading and Imaging Processes Together, page I-7.

Case 1: Performing the Downloading and Imaging Processes Separately

Process 1: To download the image to the backup partition:

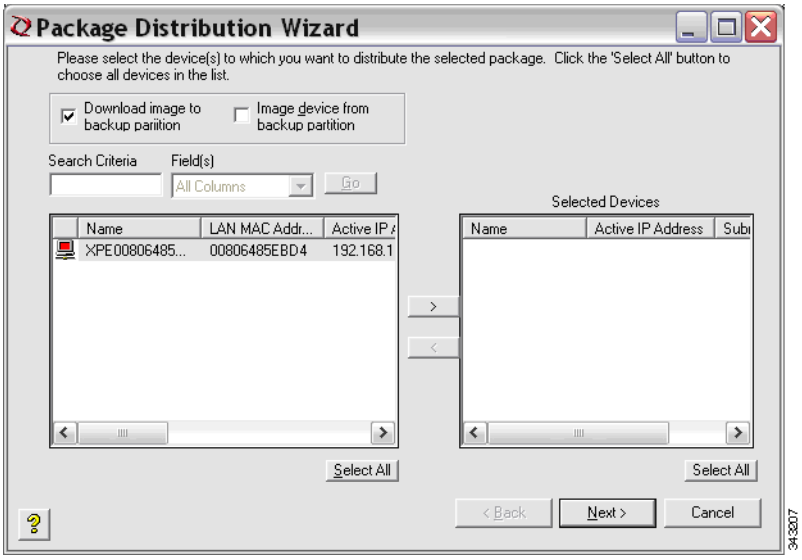
Step 1 Check the **Download image to backup partition** check box to download the image to the backup partition of the Autogenic Capable Device, and then click Next. The Package Distribution Wizard window appears with default values.

Step 2 Leave the default values and click **Next**.

Step 3 Choose either the PXE or Non-PXE option based on the device configuration, and then click **Next**.

Step 4 Click **Finish** to schedule the Autogenic Capable Image package to the Autogenic Capable Device.

Figure I-5 Package Distribution



Step 5 Note the following:

- The image download in the backup partition is now scheduled to the device.
- The scheduled image package now appears in the Update Manager View.
- After finishing the imaging task, the backup image now resides on the backup partition of the device.
- The image download will happen in the background at the device end. The device will only receive the QU to schedule the imaging task. The rest of the process will occur in background.

Step 6 You must now update the Cisco VXC Manager Agent to version 5.1.1.32 on the Autogenic Capable Device to support Autogenic Imaging.

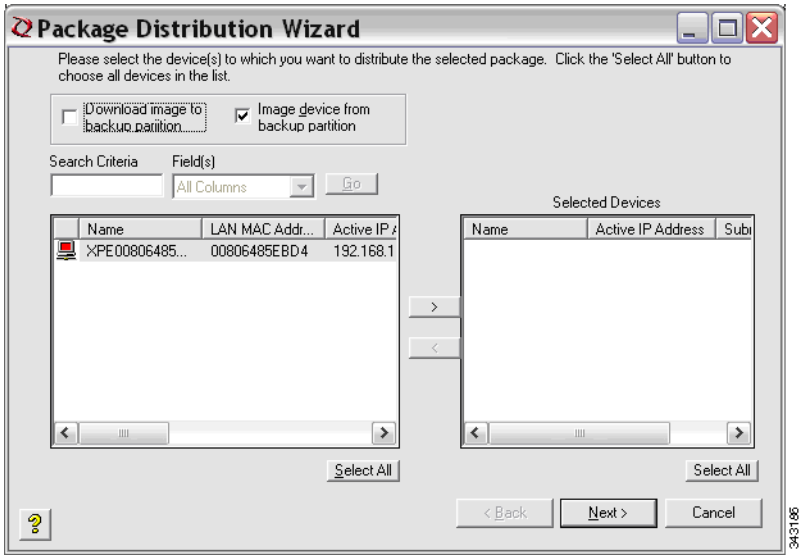
Step 7 After updating the Cisco VXC Manager Agent, go to **Device Manager View-> Network Info** tab to view the details of the backup partition.

Step 8 After downloading the Autogenic Capable Image to the backup partition of the Autogenic Capable Device, you can then schedule an imaging task (with the Autogenic Capable Image) to the Autogenic Capable Device containing the Autogenic Capable Image in the backup partition.

Caution Before scheduling the image task, be sure to change the Autogenic Capable Device boot order settings to boot from the disk first instead of the network.

Process 2: To schedule imaging the device from the backup partition:

Figure I-6 Image Device



Step 1 Choose the Image device from backup partition check box to image the Autogenic Capable Device from the backup partition of the device, and then click Next. The Package Distribution Wizard window appears with default values.

Step 2 Leave the default values and click Next.

Step 3 Choose the Non-PXE option, and then click Next.

Step 4 Click Finish to schedule the Autogenic Capable Image package to the Autogenic Capable Device.

Step 5 Note the following:

- The scheduled image package now appears in the Update Manager View.
- The Merlin Imaging Agent will start the imaging from the backup partition.

Step 6 After the imaging is complete, again update the Cisco VXC Manager Agent to version 5.1.1.32 on the Autogenic Capable Device to verify that the image version on the device is the correct image that appears in the backup partition details.

Case 2: Performing the Downloading and Imaging Processes Together

To download the image to the backup partition and schedule imaging the device from the backup partition:

Procedure

Step 1 Choose the Download image to backup partition and the Image device from backup partition check boxes to download the image to the backup partition of the Autogenic Capable Device and image the Autogenic Capable Device from the backup partition, and then click Next. The Package Distribution Wizard window appears with default values.

Step 2 Leave the default values and click Next.

Step 3 Choose either the PXE or Non-PXE option based on the device configuration, and then click Next.

Step 4 Click Finish to schedule the Autogenic Capable Image package to the Autogenic Capable Device. The Autogenic Capable Image will be downloaded to the backup partition of the Autogenic Capable Device and then (after the download is complete) the Autogenic Capable Device will be imaged from the backup image residing on the backup partition of the Autogenic Capable Device.

Step 5 After the imaging is complete, again update the Cisco VXC Manager Agent to version 5.1.1.32 on the Autogenic Capable Device to verify that the image version on the device is the correct image that appears in the backup partition details.

Autogenic Imaging Technical Details

Be aware of the following Update Manager and Cisco VXC Manager details.

Update Manager (Autogenic Imaging Technical Details)

When an Autogenic Image is scheduled to a device, a form must be designed to schedule the Autogenic Image.

Refer to the figures in Case 1: Performing the Downloading and Imaging Processes Separately, page I-5.

- When the Download image to backup partition check box is selected, the GUI will update the ComandArg table in the database with ArgID 9 and the value of the corresponding ArgID will be BI.
- When the Image device from backup partition check box is selected, the GUI will update the ComandArg table in the database with ArgID 9 and the value of the corresponding ArgID will be PI.
- When both Download image to backup partition and Image device from backup partition check boxes are selected, the GUI will add two entries in ComandArg table in the database with ArgID 9 and the corresponding values will be BI and PI.
- There are 2 commands that the HAgent can receive from HServer for Autogenic Imaging: BI and PI. The BI command is sent if the user wants to only download an image from the repository into the backup partition. The PI image is sent if the user wants to image the device by using the image already residing in the backup partition. The BI command only downloads the image into the backup partition, and upon completion, sends a V02 and does not reboot. If the PI command is encountered, then the HAgent loads the Merlin BA partition, copies the Grub_merlin file residing in the root folder to /Grub folder, and then renames the file to Grub.config. This is basically a process of ensuring that Merlin loads after devices reboot. After PI executes, the HAgent creates the Imagestatus.log file, enters Cmdid into it, and then reboots the device.

Cisco VXC Manager (Autogenic Imaging Technical Details)

Cisco VXC Manager expects the HAgent to check in with a flag

|SupportImgBackup = 1|BackupImagePresent=1|BackImageVer=XXXX|

Procedure

Step 1 The registered image contains a tag <BackupImage> to indicate that this image is for the Autogenic Imaging feature.

Step 2 If the devices do support Image Backup functionality, Cisco VXC Manager will offer user 2 choices:

- Back up the image: Just to back up the image.
- Image the active OS partition: Image the partition.

Step 3 Upon scheduling the image, the image script (RSP file) will have instructions:

- For the agent to download the image from the Master (or remote) repository to the backup partition.
- Change the grub.conf to instruct Merlin to image from the backup partition.
- Reboot the device.

Step 4 Cisco VXC Manager will specify the following commands for each of the operations specified above:

- BI command, just to copy the image from the repository onto the backup partition.
- PI command to initiate the imaging operation.
- Combination of both to indicate, backing up the image and starting the imaging operation.

Step 5 Upon reboot, the non-PXE Merlin agent comes up, reads the script file and completes the imaging task.

Step 6 After the imaging task is complete, the Merlin agent writes the status of imaging in the grub.conf file. The status will be read by the HAgent upon next boot.

Step 7 After reading the imaging status the HAgent sends a V02 to the server accordingly and deletes the status from the Grub.conf file.