CHAPTER 7

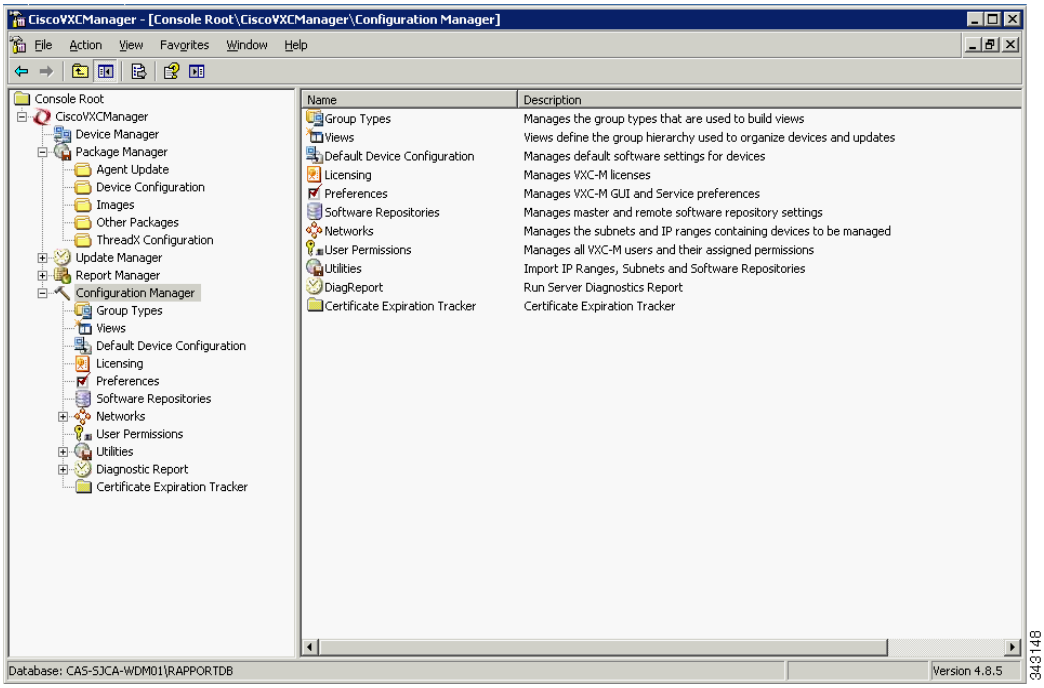
Configuration Manager

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

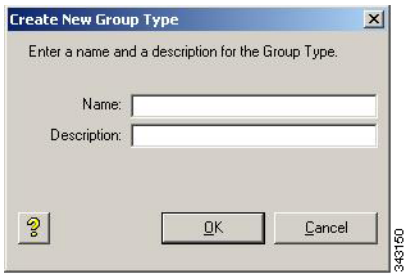
Creating Custom Group Types

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

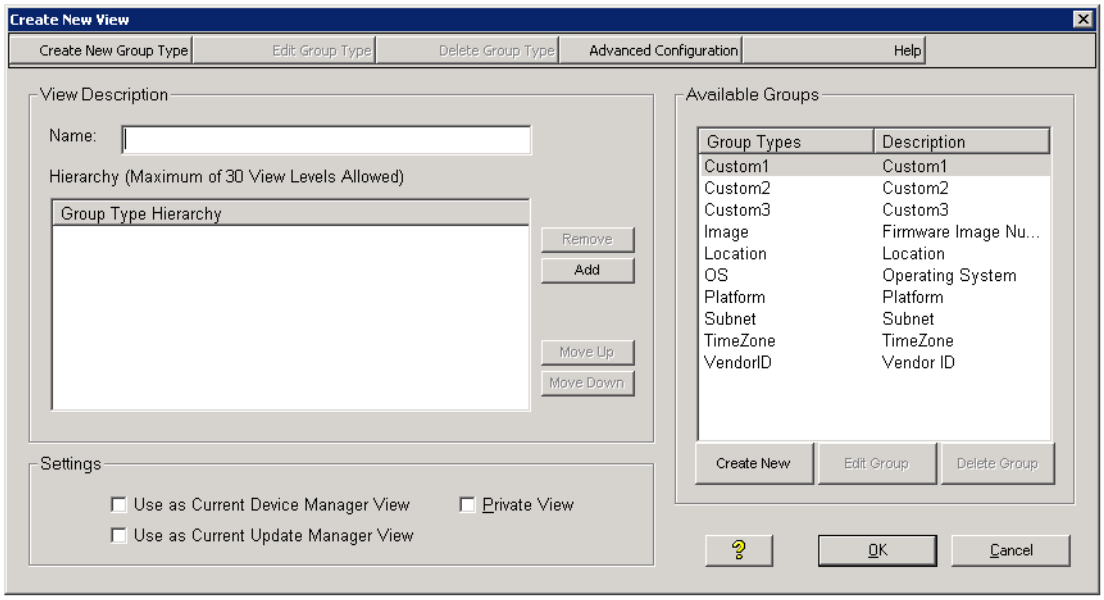
Use the following procedure to create views.

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).

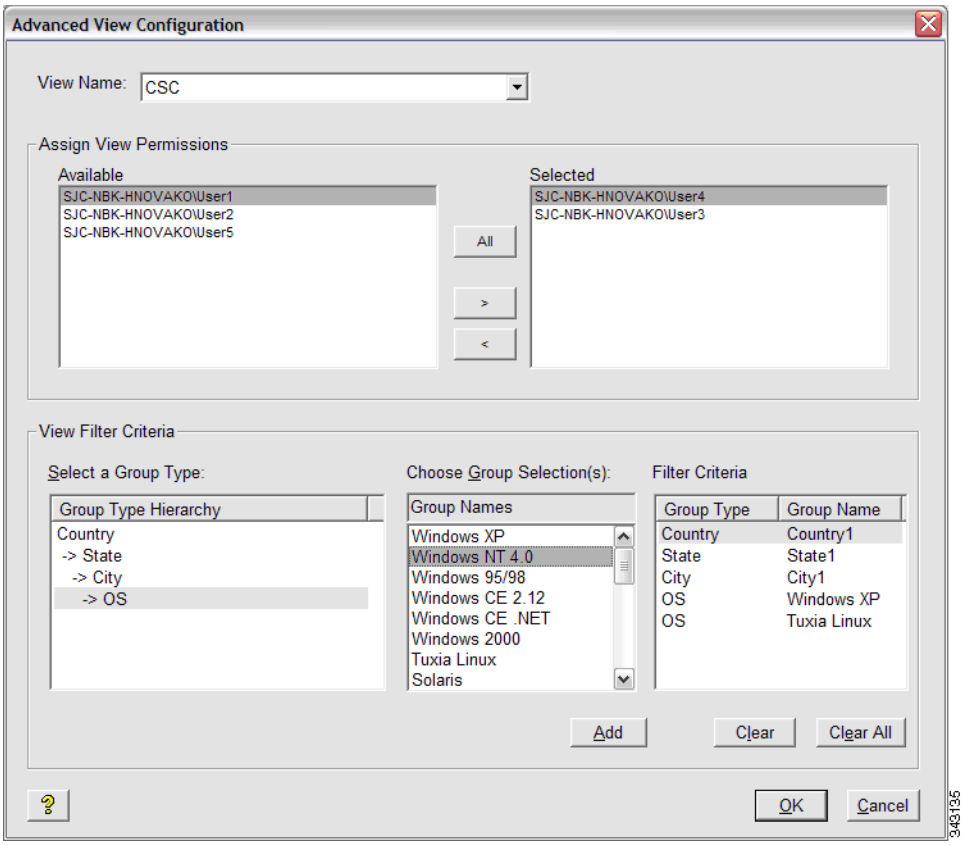
Using Advanced View Configuration Options

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**.

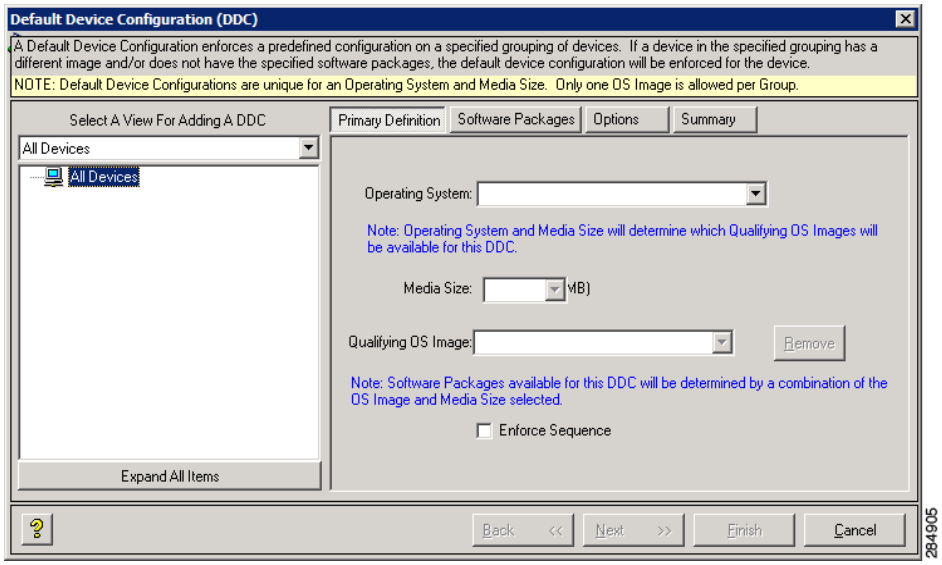
Creating and Assigning Default Device Configurations

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.

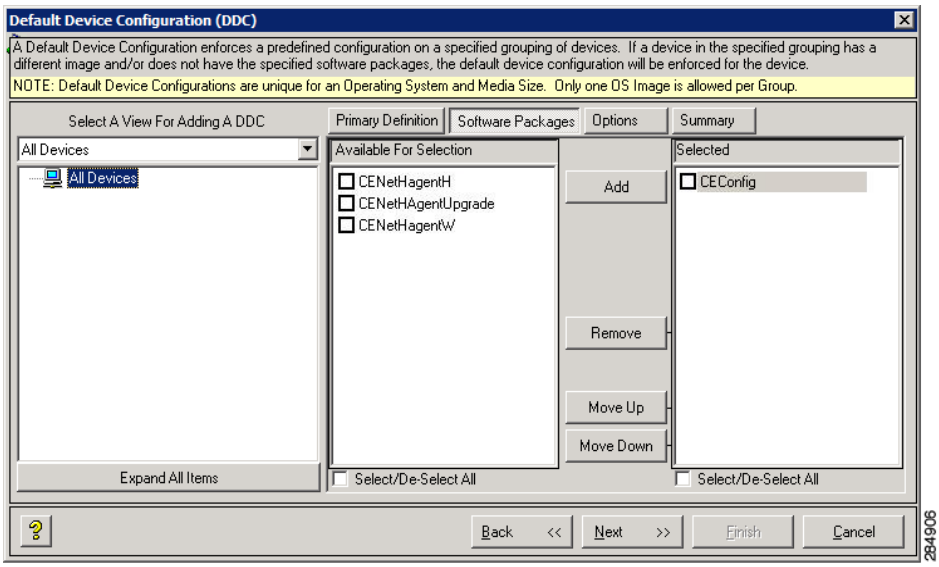
Tip You can assign different images and packages to different View folders.

- 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



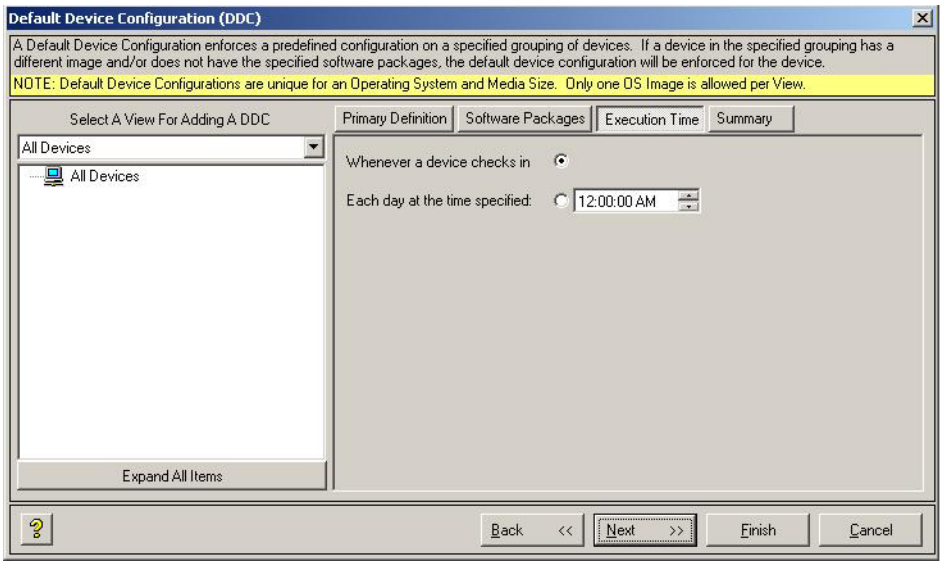
Step 4 Choose the Cisco VXC Manager packages in the Available For Selection list that you want to include in the DDC and click **Add** to move them to the Selected list.

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:

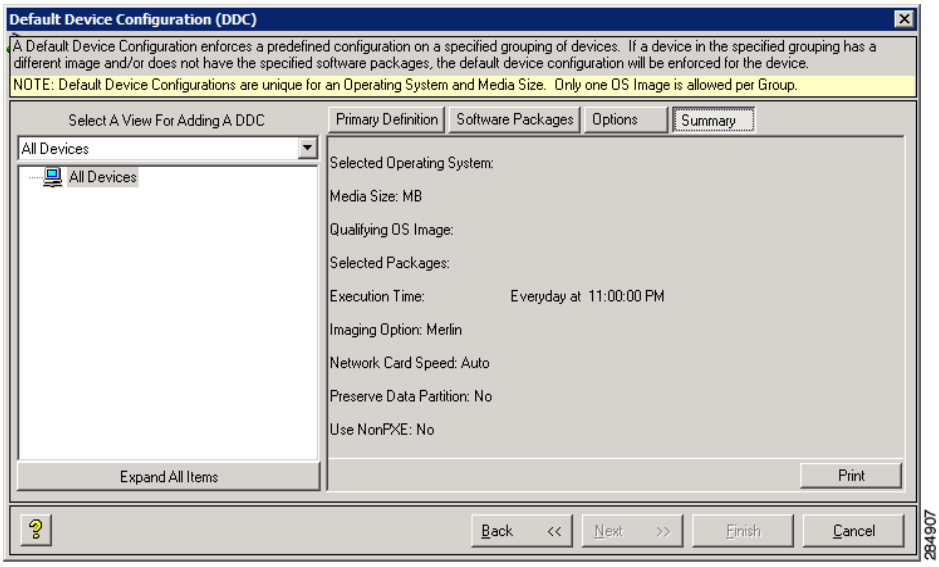
  Click either the **Whenever a device checks in** radio button or the **Each day at the time specified** radio button for DDC execution (if you click the **Each day at the time specified** radio button, be sure to enter or choose the time you want).

- 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

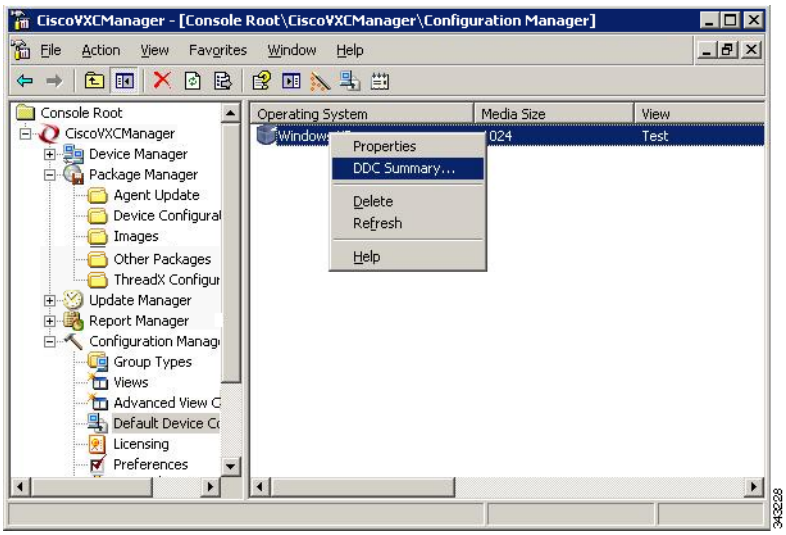
Use the following procedure to view the summary of a Default Device Configuration.

Procedure

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

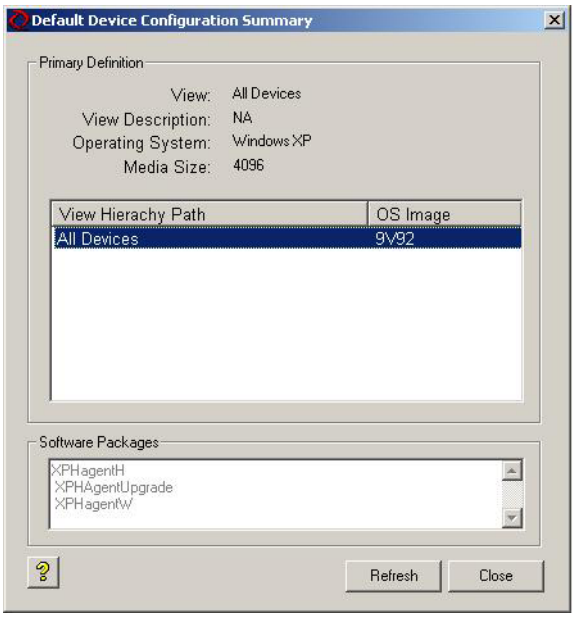
Step 2 Right-click the DDC for which you want to see the summary and choose **DDC Summary**.

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.

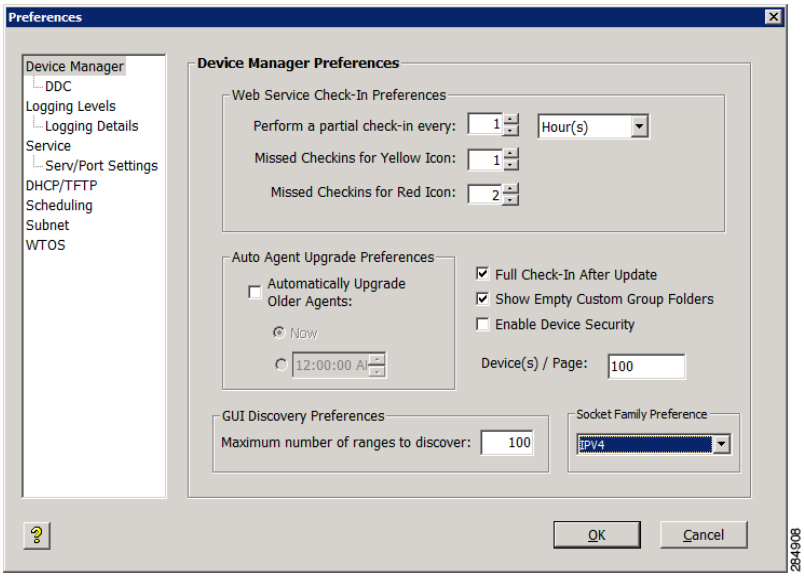
Step 3 Depending on the preferences you want to configure, refer to the following:

- 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

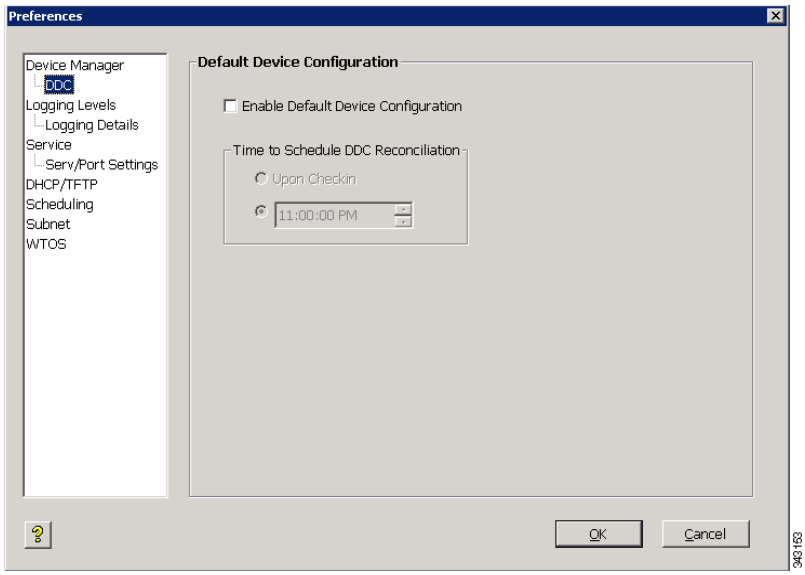


Use the following guidelines:

- 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



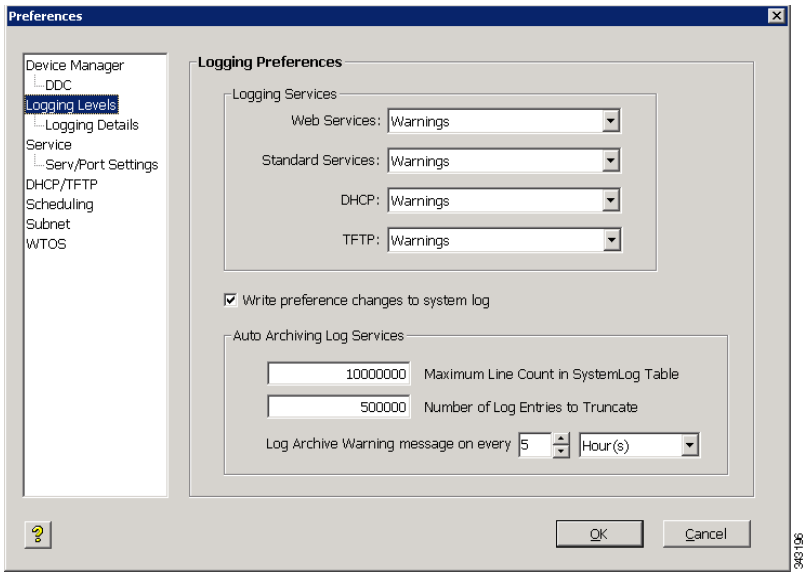
Use the following guidelines:

- 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:

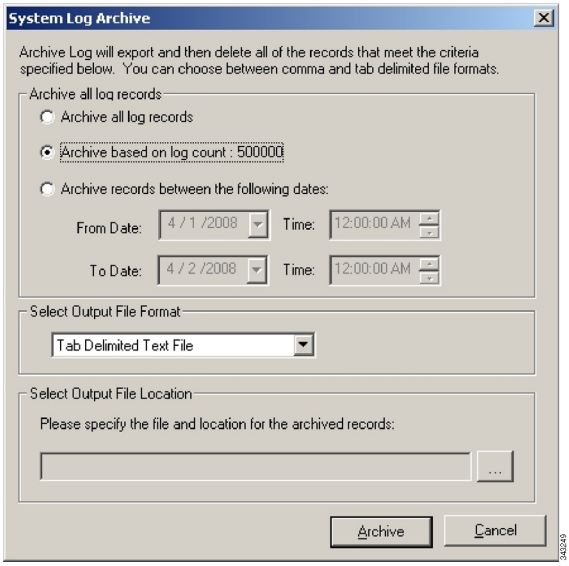
- Logging Services area—Choose the logging level for each of the communication protocols. Options include:
  - Errors—Consisting of simple error messages.
  - Warning—Consisting of warnings in addition to error messages (this is the default option).
  - Informational—Consisting of other information items 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).

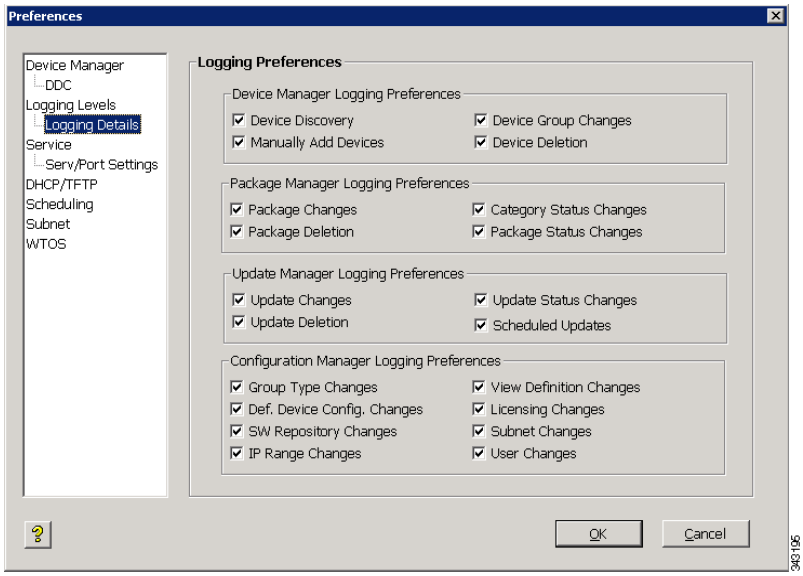
Figure 7-14 System Log Archive Window



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

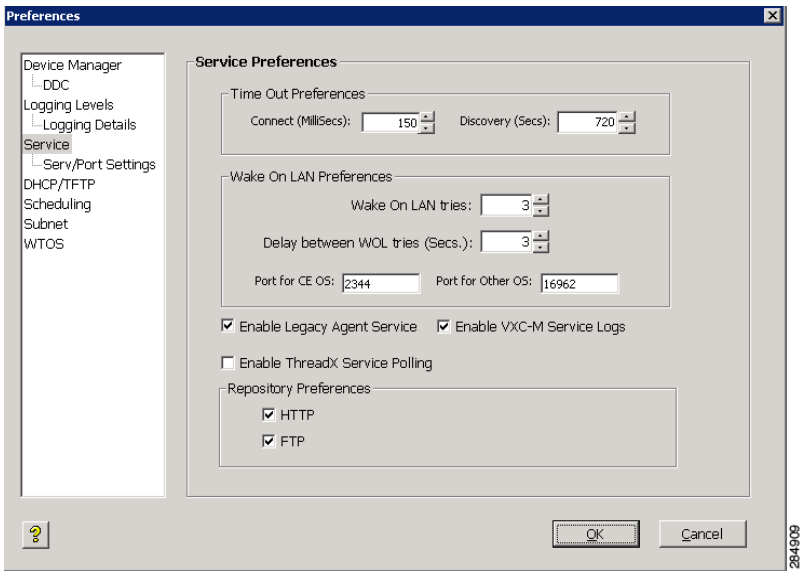


Tip Category Status Changes refers to whether a Cisco VXC Manager package changed from one category to another (for example, if you edit the script file for a Cisco VXC Manager package and change it from Image to Client Configuration), while Package Status Changes refers to whether a package changes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

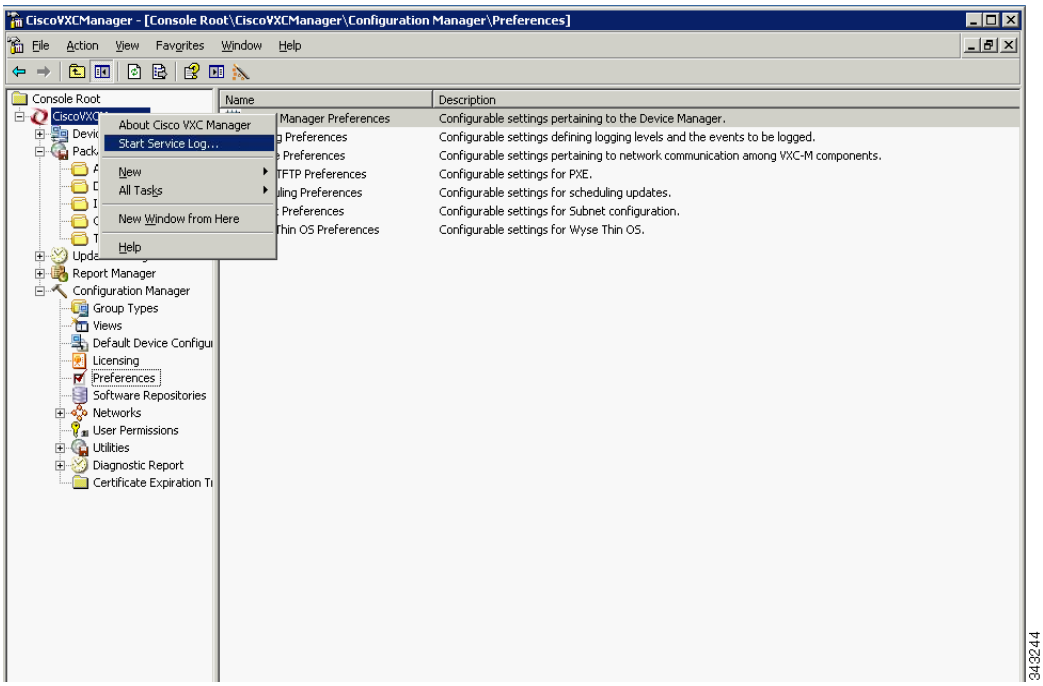


Figure 7-18 Stop Service Log

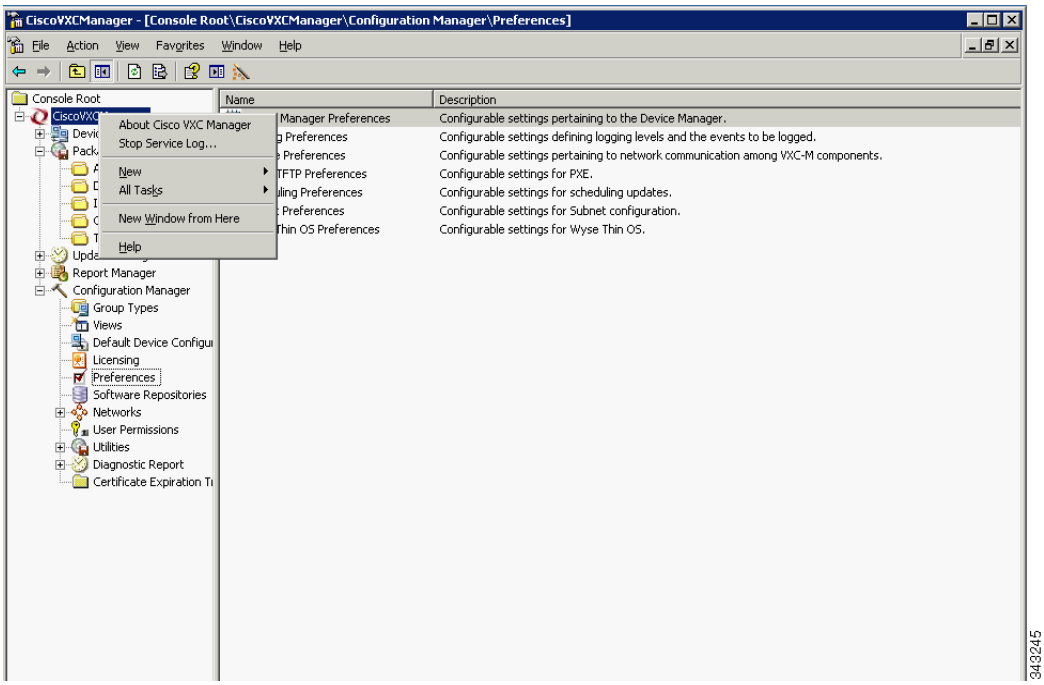


Table 7-1 Protocol Used to Register Cisco VXC Manager Packages to Master Software Repository

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

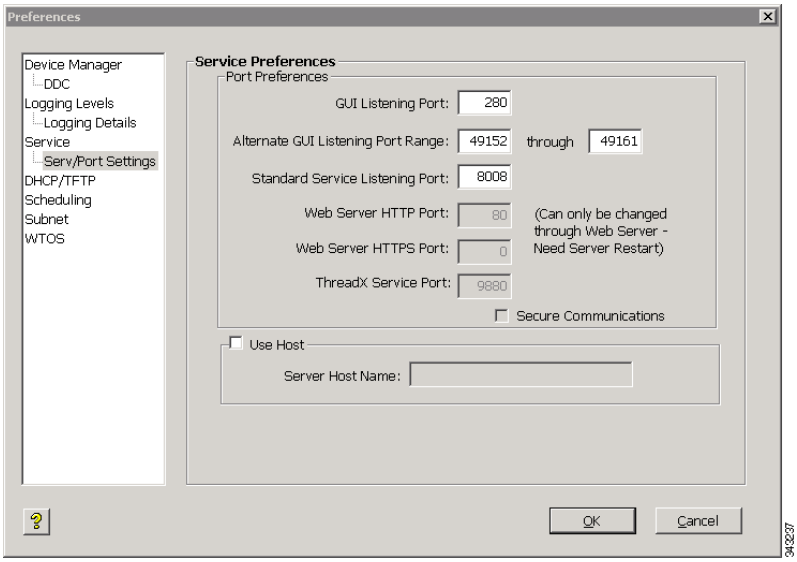
Global Repository Preference Setting	Preference Setting for Repository Used by Client	Protocol Used to Transfer Package
HTTP	FTP	HAgent on client device uses Master HTTP(S) repository only
HTTP	HTTP(S) and FTP	HAgent on client device uses assigned HTTP(S) repository only
FTP	FTP	HAgent on client device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

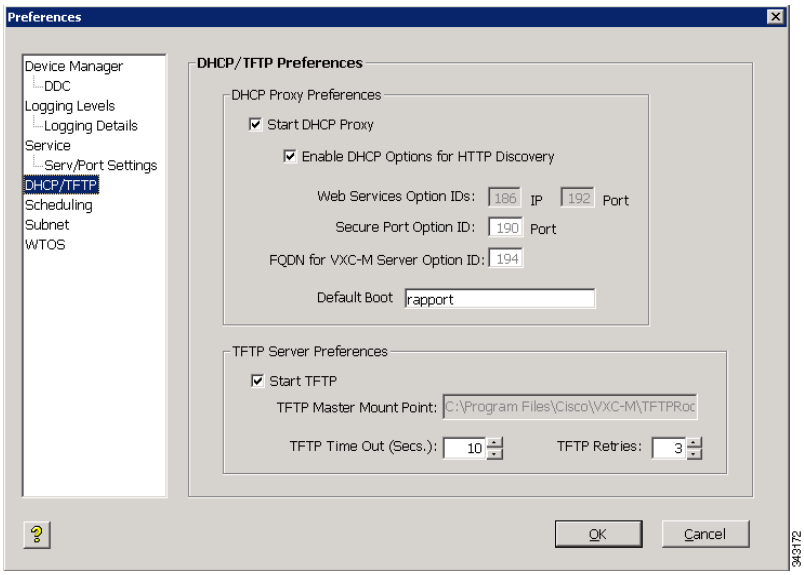
- **ThreadX Service Port**—Port Cisco VXC Manager uses to issue real-time commands (such as Quick Device Commands or device updates at a specific time). Normally this is port 9880. Note that you can change this port only through your Web Server.
- **Secure Communications**—This is a read-only box that 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:

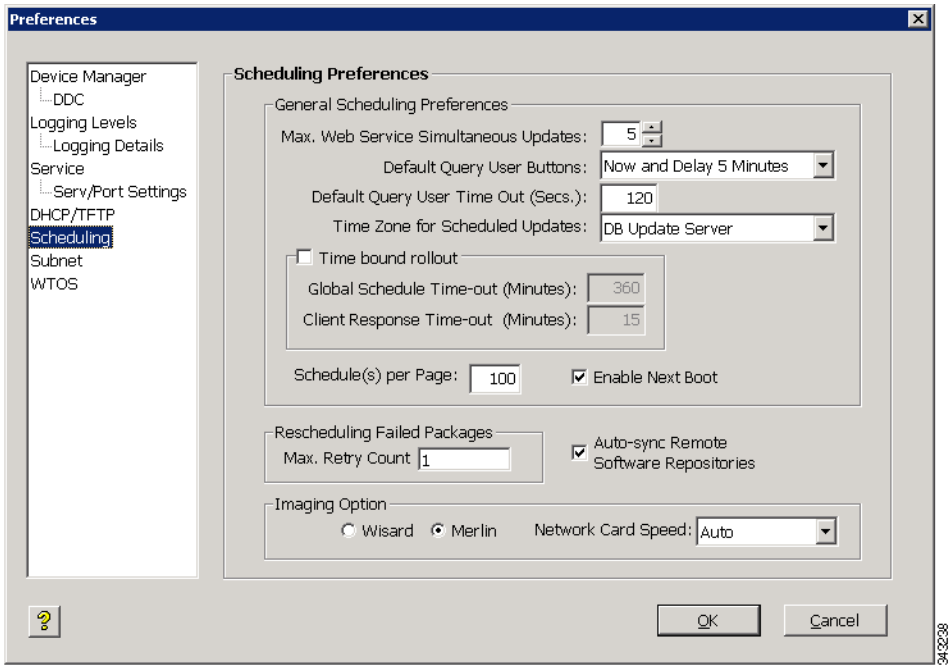
- DHCP Proxy Preferences area:

  - 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.

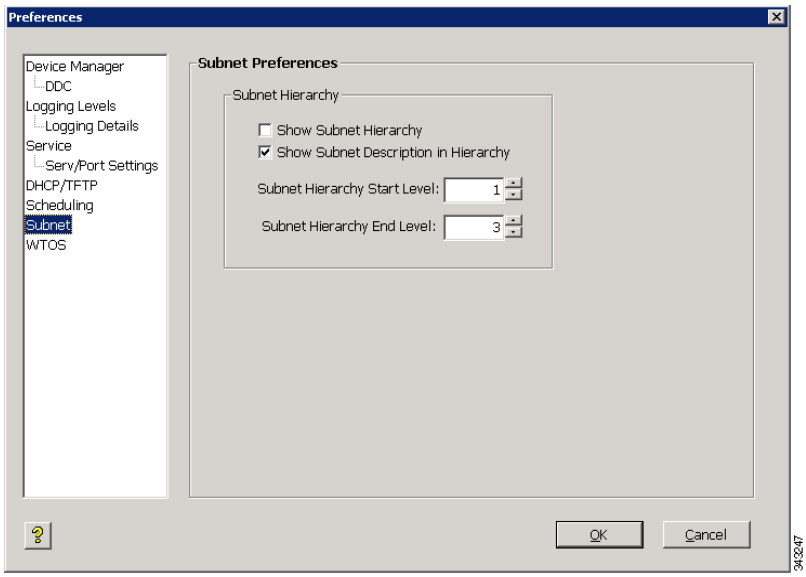
    - Client Response Time-out (Minutes)—Specify the time period for which the Cisco VXC Manager server will wait for the client to check in after Cisco VXC Manager has successfully sent the notification to the client.

- 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:

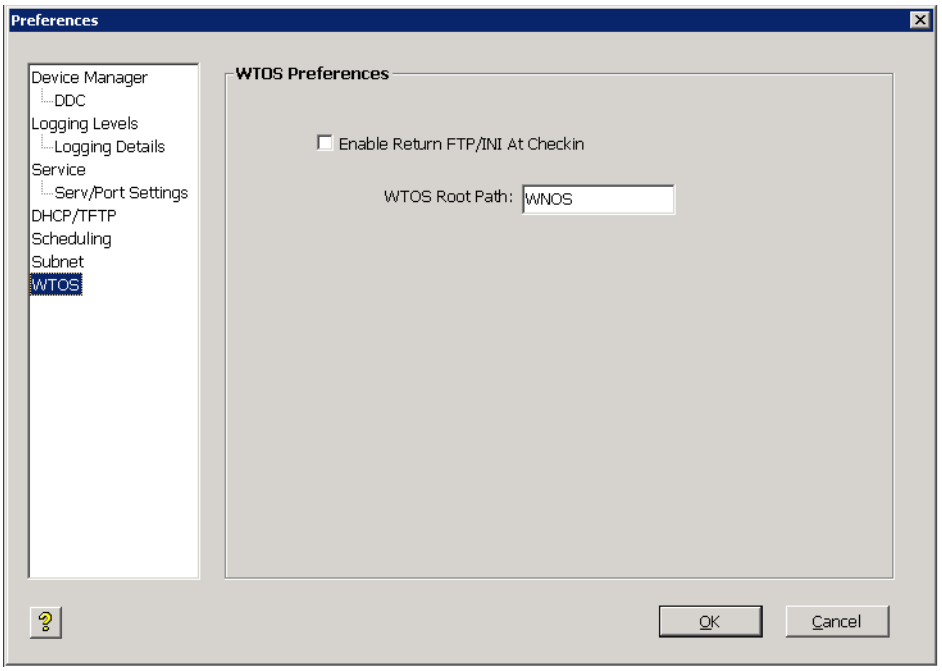
- Show Subnet Hierarchy—Check this check box to allow any subnet views to include the hierarchical view of the subnet.
- Show Subnet Description in Hierarchy—Check this check box to display hierarchical subnet views by the descriptions of the subnets rather than by their address. Note that the default 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

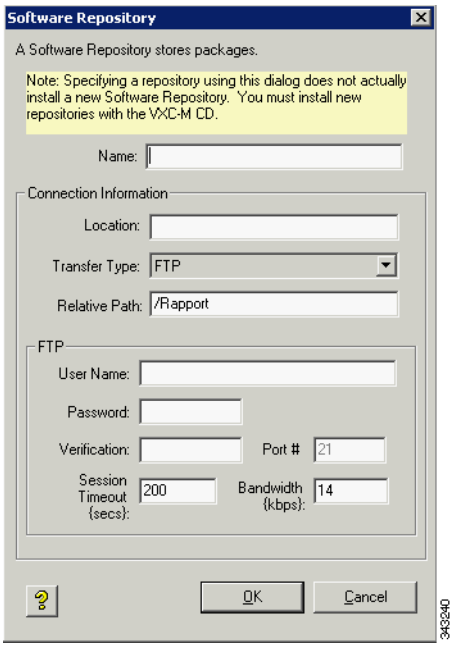
After installing an additional Remote Software Repository, you must register it in the Cisco VXC Manager Database and then assign the Remote Software Repository to a subnet.

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:

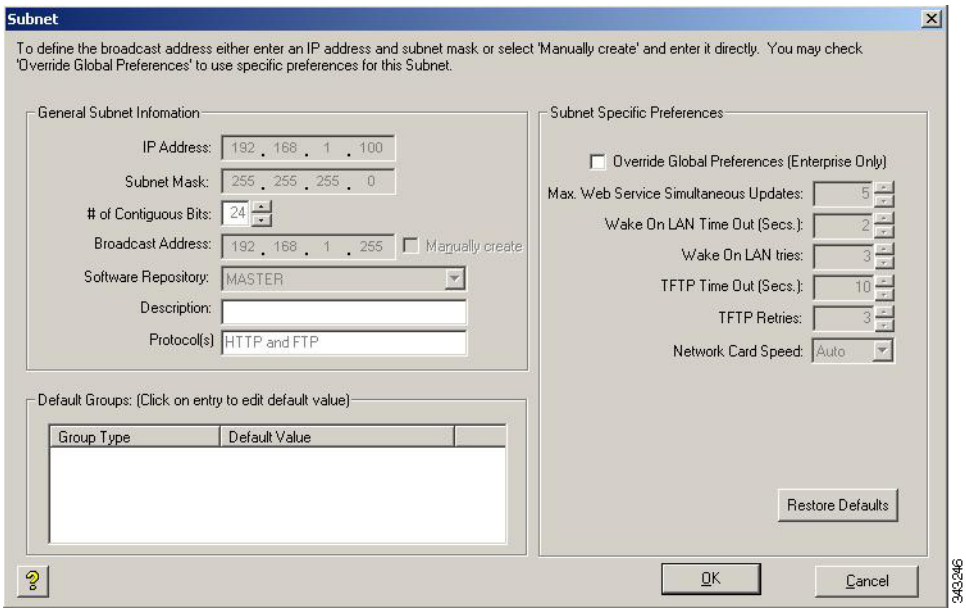
Adding Subnets to Cisco VXC Manager Manually

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:

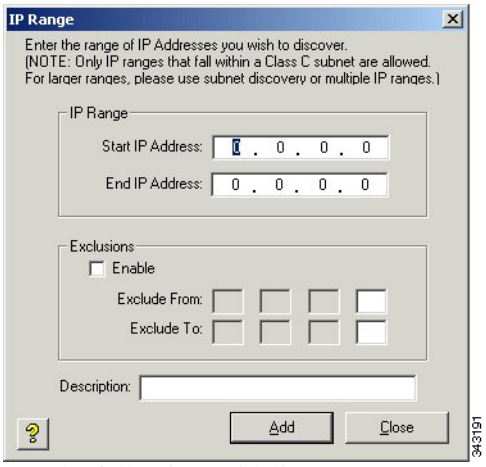
Adding IP Ranges to Cisco VXC Manager Manually

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

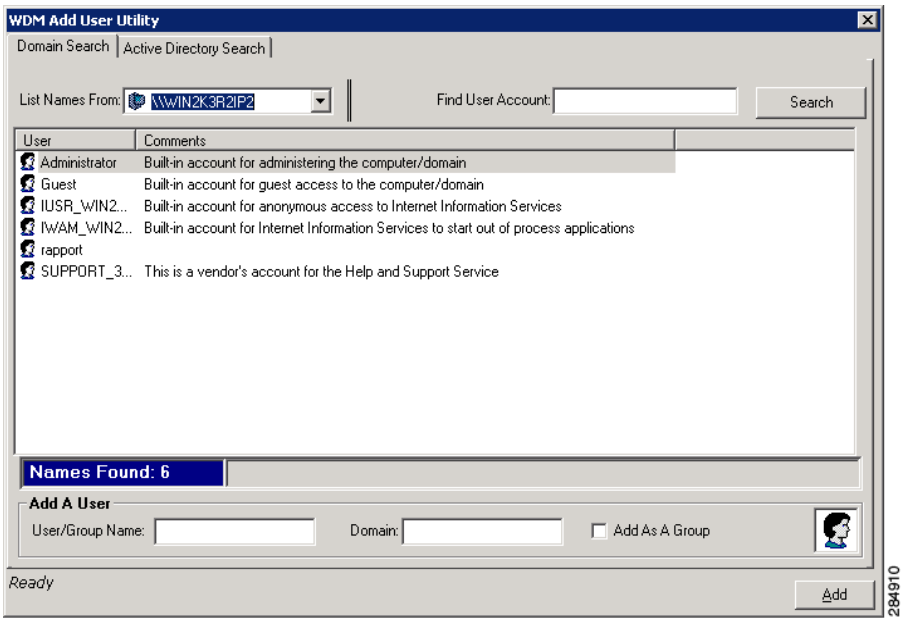
Use the following procedure to add users from local computer accounts.

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

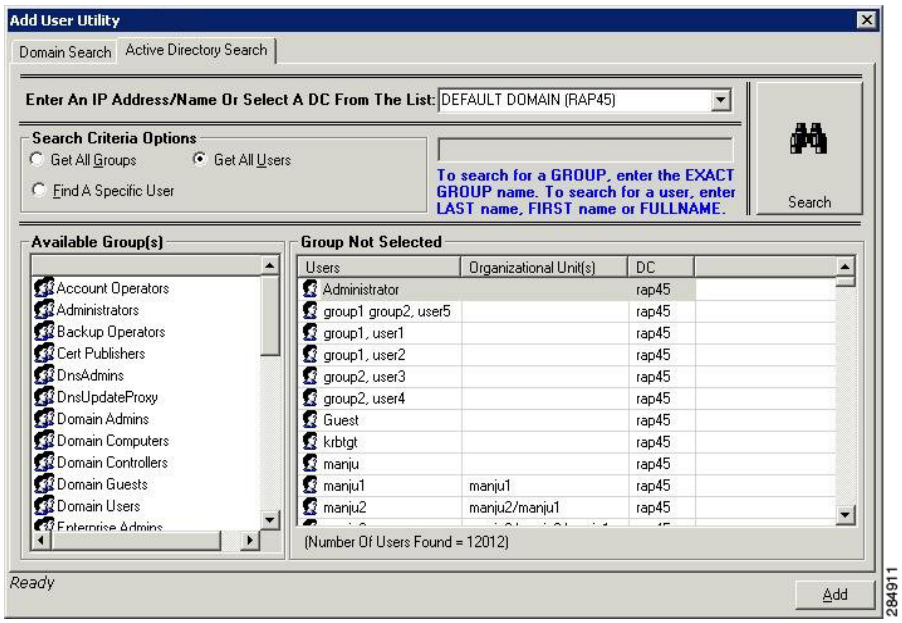
Use the following procedure to add users and groups from Active Directory.

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.

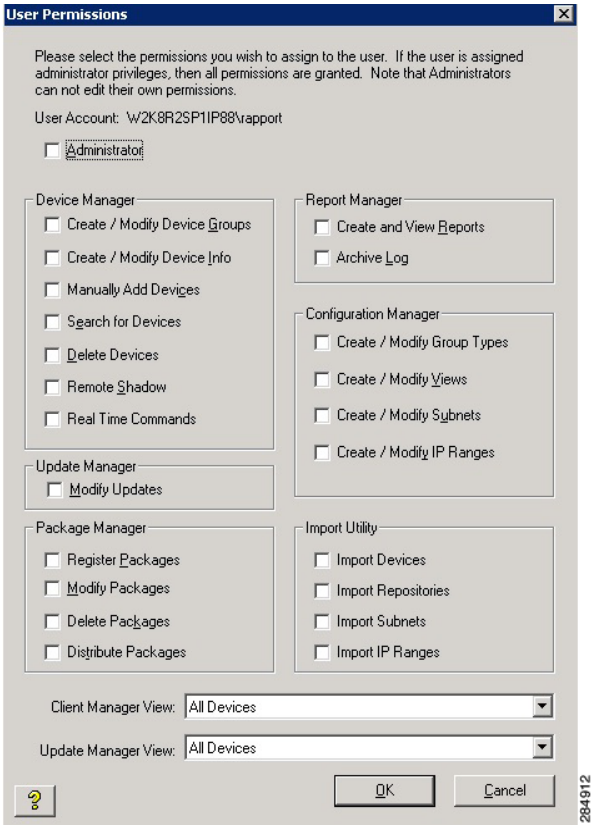
Tip You cannot edit your own user permissions.

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

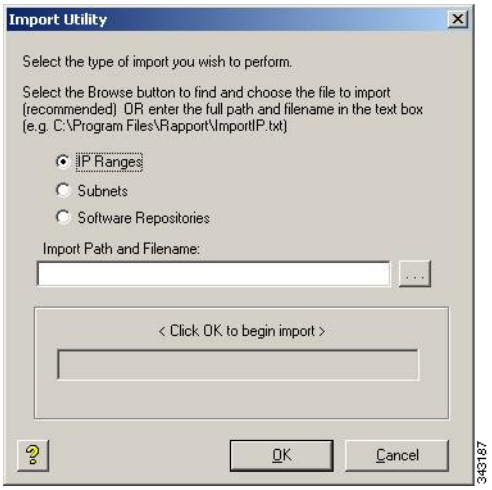
With Cisco VXC Manager, you can import IP Range data from comma-delimited and tab-delimited files into the Cisco VXC Manager Database.

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.

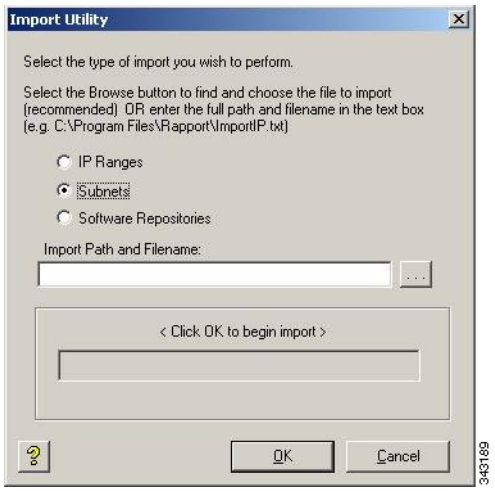
Tip For Remote Software Repositories, your Cisco VXC Manager Database must contain information about at least one Remote Software Repository before you can work with subnets (see Managing Software Repositories, page 7-87).

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

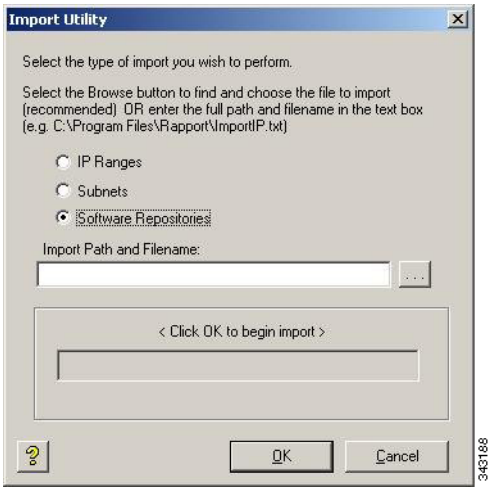
With Cisco VXC Manager, you can import Remote Software Repository data from comma-delimited and tab-delimited files into the Cisco VXC Manager Database.

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

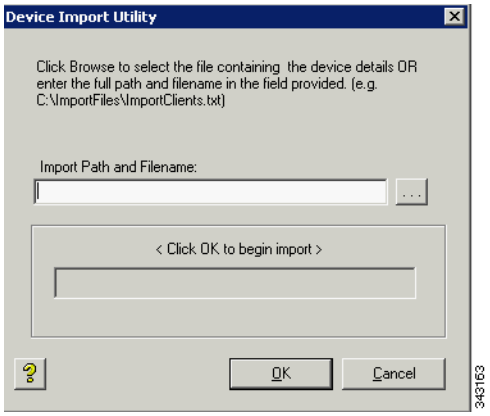
With Cisco VXC Manager, you can import Device Settings data from comma-delimited and tab-delimited files into the Cisco VXC Manager Database.

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

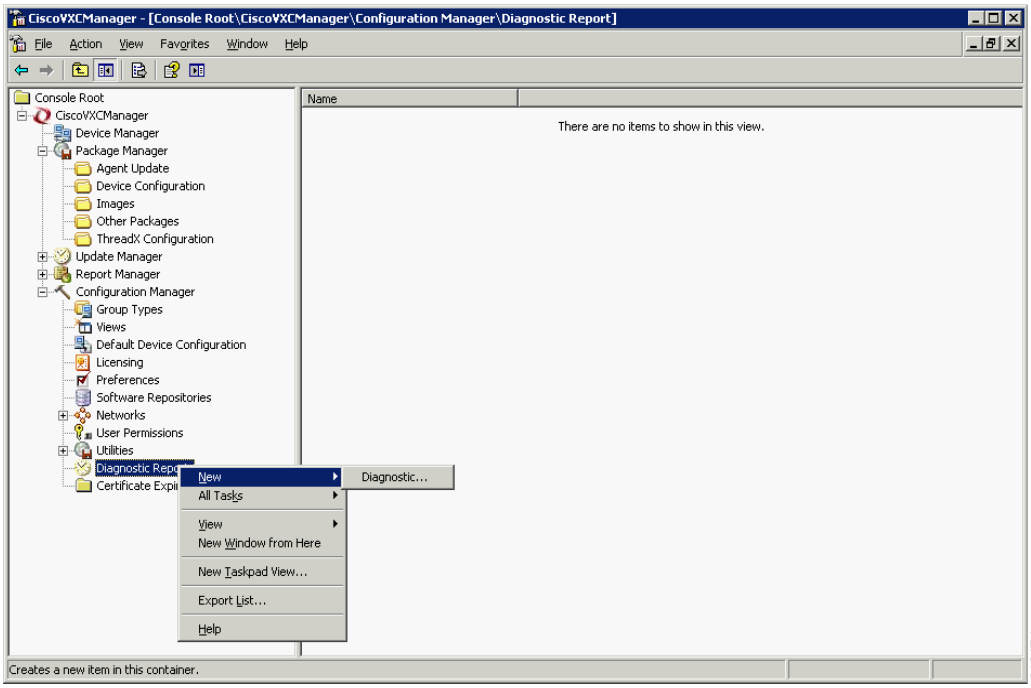
Generating Diagnostic Reports

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



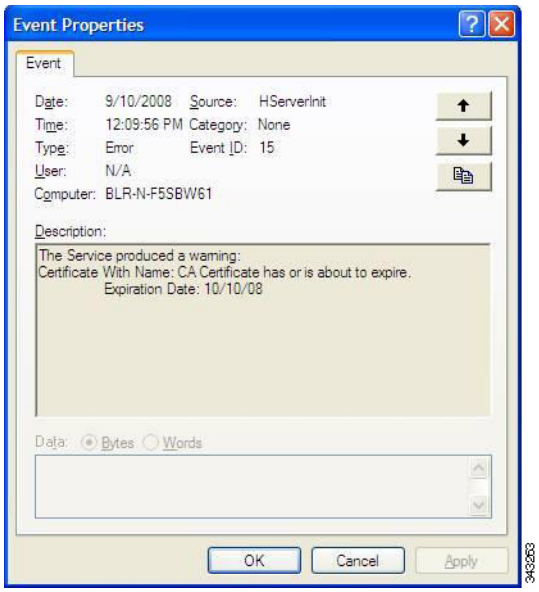
A Diagnostic Report of the Cisco VXC Manager system includes the following sections:

- 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

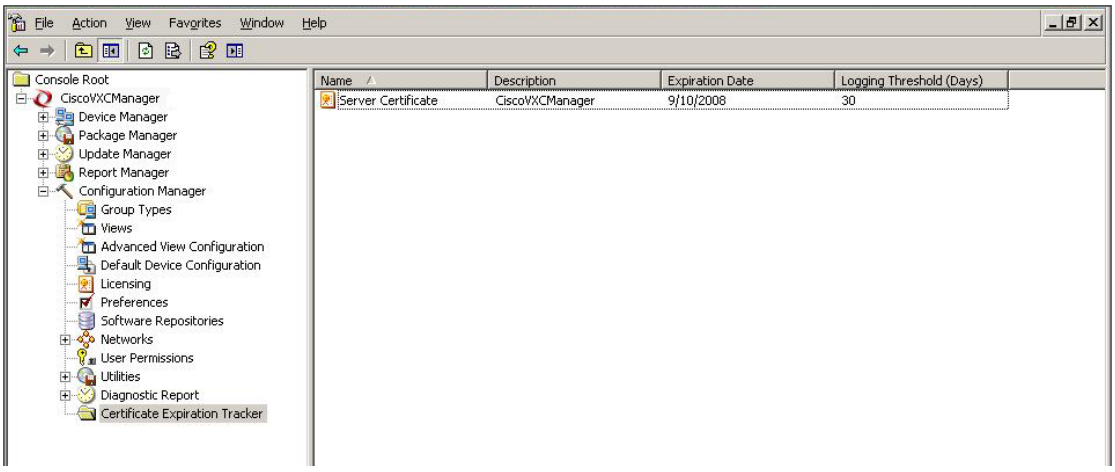


Tip For information on licensing and certificates, see Licensing and Sales Keys, page F-1.

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.

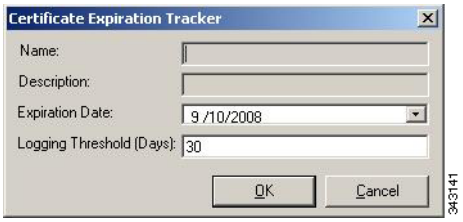
Figure 7-36 Certificate Expiration Tracker



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.