CHAPTER 4

Discovering Network Devices

The following topics tell you how to add the network devices that you want to monitor to Cisco Prime Performance Manager:

- Device Discovery Requirements, page 4-1
- Importing Prime Network Device Inventories, page 4-2
- Managing Network Discovery, page 4-5

Device Discovery Requirements

Before you begin device discovery, review the devices that Prime Performance Manager officially supports. These can be found at:

http://www.cisco.com/en/US/products/ps11715/products_device_support_tables_list.html

In addition, the Devices Readme, available from the Prime Performance Manager GUI Home page, lists the known devices and software versions that have been used by customers and Cisco labs during testing and deployments. While these devices are not formally supported, informal experience indicates they can be used successfully with Prime Performance Manager.

To produce network reports, Prime Performance Manager accesses the devices, determines their capabilities, and begins the reporting process. Before this can occur, devices must be discovered and assigned to units. The units connect to the devices using the required SNMP or Telnet and SSH credentials.

Device discovery is accomplished using one or both of the following methods:

- Import the device inventory from Cisco Prime Network or Cisco Active Network Abstraction (ANA).
- Run device discovery from Prime Performance Manager. This can be done from the Administration > Discovery tab in the GUI, or by running the ppm discovery command on the CLI.

To discover a device, the following information is required:

- The device IP address or hostname.
- The SNMP credentials authorizing Prime Performance Manager to access the device SNMP engine. SNMP V2 requires a community string. SNMP V3 requires a combination of username, authorization algorithm, authorization pass phrase, privacy algorithm, and privacy pass phrase, depending on the device configuration.
- If ITU-T Y.1731 reports are enabled, Telnet or SSH credentials are required. The number of credentials and their content depend on the device configuration.

If you import the device inventory from Cisco Prime Network, Prime Performance Manager gets the device IP addresses and SNMP, Telnet, and SSH credentials from the Prime Network. If you run device discovery from Prime Performance Manager, you must add the SNMP, Telnet, or SSH credentials to Prime Performance Manager before you run the device discovery.

Importing Prime Network Device Inventories

To import a Prime Network or Cisco ANA device inventory, Prime Performance Manager connects to the Prime Network gateway and retrieves the Prime Network device IP addresses and SNMP, Telnet, or SSH credentials. All devices are retrieved except those whose VNEs are in Maintenance investigation state, or the VNE is ICMP or a cloud VNE. Prime Performance Manager then connects to the devices and probes them for supported MIBs. The MIBs are used to generate reports.

After the device connections are established and MIB profiles created, Prime Performance Manager maintains communication with the Prime Network gateway. If new Prime Network devices are added, Prime Performance Manager devices are updated with the new devices. If a Prime Network device VNE goes into Maintenance state, Prime Performance Manager changes the device to unmanaged stops polling. When the VNE state changes, Prime Performance Manager changes the device state and begins polling.

When you import Prime Network devices, you have the option to enable strict synchronization. Enabling strict synchronization restricts Prime Performance Manager to Prime Network devices; you cannot discover or manage devices that reside outside of Prime Network. Additionally, you cannot edit SNMP, Telnet, or SSH entries and you cannot edit device names. If strict synchronization is not enabled, all device discovery and SNMP, Telnet, or SSH device editing capabilities remain enabled. Strict synchronization is useful when you want a tight relationship between Prime Performance Manager and Prime Network to ensure all reports are Prime Network device reports.

To import Prime Network devices, you need the following Prime Network gateway information:

- IP address or hostname
- Port.
- Prime Network administrator or configurator username and password. The user must have a device scope set for all network elements.

Complete the following steps to import the device inventory from Cisco Prime Network or Cisco ANA using the Prime Performance Manager GUI. This procedure requires a Level 5 (administrator) user level.

Note You can use the ppm inventoryimport command to import Prime Network device information from Prime Network using the CLI. For information, see ppm inventoryimport, page B-25.

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 On the navigation tree, click **Administrative**.

Step 3 On the Administrative window click the **Prime Network** tab.

Step 4 In the Prime Network window, enter the following information:

- Host Name or IP Address—Enter the Prime Network gateway hostname or IP address.
- Port—Enter the Prime Network gateway port. The default Cisco Prime Network web services port is 9003. The Port field accepts values from 1 to 65535.
- User Name—Enter the Prime Network gateway administrator or configurator username.

- Password—Enter the Prime Network user password.
- Strict Sync—Check this box if you want Prime Performance Manager to monitor only Prime Network devices. If you check Strict Sync, Prime Performance Manager cannot connect to devices that haven't been added to Prime Network first, and certain functionality is disabled, including the Discovery tab and the ability to edit SNMP, Telnet, and SSH entries.

Step 5 From the Prime Network toolbar, click the **Import Inventory** tool.

The Prime Network device inventory import proceeds.

Step 6 After it completes, go to the Prime Performance Manager navigation tree and click the **Devices** summary list to review the devices that were added. For information about using the Devices summary lists, see **Using the Devices Summary List, page 8-1.**

Enabling Prime Performance Manager Cross-Launches from Prime Network

In addition to Prime Network device inventory imports, you can enable cross launching so that Prime Network users can launch Prime Performance Manager from Prime Network Vision objects.

Complete the following steps to enable Prime Performance Manager cross-launches from Prime Network:

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 On the navigation tree, click **Administrative**.

Step 3 On the Administrative window click the **Prime Network** tab.

Step 4 From the Prime Network toolbar, click the **Install Cross Launch** tool.

Running Device Discovery from Prime Performance Manager

You can discover network devices by running discovery from Prime Performance Manager. Use this discovery approach when:

- You are not running Prime Network or do not wish to enable reports on Prime Network devices.
- You imported Prime Network devices but did not enable strict synchronization. In this case, you can run device discovery from Prime Performance Manager to add devices not in the Prime Network inventory.

Before you run device discovery from Prime Performance Manager, you must add the SNMP credentials. See Adding SNMP Credentials, page 4-4. If you are enabling ITU-T Y.1731 reports, you must set up the Telnet and SSH credentials. See Adding Telnet and SSH Credentials, page 16-1.

Adding SNMP Credentials

Complete the following steps to add the SNMP credentials required for communication with discovered network devices.

Note You can use the ppm addsnmpcomm command to add SNMP community strings using the CLI. For information, see ppm addsnmpcomm, page B-5.

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 On the navigation tree, click **Administrative**.

Step 3 On the Administrative window, click the **SNMP** tab.

Step 4 From the SNMP Editor toolbar, click the **Add a New SNMP Entry** tool.

Step 5 In the Add SNMP Entry dialog box, enter the following information:

- IP Address Range or Hostname—Enter the device IP address or DNS name, or range of devices. An asterisk (*) indicates a wildcard value.
- Read Community—Enter the SNMP community name used by the device for read access to the information maintained by the SNMP agent on the device.
- Username (v3)—Enter the username (SNMP v3).
- Authorization Algorithm (v3)—Enter the authorization algorithm (SNMP v3):
  - md5—Uses the Hash-based Message Authentication Code (HMAC) MD5 algorithm for authentication
  - sha—Uses the HMAC SHA algorithm for authentication
- Authorization Passphrase (v3)—Enter the authorization passphrase (SNMP v3),
- Privacy Algorithm (v3)—Enter the privacy algorithm (SNMP v3):
  - 3des—Uses Data Encryption Standard (DES) v3.
  - des—Uses the Data Encryption Standard (DES).
  - aes128—Uses Advanced Encryption Standard (AES) 128-bit encryption.
- Privacy Passphrase (v3)—Enter the privacy algorithm (SNMP v3).

Step 6 Click **OK**.

Step 7 On the SNMP Editor toolbar, click **Save All SNMP Entries**.

Editing SNMP Credentials

Complete the following steps to edit the SNMP credentials required for communication with discovered network devices.

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 On the navigation tree, click **Administrative**.

Step 3 On the Administrative window, click the **SNMP** tab.

Step 4 In the SNMP table, edit any of the following SNMP parameters. See Adding SNMP Credentials, page 4-4, for parameter descriptions.

- IP Address Range or Hostname
- Read Community
- Username (v3)
- Authorization Algorithm (v3):
  - md5
  - sha
- Authorization Passphrase (v3)
- Privacy Algorithm (v3):
  - 3des
  - des
  - aes128
- Privacy Passphrase (v3)

Step 5 When finished, on the SNMP Editor toolbar, click **Save All SNMP Entries**.

Deleting SNMP Credentials

Complete the following steps to delete the SNMP credentials from Prime Performance Manager.

Step 1 Log into the Prime Performance Manager GUI as an administrator (Level 5) user.

Step 2 On the navigation tree, click **Administrative**.

Step 3 On the Administrative window, click the **SNMP** tab.

Step 4 Select the SNMP credential table row that you want to remove, then under the Action column, click Delete this Entry.

Step 5 When finished, on the SNMP Editor toolbar, click **Save All SNMP Entries**.

Managing Network Discovery

The Prime Performance Manager web interface Discovery tab allows you to discover the network. To view the Discovery tab information, click **Administrative** in the navigation tree and then click **Discovery** in the right pane. Table 4-1 lists the Discovery window options.

Table 4-1 Discovery Network Window Options

Option	Tool	Description
Load Seeds	📁	Opens Load File Dialog Window window, enabling you to load a seed file into Prime Performance Manager.
Save Seeds	💾	Saves the changes you have made to the chosen seed file.
Save As	📝	Opens the Save File Dialog Box, using which you can save the updated seed file with a new name, or overwrite an existing seed file.
Discover Network	—	Begins network discovery. If you have not defined at least one seed device in the Seed Settings tab, Prime Performance Manager prompts you to do so. When Discovery begins: • The **Discover Network** button changes to **Stop Discovery**. • The `Discovery In Progress` message appears in the title bar of all Prime Performance Manager client windows. Discovery progresses in bursts. You might see a number of updates, followed by a pause, followed by more updates. The information that Prime Performance Manager windows displays, is not fully updated until Discovery is complete. By default, Discovery times out after 600 seconds (10 minutes). To change the Discovery timeout, change the value of the DISCOVERY_TIMELIMIT entry in the Server.properties file: • If you installed Prime Performance Manager in the default directory, /opt, then the location of the Server.properties file is /opt/CSCOppm-gw/properties/Server.properties. • If you installed Prime Performance Manager in a different directory, then the Server.properties file resides in that directory. Because Prime Performance Manager is asynchronous, with the Prime Performance Manager server contacting clients one at a time, and because clients might run at different speeds, the information that Prime Performance Manager clients display during Discovery might not always be synchronized. All other Prime Performance Manager windows (Device) are also populated with the newly discovered network data.

Load File Dialog Window

Table 4-2 lists the options and information provided in the Load File window.

Table 4-2 Load File Dialog Box

Field or Button	Description
Seed File List	Seed File List pane information and options include: • Go up one Folder—Click this icon to go up one folder in the directory structure. • Type—Icon indicating whether the item in the table is a file or a folder. • Name—Name of the seed file or folder. • Last Modified—Date and time the seed file or folder was last modified. • Size (bytes)—Size of the seed file or folder, in bytes.

Table 4-2 Load File Dialog Box (continued)

Field or Button	Description
Make this my preferred startup	Specifies whether the chosen seed file should be loaded automatically whenever this Prime Performance Manager client is started or the Discovery dialog box is opened. By default, this option is not selected for all seed files. That is, no seed file is loaded automatically when Prime Performance Manager client is started or the Discovery dialog box is opened.
OK	Loads the chosen seed file, saves any changes you made to the list of files, and closes the dialog box. To load a seed file: • Double-click it in the list, select it in the list and click **OK**, Or • Enter the name of the file and click **OK**. Prime Performance Manager saves any changes you made to the list of files, closes the Load File Dialog: Seed File List dialog box, loads the seed file, and returns to the Discovery dialog box. Prime Performance Manager lists all of the seed devices in the seed file in the Seed Devices pane, and displays details of the SNMP settings for the seed devices in the Seed Details pane.
Delete	Deletes the chosen file from the seed file list. Prime Performance Manager displays an informational message containing the name and location of the deleted file.
Cancel	Closes the dialog box without loading a seed file or saving any changes to the seed file list.

Save File Dialog Box

Table 4-3 lists information and options provided in the Save File dialog box.

Table 4-3 Save File Dialog Window

Field or Button	Description
Seed File List	The Seed File List pane contains: • Go up one Folder—Click this icon to go up one folder in the directory structure. • New Folder 1. Click **New Folder** to create a new folder in the current directory. This action opens the Input dialog box. 2. Enter a folder name and click **OK**. The new folder appears in the Save File dialog box. 3. Double-click the folder to open it. You can save files in this folder or create another folder at this level. • Type—Icon indicating whether the item in the table is a file or a folder. • Name—Name of the seed file or folder. • Last Modified—Date and time the seed file or folder was last modified. • Size (bytes)—Size of the seed file or folder, in bytes.
Filename	Name by which you want to save the seed file. If you create a new seed filename, you can use any letters, numbers, or characters in the name that are allowed by your operating system. However, if you include any spaces in the new name, Prime Performance Manager converts those spaces to hyphens. For example, Prime Performance Manager saves file *a b c* as *a-b-c*.
Make this my preferred start option	Specifies whether the chosen seed file should be loaded automatically whenever this Prime Performance Manager client is started or the Discovery dialog box is opened. By default, this option is not selected. That is, a seed file is not loaded automatically when Prime Performance Manager client is started or when the Discovery dialog box is opened.
OK	Saves the seed file and any changes you made to the seed file list and closes the dialog box. To save the seed file with a new name, you can either save the file with: • A completely new name. Enter the new name and click **OK**. • An existing name, overwriting an old seed file. Select the name in the list and click **OK**. Prime Performance Manager: 1. Saves the seed file with the new name 2. Saves any changes you made to the list of files 3. Closes the Save File Dialog: Seed File List dialog box 4. Returns to the Discovery dialog box

Table 4-3 Save File Dialog Window (continued)

Field or Button	Description
Delete	Deletes the chosen file from the seed file list. Prime Performance Manager displays an informational message containing the name and location of the deleted file.
Cancel	• Closes the dialog box without saving the seed file or saving any changes to the seed file list.

Discovery Seeds Pane

The Discovery Seeds pane contains a Seed Devices File panel and a Seed Details panel. Seed Devices File options include:

- IP Address, Address Range, Subnet, CIDR, or DNS Hostname—The address or name of the chosen seed device. To create a new seed file, enter the name or address of a seed device in this field. Examples of acceptable input include:
  - IP Address: 1.2.3.4 (see the guidelines for IP addresses in).
  - Address Range: 1.2.3.2-15
  - Subnet, CIDR: 1.2.3.0/24, 1.2.3.0/255.255.255.0
  - DNS Hostname: Prime Performance Manager.cisco.com
- Add—Adds a new seed device to Prime Performance Manager.username
- Delete—Deletes the chosen seed device. A confirmation message is displayed before deleting the seed device.

The Seed Details panel lists the SNMP and Telnet/SSH parameters of discovered devices:

- SNMP Parameters:
  - IP Address Range or Hostname—IP address or DNS name of a device or range of devices. An asterisk (*) indicates a wildcard value.
  - Read Community—SNMP community name used by the device for read access to the information maintained by the SNMP agent on the device.
  - Username (v3)—Supports the SNMP v3 Username parameter. This is useful in determining whether the device will be polled using SNMPv2 or SNMPv3. SNMPv2 and SNMPv3 credentials can be provided. However, Prime Performance Manager only uses one SNMP version to communicate with devices. If both SNMPv2 and SNMPv3 are provided, Prime Performance Manager uses SNMPv3.
  - Timeout (secs)—Time, in seconds, Prime Performance Manager waits for a response from the device.
  - Retries—Number of times Prime Performance Manager attempts to connect to the device.
  - Poll Interval (mins)—Time, in minutes, between polls for the device.
- Telnet/SSH Parameters:
  - IP Address Range or Hostname—IP address or DNS name of a device or range of devices. An asterisk (*) indicates a wildcard value.
  - User Name—the device login username.
  - Password—The password for the login user.
  - Enable User Name—The privileged username.

- Enable Password—The privileged user password.
- Protocol—the transport protocol to be used to communicate with device: Telnet, SSHv1, SSHv2, or WSMA_SSH (Web Services Management Agent over SSHv2).
- Port—The device port to be used by the transport protocol chosen in the Protocol field.
- Sub System—The subsystem used by transport protocol. A blank string is the default subsystem for SSH. The default subsystem for WSMA is “wsma”.

Verifying Discovery

To view the devices that Prime Performance Manager discovered, from the navigation tree select **Summary List > Devices**. (For more information about the Devices summary list, see Using the Devices Summary List, page 8-1.) By default, the Devices table is sorted by alarm severity. If you suspect that Prime Performance Manager did not discover all of the devices, verify that:

- Prime Performance Manager server can ping the devices.
- SNMP is enabled on the devices.
- Prime Performance Manager is configured with the correct SNMP community name.

If you suspect that Prime Performance Manager did not discover all the devices, run the device discovery again.