CHAPTER 4

Setting Up Physical Inventory

Devices

Every network element that Cisco Prime Fulfillment manages must be defined as a device in the system. An element is any device from which Prime Fulfillment can collect information. In most cases, devices are Cisco IOS routers that function as Provider Edge Routers (PEs) or Customer Edge Routers (CEs) in the MPLS VPN.

Note To provision services with Prime Fulfillment, you must have IPv4 connectivity.

This section describes how to configure SSH or SSHv2, set up SNMP, manually enable an RTR responder, and create, edit, delete, and configure various types of supported devices. This section includes the following:

Configuring SSH or SSHv2

Prime Fulfillment needs a mechanism to securely access and deploy configuration files on devices, which include routers and switches. And, to securely download a configlet and upload a configuration file from a device, Secure Shell (SSH) or SSH version 2(SSHv2) must be enabled.

The following sections describe:

Configuring SSH on Cisco IOS Routers Using a Domain Name

The procedure for configuring SSH on a Cisco IOS router is as follows:

	Command	Description
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# ip domain-name <domain_name>`	Specifies the IP domain name.
Step 3	`Router(config)# username <username> password <password>`	Configures the user ID and password. Enter your Prime Fulfillment username and password. For example: `username admin password iscpwd`
Step 4	`Router(config)# crypto key generate rsa`	Generates keys for the SSH session.
Step 5	You will see the following prompt: `Choose the size of the key modulus in the range of 360 to 2048 for your general purpose keys. How many bits in the modulus (nnn):` Press **Enter** to accept the default number of bits.	Sets the number of bits.
Step 6	`Router(config)# line vty 0 4`	Enables SSH as part of the vty login transport.
Step 7	`Router(config-line)# login local`	The **login local** command indicates that the router stores the authentication information locally.
Step 8	`Router(config-line)# transport input telnet ssh`	Enables SSH transport.
Step 9	`Router(config-line)# Ctrl+Z`	Returns to Privileged Exec mode.
Step 10	`Router# copy running startup`	Saves the configuration changes to nonvolatile random-access memory (NVRAM).

Configuring SSHv1 or SSHv2 on Cisco IOS Routers Using RSA Key Pairs

The procedure for configuring SSHv1 or SSHv2 on a Cisco IOS router is as follows.

	Command	Description
Step 1	`Router# enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# ip ssh rsa keypair-name <keypair-name>`	Specifies which RSA keypair to use for SSH usage. Note: A Cisco IOS router can have many RSA key pairs.

	Command	Description
Step 4	`Router(config)# crypto key generate rsa usage-keys label <key-label> modulus <modulus-size>`	Enables the SSH server for local and remote authentication on the router. For SSH Version 2, the modulus size must be at least 768 bits. Note: To delete the Rivest, Shamir, and Adelman (RSA) key-pair, use the **crypto key zeroize rsa** command. After you have deleted the RSA command, you automatically disable the SSH server.
Step 5	`Router(config)# ip ssh [timeout <seconds> | authentication-retries <integer>]`	Configures SSH control variables on your router.
Step 6	`Router(config)# ip ssh version [1 | 2]`	Specifies the version of SSH to be run on a router.

Configuring SSH or SSHv2 on Cisco IOS XR Routers

The procedure for configuring SSHv2 on a Cisco IOS XR router is as follows.

	Command	Description
Step 1	`RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	`RP/0/RP0/CPU0:router(config)# hostname <hostname>`	Configures a hostname for your router.
Step 3	`RP/0/RP0/CPU0:router(config)# domain name <domain-name>`	`Defines a default domain name that the software uses to complete unqualified host names.`
Step 4	`RP/0/RP0/CPU0:router(config)# exit`	Exits global configuration mode, and returns the router to EXEC mode.
Step 5	`RP/0/RP0/CPU0:router(config)# crypto key generate rsa [usage keys | general-keys] [<keypair-label>]`	Generates an RSA key pair.
Step 6	`RP/0/RP0/CPU0:router# crypto key generate dsa`	Enables the SSH server for local and remote authentication on the router. The recommended minimum modulus size is 1024 bits. Generates a DSA key pair. To delete the DSA key pair, use the **crypto key zeroize dsa** command. This command is used only for SSHv2.
Step 7	`RP/0/RP0/CPU0:router# configure`	Enters global configuration mode.
Step 8	`RP/0/RP0/CPU0:router# ssh timeout <seconds>`	(Optional) Configures the timeout value for user authentication to authentication, authorization, and accounting (AAA). If the user fails to authenticate itself to AAA within the configured time, the connection is aborted. If no value is configured, the default value of 30 is used for 30 seconds. The range is from 5 to 120.

	Command	Description

Step 9	`RP/0/RP0/CPU0:router(config)# ssh server`
	or
	`RP/0/RP0/CPU0:router(config)# ssh server v2`
		Brings up an SSH server.
		To bring down an SSH server, use the **no ssh server** command.
		(Optional) Forces the SSH server to accept only SSHv2 clients if you configure the SSHv2 option by using the **ssh server v2** command. If you choose the **ssh server v2** command, only the SSH v2 client connections are accepted.

Step 10	`RP/0/RP0/CPU0:router(config)# end`
	or
	`RP/0/RP0/CPU0:router(config)# commit`
		Saves configuration changes.
		When you issue the **end** command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]
		Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Step 11	`RP/0/RP0/CPU0:router# show ssh`	(Optional) Displays all of the incoming and outgoing SSHv1 and SSHv2 connections to the router.
Step 12	`RP/0/RP0/CPU0:router# show ssh session details`	(Optional) Displays a detailed report of the SSHv2 connections to and from the router.

Setting Up SNMP

To work with Prime Fulfillment, SNMP must be configured on each CPE device in the customer network. In Prime Fulfillment, SNMP is used to:

- collect from the Interface MIB
- provision and collect SLA data.

Two security models are available: SNMPv1/v2c and SNMPv3. Table 4-1 identifies the combinations of security models and levels.

Table 4-1 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	Description
v1/v2c	No Authentication/ No Encryption	Community String	No	Uses a community string match for authentication.
v3	No Authentication/ No Encryption	Username	No	Uses a username match for authentication.
v3	Authentication/ No Encryption	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	Authentication/ Encryption	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms, and provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

SNMPv3 provides for both security models and security levels. A *security model* is an authentication strategy that is set up for a user and the group in which the user resides. A *security level* is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

The security features provided in SNMPv3 are as follows:

- Message integrity—Ensures that a packet has not been tampered with in-transit.
- Authentication—Determines the message is from a valid source.
- Encryption—Encoding the contents of a packet to prevent it from being read by an unauthorized source.

SNMPv3 objects have the following characteristics:

- Each user belongs to a group.
- The group defines the access policy for a set of users and determines the list of notifications its users can receive. The group also defines the security model and security level for its users.
- The access policy defines which SNMP objects can be accessed for reading, writing, or creation.
- SNMPv3 is not supported for Discovery.

Setting Up SNMPv1/v2c on Cisco IOS Routers

To determine whether SNMP is enabled, and to set the SNMP community strings on a Cisco IOS router, perform the following steps for each router:

	Command	Description
Step 1	`Router> enable` `Router> <enable_password>`	Enters enable mode, and then enters the enable password.
Step 2	`Router# show snmp`	Check the output of the **show snmp** command to see whether the following statement is present: "`SNMP agent not enabled.`" If SNMP is not enabled, complete the steps in this procedure.
Step 3	`Router# configure terminal`	Enters global configuration mode.
Step 4	`Router(config)# snmp-server community <userstring> RO`	Sets the community read-only string.
Step 5	`Router(config)# snmp-server community <userstring> RW`	Sets the community read-write string.
Step 6	`Router(config)# Ctrl+Z`	Returns to Privileged Exec mode.
Step 7	`Router# copy running startup`	Saves the configuration changes to NVRAM.

Tip The SNMP community strings defined in Prime Fulfillment for each target device must be identical to those configured on the device.

Setting SNMPv3 Parameters on Cisco IOS Routers

This section describes how to set the SNMPv3 parameters on Cisco IOS routers. SNMPv3 is only supported on IOS crypto images. For Authentication/Encryption, the IOS image must have DES56.

Tip The SNMP users defined in Prime Fulfillment for each target device must be identical to those configured on the device.

To check the existing SNMP configuration, use these commands in the router terminal session:

- **show snmp group**
- **show snmp user**

To set the SNMPv3 server group and user parameters on a Cisco IOS router, perform the following steps:

Note The group must be created first and then the user.

	Command	Description
Step 1	`Router> enable` `Router> <enable_password>`	Enters enable mode, then enter the enable password.
Step 2	`Router# configure terminal`	Enters global configuration mode.

	Command	Description
Step 3	`Router(config)# snmp-server group [<groupname> {v1 | v2c | v3 {auth | noauth | priv}}] [read <readview>] [write <writeview>] [notify <notifyview>] [access <access-list>]`	The **snmp-server group** command configures a new SNMP group or a table that maps SNMP users to SNMP views. Each group belongs to a specific security level. Example: **snmp-server group v3auth v3 auth read v1default write v1default**
Step 4	`Router(config)# snmp-server user <username> [<groupname> remote <ip-address> [udp-port <port>] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} <auth-password> [priv des56 <priv-password>]] [access <access-list>]`	The **snmp-server user** command configures a new user to an SNMP group. Example: **snmp-server user user1 v3auth v3 auth md5 user1Pass**
Step 5	`Router(config)# Ctrl+Z`	Returns to Privileged Exec mode.
Step 6	`Router# copy running startup`	Saves the configuration changes to NVRAM.

Manually Enabling RTR Responder on Cisco IOS Routers

Note SNMP must be configured on the router.

To manually enable an RTR Responder on a Cisco IOS router, execute the following steps:

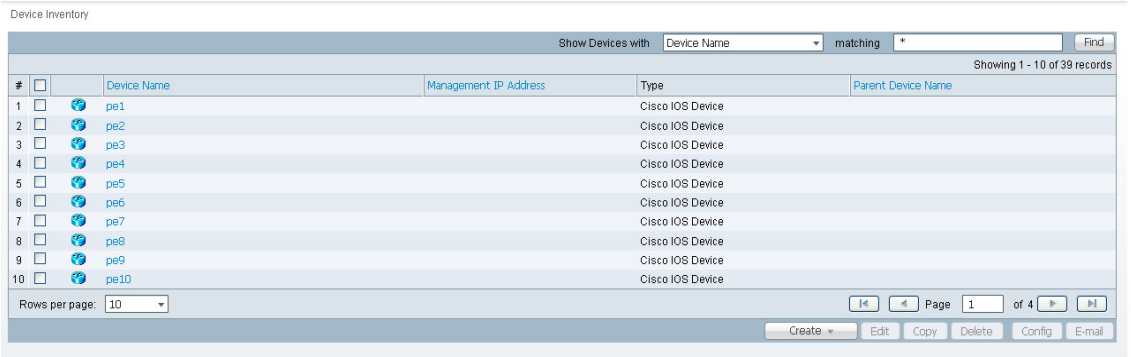
	Command	Description
Step 1	`Router> enable` `Router> <enable_password>`	Enters enable mode, and then enters the enable password.
Step 2	`Router# configure terminal`	Enters the global configuration mode.
Step 3	`Router(config)# rtr responder`	Enables the SA responder on the target router of SA Agent operations.
Step 4	`Router(config)# Ctrl+Z`	Returns to Privileged Exec mode.
Step 5	`Router# copy running startup`	Saves the configuration changes to NVRAM.

Accessing the Devices Window

The Devices feature is used to create, edit, delete, and configure devices, and e-mail the device owner.

Choose **Inventory > Physical Inventory > Devices**, as shown in the following figure.

Figure 4-1 Devices List Window



The Devices window contains the following:

- **Device Name**—Lists the fully qualified host and domain name of the device. You can sort the list of devices by device name.
- **Management IP Address**—Lists the management IP address or the IE2100 address. You can sort the list of devices by this field.
- **Type**—Lists the type of the device. Types include: Cisco IOS Device, CatOs Device, Terminal Server, and IE2100.
- **Parent Device Name**—The name of the parent device.

In the Devices window, you can create, edit, delete, or configure devices, e-mail the device owner, or copy using the following buttons:

- **Create**—Click to create new devices. Enabled only if no devices are selected.
- **Edit**—Click to edit selected device (select device by checking the corresponding box). Enabled only if a single device is selected.
- **Copy**—Click to copy selected device (select device by checking the corresponding box). Enabled only if a single device is selected.
- **Delete**—Click to delete selected device (select device by checking the corresponding box). Enabled only if one or more devices are selected.
- **Config**—Click to change the selected device configuration (select device by checking the corresponding box). Enabled only if a single device is selected.
- **E-mail**—Click to send e-mail to the owner of the selected device(s) (select device(s) by checking the corresponding box(es)). Enabled only if one or more devices are selected.

Creating a Device

From the Create window, you can define different types of devices.

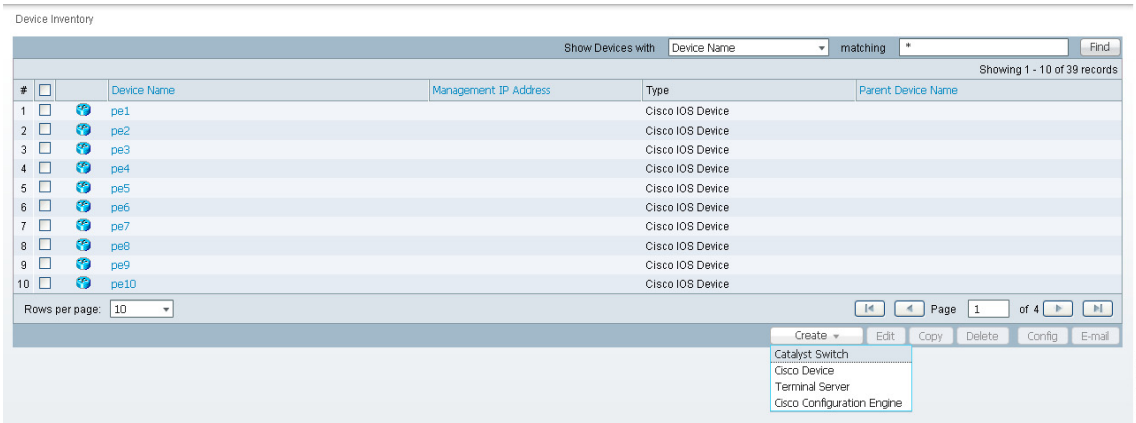
To create a device, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Devices**.

Step 2 Click the **Create** button.

The Create options window appears, as shown in the following figure.

Figure 4-2 Create Options Window



The **Create** options include the following:

- **Catalyst Switch**—A Catalyst device running the Catalyst Operating System.
- **Cisco Device**—Any router that runs the Cisco IOS. This includes Catalyst devices running Cisco IOS.
- **Terminal Server**—A device that represents the workstation that can be used to provision edge routers.
- **Cisco Configuration Engine (IE2100)**—Any Cisco Intelligence Engine (IE) 2100 series network device.

Step 3 See the following sections for instructions on creating each type of device.

- Creating a Catalyst Switch, page 4-9
- Creating a Cisco Device, page 4-14
- Creating a Terminal Server, page 4-20
- Creating a Cisco Configuration Engine Server, page 4-25

Creating a Catalyst Switch

To create a Catalyst switch, follow these steps:

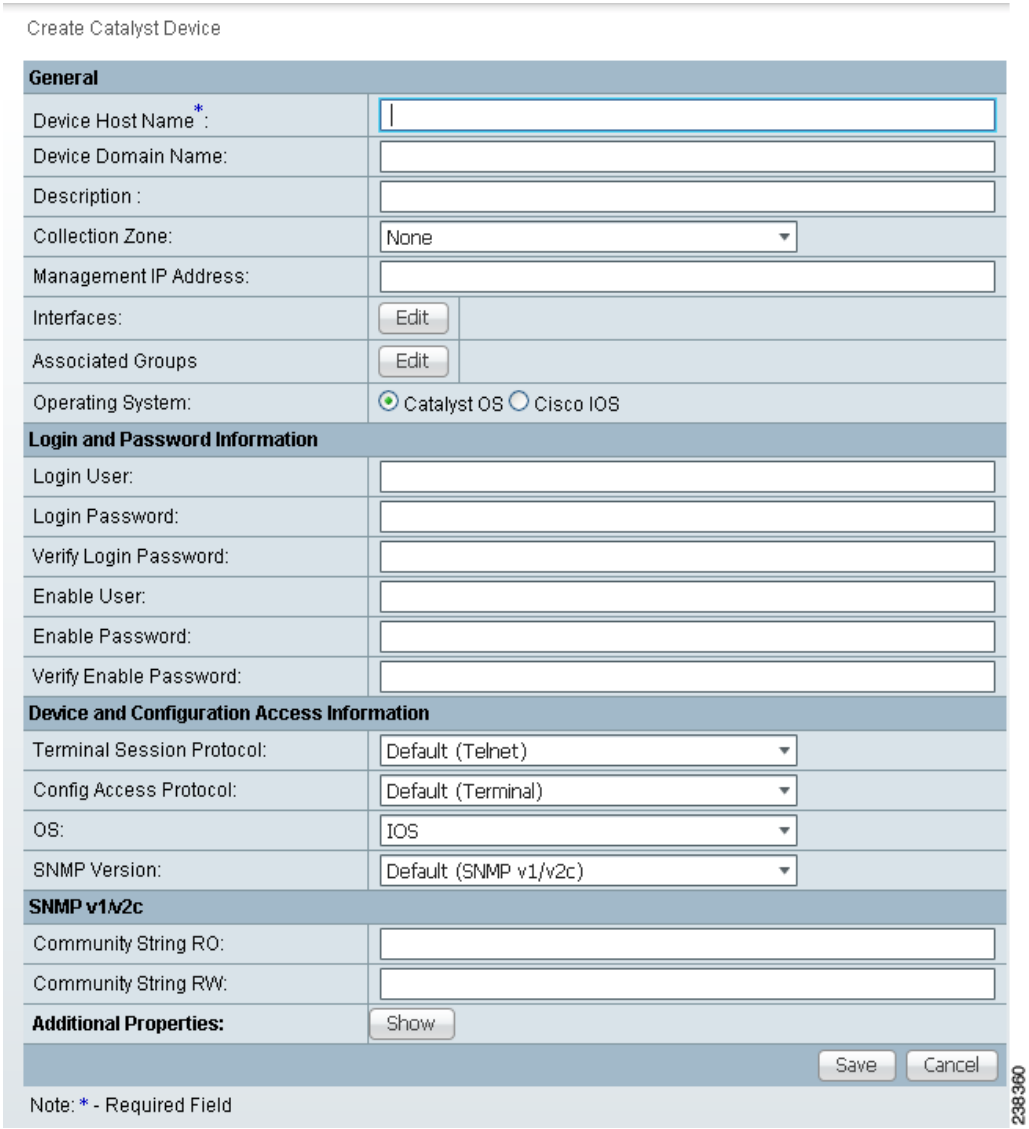
Step 1 Choose **Inventory > Physical Inventory > Devices**.

Step 2 Click the **Create** button.

Step 3 Select **Catalyst Switch**.

The Create Catalyst Device window appears, as shown in the following figure.

Figure 4-3 Create Catalyst Device Window



The General section of the Create Catalyst Device window contains the following fields:

- **Device Host Name** (required)—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field must match the name configured on the target router device. Limited to 256 characters.
- **Device Domain Name** (optional)—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Description** (optional)—Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **Collection Zone** (optional)—Drop-down list of all collection zones within the Prime Fulfillment. Choices include: None and all collection zones within the Prime Fulfillment. Default: None.

- **Management IP Address** (optional)—Valid IP address of the device that Prime Fulfillment uses to configure the target router device.
- **Interfaces** (optional)—Click the **Edit** button to view, add, edit, and delete all interfaces associated with the device. See Table 4-2 for a description of the Interfaces fields.

Table 4-2 Create Catalyst Device Interfaces Fields

Field	Description	Additional
Interface Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
IPV4 Address	IPv4 address associated with this interface.	
IPV6 Address	IPv6 address associated with this interface.	
Encapsulation	The Layer 2 Encapsulation for this device.	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE
Port Type		NONE ACCESS TRUNK ROUTED
Description	Description of the device interface.	Description of the device interface.
IP Address Type	IP address type.	IP address type.

- **Associated Groups** (optional)—Click the **Edit** button to view, add, and remove all Device Group associations.

- **Operating System** (optional)—Click the radio button for the operating system currently running on the CAT switch. Choices include: Catalyst OS or Cisco IOS. Default: Catalyst OS. When you choose the IOS operating system, VPNSM is available under the heading Catalyst Properties. If you click the **Edit** button for **VPNSM**, you can **Create**, **Edit**, and **Delete** VPN Service Modules (VPNSMs).

The Login and Password Information section of the Create Catalyst Device window contains the following fields:

- **Login User** (optional)—Not required by Prime Fulfillment. However, collection and upload/download will not function without the Login User and Login Password as Prime Fulfillment will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password** (optional)—Not required by Prime Fulfillment. However, collection and upload/download will not function without the Login User and Login Password, because Prime Fulfillment will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Login Password** (optional)—Must match the Login Password field. Limited to 80 characters.
- **Enable User** (optional)—Not required by Prime Fulfillment. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password** (optional)—Not required by Prime Fulfillment. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Enable Password** (optional)—Must match the Enable Password field. Limited to 80 characters.

The Device and Configuration Access Information section of the Create Catalyst Device window contains the following fields:

- **Terminal Session Protocol** (optional)—Configures the method of communication between Prime Fulfillment and the device. Choices include: Telnet, Secure Shell (SSH), CNS, RSH, and SSH version 2 (SSHv2). In previous versions of Prime Fulfillment, this field was called the Transport field. Default: The default set in the DCPL properties.
- **Config Access Protocol** (optional)—Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, FTP, and RCP. Default: The default set in the DCPL properties.
- **SNMP Version** (optional)—Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: The default set in the DCPL properties.

The SNMP v1/v2c section of the Create Catalyst Device window contains the following fields:

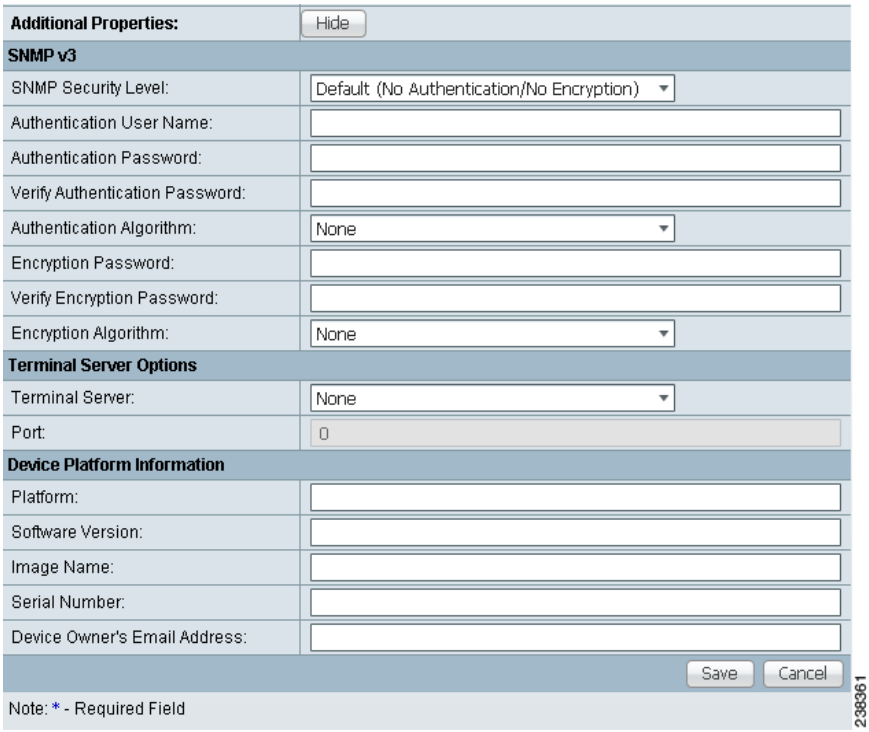
- **Community String RO** (optional)—SNMP Read-Only Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **Community String RW** (optional)—SNMP Read-Write Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

Step 4 Enter the desired information for the Catalyst device you are creating.

Step 5 To access the Additional Properties section of the **Create Catalyst Device**, click **Show**.

The Additional Properties window appears, as shown in Figure 4-4.

Figure 4-4 Catalyst Device Additional Properties Window



The SNMP v3 section of the Catalyst Device Properties window contains the following fields:

- **SNMP Security Level** (optional)—Choices include: Default (<*default_set_in_DCP*L>), Authentication/No Encryption, Authentication/Encryption, and No Authentication/No Encryption. Default: Default (<*default_set_in_DCP*L>). Note: When you change the DCPL property, the <*default_set_in_DCP*L> variable changes.
- **Authentication User Name** (optional)—User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password** (optional)—Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Authentication Password** (optional)—Must match the Encryption Password field. Limited to 80 characters.
- **Authentication Algorithm** (optional)—Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password** (optional)—In previous versions of Prime Fulfillment, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.
- **Verify Encryption Password** (optional)—Must match the Encryption Password field. Limited to 80 characters.

- **Encryption Algorithm** (optional)—In previous versions of Prime Fulfillment, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

The Terminal Server Options section of the Catalyst Device Properties window contains the following fields:

- **Terminal Server** (optional)—Choices include: None and the list of existing Terminal Server names. Default: None.
- **Port** (optional)—Disabled until a Terminal Server is selected. Range: 0-65535. Default: 0.

The Device Platform Information section of the Catalyst Device Properties window contains the following fields:

- **Platform** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Device Owner's Email Address** (optional)—Used in the To: field when the Email button is selected from the device list. Limited to 80 characters and must be valid Email format.

Step 6 Enter any desired Additional Properties information for the Catalyst device you are creating.

Step 7 Click **Save**.

The Devices window reappears with the new Catalyst device listed.

Creating a Cisco Device

To create a Cisco device, follow these steps:

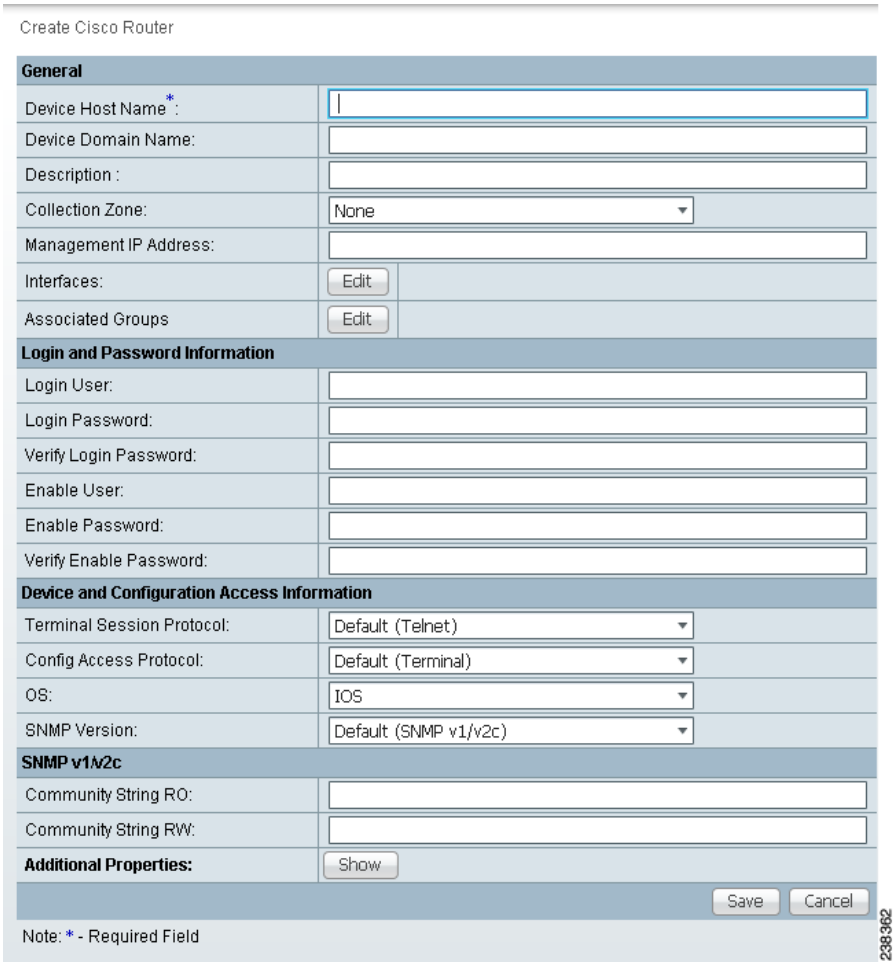
Step 1 Choose **Inventory > Physical Inventory > Devices**.

Step 2 Click the **Create** button.

Step 3 Select **Cisco Device**.

The Create Cisco Device window appears, as shown in Figure 4-5.

Figure 4-5 Create Cisco Device Window



The General section of the Create Cisco IOS Device window contains the following fields:

- **Device Host Name**—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field is required and must match the name configured on the target router device. Limited to 256 characters.
- **Device Domain Name** (optional)—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Description** (optional)—Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **Collection Zone** (optional)—Drop-down list of all collection zones within the Prime Fulfillment. Choices include: None and all collection zones within the Prime Fulfillment. Default: None.
- **Management IP Address** (optional)—Valid IP address of the device that Prime Fulfillment uses to configure the target router device.
- **Interfaces** (optional)—Click the Edit button to view, add, edit, and delete all interfaces associated with the device. See Table 4-3 for a description of the Interface fields

Table 4-3 Create Cisco Device Interface Fields

Field	Description	Additional
Interface Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
IPV4 Address	IP address associated with this IPv4 interface.	
IPV6 Address	IP address associated with this IPv6 interface.	
Encapsulation	The Layer 2 Encapsulation for this device.	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE

Table 4-3 Create Cisco Device Interface Fields (continued)

Field	Description	Additional
Description	Description of the device interface.	Description of the device interface.
IP Address Type	IP address type.	IP address type.

- **Associated Groups** (optional).
- Click the **Edit** button to view, add, and remove all Device Group associations.

The Login and Password Information section of the Create Cisco IOS Device window contains the following fields:

- **Login User** (optional)—Not required by Prime Fulfillment. However, collection and upload/download will not function without the Login User and Login Password as Prime Fulfillment will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Login Password** (optional)—Displayed as stars (*). Not required by Prime Fulfillment. However, collection and upload/download will not function without the Login User and Login Password as Prime Fulfillment will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Login Password** (optional)—Displayed as stars (*). Must match the Login Password field. Limited to 80 characters.
- **Enable User** (optional)—Not required by Prime Fulfillment. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password** (optional)—Displayed as stars (*). Not required by Prime Fulfillment. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Enable Password** (optional)—Displayed as stars (*). Must match the Enable Password field. Limited to 80 characters.

The Device and Configuration Access Information section of the Create Cisco IOS Device window contains the following fields:

- **Terminal Session Protocol** (optional)—Configures the method of communication between Prime Fulfillment and the device. Choices include: Telnet, Secure Shell (SSH), CNS, RSH, and SSH version 2 (SSHv2).
- **Config Access Protocol** (optional)—Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, FTP, and RCP. Default: The default set in the DCPL properties.
- **OS** (optional)—The choices are: IOS and IOS_XR.
- **SNMP Version** (optional)—Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: The default set in the DCPL properties.

The SNMP v1/v2c section of the Create Cisco IOS Device window contains the following fields:

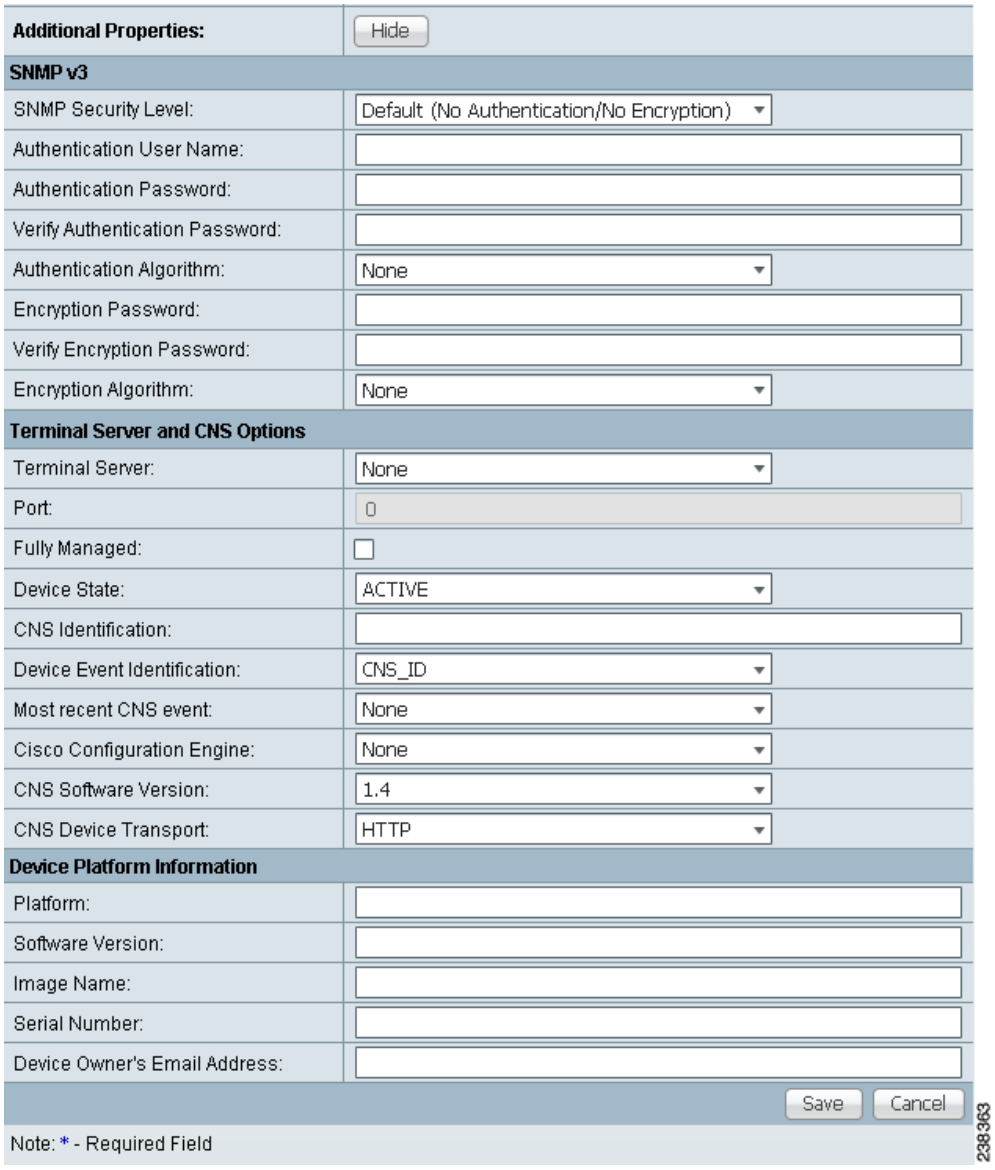
- **Community String RO** (optional)—SNMP Read-Only Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **Community String RW** (optional)—SNMP Read-Write Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

Step 4 Enter the desired information for the Cisco IOS device you are creating.

Step 5 To access the Additional Properties section of the **Create Cisco Device**, click **Show**.

The Additional Properties window appears, as shown in Figure 4-6.

Figure 4-6 Additional Properties for the Cisco Device Properties Window



The SNMP v3 section of the Cisco IOS Device Properties window contains the following fields:

- **SNMP Security Level** (optional)—Choices include: Default (<*default_set_in_DCP*L>), Authentication/No Encryption, Authentication/Encryption, and No Authentication/No Encryption. Default: Default (<*default_set_in_DCP*L>). Note: When you change the DCPL property, the <*default_set_in_DCP*L> variable changes.
- **Authentication User Name** (optional)—User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password** (optional)—Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Authentication Password** (optional)—Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Authentication Algorithm** (optional)—Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password** (optional)—Displayed as stars (*). In previous versions of Prime Fulfillment, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.
- **Verify Encryption Password** (optional)—Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Encryption Algorithm** (optional)—In previous versions of Prime Fulfillment, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

The Terminal Server and CNS Options section of the Cisco IOS Device Properties window contains the following fields:

- **Terminal Server** (optional)—Choices include: None and the list of existing Terminal Server names. Default: None.
- **Port** (optional)—Disabled until a Terminal Server is selected. Range: 0-65535. Default: 0.
- **Fully Managed** (optional)—If the Fully Managed check box is checked, the device becomes a fully managed device. Prime Fulfillment performs additional management actions only for fully managed devices. These actions include e-mail notifications upon receipt of device configuration changes originated outside Prime Fulfillment and the scheduling of enforcement audit tasks upon detection of possible intrusion. Default: Not selected and therefore not selected.
- **Device State** (optional)—Choices include: ACTIVE and INACTIVE. ACTIVE indicates that the router has been plugged on the network and can be part of Prime Fulfillment tasks such as collect config and provisioning. INACTIVE indicates the router has not been plugged-in. Default: ACTIVE.
- **CNS Identification**—Required if the Device Event Identification field is set to CNS_ID. Only valid characters that Cisco IOS allows are alphanumeric characters and (.) (-) (_).
- **Device Event Identification** (optional)—Indicates whether the CNS Identification field contains a HOST_NAME or CNS_ID. Default: HOST_NAME.
- **Most Recent CNS event** (optional)—Choices include: None, CONNECT, and DISCONNECT. Changing from the default to None is not recommended. Note: The last connect or disconnect CNS TIBCO event received by Prime Fulfillment for each CNS-enabled IOS device is automatically recorded.

- **IE2100** (optional)—Disabled unless the Device State field is INACTIVE or the Terminal Session Protocol field is CNS. A valid IE2100 must be selected if the Terminal Session Protocol is CNS. Choices include: None and the list of existing IE2100 names. Default: None.
- **Cisco Configuration Engine Software Version** (optional)—Choices include: 1.3, 1.3.1, 1.3.2, 1.4, 1.5, 2.0, 3.0, and 3.5. This is the release version of Cisco Configuration Engine that manages the IOS device. Default: 1.4.
- **CNS Device Transport** (optional)—Choices include: HTTP and HTTPS. This field determines what will be the transport mechanism used by Prime Fulfillment to create, delete, or edit devices in the Cisco Configuration Engine repository. If HTTPS is used, the Cisco Configuration Engine must be running in secure mode. Default: HTTP.

The Device Platform Information section of the Cisco IOS Device Properties window contains the following fields:

- **Platform** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Device Owner's Email Address** (optional)—Used in the To: field when the Email button is selected from the device list. Limited to 80 characters and must be valid Email format.

Step 6 Enter any desired Additional Properties information for the Cisco IOS device you are creating.

Step 7 Click **Save**.

The Devices window reappears with the new Cisco IOS device listed.

Creating a Terminal Server

To create a Terminal Server device, follow these steps:

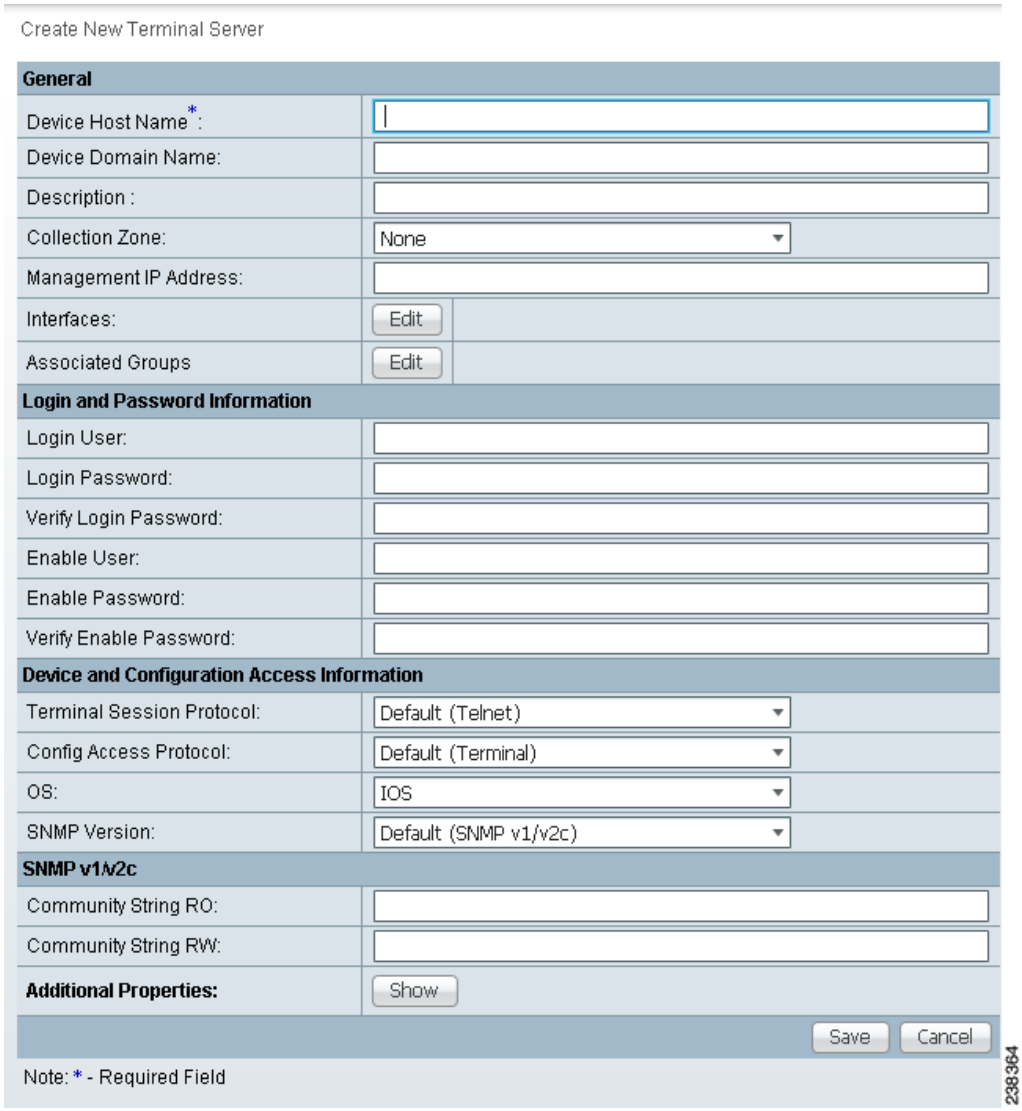
Step 1 Choose **Inventory > Physical Inventory > Devices**.

Step 2 Click the **Create** button.

Step 3 Select **Terminal Server**.

The Create Terminal Server window appears, as shown in Figure 4-7.

Figure 4-7 Create Terminal Server Window



The General section of the Create Terminal Server window contains the following fields:

- **Device Host Name** (required)—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field must match the name configured on the target router device. Limited to 256 characters.
- **Device Domain Name** (optional)—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Description** (optional)—Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **Collection Zone** (optional)—Drop-down list of all collection zones within the Prime Fulfillment. Choices include: None and all collection zones within the Prime Fulfillment. Default: None.
- **Management IP Address** (optional)—Valid IP address of the device that Prime Fulfillment uses to configure the target router device.

- **Interfaces** (optional)—Click the **Edit** button to view, add, edit, and delete all interfaces associated with the device. See Table 4-4 for a description of the Interfaces fields.

Table 4-4 Create Terminal Server Device Interfaces Fields

Field	Description	Additional
Interface Name	Name of this interface.	List can be sorted by this field. Limited to 80 characters.
Encapsulation	The Layer 2 Encapsulation for this device.	DEFAULT DOT1Q ETHERNET ISL FRAME_RELAY FRAME_RELAY_IETF HDLC PPP ATM AAL5SNAP AAL0 AAL5 AAL5MUX AAL5NLPID AAL2 ENCAP_QinQ GRE
Port Type		NONE ACCESS TRUNK ROUTED
Description	Description of the device interface.	Description of the device interface.
IP Address Type	IP address type.	IP address type.

- **Associated Groups** (optional)—Click the **Edit** button to view, add, and remove all Device Group associations.

The Login and Password Information section of the Create Terminal Server window contains the following fields:

- **Login User** (optional— Not required by Prime Fulfillment. However, collection and upload/download will not function without the Login User and Login Password as Prime Fulfillment will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.

- **Login Password** (optional)—Displayed as stars (*). Not required by Prime Fulfillment. However, collection and upload/download will not function without the Login User and Login Password as Prime Fulfillment will not be able to access the device. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Login Password** (optional)—Displayed as stars (*). Must match the Login Password field. Limited to 80 characters.
- **Enable User** (optional)—Not required by Prime Fulfillment. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Enable Password** (optional)—Displayed as stars (*). Not required by Prime Fulfillment. However, collection and upload/download only function if the Login User has sufficient privileges to configure the router in EXEC mode. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Enable Password** (optional)—Displayed as stars (*). Must match the Enable Password field. Limited to 80 characters.

The Device and Configuration Access Information section of the Create Terminal Server window contains the following fields:

- **Terminal Session Protocol** (optional)—Configures the method of communication between Prime Fulfillment and the device. Choices include: Telnet, Secure Shell (SSH), CNS, RSH, and SSH version 2 (SSHv2). In previous versions of Prime Fulfillment, this field was called the Transport field. Default: The default set in the DCPL properties.
- **Config Access Protocol** (optional)—Administers the access protocol for config upload and download. Choices include: Terminal, TFTP, FTP, and RCP. Default: The default set in the DCPL properties.
- **OS** (optional)—The choices are: IOS and IOS_XR.
- **SNMP Version** (optional)—Configures the version of SNMP to use when communicating with the device. Choices include: SNMP v1/v2c and SNMP v3. Default: The default set in the DCPL properties.

The SNMP v1/v2c section of the Create Terminal Server window contains the following fields:

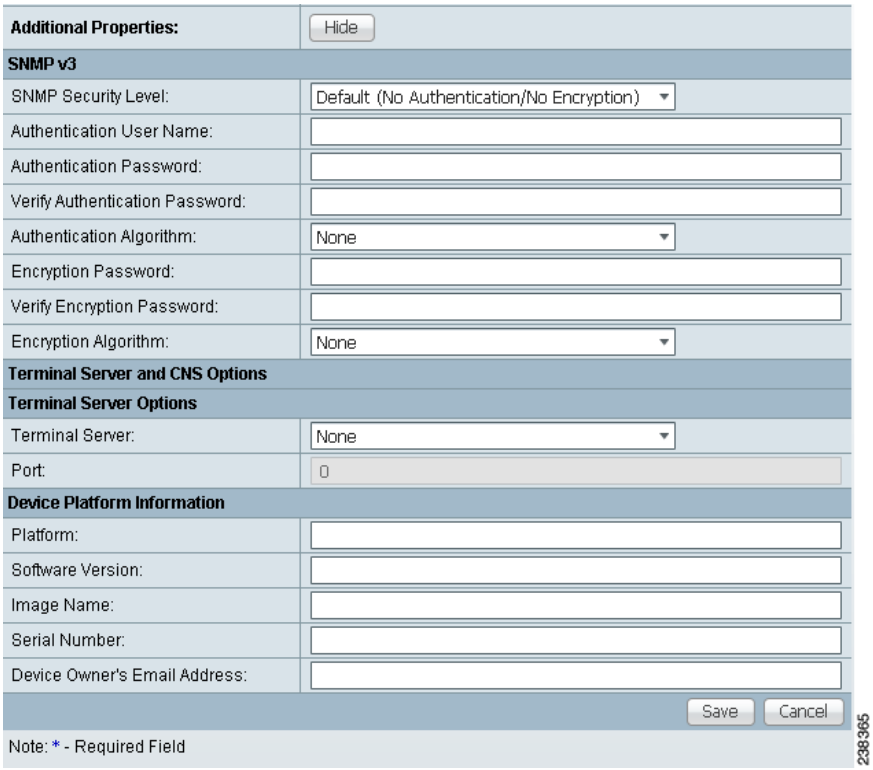
- **Community String RO** (optional)—SNMP Read-Only Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.
- **Community String RW** (optional)—SNMP Read-Write Community String. Many tasks use SNMP to access the device. This field must match what is configured on the target router device. Limited to 80 characters.

Step 4 Enter the desired information for the Terminal Server you are creating.

Step 5 To access the Additional Properties section of the **Create Terminal Server**, click **Show**.

The Additional Properties window appears, as shown in Figure 4-8.

Figure 4-8 Additional Properties for the Terminal Server Device Properties Window



The SNMP v3 section of the Terminal Server Device Properties window contains the following fields:

- **SNMP Security Level** (optional)—Choices include: Default (<*default_set_in_DCP*L>), Authentication/No Encryption, Authentication/Encryption, and No Authentication/No Encryption. Default: Default (<*default_set_in_DCP*L>). Note: When you change the DCPL property, the <*default_set_in_DCP*L> variable changes.
- **Authentication User Name** (optional)—User name configured on the specified device router. User must have permission to the object identification numbers (OIDs) specified in the security request (that is, write permission for a set request, and read permission for a get request). Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Limited to 80 characters.
- **Authentication Password** (optional)—Displayed as stars (*). Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Should match what is configured on the target router device. Limited to 80 characters.
- **Verify Authentication Password** (optional)—Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Authentication Algorithm** (optional)—Should be provisioned if the SNMP Security Level is Authentication/No Encryption or Authentication/Encryption. Choices include: None, MD5, and SHA. Default: None.
- **Encryption Password** (optional)—Displayed as stars (*). In previous versions of Prime Fulfillment, this field was called Privacy Password. Should match what is configured on the target router device. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Limited to 80 characters.

- **Verify Encryption Password** (optional)—Displayed as stars (*). Must match the Encryption Password field. Limited to 80 characters.
- **Encryption Algorithm** (optional)—In previous versions of Prime Fulfillment, this field was called Privacy Protocol. Should be provisioned if the SNMP Security Level is Authentication/Encryption. Choices include: None and DES 56. Default: None.

The Terminal Server Options section of the Terminal Server Device Properties window contains the following fields:

- **Terminal Server** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Port** (optional)—An integer that indicates the port; default is 0.

The Device Platform Information section of the Terminal Server Device Properties window contains the following fields:

- **Platform** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Software Version** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Image Name** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Serial Number** (optional)—Should match what is configured on the target router device. Limited to 80 characters.
- **Device Owner's Email Address** (optional)—Used in the To: field when the Email button is selected from the device list. Limited to 80 characters and must be valid Email format.

Step 6 Enter any desired Additional Properties information for the Terminal Server device you are creating.

Step 7 Click **Save**.

The Devices window reappears with the new Terminal Server device listed.

Creating a Cisco Configuration Engine Server

Note To use the Cisco Configuration Engine server functionality on Prime Fulfillment, you must first set up the Cisco Configuration Engine server and the Prime Fulfillment workstation as explained in Appendix B, "Setting Up Cisco Configuration Engine with Prime Fulfillment" in the *Cisco Prime Fulfillment Installation Guide 6.1*. You must also create a Cisco IOS device to communicate with the Cisco Configuration Engine server. See Appendix A, "Creating a Cisco IOS Device Using the Cisco CNS Device Access Protocol". The cisco configuration engine server is referred to as IE2100 throughout the Prime Fulfillment user interface. This is the model number of an appliance that is sued to run the configuration engine software.

To create a Cisco Configuration Engine server, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Devices**.

Step 2 Click the **Create** button.

Step 3 Select **Cisco Configuration Engine**.

The Create New Cisco Configuration Engine window appears, as shown in Figure 4-9.

Figure 4-9 Create IE2100 Device Window

The General section of the Create IE2100 Device window contains the following fields:

- **Device Host Name** (required)—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. This field must match the name configured on the target router device. Limited to 256 characters.
- **Device Domain Name** (optional)—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. The name must match the domain name on the target router device.
- **Description** (optional)—Limited to 80 characters. Can contain any pertinent information about the device such as the type of device, its location, or other information that might be helpful to service provider operators.
- **IPV4 Address** (optional)—Valid IPv4 address of the Cisco Configuration Engine server that Prime Fulfillment uses to configure the target router device.

Step 4 Enter the desired information for the Cisco Configuration Engine server you are creating.

Step 5 Click **Save**.

The Devices window reappears with the new Cisco Configuration Engine server listed.

Editing a Device

From the Edit window, you can modify the fields that have been specified for a particular device.

To access the Edit window, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Devices** to access the Devices window shown in Figure 4-1.

Step 2 Select a single device to edit by checking the box to the left of the Device Name. You can also select a device to edit by clicking on the hyperlink of the device name.

Step 3 Click the **Edit** button. This button is only enabled if a device is selected.

The Edit window appropriate to the type of device selected appears. For example, if you selected a Cisco IOS device the Edit Cisco IOS Device window appears.

Step 4 Enter the changes you want to make to the selected device.

Step 5 Click **Save**.

The changes are saved and the Devices window reappears.

Deleting Devices

From the Delete window, you can remove selected devices from the database.

To access the Delete window, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Devices** to access the Devices window shown in Figure 4-1.

Step 2 Select one or more devices to delete by checking the check box(es) to the left of the Device Name(s).

Step 3 Click the **Delete** button. This button is only enabled if one or more devices are selected.

The Confirm Delete window appears.

Step 4 Click the **Delete** button to confirm that you want to delete the device(s) listed.

The Devices window reappears with the specified device(s) deleted.

Editing a Device Configuration

From the Config window, you can edit the configuration for a specified device.

To access the Config window, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Devices** to access the Devices window shown in Figure 4-1.

Step 2 Select a single device to modify by checking the check box to the left of the Device Name.

Step 3 Click the **Config** button.

The Device Configurations window for the selected device appears.

Step 4 Check the box to the left of the Date for the configuration that you want to modify and click the **Edit** button. This button is only enabled if a device is selected.

The Device Configuration window for the selected device appears.

Step 5 Enter the changes you want to make to the selected device configuration.

Step 6 Click **Save**.

The changes are saved and the Device Configurations window reappears.

Step 7 Click **OK** to return to the Devices window.

E-mailing a Device's Owner

From the E-mail window, you can send a device report via e-mail to the owners of specified devices.

To access the E-mail window, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Devices** to access the Devices window shown in Figure 4-1.

Step 2 Select the devices for which you want to send a device report by checking the check box(es) to the left of the Device Name(s).

Step 3 Click the **E-mail** button. This button is only enabled if one or more devices are selected.

The Send Mail to Device Owners window appears.

Step 4 Compose the e-mail that you want to send to the selected device owners.

Step 5 Click **Send**.

The e-mail is sent and the Devices window reappears.

Copying a Device

From the Copy window, you receive a copy of the chosen device and can name it and change values.

To access the Copy window, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Devices** to access the Devices window shown in Figure 4-1.

Step 2 Select a single device to copy by checking the check box to the left of the Device Name.

Step 3 Click the **Copy** button. This button is only enabled if a device is selected.

A window appropriate to the type of device selected to copy appears. You receive an exact copy of the selected device but the Name, Management IP Address, all Interfaces, and VPNSM blades for a Catalyst Switch running Cisco IOS are blanked out and you must fill in the required information and save this new device. See the "Creating a Device" section on page 4-8 for specifics.

Device Groups

Every network element that Cisco Prime Fulfillment manages must be defined as a device in the system. After you have defined your network elements as devices, you can organize the devices into groups for collection and management purposes.

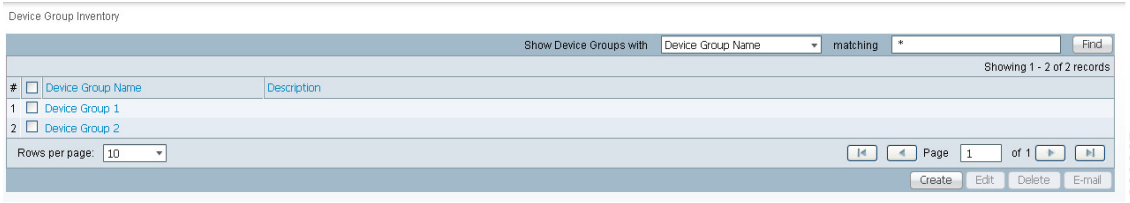
This section describes how to create, edit, and delete device groups and e-mail device group owners. This section includes the following:

Accessing the Device Groups Window

The Device Groups feature is used to create, edit, and delete device groups and e-mail device group owners.

Choose **Inventory > Physical Inventory > Device Groups** to access the Device Groups window shown in Figure 4-10.

Figure 4-10 Device Groups Window



The Device Groups window contains the following:

- **Device Group Name**—Lists the name of the device group. You can sort the list by device group name.
- **Description**—Lists the description of the device group.

From the Device Groups window, you can create, edit, or delete device groups or e-mail device group owners using the following buttons:

- **Create**—Click to create new device groups. Enabled only if no device group is selected.
- **Edit**—Click to edit a selected device group (select device group by checking the corresponding box). Enabled only if a single device group is selected.
- **Delete**—Click to delete selected device group(s) (select device group by checking the corresponding box). Enabled only if one or more device groups are selected.
- **E-mail**—Click to send e-mail to the owner of a selected device group (select device group by checking the corresponding box). Enabled only if one or more device groups are selected.

Creating a Device Group

From the Create Device Group window, you can create different device groups.

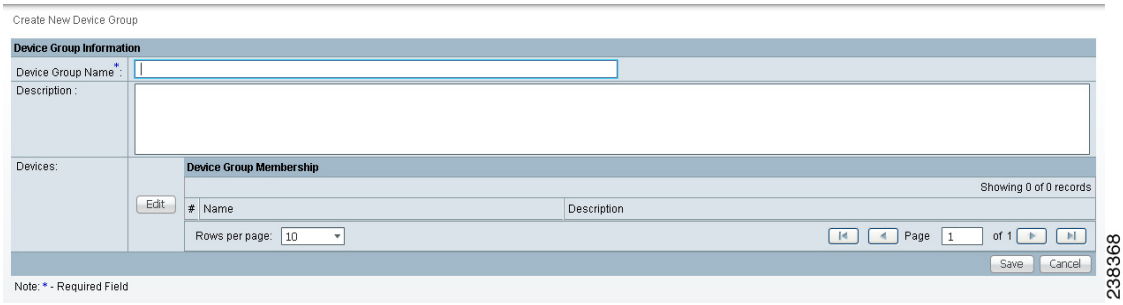
To create a device group, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Device Groups**.

Step 2 Click the **Create** button.

The Create Device Group window appears, as shown in Figure 4-11.

Figure 4-11 Create Device Group Window



The Create Device Group window contains the following fields:

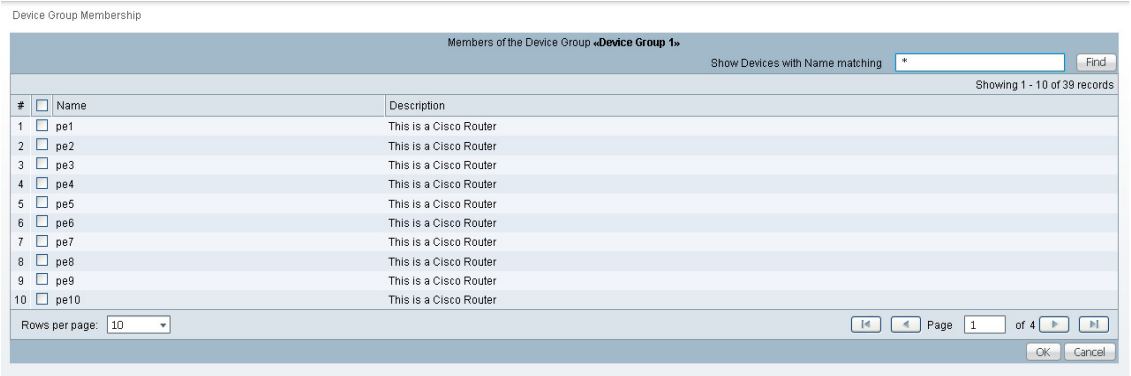
- **Name** (required)—Must begin with a letter, digit, or underscore followed by letters, digits, underscores, spaces, hyphens, or dots ending with a letter, digit, or underscore. Limited to 80 characters.
- **Description** (optional)—Any pertinent information about the device group that could be helpful to service provider operators. Limited to 512 characters.

Step 3 Enter the name and the description of the Device Group that you are creating.

Step 4 Click **Edit**.

The Select Group Members window appears, as shown in Figure 4-12.

Figure 4-12 Select Group Members Window



Step 5 Select the devices that you want to be group members by checking the check box to the left of the device name.

Step 6 Click **OK**.

The Create Device Group window appears listing the selected devices.

Step 7 Click **Save**.

The Device Groups window reappears with the new device group listed.

Editing a Device Group

From the Edit Device Group window, you can modify the fields that have been specified for a particular device group.

To access the Edit Device Group window, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Device Groups**.

Step 2 Select a single device group to modify by checking the check box to the left of the Device Group Name.

Step 3 Click the **Edit** button. This button is only enabled if a device group is selected.

The Edit Device Group window appears.

Step 4 Enter the changes you want to make to the selected device group.

Step 5 Click **Save**.

The changes are saved and the Device Groups window reappears.

Deleting Device Groups

From the Delete window, you can remove selected device groups from the database.

To access the Delete window, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Device Groups.**

Step 2 Select one or more device groups to delete by checking the check box(es) to the left of the Device Group Names.

Step 3 Click the **Delete** button. This button is only enabled if one or more device groups are selected.

The Confirm Delete window appears.

Step 4 Click the **Delete** button to confirm that you want to delete the device group(s) listed.

The Device Groups window reappears with the specified device group(s) deleted.

E-mailing a Device Group

From the E-mail window, you can send a device report via e-mail to the owners of specified device groups.

To access the E-mail window, follow these steps:

Step 1 Choose **Inventory > Physical Inventory > Device Groups**.

Step 2 Select the device groups for which you want to send a device report by checking the check box to the left of the Device Group Name.

Step 3 Click the **E-mail** button. This button is only enabled if one or more device groups are selected.

The Send Mail to Device owners of selected groups window appears.

Step 4 Compose the e-mail that you want to send to the selected device group owners.

Step 5 Click **Send**.

The e-mail is sent and the Device Groups window reappears.