Table 3-7 New Device Wizard, Device Information Page When Adding Devices from Inventory Files (continued)

Element	Description
Transport	
The transport settings determine the method Security Manager will use to contact the device. Each device type has a default method, but you can select your preferred transport method. The device must be configured to respond to the method you select. If you are not performing device discovery, the device is not contacted.	
Protocol	The protocol Security Manager should use when connecting to the device.
Server	For devices that use them, the name of the Auto Update Server (AUS) or Configuration Engine server the device uses to obtain configuration updates. The server must already be defined in Security Manager, or you must select the server from the import list, to import devices that use these servers.
Device Identity	For devices that use servers, the string value that uniquely identifies the device in the Auto Update Server or the Configuration Engine.

Working with the Device Inventory

The following topics describe tasks related to managing the device inventory.

- Adding, Editing, or Deleting Auto Update Servers or Configuration Engines, page 3-36
- Adding or Changing Interface Modules, page 3-40
- Viewing or Changing Device Properties, page 3-41
- Changing Critical Device Properties, page 3-52
- Showing Device Containment, page 3-56
- Cloning a Device, page 3-56
- Deleting Devices from the Security Manager Inventory, page 3-58

In addition to these topics, see the following related topics:.

- Adding Devices to the Device Inventory, page 3-7
- Exporting the Device Inventory, page 10-6
- Importing Policies or Devices, page 10-13

Adding, Editing, or Deleting Auto Update Servers or Configuration Engines

If you want to use Security Manager to manage devices that use other servers to manage their configuration (for example, devices that have dynamic IP addresses supplied by a DHCP server, an address that might not stay constant between device reboots), you must identify the server in Security Manager. These are the servers you can use:

- Auto Update Server (AUS), which is used for upgrading device configuration files on PIX Firewall and ASA devices that use the auto update feature.

- Cisco Configuration Engine, which is used for upgrading device configuration files on Cisco IOS routers, ASA devices, and PIX Firewalls that use the configuration engine feature.

Security Manager cannot initiate direct communication with devices that acquire their interface addresses using DHCP because their IP addresses are not known ahead of time. Furthermore, these devices might not be running, or they might be behind firewalls and NAT boundaries when the management system must make changes. These devices connect to an Auto Update Server or Configuration Engine to get device information.

You can add AUS and Configuration Engine servers to the device inventory when you add devices manually or when you view device properties. You do not have to be adding or viewing the properties of a device that uses one of these servers, you just have to get to the appropriate field to access the controls to add, edit, or delete these servers.

You can also add these servers if you import them from an inventory file exported from CiscoWorks Common Services Device Credential Repository (DCR) or from another Security Manager server. If you import the server, you bypass the procedure described in this section. For more information about importing devices, see Adding Devices from an Inventory File, page 3-31.

Note Beginning with version 4.18, Cisco Security Manager provides support for ASA 9.10(1) devices that are configured on Umbrella servers. Whenever, the device ID is changed, you must re-discover the device in Cisco Security Manager.

Before You Begin

If you want to populate the Security Manager inventory with your list of AUS and Configuration Engine servers without respect to adding devices, the best approach is to use the New Device wizard and to select **Add New Device** as the add method. This approach is described in this procedure.

You can also add or edit servers by selecting a device in the Device selector and clicking **Tools > Device Properties**. Click **General** in the device properties table of contents. The Server field is in either the Auto Update or Configuration Engine groups. You can add or edit only the type of server identified in the group name.

Tip Security Manager cannot determine the software version running on a Configuration Engine when you add it. However, Security Manager cannot deploy configurations correctly to all versions of Configuration. Ensure that your Configuration Engines are running a supported release (see the release notes for this version of the product to see which Configuration Engine versions are supported at http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html).

Related Topics

- Adding Devices from the Network, page 3-12
- Adding Devices by Manual Definition, page 3-26
- Viewing or Changing Device Properties, page 3-41

Step 1 Locate the field that allows you to identify and manage either AUS or Configuration Engine entries in the device inventory:

a. Select **File > New Device** to open the New Device wizard, select **Add New Device** on the Choose Method page, and click **Next**.