



APPENDIX **C**

Device Inventory User Interface Reference

The following topics describe the user interface information for pages related to device inventory management:

- [Create Filter Dialog Box, page C-1](#)
- [New Device Wizard, page C-3](#)
- [Device Delete Validation Page, page C-33](#)
- [Create a Clone of Device Dialog Box, page C-34](#)
- [Device Properties Page, page C-36](#)
- [Export Inventory Dialog Box, page C-44](#)
- [Edit Device Groups Dialog Box, page C-45](#)
- [Add Devices to Group Dialog Box, page C-46](#)
- [Add Group Dialog Box, page C-47](#)
- [Device Server Assignment Dialog Box, page C-48](#)
- [Inventory Status Window, page C-49](#)

Create Filter Dialog Box

Use the Create Filter dialog box to filter and display a subset items in a selector or a table. Creating filters helps you find items more easily when viewing large lists.

Create Filter Dialog Box

For more information on filtering, see these topics:

- [Filtering Items in Selectors, page 3-20](#)
- [Filtering Tables, page 3-24](#)

Navigation Path

Do one of the following:

- Select **Create Filter** from the Filter field in a selector tree.
- Select **Advanced Filter** from the Filter field above a table.

Field Reference

Table C-1 Create Filter Dialog Box

Element	Description
Match All of the Following	<p>When you select this option an AND relationship is created among the filtering criteria you define. An item must satisfy every rule in the filter to be displayed in the list.</p> <p>For example, if you define the following criteria:</p> <ul style="list-style-type: none"> • Name contains OSPF • Name contains West <p>When you click OK, the filter is defined as: Name contains OSPF and Name contains West.</p>
Match Any of the Following	<p>When you select this option an OR relationship is created among the filtering criteria you define. An item must satisfy only one of the rules in the filter to be displayed in the list.</p> <p>For example, if you define the following criteria:</p> <ul style="list-style-type: none"> • Name contains OSPF • Name contains RIP <p>When you click OK, the filter is defined as: Name contains OSPF or Name contains RIP.</p>
Filter Type (First field)	<p>The type of property on which you are filtering. For tables, this is the column heading. You might have only one option for filtering certain lists (for example, you might only be able to filter by the name of the item).</p>

Table C-1 Create Filter Dialog Box (Continued)

Filter Operator (Second field)	The relationship between the filter type and the filter value. The available options depend on the selected type.
Filter Value (Third field)	The value on which you want to filter. Depending on the selected type, you either enter a text string in this field, or you select a value from the list.
Filter Content Area	The filter type, operator, and value that you have selected for each criterion.
Add button	<ul style="list-style-type: none"> To add a criterion, create it in the fields above this area and click Add.
Remove button	<ul style="list-style-type: none"> To remove a criterion, select it and click Remove.

New Device Wizard

Use the New Device wizard to add devices to the device inventory. Devices must be added to the inventory before you can manage them.

The New Device wizard guides you through the process of adding devices to the inventory. You can add devices from many different sources, and the path through the wizard differs significantly based on the method you are using. You select the method on the first page of the wizard.

To start the wizard, from Device view, select **File > New Device**, or click the **Add** button in the device selector.

The following topics describe the pages in the wizard. The first page is common to all methods. The subsequent pages depend on your selection on the first page.

- [Choose Method Page, page C-4](#)
- Adding devices from the network:
 - [Device Information Page – Add Device from Network, page C-5](#)
 - [Device Credentials Page, page C-22](#)
 - [Device Grouping Page, page C-32](#)
- Adding devices from configuration files:
 - [Device Information Page—Configuration File, page C-10](#)
 - [Device Grouping Page, page C-32](#)

- Adding devices manually:
 - [Device Information Page—New Device](#), page C-12
 - [Device Credentials Page](#), page C-22
 - [Device Grouping Page](#), page C-32
- Adding devices from an export file:
 - [Device Information Page—Add Device from File](#), page C-19
 - [Device Grouping Page](#), page C-32

Choose Method Page

Use the Choose Method page of the New Device wizard to select how you want to add devices to the device inventory.

Navigation Path

To start the New Device wizard, from Device view, select **File > New Device**, or click the **Add** button in the device selector.

Related Topics

- [Adding Devices from the Network](#), page 6-10
- [Adding Devices from Configuration Files](#), page 6-13
- [Adding Devices by Manual Definition](#), page 6-14
- [Adding Devices from an Export File](#), page 6-16

Field Reference

Table C-2 Choose Method Page, New Device Wizard

Element	Description
Add Device from Network	Select this option to add devices that are currently active on the network. Security Manager connects directly and securely to the device and discovers its identifying information and properties.
Add from Configuration File	Select this option to add devices by using a copy of the device configuration files.

Table C-2 Choose Method Page, New Device Wizard (Continued)

Add New Device	Select this option to add a device that does not yet exist in the network, so that you can pre-provision it in Security Manager. You can create the device in the system, assign policies to the device, and generate configuration files before installing the device hardware.
Add Device from File	Select this option to add devices from an inventory file exported from CiscoWorks Common Services Device Credential Repository (DCR) or Cisco Security Monitoring, Analysis and Response System (CS-MARS).

Device Information Page – Add Device from Network

Use the New Device wizard's Device Information page for adding devices from the network to specify the device's identifying information.

Navigation Path

To start the New Device wizard, from Device view, select **File > New Device**, or click the **Add** button in the device selector.

Related Topics

- [Understanding the Device View, page 6-2](#)
- [Adding Devices from the Network, page 6-10](#)
- [Device Credentials Page, page C-22](#)
- [Device Grouping Page, page C-32](#)
- [Discovering Policies, page 7-7](#)

Field Reference

Table C-3 *New Device Wizard, Device Information Page When Adding Devices from the Network*

Element	Description
Identity	
IP Type	<p>Whether the IP address for the device is static (defined on the device) or dynamic (supplied by a DHCP server). Depending on the IP type you select, the displayed fields differ.</p> <p>Note You can select Dynamic only for Cisco IOS routers that obtain their IP addresses from a CNS Gateway running on an Auto Update Server. You cannot use the add from network procedure to add any other type of device that has a dynamic IP address.</p>
Hostname (Static IP only)	<p>The DNS hostname for the device. Enter the DNS hostname if the IP address is not known.</p> <p>Note You must enter either the DNS hostname or the IP address, or both.</p>
Domain Name (Static IP only)	The DNS domain name for the device.
IP Address (Static IP only)	<p>The management IP address of the device. The IP address must be in the dotted quad format, for example, 10.64.3.8.</p> <p>Note You must enter either the IP address or the DNS hostname, or both.</p>
Display Name	<p>The name to display in the Security Manager Device selector. If you enter a hostname or IP address, it is entered automatically in this field, but you can change it.</p> <p>The maximum length is 70 characters. Valid characters are: 0–9; uppercase A–Z; lowercase a–z; and the following characters: _ - . : and space.</p> <p>Note Two devices cannot have the same display name.</p>
Device Identity (Dynamic IP only)	The string value that uniquely identifies the device in Auto Update Server.

Table C-3 ***New Device Wizard, Device Information Page When Adding Devices from the Network (Continued)***

<p>CNS Gateway (Dynamic IP only)</p>	<p>The Auto Update Server that is running the CNS Gateway protocol. Security Manager communicates with the AUS running the CNS Gateway protocol to retrieve the IP address of an IOS device, then discovers directly from the IOS device.</p> <p>You can add servers to the list by selecting Add Servers, which opens the Server Properties dialog box (see Server Properties Dialog Box, page C-15). You can also edit the properties of a server by selecting Edit Server, which opens the Available Servers dialog box (see Available Servers Dialog Box, page C-18).</p> <p>For more information on managing this list of servers, see Adding, Editing, or Deleting Auto Update Servers or Configuration Engines, page 6-19</p> <p>Note Only Cisco IOS routers with dynamic IP addresses can be associated with an Auto Update Server running the CNS Gateway protocol.</p>
<p>OS Type</p>	<p>The family of the operating system running on the device. You must be careful to select the correct type, because your selection affects how Security Manager tries to log into the device and obtain its configuration. The options are:</p> <ul style="list-style-type: none"> • IOS 12.3+—For Cisco routers running Cisco IOS Software Release 12.3 or higher. Do not select this for Catalyst 6500/7600 or other Catalyst devices. • IOS - 12.2, 12.1—For Cisco routers running Cisco IOS Software Releases 12.2 or 12.1. Do not select this for Catalyst 6500/7600 or other Catalyst devices. • IOS - Catalyst Switch/7600—For all Catalyst switches and 7600 devices. • ASA—For all ASA devices. • FWSM—For all FWSM devices. • IPS—For all devices running the IPS software. • PIX—For all PIX devices.

Table C-3 ***New Device Wizard, Device Information Page When Adding Devices from the Network (Continued)***

Transport Protocol (Static IP only)	The protocol Security Manager should use when connecting to the device. Select a protocol that is configured on the device and for which you can supply credentials. Each device type has a default protocol that is the method normally used with the device.
System Context	<p>Whether to discover the system execution space of a PIX Firewall 7, ASA, or FWSM device that is running in multiple-context mode. If you are discovering a device that hosts multiple security contexts, whether you select this check box has important implications in how you can configure the device in Security Manager. What gets discovered on the device also depends on whether you select the Discover Policies for Security Contexts check box.</p> <ul style="list-style-type: none"> • Both System Context and Discover Policies for Security Contexts selected—This is the recommended selection. Security Manager discovers the system execution space and all of the security contexts defined on the device, and lists them in the device selector. The base display name represents the system execution space (for example, 10.10.11.24), whereas the security contexts are represented by nodes with the context name appended to the device name (for example, 10.10.11.24_admin), unless you changed the default naming convention configured on the Discovery page (see Discovery Page, page A-20). • System Context selected, Discover Policies for Security Contexts deselected—The system execution space is discovered and added to the device selector. You can then discover the policies for the security contexts at a later time. This method might be appropriate if you have one group of people who discover inventory and another group that discovers policies. • Neither check box selected—Only the Admin context gets discovered and added to the device selector. You cannot discover the other security contexts or manage them.

Table C-3 ***New Device Wizard, Device Information Page When Adding Devices from the Network (Continued)***

Discover Device Settings	
Discover	<p>The type of elements that should be discovered and added to the inventory. You have these options:</p> <ul style="list-style-type: none"> • Policies and Inventory—Discover policies, interfaces, and service modules (if applicable). This is the default and recommended option. <p>When policy discovery is initiated, the system analyzes the configuration on the device, then imports the configured service and platform policies. When inventory discovery is initiated, the system analyzes the interfaces on the device and then imports the interface list. If the device is a composite device, all the service modules in the device are discovered and imported.</p> <p>If you select this option, the check boxes below are activated and you can use them to control the types of policies that are discovered.</p> <p>Note During discovery, if you import an ACL that is inactive, it is shown as disabled in Security Manager. If you deploy the same ACL, it will be removed by Security Manager.</p> <ul style="list-style-type: none"> • Inventory Only—Discovers interfaces and service modules (if applicable). • No Discovery—All discovery is skipped. No policy, interface, or service module information for the device is added to the device inventory.
Platform Settings	<p>Whether to discover the platform settings, which are also called platform-specific policy domains. Platform-specific policy domains exist on firewall devices and Cisco IOS routers. These domains contain policies that configure features that are specific to the selected platform. For more information, see Service Policies vs. Platform-Specific Policies, page 7-3.</p>
Firewall Policies	<p>Whether to discover firewall policies, which are also called firewall services. Firewall services include policies such as access rules, inspection rules, AAA rules, web filter rules, and transparent rules. For details see, Chapter J, “Firewall Services User Interface Reference”</p>
IPS Policies	<p>Whether to discover IPS policies such as signatures and virtual sensors.</p>

Table C-3 *New Device Wizard, Device Information Page When Adding Devices from the Network (Continued)*

RA VPN Policies	Whether to discover remote access VPN policies such as IKE proposals and IPsec proposals.
Discover Policies for Security Context	Whether to discover policies for security contexts. Security contexts apply to PIX Firewall, ASA, or FWSM devices. This field is active only if you select Static for IP Type and System Context .

Device Information Page—Configuration File

Use the New Device wizard's Device Information page for adding devices from configuration files to select the configuration files and to specify policy discovery options.

Navigation Path

To start the New Device wizard, from Device view, select **File > New Device**, or click the **Add** button in the device selector.

Related Topics

- [Understanding the Device View, page 6-2](#)
- [Adding Devices from Configuration Files, page 6-13](#)
- [Device Grouping Page, page C-32](#)
- [Discovering Policies, page 7-7](#)

Field Reference

Table C-4 *New Device Wizard, Device Information Page When Adding Devices from Configuration Files*

Element	Description
Device Type selector	Organizes the devices by device-type and device-family. Select the device type for the new device. You must select the correct device type for the configuration file you are adding.
System Object ID	The system object identifiers for the device type you selected from the Device Type selector. Select the correct ID for your device.

Table C-4 *New Device Wizard, Device Information Page When Adding Devices from Configuration Files (Continued)*

Configuration Files	<p>The configuration files from the devices you are adding to the inventory. You can specify more than one configuration file, but they must all be for the same device type. Separate the file names with commas.</p> <p>Click Browse to select the files from the Security Manager server, or manually type in the file names (including the full path). For information on selecting files, see Selecting or Specifying a File or Directory on the Server File System, page 3-31.</p>
Options	<p>The additional options available on the device. Select IPS if the IPS feature is available on the device.</p>
Discover Device Settings	
Discover	<p>The type of elements that should be discovered and added to the inventory. You have these options:</p> <ul style="list-style-type: none"> • Policies and Inventory—Discover policies, interfaces, and service modules (if applicable). This is the default and recommended option. <p>When policy discovery is initiated, the system analyzes the configuration file, then imports the configured service and platform policies. When inventory discovery is initiated, the system analyzes the interfaces defined in the file and then imports the interface list.</p> <p>If you select this option, the check boxes below are activated and you can use them to control the types of policies that are discovered.</p> <p>Note During discovery, if you import an ACL that is inactive, it is shown as disabled in Security Manager. If you deploy the same ACL, it will be removed by Security Manager.</p> <ul style="list-style-type: none"> • Inventory Only—Discovers interfaces and service modules (if applicable). • No Discovery—All discovery is skipped. No policy, interface, or service module information for the device is added to the device inventory.
Platform Settings	<p>Whether to discover the platform settings, which are also called platform-specific policy domains. Platform-specific policy domains exist on firewall devices and Cisco IOS routers. These domains contain policies that configure features that are specific to the selected platform. For more information, see Service Policies vs. Platform-Specific Policies, page 7-3.</p>

Table C-4 ***New Device Wizard, Device Information Page When Adding Devices from Configuration Files (Continued)***

Firewall Policies	Whether to discover firewall policies, which are also called firewall services. Firewall services include policies such as access rules, inspection rules, AAA rules, web filter rules, and transparent rules. For details see, Chapter J, “Firewall Services User Interface Reference”
IPS Policies	Whether to discover IPS policies such as signatures and virtual sensors.
RA VPN Policies	Whether to discover remote access VPN policies such as IKE proposals and IPsec proposals.
Finish button	Saves your wizard definitions and closes the wizard. The Discovery Status dialog box opens to display the status of the configuration file import and discovery (see Discovery Status Dialog Box, page D-19).

Device Information Page—New Device

Use the New Device wizard’s Device Information page for adding new devices (that do not yet exist in the network) to specify the device’s identifying information.

Navigation Path

To start the New Device wizard, from Device view, select **File > New Device**, or click the **Add** button in the device selector.

Related Topics

- [Understanding the Device View, page 6-2](#)
- [Adding Devices by Manual Definition, page 6-14](#)
- [Device Credentials Page, page C-22](#)
- [Device Grouping Page, page C-32](#)

Field Reference

Table C-5 *New Device Wizard, Device Information Page When Adding New Devices*

Element	Description
Device Type	
Device Type selector	Organizes the devices by device-type and device-family. Select the device type for the new device.
System Object ID	The system object identifiers for the device type you selected from the Device Type selector. Select the correct ID for your device.
Identity	
IP Type	Whether the IP address for the device is static (defined on the device) or dynamic (supplied by a DHCP server). Depending on the IP type you select, the displayed fields differ.
Hostname (Static IP only)	<p>The DNS hostname for the device. Enter the DNS hostname if the IP address is not known.</p> <p>The maximum length is 70 characters. Valid characters are: 0–9; uppercase A–Z; lowercase a–z; and hyphen (-).</p> <p>Note You must enter either the DNS hostname or the IP address, or both.</p> <p>Two devices cannot have the same DNS hostname and domain name combination.</p>
Domain Name (Static IP only)	<p>The DNS domain name for the device.</p> <p>The maximum length is 70 characters. Valid characters are: 0–9; uppercase A–Z; lowercase a–z; period (.) and hyphen (-).</p>
IP Address (Static IP only)	<p>The management IP address of the device. The IP address must be in the dotted quad format, for example 10.64.3.8.</p> <p>Note You must enter either the IP address or the DNS hostname, or both.</p>
Display Name	<p>The name to display in the Security Manager Device selector. If you enter a hostname or IP address, it is entered automatically in this field, but you can change it.</p> <p>The maximum length is 70 characters. Valid characters are: 0–9; uppercase A–Z; lowercase a–z; and the following characters: _ - . : and space.</p> <p>Note Two devices cannot have the same display name.</p>

Table C-5 ***New Device Wizard, Device Information Page When Adding New Devices (Continued)***

Operating System	
OS Type	The type of operating system. Based on the device type, the OS type is selected automatically.
Image Name	The name of the image that will run on the device.
Target OS Version	The target OS version for which you want to apply the configuration. This selection determines the type of commands used when Security Manager generates configuration files.
Options	The additional options available on the device. Select IPS if the IPS feature is available on the device.
Contexts	Whether the device hosts a single security context (Single) or multiple security contexts (Multi). This field is displayed only if the OS type is an FWSM, ASA, or PIX Firewall 7.0.
Operational Mode	The mode in which the device is operating. This field is displayed only if the OS type is FWSM, ASA, or PIX Firewall 7.0. The options available are: Transparent, Routed, or Mixed. Mixed applies only to FWSM 3.1 and higher devices when you select Multi for Contexts.

Auto Update or CNS-Configuration Engine

This group is named differently depending on the device type you select:

- Auto Update—For PIX Firewall and ASA devices.
- CNS-Configuration Engine—For Cisco IOS Routers.

Use these fields to identify the server that manages a device with a dynamic IP address, or a Cisco IOS router with a static IP address that uses a Configuration Engine.

Note For Catalyst 6500/7600 and FWSM devices, this field is not active.

Server	<p>The Auto Update Server or Configuration Engine that manages the device.</p> <p>You can add servers to the list by selecting Add Servers, which opens the Server Properties dialog box (see Server Properties Dialog Box, page C-15). You can also edit the properties of a server by selecting Edit Server, which opens the Available Servers dialog box (see Available Servers Dialog Box, page C-18).</p> <p>For more information on managing this list of servers, see Adding, Editing, or Deleting Auto Update Servers or Configuration Engines, page 6-19</p>
--------	---

Table C-5 *New Device Wizard, Device Information Page When Adding New Devices (Continued)*

Device Identity	The string value that uniquely identifies the device in Auto Update Server or the Configuration Engine.
Additional Fields	
Manage in Cisco Security Manager	<p>Whether Security Manager manages the device. This check box is selected by default.</p> <p>If the only function of the device you are adding is to serve as a VPN end point, deselect this check box. Security Manager will not manage configurations nor will it upload or download configurations on this device.</p>
Security Context of Unmanaged Device	<p>Whether to manage a security context whose parent (the PIX Firewall, ASA, or FWSM device) is not managed by Security Manager.</p> <p>This field is active only if the device you selected in the Device selector is a firewall device, such as PIX Firewall, ASA, or FWSM and that firewall device supports security contexts.</p> <p>You can partition a PIX Firewall, ASA, or FWSM into multiple security firewalls, also known as security contexts. Each context is an independent system with its own configuration and policies. You can manage these standalone contexts in Security Manager, even though the parent device is not managed by Security Manager. For more information, see Configuring Security Contexts on Firewall Devices, page 16-117.</p> <p>Note If you select this check box, the available target OS version for the security module is displayed in the Target OS Version field.</p>
Finish button	<p>Saves your wizard definitions and closes the wizard.</p> <p>When you click Finish, the system performs device validation tasks. If your entries are valid, the device definitions are saved and the wizard closes. The device is added to the inventory and it appears in the Device selector.</p> <p>If errors are found, the system generates error messages and displays the wizard page where the error occurs.</p>

Server Properties Dialog Box

Use the Server Properties dialog box to specify the properties of an Auto Update Server or Configuration Engine.

Depending on how you open this dialog box, the title of the dialog box might specify the type of server (for example, Auto Update Server Properties or CNS-Configuration Engine Properties). The dialog boxes are essentially identical.

Navigation Path

To open this dialog box, do one of the following:

- Select **Add Server...** from the **Server** field in the Auto Update Server or CNS-Configuration Engine groups on the Device Information page of the New Device wizard when adding a device manually. The selection might also be named Add Auto Update Server or Add Configuration Engine.
- Select **Add Auto Update Server...** from the **CNS Gateway** field on the Device Information page of the New Device wizard when adding a device with a dynamic IP address from the network.
- Select **Add Server...** from the **Server** field in the Auto Update Server or CNS-Configuration Engine groups on the Device Properties—General page. The selection might also be named Add Auto Update Server or Add Configuration Engine.
- Click **Create**, or select a server and click **Edit**, in the Available Servers dialog box (see [Available Servers Dialog Box](#), page C-18).

Related Topics

- [Available Servers Dialog Box](#), page C-18
- [Device Information Page—New Device](#), page C-12
- [Device Information Page – Add Device from Network](#), page C-5
- [Adding, Editing, or Deleting Auto Update Servers or Configuration Engines](#), page 6-19
- [Viewing or Changing Device Properties](#), page 6-23

Field Reference

Table C-6 Server Properties Dialog Box

Element	Description
Type	<p>The type of server you are defining, either Auto Update Server or Configuration Engine.</p> <p>This field is displayed only if you are adding a server. You cannot change the type of an existing server.</p> <p>For new servers, this field is also not displayed if the title of the dialog box specifies the type of server you are adding.</p>
Server Name	The DNS hostname of the server.
Domain Name	The DNS domain name of the server.
IP Address	The IP address of the server.
Display Name	The name to display in Security Manager for the server.
Username	The username for logging into the server.
Password	The password for accessing the server. In the Confirm field, enter the password again.
Port	The port number that the device managed by the Auto Update Server or Configuration Engine uses to communicate with the server. The port number is typically 443.
URN	<p>This field is displayed only for Auto Update Servers.</p> <p>The uniform resource name for the Auto Update Server. The URN is the name that identifies the resource on the Internet. The URN is part of a URL, for example, /autoupdate/AutoUpdateServlet. The full URL could be: <code>https://: server ip:443/autoupdate/AutoUpdateServlet</code></p> <p>where:</p> <ul style="list-style-type: none"> • <code>server ip</code> is the IP address of the Auto Update Server. • 443 is the port number of the Auto Update Server. • /autoupdate/AutoUpdateServlet is the URN of the Auto Update Server.

Available Servers Dialog Box

Use the Available Servers dialog box to add, edit, or delete an Auto Update Server or Configuration Engine.

Depending on how you open this dialog box, the title of the dialog box might specify the type of servers listed (for example, Available Auto Update Servers or Available Configuration Engines). The dialog boxes are essentially identical.

Navigation Path

To open this dialog box, do one of the following:

- Select **Edit Server...** from the **Server** field in the Auto Update Server or CNS-Configuration Engine groups on the Device Information page of the New Device wizard when adding a device manually. The selection might also be named Edit Auto Update Server or Edit Configuration Engine.
- Select **Edit Auto Update Server...** from the **CNS Gateway** field on the Device Information page of the New Device wizard when adding a device with a dynamic IP address from the network.
- Select **Edit Server...** from the **Server** field in the Auto Update Server or CNS-Configuration Engine groups on the Device Properties—General page. The selection might also be named Edit Auto Update Server or Edit Configuration Engine.

Related Topics

- [Device Information Page—New Device, page C-12](#)
- [Device Information Page – Add Device from Network, page C-5](#)
- [Adding, Editing, or Deleting Auto Update Servers or Configuration Engines, page 6-19](#)
- [Viewing or Changing Device Properties, page 6-23](#)

Field Reference

Table C-7 Available Servers Dialog Box

Element	Description
Display Name	The name that is displayed in Security Manager for the server.
Type	The type of server: AUS or CE (CNS-Configuration Engine). This field is not displayed if the title of the dialog box specifies the server type.
IP Address	The IP address of the server.
Server Name	The DNS hostname of the server.
Domain Name	The DNS domain name of the server.
Create button	Opens the Server Properties dialog box where you can add a new server (see Server Properties Dialog Box, page C-15).
Edit button	Opens the Server Properties dialog box where you can edit the information for the selected server (see Server Properties Dialog Box, page C-15).
Delete button	Deletes the selected server. You are asked to confirm the deletion.

Device Information Page—Add Device from File

Use the New Device wizard's Device Information page for adding devices from an export file to select the file and to specify policy discovery options. The export file must be on the Security Manager server; you cannot use an export file on a client system.

Navigation Path

To start the New Device wizard, from Device view, select **File > New Device**, or click the **Add** button in the device selector.

Related Topics

- [Understanding the Device View, page 6-2](#)
- [Adding Devices from an Export File, page 6-16](#)
- [Device Grouping Page, page C-32](#)
- [Discovering Policies, page 7-7](#)

Field Reference

Table C-8 *New Device Wizard, Device Information Page When Adding Devices from Export Files*

Element	Description
Import Devices From	<p>The export file that contains the devices you want to import. Click Browse to select the file on the Security Manager server.</p> <p>When selecting the file, you must also select the correct file type. The export file is a comma-separated values (CSV) file, but it can be in various formats. The export file must be in either CiscoWorks Common Services Device Credential Repository (DCR) or Cisco Security Monitoring, Analysis and Response System (CS-MARS) format.</p>

Device Import Table

After you select a file, Security Manager evaluates its contents and displays the list of devices defined in the file in the table in the upper pane of the page. Security Manager automatically selects all devices whose status is Ready to Import. Typically, these are the devices that do not already exist in the device inventory.

The table contains the following columns.

Import	Select this check box to add the device to the inventory.
Display Name	The name that will be displayed in the Security Manager Device selector.
Host Name	The host name defined on the device.
Transport	The transport protocol that should be used to connect to the device.
Status	Whether Security Manager can import the device. Devices can be imported only if they have the status Ready to Import. For detailed information on a device's status, select it and read the expanded status information in the Status text box in the lower right corner of the page.
Device Type	The type of device.

Details Pane

Below the device import table is a pane that displays the details for the device selected in the table. The Identity information repeats the table fields. The Status text box displays an extended explanation of the import status.

The Discover Device Settings and Transport groups let you specify how Security Manager should import the device, and are explained below.

Table C-8 ***New Device Wizard, Device Information Page When Adding Devices from Export Files (Continued)***

Discover Device Settings	
Discover	<p>The type of elements that should be discovered and added to the inventory. You have these options:</p> <ul style="list-style-type: none"> • Policies and Inventory—Discover policies, interfaces, and service modules (if applicable). This is the default and recommended option. <p>When policy discovery is initiated, the system analyzes the configuration on the device, then imports the configured service and platform policies. When inventory discovery is initiated, the system analyzes the interfaces on the device and then imports the interface list. If the device is a composite device, all the service modules in the device are discovered and imported.</p> <p>If you select this option, the check boxes below are activated and you can use them to control the types of policies that are discovered.</p> <p>Note During discovery, if you import an ACL that is inactive, it is shown as disabled in Security Manager. If you deploy the same ACL, it will be removed by Security Manager.</p> <ul style="list-style-type: none"> • Inventory Only—Discovers interfaces and service modules (if applicable). • No Discovery—All discovery is skipped. No policy, interface, or service module information for the device is added to the device inventory.
Platform Settings	<p>Whether to discover the platform settings, which are also called platform-specific policy domains. Platform-specific policy domains exist on firewall devices and Cisco IOS routers. These domains contain policies that configure features that are specific to the selected platform. For more information, see Service Policies vs. Platform-Specific Policies, page 7-3.</p>
Firewall Policies	<p>Whether to discover firewall policies, which are also called firewall services. Firewall services include policies such as access rules, inspection rules, AAA rules, web filter rules, and transparent rules. For details see, Chapter J, “Firewall Services User Interface Reference”</p>
IPS Policies	<p>Whether to discover IPS policies such as signatures and virtual sensors.</p>
RA VPN Policies	<p>Whether to discover remote access VPN policies such as IKE proposals and IPsec proposals.</p>

Table C-8 ***New Device Wizard, Device Information Page When Adding Devices from Export Files (Continued)***

Transport	
<p>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.</p>	
Protocol	The protocol Security Manager should use when connecting to the device.
Server	For devices with dynamic IP addresses, the name of the Auto Update Server (AUS) or Configuration Engine server the device uses to obtain an address. 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 with dynamic IP addresses, the string value that uniquely identifies the device in the Auto Update Server or the Configuration Engine.
Next button	Click Next to continue to an optional page where you can select a device group for the added files. Otherwise, click Finish .
Finish button	<p>In either case, the Discovery Status page appears, displaying the status of the device import and discovery. Security Manager attempts to log into each device and obtain the type of information you selected, even if you selected no discovery. The login attempts must be successful for the devices to be added to the inventory.</p> <p>If you are adding devices that contain modules, for example, a Catalyst switch with an FWSM, you are prompted for module discovery information.</p>

Device Credentials Page

Use the Device Credentials page of the New Device wizard to add credentials for the device. For information about device credentials, see [Understanding Device Credentials, page 6-4](#).

You are prompted for credentials only when adding devices manually or from the network.

Navigation Path

To start the New Device wizard, from Device view, select **File > New Device**, or click the **Add** button in the device selector.

Related Topics

- [Understanding Device Credentials, page 6-4](#)
- [Adding Devices from the Network, page 6-10](#)
- [Adding Devices by Manual Definition, page 6-14](#)
- [Device Communication Page, page A-14](#)
- [Viewing or Changing Device Properties, page 6-23](#)

Field Reference**Table C-9** **Device Credentials Page, New Device Wizard**

Element	Description
Primary Credentials	
Required for all device types. These credentials are used for SSH and Telnet connections, and for HTTP and HTTPS connections if you select Use Primary Credentials in the HTTP group.	
Username	The username for logging into the device.
Password	The password for logging into the device (User EXEC mode). In the Confirm field, enter the password again.
Enable Password	The password that activates enable mode (Privileged EXEC mode) on the device if the mode is configured on that device. In the Confirm field, enter the password again.
HTTP Credentials	
Credentials for making HTTP or HTTPS connections to a device. Some devices support this type of connection, and other devices (such as IPS devices) require it.	
Use Primary Credentials	Whether Security Manager should use the configured primary credentials for HTTP and HTTPS connections. If the device uses different credentials for HTTP/HTTPS connections, deselect Use Primary Credentials and enter the username and password configured for HTTP/HTTPS. Reenter the password in the Confirm field.
Username	
Password	
HTTP Port	The port to use for HTTP connections. The default is port 80. Change this setting only if the device is configured to accept HTTP connections on a different port.

Table C-9 Device Credentials Page, New Device Wizard (Continued)

HTTPs Port	The port to use for HTTPS connections. The default is port 443 (unless a different default is configured in the Security Manager device communication settings). To change the default, first deselect Use Default . Change this setting only if the device is configured to accept HTTPS connections on a different port.
IPS RDEP Mode	The connection method to use for contacting IPS devices when making RDEP or SDEE connections (for event monitoring).
Certificate Common Name	The name assigned to the certificate. The common name can be the name of a person, system, or other entity that was assigned to the certificate. In the Confirm field, enter the common name again.
Additional Buttons	
RX-Boot Mode button	Opens the RX-Boot Mode Credentials dialog box, where you can enter the credentials for booting the router from a reduced command-set image (RX-Boot). See RX-Boot Mode Credentials Dialog Box, page C-25 . If these credentials are for a Cisco router that runs from flash memory (where it boots only from the first file in flash), you must run an image other than the one in flash to upgrade the flash image. The RX-Boot credentials are for running this other image.
SNMP button	Opens the SNMP Credentials dialog box, where you can specify the SNMP community strings defined on the device. See SNMP Credentials Dialog Box, page C-26 .
Test Connectivity button	Tests whether Security Manager can connect to the device using the credentials you entered and the configured transport method. For more information about testing device connectivity, see Testing Device Connectivity, page 6-21 . This button appears only if you are adding a device manually. If you are adding a device from the network, Security Manager automatically performs the test when you click Next or Finish .
Next button	Continues to the next wizard page. If you are adding devices from the network, Security Manager tests whether it can connect to the device using the identity and credentials you supplied. The Device Connectivity Test dialog box stays open while the test is in progress (see Device Connectivity Test Dialog Box, page C-27). If the test fails, click Details to see detailed error information.

Table C-9 **Device Credentials Page, New Device Wizard (Continued)**

Finish button	<p>Saves your wizard changes and closes the wizard.</p> <p>The behavior of clicking Finish differs depending on whether you are adding devices from the network or you are manually defining a device.</p> <ul style="list-style-type: none"> • Adding Devices from the Network—Security Manager tests whether it can connect to the device using the identity and credentials you supplied. <p>If the test succeeds, the Discovery Status page appears, displaying the status of the device import and discovery. Security Manager attempts to log into each device and obtain the type of information you selected, even if you selected no discovery. The login attempts must be successful for the devices to be added to the inventory.</p> <p>If you are adding devices that contain modules, for example, a Catalyst switch with an FWSM, you are prompted for module discovery information.</p> <ul style="list-style-type: none"> • Adding Devices Manually—The system performs device validation tasks. If the data you entered is incorrect, the system generates error messages and displays the wizard page where the error occurs with a red error icon corresponding to it.
---------------	--

RX-Boot Mode Credentials Dialog Box

Use the RX-Boot Mode Credentials dialog box to add RX-Boot mode credentials, which are used for booting the router from a reduced command-set image (RX-Boot).

Navigation Path

To open the RX-Boot Mode Credentials dialog box, click **RX-Boot Mode** in the Device Credentials page in either the New Device wizard (when adding a device manually or from the network), or the Device Properties page. For more information on getting to these pages, see:

- [Device Credentials Page, page C-22](#)
- [Credentials Page, page C-39](#)

Related Topics

- [Understanding Device Credentials, page 6-4](#)

Field Reference**Table C-10** *RX-Boot Mode Credentials Dialog Box*

Element	Description
Username	The RX-Boot Mode username.
Password	The RX-Boot Mode password. In the Confirm field, enter the password again.

SNMP Credentials Dialog Box

Use the SNMP Credentials dialog box to add SNMP credentials.

Navigation Path

To open the SNMP Credentials dialog box, click **SNMP** in the Device Credentials page in either the New Device wizard (when adding a device manually or from the network), or the Device Properties page. For more information on getting to these pages, see:

- [Device Credentials Page, page C-22](#)
- [Credentials Page, page C-39](#)

Related Topics

- [Understanding Device Credentials, page 6-4](#)

Field Reference**Table C-11** *SNMP Credentials Dialog Box*

Element	Description
SNMP V2C	
These are the credentials for devices running SNMP version 2.	
RO Community String	The read-only community string. In the Confirm field, enter the community string again.

Table C-11 *SNMP Credentials Dialog Box (Continued)*

RW Community String	The read-write community string. In the Confirm field, enter the community string again.
SNMP V3	
These are the credentials for devices running SNMP version 3.	
Username	The SNMP version 3 username.
Password	The SNMP version 3 password. In the Confirm field, enter the password again.
Auth Algorithm	The authorization algorithm for encrypting the password. You can select MD5 or SHA-1.

Device Connectivity Test Dialog Box

Use the Device Connectivity Test dialog box to view whether Security Manager can contact the device using the configured credentials.

Navigation Path

To start the device connectivity test, click **Test Connectivity** from the Credentials page in one of these areas:

- New Device wizard when adding a device manually. See [Adding Devices by Manual Definition, page 6-14](#).
- Device Properties. To open the page, double-click a device in the Device selector or select **Tools > Device Properties**.

The connectivity test is done automatically when you click **Next** or **Finish** on the Credentials page when adding a device from the network.

Related Topics

- [Testing Device Connectivity, page 6-21](#)
- [Device Credentials Page, page C-22](#)
- [Device Properties Page, page C-36](#)
- [Viewing or Changing Device Properties, page 6-23](#)

Field Reference

Table C-12 Device Connectivity Test Dialog Box

Element	Description
Connectivity Protocol	The transport protocol being used to log into the device. Security Manager uses the protocol specified in the device properties for the device, which is usually the default protocol configured on the Device Communications page (see Device Communication Page , page A-14).
Connectivity Status	Displays the status of the test and the time elapsed since the start of the test.
Details button	Click this button to display detailed information about the result of the test. <ul style="list-style-type: none"> Passed tests—The details display the output of the show version command for PIX Firewall, Adaptive Security Appliances (ASA), Firewall Service Modules (FWSM), Cisco IOS routers, and VPN Services Modules (VPNSM), or the output of the getVersion command for IPS Sensors and Cisco IOS IPS Sensors. You can copy the command output and paste it into a file for analysis. Failed tests—The detailed error message.
Abort button	Stops the connectivity test before it is completed.

Service Module Credentials Dialog Box

Use the Service Module Credentials dialog box to add the credentials required to log into supported service modules in a Catalyst 6500/7600 device.

The dialog box includes a group for each slot that contains a supported module, and the type of module is indicated. For example, a group might be called **Slot 3 (IDSM) Credentials**, which indicates that there is an IDSM in the third slot of the chassis.

**Note**

Although Security Manager discovers VPN Shared Port Adapter (SPA) modules, the discovery is done through the chassis and no credentials are required.

Navigation Path

After you discover policies on a Catalyst 6500/7600 chassis, you are asked if you want to discover its service modules. If you click **Yes**, this dialog box appears. You can perform policy discovery using any of these methods:

- When adding a device from the network. See [Adding Devices from the Network, page 6-10](#).
- When adding devices from an export file. See [Adding Devices from an Export File, page 6-16](#).
- When performing policy discovery on a device that is already in the inventory. See [Discovering Policies on Devices Already in Security Manager, page 7-10](#).

Related Topics

- [Configuring Security Contexts on Firewall Devices, page 16-117](#)

Field Reference

Table C-13 Service Module Credentials Dialog Box

Element	Description
Discovery Mode	<p>The types of policies to discovery for this module:</p> <ul style="list-style-type: none"> • Discover Inventory and Policies—Discover inventory and security policies. This is the recommended option. • Discover Inventory Only—Do not discover security policies, but discover inventory, such as VLAN configuration, security contexts, and interfaces. You can discover the policy configuration later by right-clicking the service module and then selecting Discover Policies on Device. • Do Not Discover Module—Skip discovery on this module and do not add it to the inventory.
Connect to FWSM	<p>How Security Manager should access the FWSM:</p> <ul style="list-style-type: none"> • Directly—Connect to the FWSM using its management IP address. This is the recommended approach. It is the required method if you are connecting to a failover device; otherwise, Security Manager might connect to a standby FWSM after a failover. • via Chassis—Connect to the FWSM through the chassis. This method has the restriction that there should be fewer than 20 security contexts defined on the FWSM. Security Manager connects to the Catalyst 6500/7600 device through SSH and then to the FWSM through the session command. The number of concurrent SSH sessions is limited on a Catalyst 6500/7600 device, with a default of 5. Policy discovery uses one SSH session for each security context, so a large number of contexts might lead to connection failures. If you select Directly, Security Manager connects to the FWSM through SSL, which has a greater concurrent session limit.
Management IP	<p>The management IP address for the service module.</p> <p>For FWSMs, this field is not available if you select via Chassis for the connection method.</p>

Table C-13 Service Module Credentials Dialog Box (Continued)

Username	The username for the service module. For FWSMs running in multiple-context mode, a footnote explains which context's username and password to enter, either the system or the admin context. If you are connecting to a multiple-context mode device through the switch chassis, you must configure the same username and password for both the system execution space and the admin context, and specify those credentials in this dialog box.
Password	The User EXEC mode password for the service module. In the Confirm field, enter the password again.
Enable Password (FWSM only)	The Privileged EXEC mode password for the service module. In the Confirm field, enter the password again.

AIM-IPS Module Discovery Dialog Box

Use the AIM-IPS Module Discovery dialog box to add the credentials required to log into an AIM-IPS module on a router you are adding to the inventory.

Navigation Path

After you discover policies on a router chassis that contains an AIM-IPS module, you are asked if you want to discover its modules. If you click **Yes**, this dialog box appears. You can perform policy discovery using any of these methods:

- When adding a device from the network. See [Adding Devices from the Network, page 6-10](#).
- When adding devices from an export file. See [Adding Devices from an Export File, page 6-16](#).
- When performing policy discovery on a device that is already in the network. See [Discovering Policies on Devices Already in Security Manager, page 7-10](#).

Field Reference

Table C-14 AIM-IPS Module Discovery Dialog Box

Element	Description
Discovery	The type of discovery for this module: <ul style="list-style-type: none"> Discover Inventory and Policies—Discover inventory and security policies. This is the recommended option. Do Not Discover Module—Skip discovery on this module and do not add it to the inventory.
IP Address	The management IP address for the module.
HTTP Credentials Group	
The credentials required to log into the module.	
Username	The username for the module.
Password	The password for the specified username. In the Confirm field, enter the password again.
HTTP Port	The port configured for HTTP access to the module. The default is 80.
HTTPS Port	The port configured for SSL (HTTPS) access to the module. The default is defined on the Device Communication page (Tools > Security Manager Administration > Device Communication , for more information, see Device Communication Page, page A-14). The port typically used is 443. To override the default, deselect Use Default and enter the correct port number.
IPS RDEP Mode	The connection method to use for contacting IPS devices when making RDEP or SDEE connections (for event monitoring).
Certificate Common Name	The name assigned to the certificate. The common name can be the name of a person, system, or other entity that was assigned to the certificate. In the Confirm field, enter the common name again.

Device Grouping Page

Use the Device Grouping page of the New Device wizard to assign devices to groups.

Navigation Path

To start the New Device wizard, from Device view, select **File > New Device**, or click the **Add** button in the device selector.

Related Topics

- [Understanding Device Grouping, page 6-36](#)
- [Adding Devices to the Device Inventory, page 6-8](#)

Field Reference

Table C-15 *Device Grouping Page, New Device Wizard*

Element	Description
Group Types, such as Department and Location	<p>The group types defined in Security Manager, for example, Department or Location. Each field contains a list of the device groups defined within that group type. Select the device groups to which the device should belong.</p> <p>If you want to create a new device group, or group type, select Edit Groups from the drop-down list for any of the existing group types. This opens the Edit Device Groups page, where you can create new groups and group types or delete them (see Edit Device Groups Dialog Box, page C-45).</p>
Set values as default	Whether to set the selected groups as the default groups. If you select this option, other devices you add are automatically added to these groups.
Finish button	<p>Saves your wizard definitions and closes the wizard.</p> <p>After you click Finish, the system performs device validation tasks. If the data you entered is incorrect, the system generates error messages and displays the wizard page where the error occurs with a red error icon corresponding to it. Depending on the method you are using to add devices to the inventory, the Discovery Status dialog box might open displaying the status of policy and inventory discovery.</p>

Device Delete Validation Page

Use the Device Delete Validation page to view error and warning messages during device deletion.

Create a Clone of Device Dialog Box

Navigation Path

Select a device from the Device selector, then click the **Delete** button or select **File > Delete Device**. This page appears only when there is an error or warning regarding the deletion.

Related Topics

- [Deleting Devices from the Security Manager Inventory, page 6-30](#)

Field Reference

Table C-16 *Device Delete Validation Page*

Element	Description
Severity	Displays one or all of the following: <ul style="list-style-type: none"> • Error icon—A problem was detected that will prevent you from deleting the device. • Warning icon—Proceed with caution. • Information icon—A minor problem exists.
Device	Displays the name of the device that you are trying to delete.
Result	Provides detailed information about the problem. Double click a row or click the Details button to view long messages.
Details button	Displays the Device Delete Validation Details dialog box, which displays the same information about the select row in a more readable format.
OK button	Proceeds with deletion. The OK button appears only if the problem severity is less than Error. If you want to continue with deleting the device, click OK .

Create a Clone of Device Dialog Box

Use the Create a Clone of Device dialog box to duplicate a device.

Navigation Path

Select the device and select **File > Clone Device**, or right-click the device in the Device selector and select **Clone Device**.

Related Topics

- [Cloning a Device, page 6-29](#)
- [Copying Policies Between Devices, page 7-21](#)

Field Reference**Table C-17** **Create a Clone of Device Dialog Box**

Element	Description
IP Type	The device IP type of the cloned device: Static or Dynamic. You cannot change the IP type when cloning a device.
Hostname (Static IP only)	The DNS hostname for the cloned device. The maximum length is 70 characters. Valid characters are: 0-9; uppercase A-Z; lowercase a-z; and the following characters: -
Domain Name (Static IP only)	The DNS domain name for the cloned device. If you do not provide the domain name, Security Manager uses the default domain name configured on the server.
IP Address (Static IP only)	The management IP address of the cloned device, for example, 10.10.100.1. Note If you do not know the IP address, enter the DNS hostname in the appropriate field. You must enter either the IP address or the DNS hostname for devices with static IP addresses.
Display Name	The unique name for the cloned device. This is the name that appears in Security Manager device lists. The maximum length is 70 characters. Valid characters are: 0-9; uppercase A-Z; lowercase a-z; and the following characters: _ - . : and space.
Device Identity (Dynamic IP only)	The string value that uniquely identifies the device in Auto Update Server or Configuration Engine.
Clone VPN Assignments	Whether to copy the VPN assignments defined for the device. This field is displayed only if the device supports VPN assignments.

Device Properties Page

You can open the Device Properties page in three ways:

- From the Device selector, right-click a device and select **Device Properties**.
- From the Device selector, double-click a device.
- Select a device and select **Tools > Device Properties**.

The Device Properties page has a table of contents in the left pane. Click an entry to view the related page in the right pane. The following topics describe the property categories:

- [General Page, page C-36](#)
- [Credentials Page, page C-39](#)
- [Device Groups Page, page C-42](#)
- [Policy Object Override Pages, page C-42](#)

General Page

Use the Device Properties General page to add or edit information about the basic properties of the device.

Navigation Path

- From the Device selector, right-click a device and select **Device Properties**, then click **General**.
- From the Device selector, double-click a device, then click **General**.
- Select a device and select **Tools > Device Properties**, then click **General**.

Related Topics

- [Understanding Device Properties, page 6-6](#)
- [Credentials Page, page C-39](#)
- [Device Groups Page, page C-42](#)
- [Policy Object Override Pages, page C-42](#)

Field Reference

Figure C-1 Device Properties General Page

Element	Description
Identity	
Device Type	The type of device.
IP Type	Whether the IP address for the device is static (defined on the device) or dynamic (supplied by a DHCP server). Depending on the IP type you select, the displayed fields differ.
Hostname (Static IP only)	<p>The DNS hostname for the device.</p> <p>This is not necessarily the same name that is configured as the hostname on the device. This property is not updated with the hostname specified in the Hostname device property. It is also not updated with the name defined in the device configuration if you rediscover the device.</p> <p>If you added the device to Security Manager by adding its configuration file, the hostname is initially set to the name specified in the configuration file. If no hostname is specified in the configuration, the name of the file is used as the DNS hostname.</p>
Domain Name (Static IP only)	The DNS domain name for the device.
IP Address (Static IP only)	The management IP address of the device, for example 192.168.3.8.
Display Name	<p>The name to display in the Security Manager Device selector.</p> <p>The maximum length is 70 characters. Valid characters are: 0–9; uppercase A–Z; lowercase a–z; and the following characters: _ - . : and space.</p>
Operating System	
OS Type	The family of the operating system running on the device.
Image Name	The name of the image running on the device.
Running OS Version	The version of the operating system running on the device.
Target OS Version	The OS version on which you want to base the device's configuration. When creating a configuration file using the rules you configure, Security Manager uses commands available in the target OS version.

Figure C-1 Device Properties General Page (Continued)

Options	A read-only field whose values are NONE or IPS. The value IPS indicates that the IPS feature is available on the device.
IPS Running OS Version	A read-only field that displays the version of IOS IPS running on the router. This field does not appear if the Options field has the value of NONE.
IPS Target OS Version	A read-only field that displays the target version of IOS IPS running on the router. This field does not appear if the Options field has the value of NONE.
Contexts	Whether the device hosts a single security context (Single) or multiple security contexts (Multi). This field is displayed only if the OS type is an FWSM, ASA, or PIX Firewall 7.0.
Operational Mode	The mode in which the device is operating. This field is displayed only if the OS type is FWSM, ASA, or PIX Firewall 7.0. The options available are: Transparent, Routed, or Mixed. Mixed applies only to FWSM 3.1 and higher devices when you select Multi for Contexts.

Device Communication Settings

Transport Protocol	<p>The transport protocol that Security Manager should use when accessing the device or deploying configurations to it. If you select Use Default, the transport protocol set in the Device Communication page (Tools > Security Manager Administration > Device Communication) is used. You can select a different protocol if the device is not configured to use the default protocol.</p> <p>The available transport protocols differ depending on what the device type supports.</p>
--------------------	--

CS-MARS Monitoring

Monitored By	<p>The CS-MARS server that monitors this device, if any.</p> <p>Click Discover CS-MARS to have Security Manager determine which CS-MARS server is monitoring the device. If only one CS-MARS server is monitoring it, the field is updated with the server name. If there is more than one, you are prompted to select the CS-MARS server to use. Your selection determines which server is accessed when you try to view CS-MARS collected syslogs or events when viewing firewall access rules or IPS signatures in the policy rule tables for the device.</p> <p>Before you can discover a CS-MARS server for the device, the server must be register with Security Manager on the CS-MARS administration page (Tools > Security Manager Administration > CS-MARS). For more information, see CS-MARS Page, page A-4.</p>
--------------	---

Figure C-1 **Device Properties General Page (Continued)****Auto Update or CNS-Configuration Engine**

This group is named differently depending on the device type:

- Auto Update—For PIX Firewall, FWSM, and ASA devices.
- CNS-Configuration Engine—For Cisco IOS routers.

Use these fields to identify the server that manages a device with a dynamic IP address, or a Cisco IOS router with a static IP address that uses a Configuration Engine.

Server	<p>The Auto Update Server or Configuration Engine that manages the device.</p> <p>You can add servers to the list by selecting Add Servers, which opens the Server Properties dialog box (see Server Properties Dialog Box, page C-15). You can also edit the properties of a server by selecting Edit Server, which opens the Available Servers dialog box (see Available Servers Dialog Box, page C-18).</p> <p>For more information on managing this list of servers, see Adding, Editing, or Deleting Auto Update Servers or Configuration Engines, page 6-19</p>
Device Identity	<p>The string value that uniquely identifies the device in Auto Update Server or the Configuration Engine.</p>
Manage in Cisco Security Manager	<p>Whether Security Manager manages the device.</p> <p>If the only function of the device is to serve as a VPN end point, deselect this check box. Security Manager will not manage configurations nor will it upload or download configurations on this device.</p>

Credentials Page

Use the Credentials page to edit device credential information. For information about device credentials, see [Understanding Device Credentials, page 6-4](#).

Navigation Path

Double-click a device in the Device selector, then click **Credentials** on the Device Properties page.

Related Topics

- [Understanding Device Properties, page 6-6](#)
- [General Page, page C-36](#)
- [Device Groups Page, page C-42](#)
- [Policy Object Override Pages, page C-42](#)
- [Managing Device Communication Settings and Certificates, page 6-24](#)

Field Reference**Table C-18** **Credentials Page, Device Properties**

Element	Description
Primary Credentials	
Required for all device types. These credentials are used for SSH and Telnet connections, and for HTTP and HTTPS connections if you select Use Primary Credentials in the HTTP group.	
Username	The username for logging into the device.
Password	The password for logging into the device (User EXEC mode). In the Confirm field, enter the password again.
Enable Password	The password that activates enable mode (Privileged EXEC mode) on the device if the mode is configured on that device. In the Confirm field, enter the password again.
HTTP Credentials	
Credentials for making HTTP or HTTPS connections to a device. Some devices support this type of connection, and other devices (such as IPS devices) require it.	
Use Primary Credentials	Whether Security Manager should use the configured primary credentials for HTTP and HTTPS connections. If the device uses different credentials for HTTP/HTTPS connections, deselect Use Primary Credentials and enter the username and password configured for HTTP/HTTPS. Reenter the password in the Confirm field.
Username	
Password	
HTTP Port	The port to use for HTTP connections. The default is port 80. Change this setting only if the device is configured to accept HTTP connections on a different port.

Table C-18 **Credentials Page, Device Properties (Continued)**

HTTPs Port	<p>The port to use for HTTPS connections. The default is port 443 (unless a different default is configured in the Security Manager device communication settings). To change the default, first deselect Use Default. Change this setting only if the device is configured to accept HTTPS connections on a different port.</p> <p>Note If you configure the local HTTP policy to be a shared policy and assign the HTTP policy to multiple devices, the HTTPS port number setting in the shared policy overrides the port number configured in the Device Credentials page for all devices to which the policy is assigned.</p>
IPS RDEP Mode	The connection method to use for contacting IPS devices when making RDEP or SDEE connections (for event monitoring).
Certificate Common Name	The name assigned to the certificate. The common name can be the name of a person, system, or other entity that was assigned to the certificate. In the Confirm field, enter the common name again.
Additional Fields and Buttons	
Authentication Certificate Thumbprint	The certificate thumbprint for the device that is available in the Security Manager certificate data store. Click Retrieve From Device to obtain the current certificate from the device and to replace the one stored in Security Manager.
RX-Boot Mode button	<p>Opens the RX-Boot Mode Credentials dialog box, where you can enter the credentials for booting the router from a reduced command-set image (RX-Boot). See RX-Boot Mode Credentials Dialog Box, page C-25.</p> <p>If these credentials are for a Cisco router that runs from flash memory (where it boots only from the first file in flash), you must run an image other than the one in flash to upgrade the flash image. The RX-Boot credentials are for running this other image.</p>
SNMP button	Opens the SNMP Credentials dialog box, where you can specify the SNMP community strings defined on the device. See SNMP Credentials Dialog Box, page C-26 .
Test Connectivity button	Tests whether Security Manager can connect to the device using the credentials you entered and the configured transport method. For more information about testing device connectivity, see Testing Device Connectivity, page 6-21

Device Groups Page

Use the Device Groups page to assign the device to device groups. You can also edit or delete device groups from this page.

Navigation Path

Double-click a device in the Device selector, then click **Device Groups** on the Device Properties page.

Related Topics

- [Understanding Device Properties, page 6-6](#)
- [General Page, page C-36](#)
- [Credentials Page, page C-39](#)
- [Policy Object Override Pages, page C-42](#)

Field Reference

Table C-19 *Device Groups Page, Device Properties*

Element	Description
Group Types, such as Department and Location	The group types defined in Security Manager, for example, Department or Location. Each field contains a list of the device groups defined within that group type. Select the device groups to which the device should belong. If you want to create a new device group, or group type, select Edit Groups from the drop-down list for any of the existing group types. This opens the Edit Device Groups page, where you can create new groups and group types or delete them (see Edit Device Groups Dialog Box, page C-45).
Set values as default	Whether to set the selected groups as the default groups. If you select this option, other devices you add are automatically added to these groups.

Policy Object Override Pages

You can override the global settings for many types of policy objects from the Device Properties window of a selected device. This enables you to customize the definition of an object on that device. For more information, see [Overriding Global Objects for Individual Devices, page 9-214](#).

**Note**

For information about the columns specific to each object type, see [Chapter F, “Policy Object Manager User Interface Reference”](#), then click the link for the relevant object page.

Navigation Path

Double-click a device in the Device selector, then click the desired policy object type in the **Policy Object Overrides** folder in the table of contents in the left pane.

Related Topics

- [Policy Object Overrides Window, page F-597](#)
- [Allowing a Global Object to Be Overridden, page 9-215](#)
- [Creating Device-Level Object Overrides, page 9-216](#)
- [Deleting Device-Level Object Overrides, page 9-218](#)

Field Reference

Table C-20 **Device Properties Policy Object Override Pages—Common Fields**

Column	Description
Filter	Click the arrow to display the filtering bar, which enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24 .
Name	The name of the object.
Category	The category that is assigned to the object. See Understanding Category Objects, page 9-48 .
Value Overridden?	Indicates whether the global object definition has been overridden by values defined for the selected device. See Allowing a Global Object to Be Overridden, page 9-215 .
Description	Displays an icon if a description is defined for the object. Double-click the icon to display the description.
Create Override button	Opens the dialog box for that object type so that you can create an override object.

Table C-20 *Device Properties Policy Object Override Pages—Common Fields (Continued)*

Edit Override button	Opens the dialog box for that object type so that you can edit the selected override object.
Delete Override button	Deletes the selected override object and restores the global object definition.

Export Inventory Dialog Box

Use the Export Inventory dialog box to export the Security Manager device inventory to a comma-separated values file in either CiscoWorks Common Services Device Credential Repository (DCR) or Cisco Security Monitoring, Analysis and Response System (CS-MARS) format. You can then import the device inventory into those programs.

You can select a subset of devices for export. The list from which you choose contains only those devices to which you have the appropriate modify permissions.

Navigation Path

To open the Export Inventory dialog box, select **Tools > Export Inventory** while in Device view.

Related Topics

- [Exporting the Device Inventory in DCR or CS-MARS Format, page 6-32](#)

Field Reference

Table C-21 Export Inventory Dialog Box

Element	Description
Available Devices pane	<p>Contains two elements:</p> <ul style="list-style-type: none"> Filter field—Filters and displays a subset of devices and groups based on the filtering criteria you define. For more information, see Create Filter Dialog Box, page C-1. Device Selector—Displays the devices whose information you have the permission to export from Security Manager.
>> button	Moves the selected devices from one pane to the other pane.
<< button	<p>To add a single device or multiple devices, select the devices or a group from the Available Devices pane, then click >>. The selected devices or all of the devices in the selected group move to the Selected Devices pane.</p> <p>To remove a device from the Selected Devices pane, select the device from the Selected Devices pane, then click <<. The selected device moves to the Available Devices pane.</p>
Selected Devices pane	Displays all the devices whose information you are exporting.
Export Inventory To Browse button	<p>The file name and path where the export file should be created. You can select only a location on the Security Manager server.</p> <p>Click Browse to open the Save As dialog box, where you can navigate to the desired folder, enter a name for the file, and select the file type to specify whether you want the export file formatted for DCR or CS-MARS.</p>

Edit Device Groups Dialog Box

Use the Edit Device Groups dialog box to manage the device groups and group types defined in the device inventory.

Add Devices to Group Dialog Box

Navigation Path

Do one of the following:

- Right-click a device group type or a device group in the Device selector and select **Edit Device Groups**.
- Select **File > Edit Device Groups**.

Related Topics

- [Understanding Device Grouping, page 6-36](#)
- [Working with Device Groups, page 6-36](#)

Field Reference

Table C-22 *Edit Device Groups Dialog Box*

Element	Description
Groups	Displays the device groups and group types. To rename a group or type, select it and then click it again to make the text editable. Type in the new name and press Enter.
Add Type button	Click this button to create a new group type. The type is added with a default name. Overtyping the name and pressing Enter.
Add Group to Type button	Click this button to add a device group to the selected device group or group type.
Delete button (trash can)	Click this button to delete the selected device group or group type and all device groups that it contains. Deleting a device group or group type does not delete any devices it contains.

Add Devices to Group Dialog Box

Use the Add Devices to Group page to add devices to the selected device group.

Navigation Path

Select a device group or group type in the Device selector and select **File > Add Devices to Group**, or right-click and select **Add Devices to Group**.

Related Topics

- [Understanding Device Grouping, page 6-36](#)
- [Adding Devices to or Removing Them From Device Groups, page 6-41](#)

Field Reference**Table C-23** **Add Devices to Group Dialog Box**

Element	Description
Available Devices pane	<p>Contains two elements:</p> <ul style="list-style-type: none"> • Filter field—Filters and displays a subset of devices and groups based on the filtering criteria you define. For more information, see Create Filter Dialog Box, page C-1. • Device Selector—Displays the devices that you have the permission to manage in Security Manager.
>> button	Moves the selected devices from one pane to the other pane.
<< button	<p>To add a single device or multiple devices, select the devices or a group from the Available Devices pane, then click >>. The selected devices or all of the devices in the selected group move to the Selected Devices pane.</p> <p>To remove a device from the Selected Devices pane, select the device from the Selected Devices pane, then click <<. The selected device moves to the Available Devices pane.</p>
Selected Devices pane	Displays all the devices that you selected to add to a group.

Add Group Dialog Box

Use the Add Group dialog box to create a device group. Enter a unique name for the group.

Navigation Path

Select a device group or group type in the Device selector and select **File > New Device Group**, or right-click and select **New Device Group**.

Related Topics

- [Understanding Device Grouping, page 6-36](#)
- [Creating Device Groups, page 6-40](#)
- [Adding Devices to or Removing Them From Device Groups, page 6-41](#)

Device Server Assignment Dialog Box

Use the Device Server Assignment dialog box to choose the devices for which you want to create and assign an Auto Update Server (AUS) or Configuration Engine after upgrading from an earlier version of Security Manager to 3.2. AUS and Configuration Engines are not migrated during the upgrade and devices managed by them need to be reassigned to them after the upgrade. These devices are differentiated by a red X icon partially covering the device icon. See *Installation Guide for Cisco Security Manager 3.2* for a description of the procedure to add AUS and Configuration Engines for such devices after they are migrated to 3.2.

**Note**

You can also import AUS and Configuration Engines from an inventory file from CiscoWorks Common Services Device Credential Repository (DCR). For more information about importing devices, see [Adding Devices from an Export File, page 6-16](#).

Navigation Path

To access the Device Server Assignment dialog box, do one of the following:

- From the Device selector, right-click a device with a red X icon, then select **Update Server Info**.
- Click any red X icon in the device selection tree. A warning message is displayed stating that AUS and Configuration Engine information was not migrated after the upgrade process. Click **Yes** to add these servers manually.

Related Topics

- [Server Properties Dialog Box, page C-15](#)
- [Adding, Editing, or Deleting Auto Update Servers or Configuration Engines, page 6-19](#)

Field Reference

Table C-24 Device Server Assignment Dialog Box

Element	Description
Filter	Click the arrow to display the filtering bar, which enables you to filter the information displayed in the table. See Filtering Items in Selectors, page 3-20 .
Available Devices	Lists all devices managed by AUS and CNS with a red X icon. To assign an AUS or Configuration Engine to devices, select one or more items from this list, then click >> to add them to the Selected Devices list.
Selected Devices	Lists all devices for which you want to assign an AUS or Configuration Engine. To remove devices from this list, select the devices, then click <<.
Server	Enables you to select or add an Auto Update Server or a Configuration Engine. If the server does not appear in the list, select + Add Server... to display the Server Properties dialog box. For a description of the fields in the page, see Server Properties Dialog Box, page C-15 .
OK button	Saves your changes to the server and closes the dialog box.

Inventory Status Window

Use the Inventory Status window to view device properties and status for the devices that you are allowed to view. This window summarizes device information so that you do not have to open the device properties for each individual device.

In addition to device property information, you can view summary information about how the policies on each device are configured (whether local, shared, or not configured) and the policy objects that have overrides for each device.

If you are using Performance Monitor to monitor your devices, status information from Performance Monitor is included in the inventory summary. You can also view the status of configuration deployment to the device.

The Inventory Status window contains two panes. Use the upper pane to view a complete listing of all devices, to sort the devices by attribute, or to filter out certain ones. Use the lower pane to view the device property details of the device selected in the upper pane.

Navigation Path

Select **Tools > Inventory Status**.

Related Topics

- [Viewing Inventory Status, page 6-30](#)
- [Credentials Page, page C-39](#)
- [Device Groups Page, page C-42](#)
- [General Page, page C-36](#)
- [Configuring Status Providers, page 1-24](#)
- [Understanding Device Credentials, page 6-4](#)
- [Understanding Device Properties, page 6-6](#)

Field Reference

Table C-25 *Inventory Status Window*

Element	Description
Device Summary Information for All Devices (Upper Pane)	
You can click on the column headings to sort the list based on that field.	
Export button	Click this button to export the inventory as a comma-separated values (CSV) file. You are prompted to specify a file name and to select a folder on the Security Manager server. You can use the export file for reference or analysis.
Filter	When expanded, displays the filter bar, which enables you to filter the information based on conditions you set. For more information, see Filtering Tables, page 3-24 .
Display Name	The name of the device as it is displayed in Security Manager.
Deployment	The status of the configuration deployment for the device. This column appears only if you enabled Deployment as a status provider (see Status Page, page A-47).
Performance Monitor	The status for the device as reported by Performance Monitor. This column appears only if you configured the device to be monitored by a Performance Monitor server, and you configured Security Manager to obtain status from that server. For more information, see Status Page, page A-47 .

Table C-25 **Inventory Status Window (Continued)**

OS Type	The family of the operating system running on the device, for example, IOS, IPS, ASA, FWSM, or PIX.
Running OS Version	The version of the operating system running on the device.
Target OS Version	The target OS version for which you want to apply the configuration. Configurations are based on the commands supported by this version.
Host Name.Domain Name	The DNS host and domain names for the device.
IP Address	The management IP address of the device.
Device Type	The type of device.
Device Properties by Device (Lower Pane)	
Inventory	Lists summary information about the selected device's device properties, deployment methods, device group membership, and the parent device for modules.
Policy	Lists the current status of the policies that can be configured for the selected device, whether the policy is unassigned (not defined), a local policy, or a shared policy.
Policy Object Overrides	Lists policy objects that have overrides defined for the selected device. For more information on policy object overrides, see Policy Object Override Pages, page C-42 .

Table C-25 ***Inventory Status Window (Continued)***

Status	<p>Lists status providers with any status messages for the selected device. The time stamp indicates the time of the last change in status for the device, not the time of the latest polling of the device.</p> <p>Also shown is the highest severity level of the status messages. For Performance Monitor, the event statuses are equivalent to the following Performance Monitor event priorities:</p> <ul style="list-style-type: none"> • Critical events—P1, P2. • Major events—P3. • Minor events—P4. • Warning events—P5.
Navigation buttons	<p>Click the navigation buttons to move through the inventory list. From left to right, buttons mean go to the first device in the list, go to the previous device, go to the next device, and go to the last device. The center field indicates which device is currently selected based on the row number (for example 5/10 means the fifth of 10 devices in the list).</p>