



APPENDIX **C**

Devices User Interface Reference

The following topics describe the user interface information for the Devices page:

- [Devices Page, page C-2](#)
- [Add Device from Network Wizard, page C-7](#)
- [Add Device\(s\) from Config File Wizard, page C-29](#)
- [Add New Device Wizard, page C-34](#)
- [Add Device\(s\) from DCR Wizard, page C-45](#)
- [Device Delete Validation Page, page C-49](#)
- [Create a Clone of <device name> Page, page C-52](#)
- [Device Properties Page, page C-53](#)
- [Device Shortcut Menu Options, page C-62](#)
- [Policy Selector Shortcut Menu Options, page C-63](#)
- [Device Group Shortcut Menu Options, page C-65](#)
- [Edit Device Groups Page, page C-66](#)
- [Add Devices to Group Page, page C-67](#)
- [Add Group Dialog Box, page C-68](#)

Devices Page

Use the Devices page to view device information, to add, edit, or delete devices, and to assign policies to specific devices.

Navigation Path

To open this page, click the **Device View** button in the toolbar.

Related Topics

- [Device Selector, page C-2](#)
- [Policy Selector, page C-7](#)
- [Work Area, page C-7](#)
- [Create Filter Dialog Box, page C-3](#)
- [Understanding the Device View, page 5-24](#)

The Devices page contains two panes ([Figure 5-1](#)). The left pane contains the following two elements:

- Device selector, located in the top left pane. For more information, see [Device Selector, page C-2](#).
- Policy selector, located in the bottom left pane. For more information, see [Policy Selector, page C-7](#).

The right pane is the main content area. For more information, see [Work Area, page C-7](#).

Device Selector

Use the Device selector to filter, add, and delete devices from the Security Manager inventory.

Related Topics

- [Understanding the Device View, page 5-24](#)
- [Policy Selector, page C-7](#)
- [Work Area, page C-7](#)
- [Create Filter Dialog Box, page C-3](#)

Field Reference

Table C-1 Device Selector

Element	Description
Device selector	
Filter	Enables you to filter and display a subset of devices based on the filtering criteria you define. For more information, see Create Filter Dialog Box, page C-3 .
Add button	Opens the New Device - Choose Method wizard page that provides options, which enable you to add devices to the Security Manager inventory.
Delete button	Removes the selected device from the Security Manager inventory.
Device Tree	Lists all device groups and devices added to or created in Security Manager. Each device type is represented by an icon. For information about the icons, see Figure 5-2 .

Create Filter Dialog Box

Use the Create Filter dialog box to filter and display a subset of devices based on the filtering criteria you define.

Navigation Path

Select **Create Filter** from the Filter field in a selector tree.

Related Topics

- [Filtering the Device Selector, page 5-28](#)
- [Device Selector, page C-2](#)

Field Reference

Table C-2 Create Filter Dialog Box

Element	Description
Device selector	
Match Any of the Following	<p>When clicked, creates an “or” relationship between all filter controls that you created in the filter control area.</p> <p>For example, you add the following two controls in the filter control area:</p> <ul style="list-style-type: none"> • Name contains a • Type is ASA <p>If you click OK, the two filter controls are combined into one filter with an “or” in between them.</p> <p>Name contains a or Type is ASA</p> <p>This filter is then available from the arrow in the Filter field.</p> <p>If you select this filter option, the Device selector displays devices that contain an “a” in their name or all devices that are ASA devices. See Filter Control Relationship Example, page 5-29.</p>
Match All of the Following	<p>When clicked, creates an “and” relationship between all the filter controls that you created in the filter control area.</p> <p>For example, you add the following two controls in the filter control area:</p> <ul style="list-style-type: none"> • Name contains a • Type is ASA <p>After you click OK, the two filter controls are combined into one filter with an “and” in between them.</p> <p>Name contains a and Type is ASA</p> <p>This filter is then available from the arrow in the Filter field.</p> <p>If you select this filter option, the Device selector displays all devices that have an “a” in their names and that are ASA devices because only devices that match both criteria are displayed. So only ASA devices that contain “a” in their device name are displayed. See Filter Control Relationship Example, page 5-29.</p>

Table C-2 Create Filter Dialog Box (continued)

Element	Description
First Field—Filter Type	<p>Provides two options:</p> <ul style="list-style-type: none"> • Name—Filters the devices by device name. You specify the device name or portion of the device name in the Filter Value field (third field). • Type—Filters the devices by device type. You specify the type of device in the Filter Value field (third field).
Second Field—Filter Relation	<p>Enables you to narrow the filter results by defining additional parameters. This field establishes a relationship between the filter type and the filter value fields.</p> <ul style="list-style-type: none"> • If you select Name in the Filter Type field (first field), the following options are displayed: <ul style="list-style-type: none"> – contains – doesn't contain – is – isn't – begins with – ends with • If you select Type in the Filter Type field (first field), the following options are displayed: <ul style="list-style-type: none"> – is – isn't

Table C-2 Create Filter Dialog Box (continued)

Element	Description
Third Field—Filter Value	<ul style="list-style-type: none"> • If you select Name in the Filter Type field (first field), the Filter Value field is blank. Enter a string value; either the device name or part of the device name. • If you select Type in the Filter Type field (first field), the following options are displayed: <ul style="list-style-type: none"> – ASA – ASA IPS – PIX – Catalyst 6500/7600 – FWSM – IPSSM – Router – Cisco IDS Network Module – Sensor
Filter Control Content Area	Displays all the filter controls that you created. Filter controls are the filter name, filter relation, and filter value that you selected in a row format.
Add button	Adds a row of filter controls in the Filter Control Content area based on the filter name, filter relation, and filter value that you selected.
Remove button	Removes the selected row of filter control from the Filter Control Content area.
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

Policy Selector

Use the Policies selector located in the bottom left pane of the Devices page to display policies for the device types you select in the Device selector.

Based on the device you select in the Device selector, policies appropriate to that device type are displayed in the Policy selector. For details, see [Working with Device Policies](#), page 5-54.

Related Topics

- [Understanding the Device View](#), page 5-24
- [Working with Device Policies](#), page 5-54
- [Device Selector](#), page C-2
- [Work Area](#), page C-7

Work Area

Use the work to view information. The information displayed in the work area depends on the device you selected from the Device selector and the option you selected from the Policy selector.

Related Topics

- [Understanding the Device View](#), page 5-24
- [Device Selector](#), page C-2
- [Policy Selector](#), page C-7

Add Device from Network Wizard

To add a device from the network, click the **Add** button in the Device selector. The New Device - Choose Method wizard page appears with four options. Select **Add Device from Network**, then click **Next**.

The following topics describe the pages in the Add Device from Network wizard:

- [Device Information Page—Network](#), page C-8
- [Device Credentials Page](#), page C-15

- [Device Grouping Page, page C-28](#)

Device Information Page—Network

Use the Device Information page of the Add Device from Network wizard to add device information.

Navigation Path

You can access the Device Information page from the Add Device from Network wizard. Click the **Add** button in the Device selector, select **Add Device from Network**, then click **Next**.

Related Topics

- [Understanding the Device View, page 5-24](#)
- [Adding Devices to the Security Manager Inventory, page 5-30](#)
- [Device Credentials Page, page C-15](#)
- [Device Grouping Page, page C-28](#)
- [Auto Update Server Properties Dialog Box, page C-13](#)
- [Available Auto Update Servers Dialog Box, page C-14](#)
- [Discovering Policies, page 6-7](#)

Field Reference

Table C-3 *Device Information Page in Add Device from Network Wizard*

Element	Description
Identity—	
IP Type	<p>Provides two options:</p> <ul style="list-style-type: none"> • Static—Select this option if the device has a static IP address. • Dynamic— Applies to Cisco IOS routers only. Select this option if the device has a dynamic IP address obtained from a CNS Gateway running on an Auto Update Server. <p>The device information fields displayed differ, depending on whether you select static or dynamic.</p>

Table C-3 Device Information Page in Add Device from Network Wizard

Element	Description
Hostname	<p>Displayed for static IP types only.</p> <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 the following character: -</p> <p>Note You must enter either the DNS hostname or the IP address.</p> <p>Note Two devices cannot have the same DNS hostname and domain name combination.</p>
Domain Name	<p>Displayed for static IP types only.</p> <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; and the following characters: . -</p>
IP Address	<p>Displayed for static IP types only.</p> <p>The management IP address of the device.</p> <p>Valid characters are . and 0–9. The IP address must be in the dotted quad format, for example, 192.64.3.8.</p> <p>Note You must enter either the IP address or the DNS hostname.</p>
Display Name	<p>For static IP types—Displays the hostname, which you can change. When you enter the hostname, it is entered automatically in the Display Name field.</p> <p>For dynamic IP types—Enter the name that you want displayed for the device.</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	<p>Displayed for dynamic IP types only.</p> <p>The string value that uniquely identifies the device in Auto Update Server.</p>

Table C-3 Device Information Page in Add Device from Network Wizard

Element	Description
CNS Gateway	<p>Displayed for dynamic IP types only.</p> <p>Enables you to select or add an Auto Update Server that is running the CNS Gateway protocol.</p> <p>If the Auto Update Server does not appear in the list, select + Add Auto Update Server... to display the Auto Update Server Properties dialog box. For a description of the fields in the page, see Auto Update Server Properties Dialog Box, page C-13.</p> <p>Security Manager communicates with the AUS server running the CNS Gateway protocol to retrieve the IP address of an IOS device, then discovers directly from the IOS device.</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>Note You cannot add PIX Firewall, ASA, FWSM, or Catalyst 6500/7600 devices with a dynamic IP address from the Add Device from Network page.</p>
OS Type	<p>The family of the operating system running on the device:</p> <p>For static IP types: IOS, IOS - 12.2, 12.1, IOS - Catalyst 6500/7600, ASA, FWSM, or PIX</p> <p>For dynamic IP types: IOS, IOS - 12.2, 12.1</p> <p>Note Select IOS - 12.2, 12.1 to add routers running Cisco IOS versions 12.1, 12.2, and associated releases. However, this selection does not apply to Catalyst 6500/6000 series switches running Cisco IOS software 12.1 or 12.2. Select IOS to add routers running Cisco IOS versions 12.3 and later.</p>
System Context	<p>Discovers the device as a system context instead of a security context.</p> <p>Select the system context check box if the device you are adding is a PIX Firewall 7.0, ASA, or FWSM device that meets the following criteria:</p> <ul style="list-style-type: none"> • The device supports system contexts. • The device is running in multi-mode.

Table C-3 *Device Information Page in Add Device from Network Wizard*

Element	Description
Discover Device Settings	

Table C-3 Device Information Page in Add Device from Network Wizard


Element	Description
Discover	<p>Provides the following discovery options:</p> <ul style="list-style-type: none"> • Policies and Inventory—When selected, discovers policies and interfaces. This is the default option. <p>When policy discovery is initiated, the system analyzes the configuration on the device, then imports the configured service and platform policies into Security Manager to be managed. When inventory discovery is initiated, the system analyzes the interfaces on the device and then imports them into Security Manager to be managed. If the device is a composite device, all the service modules in that device are discovered.</p> <p>If you select this option, the following policies are displayed:</p> <ul style="list-style-type: none"> – Platform Settings—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 6-3. <p>This is the default option.</p> <ul style="list-style-type: none"> – Firewall Policies—Also called firewall services. Firewall services contain policies such as access rules, inspection rules, AAA rules, web filter rules, and transparent rules. For details see, Appendix J, “Firewall Services User Interface Reference.” <p>This is the default option.</p> <ul style="list-style-type: none"> – Discover Policies for Security Context—When selected, discovers policies for security contexts. Security contexts apply to PIX Firewall, ASA, or FWSM devices. This field is active for static IP type only. <hr/> <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> <hr/> <ul style="list-style-type: none"> • Inventory Only—When selected, discovers interfaces. If the device is a composite device, all the service modules in that device are discovered. • No Discovery—When selected, Security Manager does not initiate discovery.

Table C-3 Device Information Page in Add Device from Network Wizard

Element	Description
Back button	Returns to the previous wizard page.
Next button	Advances to the next wizard page.
Cancel button	Closes the wizard without saving your changes.
Help button	Opens help for this page.

Auto Update Server Properties Dialog Box

Use the Auto Update Server Properties dialog box to provide the Auto Update Server properties information.

Navigation Path

Select + **Add Auto Update Server...** from the CNS Gateway field in the Device Information page of the Add Device from Network wizard.

Related Topics

- [Device Information Page—Network, page C-8](#)
- [Available Auto Update Servers Dialog Box, page C-14](#)
- [Adding an Auto Update Server When Adding a Device from Network, page 5-39](#)

Field Reference

Table C-4 Auto Update Server Properties Dialog Box

Element	Description
Server Name	The hostname of the Auto Update Server.
Domain Name	The domain name of the Auto Update Server.
IP Address	The IP address of the Auto Update Server.
Display Name	The name that is displayed for the Auto Update Server.
Username	The username of the Auto Update Server.
Password	The password for accessing the Auto Update Server. In the Confirm field, enter the password again.

Table C-4 Auto Update Server Properties Dialog Box

Element	Description
Port	The port number that the AUS managed device uses to communicate with the Auto Update Server. Port number is typically 443.
URN	The uniform resource name of the Auto Update Server. URN is the name that identifies the resource on the Internet. URN is part of a URL, for example, /autoupdate/AutoUpdateServlet. The full URL could be: https://:<server ip>:443/autoupdate/AutoUpdateServlet where: <ul style="list-style-type: none"> • <server ip> 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.
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

Available Auto Update Servers Dialog Box

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

Navigation Path

Select **Edit Auto Update Servers** from the CNS Gateway field in the Device Information page of the Add Device from Network wizard.

Related Topics

- [Device Information Page—Network, page C-8](#)
- [Auto Update Server Properties Dialog Box, page C-13](#)
- [Editing the Auto Update Server Information when Adding Device from Network, page 5-42](#)
- [Adding an Auto Update Server When Adding a Device from Network, page 5-39](#)

Field Reference

Table C-5 Available Auto Update Servers Dialog Box

Element	Description
Display Name	The name that is displayed for the Auto Update Server.
IP Address	The IP address of the Auto Update Server.
Server Name	The hostname of the Auto Update Server.
Domain Name	The domain name of the Auto Update Server.
Create button	Enables you to add a new Auto Update Server. When clicked, opens the Auto Update Server Properties dialog box. For a description of the elements, see Auto Update Server Properties Dialog Box, page C-13 .
Edit button	Enables you to edit the Auto Update Server information. When clicked, opens the Auto Update Server Properties dialog box. For a description of the elements, see Auto Update Server Properties Dialog Box, page C-13 .
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

Device Credentials Page

Use the Device Credentials page to add credentials for the device. For information about device credentials, see [Understanding Device Credentials, page 5-43](#).



Note

You can use a maximum of 70 characters to define device credentials. The only restriction is that you may not add a space in the password.

Navigation Path

You can access the Device Credentials page from the Add Device from Network and from the Add New Device wizards. To access the wizards, click the **Add** button in the Device selector, then select the appropriate add device method.

Related Topics

- [Understanding Device Credentials, page 5-43](#)

- [Device Validation Error Messages](#), page C-27
- [Add Device from Network Wizard](#), page C-7
- [Add New Device Wizard](#), page C-34
- [Rx-Boot Mode Credentials Dialog Box](#), page C-17
- [SNMP Credentials Dialog Box](#), page C-18
- [HTTP Credentials Dialog Box](#), page C-19

Field Reference

Table C-6 **Device Credentials Page**

Element	Description
Primary Credentials —Required for all device types.	
Username	The username for logging into the device.
Password	The password for logging into the device. In the Confirm field, enter the password again.
Enable Password	The password that activates enable mode on a device if enable mode is configured on that device. In the Confirm field, enter the enable password again.
SDEE Credentials —Displayed for devices that support Intrusion Prevention Systems (IPS), such as Cisco IOS routers, ASA, and IDS.	
Username	The SDEE username.
Password	The SDEE password. In the Confirm field, enter the SDEE password again.
HTTP Credentials —Displayed for devices that support IPS, such as Cisco IOS routers, ASA, and IDS. This information is required for devices that support SDEE.	
HTTP Port	Port 80.
HTTPs Port	Port 443.
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.
Mode	HTTP or HTTPS.
Rx-Boot Mode Credentials Tab	
For more information, see Rx-Boot Mode Credentials Dialog Box , page C-17	
SNMP Credentials Tab	

Table C-6 **Device Credentials Page (continued)**

Element	Description
For more information, see SNMP Credentials Dialog Box, page C-18	
HTTP Credentials Tab —Displayed for PIX Firewall, FWSM, and Catalyst 6500/7600 devices.	
For more information, see HTTP Credentials Dialog Box, page C-19	
Back button	Returns to the previous wizard page.
Next button	Advances to the next wizard page.
Finish button	Saves your wizard definitions and closes the wizard. 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. Otherwise, the Task Status page appears, displaying the status of the device import and discovery.
Cancel button	Closes the wizard without saving your changes.
Help button	Opens help for this page.

Rx-Boot Mode Credentials Dialog Box

Use the RX-Boot Mode Credentials dialog box to add RX-Boot mode credentials.

Navigation Path

You can access the RX-Boot Mode Credentials dialog box from the Device Credentials page in the Add Device from Network and the Add New Device wizards. To access the wizards, click the **Add** button in the Device selector, then select the appropriate add device method.

Related Topics

- [Add Device from Network Wizard, page C-7](#)
- [Add New Device Wizard, page C-34](#)
- [Device Credentials Page, page C-15](#)

Field Reference

Table C-7 *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 Rx-Boot mode password again.
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

SNMP Credentials Dialog Box

Use the SNMP Credentials dialog box to add SNMP credentials.

Navigation Path

You can access the SNMP Credentials dialog box from the Device Credentials page in the Add Device from Network and the Add New Device wizards. To access the wizards, click the **Add** button in the Device selector, then select the appropriate add device method.

Related Topics

- [Add Device from Network Wizard, page C-7](#)
- [Add New Device Wizard, page C-34](#)
- [Device Credentials Page, page C-15](#)

Field Reference

Table C-8 *SNMP Credentials Dialog Box*

Element	Description
SNMP V2C	
RO Community String	The read-only community string. In the Confirm field, enter the community string again.

Table C-8 *SNMP Credentials Dialog Box (continued)*

Element	Description
RW Community String	The read-write community string. In the Confirm field, enter the community string again.
SNMP V3	
Username	The SNMP V3 username.
Password	The SNMP V3 password. In the Confirm field, enter the password again.
Auth Algorithm	The authorization algorithm for encrypting the password. Valid selections are MD5 or SHA-1.
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

HTTP Credentials Dialog Box

Use the HTTP Credentials dialog box to add HTTP credentials.

Navigation Path

You can access the HTTP Credentials dialog box from the Device Credentials page in the Add Device from Network and the Add New Device wizards. To access the wizards, click the **Add** button in the Device selector, then select the appropriate add device method.

Related Topics

- [Add Device from Network Wizard, page C-7](#)
- [Adding Devices to the Security Manager Inventory, page 5-30](#)
- [Device Credentials Page, page C-15](#)

Field Reference

Table C-9 HTTP Credentials Dialog Box

Element	Description
Username	The HTTP username.
Password	The HTTP password.
HTTP Port	Port 80.
HTTPS Port	Port 443.
Certificate Common Name	The common 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 password again.
Mode	HTTP or HTTPS.
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

Device Connectivity Test Dialog Box

Use the Device Connectivity Test dialog box to determine whether the device you are adding (or a device that has been added to the inventory) can be reached by Security Manager. The transport protocol used to test device connectivity, the status of connectivity test, and the time elapsed are displayed after connectivity test is complete. For the procedure, see [Verifying Device Connectivity from Security Manager, page 5-47](#).

Navigation Path

To access the Device Connectivity Test dialog box, do one of the following:

- In Device view, click the **Add** button in the Device selector, then select the [Add New Device Wizard, page C-34](#), then enter device identity information in the [Device Information Page—New Device, page C-35](#), and then enter the username, password and click **Test Connectivity** from the [Device Credentials Page, page C-15](#).
- Open the Device Properties page in one of the three ways and click **Test Connectivity**:

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

Related Topics

- [Device Credentials Page, page C-15](#)
- [Device Properties Page, page C-53](#)

Field Reference

Table C-10 **Device Connectivity Test Dialog Box**

Element	Description
Connectivity Protocol	<p>The transport protocol, such as SSL, SSH, AUS, CNS, or TMS, that is set on the device. Security Manager communicates with the device according to the transport mechanism or protocols you set on the device.</p> <p>For Cisco IOS routers and Catalyst 6500/7600 switches, the default transport protocol you have specified for all devices in the Device Communication settings window is used to test connectivity.</p>
Connectivity Status	
Connectivity Test Passed/Failed	Displays whether the connectivity test was successful.
Time Elapsed	Displays the amount of time that has elapsed since the connectivity test was started.
Details button	<p>If the device can be reached, opens the Details dialog box and displays 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.</p> <p>If the device cannot be reached, an error message states the probable cause and its possible solution. Take the recommended action to correct the error.</p>

Table C-10 **Device Connectivity Test Dialog Box (continued)**

Element	Description
Abort button	Aborts the connectivity test. Closes the dialog box. This button is enabled during the device connectivity test operation.

FWSM Credentials and VPN SPA Slot Location Dialog Box

Use the Firewall Service Module Credentials and VPN SPA Slot Location dialog box to add FWSM credentials and Catalyst VPN Shared Port Adapter (VPN SPA) subslot locations.

Navigation Path

After you have successfully added a Catalyst 6500/7600 device as described in [Adding Catalyst 6500/7600 Devices from the Network](#), you are asked if you want to proceed with FWSM inventory and policy discovery. If you click **Yes**, the Firewall Service Module Credentials and VPN SPA Slot Location window appears.

Related Topics

- [Add Device from Network Wizard, page C-7](#)
- [Adding Catalyst 6500/7600 Devices from the Network, page 5-33](#)
- [Configuring Security Contexts on Firewall Devices, page 15-105](#)

Field Reference

Table C-11 Firewall Service Module Credentials and VPN SPA Slot Location Dialog Box

Element	Description
Slot <number> Credentials	
Management IP	<p>The management IP address for the FWSM.</p> <p>Although this is optional, we recommend that you enter the management IP address because:</p> <ul style="list-style-type: none"> • If you do not enter the management IP address, 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. If there are a large number of security contexts, even with the retry mechanism in place, Security Manager might fail to connect. • If you do enter the management IP address, Security Manager connects to the FWSM through SSL, which has a greater concurrent session limit. <p>For FWSM failover management, the management IP address serves as a logical address to connect to an active FWSM. Without the management IP address, Security Manager might connect to a standby FWSM after a failover switch.</p>
Username	<p>The username for the FWSM.</p> <p>If the device you are adding is a multi-mode FWSM, and you entered the management IP address, you must configure the same username, password, and enable password for both System Space and Admin Context in the Catalyst 6500/7600 device and enter those credentials in this field. For details, see Adding Catalyst 6500/7600 Devices from the Network, page 5-33.</p>
Password	<p>The password for the FWSM. In the Confirm field, enter the password again.</p> <p>If the device you are adding is a multi-mode FWSM, and you entered the management IP address, you must configure the same username, password, and enable password for both System Space and Admin Context in the Catalyst 6500/7600 device and enter those credentials in this field. For details, see Adding Catalyst 6500/7600 Devices from the Network, page 5-33.</p>

Table C-11 Firewall Service Module Credentials and VPN SPA Slot Location Dialog Box

Element	Description
Enable Password	The enable password for the FWSM. In the Confirm field, enter the password again. If the device you are adding is a multi-mode FWSM, and you entered the management IP address, you must configure the same username, password, and enable password for both System Space and Admin Context in the Catalyst 6500/7600 device and enter those credentials in this field. For details, see Adding Catalyst 6500/7600 Devices from the Network , page 5-33.
Discover Policies check box	Discovers policies for the FWSM. This check box is selected by default. If you deselect the check box, only inventory data, such as VLAN configuration, security contexts, and interfaces are discovered. You can discover the policy configuration later by right-clicking an FWSM, then selecting Discover Policies on Device .
VPN SPA Slots	The location of any Cisco IPSec VPN SPA installed on the device. Each slot is divided into two subslots that can hold one to two VPN SPAs. Enter the slot and subslot location of each installed VPN SPA, separated by a comma. You can also click Select to open the VPN SPA Slot Selector from which you can select the slot and subslot locations from a list. For more information about configuring a VPN SPA blade, see Configuring a Catalyst VPN Shared Port Adapter (VPN SPA) Blade , page 9-43.
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

VPN SPA Slots Dialog Box

Use the VPN SPA Slots dialog box to add the locations of any VPN SPAs installed on Catalyst 6500/7600 devices.

Navigation Path

After you have successfully added a Catalyst 6500/7600 device as described in [Adding Catalyst 6500/7600 Devices from the Network](#), you are asked if you want to proceed with FWSM inventory and policy discovery. If you decide not to discover service modules and policies at this time by clicking **No**, the VPN SPA Slots Dialog Box appears.

Related Topics

- [Add Device from Network Wizard, page C-7](#)
- [Adding Catalyst 6500/7600 Devices from the Network, page 5-33](#)
- [Adding VPN SPA Slot Locations, page 5-35](#)
- [Configuring a Catalyst VPN Shared Port Adapter \(VPN SPA\) Blade, page 9-43](#)

Field Reference**Table C-12** *VPN SPA Slots Dialog Box*

Element	Description
VPN SPA Slots	The location of any VPN SPAs installed on the device. Each slot is divided into two subslots that can hold one to two VPN SPAs. Enter the slot and subslot location of each VPN SPA installed, separated by a comma. You can also click Select to open the VPN SPA Slot Selector in which you can choose the slot and subslot locations from a list. For more information about configuring a VPN SPA blade, see Configuring a Catalyst VPN Shared Port Adapter (VPN SPA) Blade, page 9-43 .
Select button	Opens the VPN SPA Slot selector. For details see VPN SPA Slot Selector, page C-25 .
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

VPN SPA Slot Selector

Use the VPN SPA Slot selector to add the locations of any Cisco VPN SPAs (VPN SPAs) installed on Catalyst 6500/7600 devices. A slot can hold two separate VPN SPAs, therefore you must enter a subslot number. The subslot number for the first subslot is 0, and for the second one is 1.

Navigation Path

You can access the VPN SPA Slot selector in one of two ways:

- Click **Select** next to the VPN SPA Slots field in the Firewall Service Module Credentials and VPN SPA Slot Location Dialog Box.
- Click **Select** next to the VPN SPA Slots field in the VPN SPA Slots dialog box that appears when you decline policy discovery for service modules on a Catalyst 6500/7600 device(s).

For the procedure, see [Adding VPN SPA Slot Locations, page 5-35](#).

Related Topics

- [Add Device from Network Wizard, page C-7](#)
- [Adding Catalyst 6500/7600 Devices from the Network, page 5-33](#)
- [Configuring a Catalyst VPN Shared Port Adapter \(VPN SPA\) Blade, page 9-43](#)

Field Reference

Table C-13 **VPN SPA Slot Selector**

Element	Description
Available Slots/Subslots	<p>Contains two elements:</p> <ul style="list-style-type: none"> • Filter field—Filters and displays a subset of devices based on the filtering criteria you define. For more information, see Create Filter Dialog Box, page C-3. • Available Slot/Subslots List—Displays list of available slots, numbered according to the number of slots on the device chassis on the left of the “/”, and two subslots numbered 0 and 1 to the right of the “/”. A VPN SPA card resides in one half of a slot, called a subslot, so each slot can contain one or two VPN SPA cards.
>> button	Moves the selected slots from one pane to the other pane.
<< button	
Selected Slots/Subslots	Displays all the Slot/Subslots that you selected.
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

Device Validation Error Messages

When you add a device, Security Manager validates the data you entered. If the data is incorrect, the system generates error messages and displays the page on which the error occurs with a red error icon corresponding to it.

Security Manager does not validate whether the data you entered will allow you to contact the device. It validates whether the data is formatted correctly, whether you have entered duplicate display name and hostname combinations, and whether the display name you entered exists in DCR. The following error messages could be displayed:

Cannot Add a Display Name that Exists in DCR

If you are in the Add New Device page and you enter a display name that already exists in DCR (but not in Security Manager), a Duplicate Device Notification window displays the following message:

A device with the same display name exists in DCR. Duplicate display names are not allowed in DCR. To change the display name, click No. To import the existing device from DCR into Cisco Security Manager, click Yes.

If you click No, the Add New Device page appears. You can enter another display name and continue adding the device. For a description of the elements in this page, see [Add New Device Wizard, page C-34](#).

If you click Yes, the Add Device from DCR page appears, with the device name selected in the DCR List of Devices pane. Click >>. The selected device moves to the Selected Devices pane. For a description of the elements in this page, see [Add Device\(s\) from DCR Wizard, page C-45](#).

Cannot Add a DNS Hostname and Domain Name Combination that Exists in DCR

When you are in the Add New Device page and you enter a hostname and domain name combination that already exists in DCR (but not in Security Manager), a Duplicate Device Notification window displays the following message:

A device with the same DNS (hostname + domain name) exists in DCR. Duplicate DNS is not allowed in DCR. To change the DNS, click No. To import the existing device from DCR into Cisco Security Manager, click Yes.

If you click No, the Add New Device page appears. You can enter another hostname and domain name combination and continue adding the device. For a description of the elements in this page, see [Add New Device Wizard, page C-34](#).

If you click Yes, the Add Device from DCR page appears, with the device name selected in the DCR List of Devices pane. Click >>. The selected device moves to the Selected Devices pane. For a description of the elements in this page, see [Add Device\(s\) from DCR Wizard, page C-45](#).

Device Grouping Page

Use the Device Grouping page to assign devices to groups.

Navigation Path

You can access the Device Grouping page from all of the add device wizards. For the procedures, see:

- [Adding Devices to the Security Manager Inventory, page 5-30](#)
- [Adding Catalyst 6500/7600 Devices from the Network, page 5-33](#)

Related Topics

- [Understanding Device Grouping, page 5-57](#)
- [Edit Device Groups Page, page C-66](#)
- [Adding Devices to the Security Manager Inventory, page 5-30](#)

Field Reference

Table C-14 Device Grouping Page

Element	Description
Group Types, such as Department and Location	The group type, for example, Department or Location, into which the device will be grouped. Enables you to select an existing group or to create a new group under a group type. To create a new group, click the arrow, then select Edit Groups . The Edit Device Groups page appears. For a description of the fields in this page, see Edit Device Groups Page, page C-66 .
Set values as default	When selected, sets the current values as defaults. These values are defaults for adding and editing device groups later.
Back button	Returns to the previous wizard page.
Finish button	Saves your wizard definitions and closes the wizard. 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. Otherwise, the Task Status page appears, displaying the status of the device import and discovery.
Cancel button	Closes the wizard without saving your changes.
Help button	Opens help for this page.

Add Device(s) from Config File Wizard

To add a device from a config file, click **Add** in the Device selector. The New Device - Choose Method wizard page appears with four options. Select **Add Devices from Config File**, then click **Next**.

The following topics describe the pages in the Add Device from Config File wizard:

- [Device Information Page—Config File, page C-30](#)
- [Device Grouping Page, page C-28](#)

Device Information Page—Config File

Use the Device Information page of the Add Device from Config File wizard to add device information.

Navigation Path

You can access the Device Information page from the Add Device from Config File wizard. Click the **Add** button in the Device selector, select **Add Device from Config File**, then click **Next**.

Related Topics

- [Understanding the Device View, page 5-24](#)
- [Adding Devices to the Security Manager Inventory, page 5-30](#)
- [Device Grouping Page, page C-28](#)
- [Device Validation Error Messages, page C-27](#)
- [Discovering Policies, page 6-7](#)

Field Reference

Table C-15 *Device Information Page in Add Device from Config File Wizard*

Element	Description
Device Type	
Device Type selector	<p>Organizes the devices by device-type and device-family. Select the device type for the new device.</p> <p>Note If you do not know the device type, select the device-family folder. Security Manager automatically selects the first available device type under that family.</p> <p>System object IDs for that device type are displayed in the SysObjectId field.</p>

Table C-15 **Device Information Page in Add Device from Config File Wizard (continued)**

Element	Description
SysObjectId	<p>The system object IDs for the device type you selected from the Device Type selector.</p> <p>When you click the device type from the Device Type selector, the system object IDs for that particular device are displayed in this field.</p> <p>When you specify the device type, the first available system object ID of the first device type is selected by default. You can select another one if needed.</p>
Configuration Files	Enter the full path to the device configuration file, or click Browse to navigate to the file in the directory structure. You can include multiple device configuration files, of the same device type, by using commas to separate the files.
Browse button	Opens the Choose Files dialog box, which enables you to navigate and locate the device configuration files. For elements in this page, see Choose Files Dialog Box, page C-33 .

Table C-15 Device Information Page in Add Device from Config File Wizard (continued)


Element	Description
Discover Device Settings	
Discover	<p>Provides the following discovery options:</p> <ul style="list-style-type: none"> • Policies and Inventory—When selected, discovers policies and interfaces. This is the default option. <p>When policy discovery is initiated, the system analyzes the configuration on the device, then imports the configured service and platform policies into Security Manager to be managed. When inventory discovery is initiated, the system analyzes the interfaces on the device and then imports them into Security Manager to be managed. If the device is a composite device, all the service modules in that device are discovered.</p> <p>If you select this option, the following policies are displayed:</p> <ul style="list-style-type: none"> – Platform Settings—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 6-3. <p>This is the default option.</p> <ul style="list-style-type: none"> – Firewall Policies—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, Appendix J, “Firewall Services User Interface Reference.” <p>This is the default option.</p> <hr/> <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> <hr/> <ul style="list-style-type: none"> • Inventory Only—When selected, discovers interfaces. If the device is a composite device, all the service modules in that device are discovered. • No Discovery—When selected, Security Manager does not initiate discovery.
Back button	Returns to the previous wizard page.

Table C-15 **Device Information Page in Add Device from Config File Wizard (continued)**

Element	Description
Next button	Advances to the next wizard page.
Finish button	Saves your wizard definitions and closes the wizard. 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. Otherwise, the Task Status page appears, displaying the status of the device import and discovery.
Cancel button	Closes the wizard without saving your changes.
Help button	Opens help for this page.

Choose Files Dialog Box

Use the Choose Files dialog box to navigate and locate the device configuration file.

Navigation Path

Click the **Browse** button in the Device Information page of the Add Device from Config File wizard.

Related Topics

- [Device Information Page—Config File, page C-30](#)

Field Reference

Table C-16 Choose Files Dialog Box

Element	Description
Left pane	Displays all the folders on the server.
Right pane	The contents of the folder that you selected in the left pane. Enables you to navigate and select the appropriate configuration files. Note You cannot choose multiple configuration files in sequence by pressing Ctrl-A (Select all), or by selecting the first file in the list and pressing the down arrow key while holding down the Shift key. Instead, click the first file in the range; then, hold down the Shift key while clicking the last configuration file in the range to add multiple files that are listed consecutively. However, you can choose multiple individual files by holding down the Ctrl key and clicking on the individual files.
File Selected	Displays the configuration files that you selected from the right pane.
File of Type	Determines the type of files you want displayed in the right pane. When you select or enter a file type, corresponding files are displayed in the right pane.
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

Device Grouping Page

For elements in the Device Grouping page, see [Device Grouping Page, page C-28](#).

Add New Device Wizard

To add a single device, click **Add** in the Device selector. The New Device - Choose Method wizard page appears with four options. Select **Add New Device**, then click **Next**.

The following topics describe the pages in the Add New Device wizard:

- [Device Information Page—New Device, page C-35](#)

- [Device Credentials Page, page C-15](#)
- [Device Grouping Page, page C-28](#)

Device Information Page—New Device

Use the Device Information page of the Add New Device wizard to add device information.

Navigation Path

You can access the Device Information page from the Add New Device wizard. Click the **Add** button in the Device selector, select **Add New Device**, then click **Next**.

Related Topics

- [Understanding the Device View, page 5-24](#)
- [Adding Devices to the Security Manager Inventory, page 5-30](#)
- [Device Credentials Page, page C-15](#)
- [Device Grouping Page, page C-28](#)
- [Device Validation Error Messages, page C-27](#)
- [Server Properties Dialog Box, page C-40](#)
- [Available Servers Dialog Box, page C-41](#)
- [CNS-Configuration Engine Properties Dialog Box, page C-42](#)
- [Available Configuration Engines Dialog Box, page C-43](#)

Field Reference

Table C-17 *Device Information Page in Add New Device Wizard*

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 IDs for that device type are displayed in the SysObjectId field.

Table C-17 **Device Information Page in Add New Device Wizard (continued)**

Element	Description
Selected Device Type	Displays the device type you selected in the Device Type selector.
SysObjectId	The system object IDs for the device type you selected from the Device Type selector. The first system object ID is selected by default. You can select another one if needed.
Identity	
IP Type	Provides two options: Static or Dynamic. Depending on the IP type you select, the displayed fields differ.
Hostname	Displayed for static IP types only. The DNS hostname for the device. Enter the DNS hostname if the IP address is not known. The maximum length is 70 characters. Valid characters are: 0–9; uppercase A–Z; lowercase a–z; and the following character: - Note You must enter either the DNS hostname or the IP address. Two devices cannot have the same DNS hostname and domain name combination.
Domain Name	Displayed for static IP types only. The DNS domain name for the device. The maximum length is 70 characters. Valid characters are: 0–9; uppercase A–Z; lowercase a–z; and the following characters: . -
IP Address	Displayed for static IP types only. The management IP address of the device. Valid characters are. and 0–9. The IP address must be in the dotted quad format, for example 192.64.3.8. Note This field is active only if the IP type is static. Note You must enter either the IP address or the DNS hostname.

Table C-17 Device Information Page in Add New Device Wizard (continued)

Element	Description
Display Name	<p>Displays the hostname, which you can change. When you enter the hostname, the same name is entered automatically in the Display Name field.</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> <p>Note If the display name you enter already exists in DCR, a dialog box appears.</p>
Operating System	
OS Type	Based on the device type, the OS type is selected automatically.
Image Name	The name of the image.
Target OS Version	The target OS version for which you want to apply the configuration.
Options	A read-only field whose values are NONE or IPS. The value IPS indicates that the IPS feature is available on the device.
Contexts	This field is displayed only if the OS type is an FWSM, ASA, or PIX Firewall 7.0. The two options available are: Single or Multi.
Operational Mode	This field is displayed only if the OS type is an FWSM, ASA, or PIX Firewall 7.0. The two options available are: Transparent, Routed, or Mixed (Mixed applies only to FWSM 3.1 when the Contexts is Multi).
Auto Update—Displayed for PIX Firewall and ASA devices.	
Note For Catalyst 6500/7600 and FWSM devices, this field is not active.	
Server	<p>Enables you to select or add an Auto Update Server or a Configuration Engine.</p> <p>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-40.</p>
Device Identity	The string value that uniquely identifies the device in Auto Update Server or the Configuration Engine.
CNS-Configuration Engine—Displayed for Cisco IOS routers.	
Note This field is not active for Catalyst 6500/7600 and FWSM devices.	

Table C-17 **Device Information Page in Add New Device Wizard (continued)**

Element	Description
Server	<p>Depending on the IP type selected, Static or Dynamic, different information is displayed:</p> <ul style="list-style-type: none"> • Cisco IOS routers with static IP addresses—Enables you to select or add a Configuration Engine. If the Configuration Engine does not appear in the list, select + Add Configuration Engine... to display the CNS-Configuration Engine Properties dialog box. For a description of the fields in the page, see CNS-Configuration Engine Properties Dialog Box, page C-42. • Cisco IOS routers with dynamic IP addresses—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-40.
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>When selected, 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, this check box should be deselected. Security Manager will not manage configurations nor will it upload or download configurations on this device.</p>

Table C-17 **Device Information Page in Add New Device Wizard (continued)**

Element	Description
Security Context of Unmanaged Device	<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 context.</p> <p>When selected, manages a security context, whose parent (PIX Firewall, ASA, or FWSM) is not managed by Security Manager.</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 (PIX Firewall, ASA, or FWSM) is not managed by Security Manager. For more information, see Configuring Security Contexts on Firewall Devices, page 15-105.</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>
Back button	Returns to the previous wizard page.
Next button	Advances to the next wizard page.
Finish button	<p>Saves your wizard definitions and closes the wizard.</p> <p>When you click Finish, the system performs device validation tasks. If all looks okay, the wizard 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>
Cancel button	Closes the wizard without saving your changes.
Help button	Opens help for this page.

Server Properties Dialog Box

Use the Server Properties dialog box to provide the Auto Update Server or Configuration Engine properties information.

Navigation Path

Click the **+ Add Server...** from the Server field in the Device Information page of the Add New Device wizard. For detailed procedure, see [Adding an Auto Update Server or Configuration Engine When Adding a New Device](#), page 5-38.

Related Topics

- [Available Servers Dialog Box](#), page C-41
- [Device Information Page—New Device](#), page C-35
- [Adding an Auto Update Server or Configuration Engine When Adding a New Device](#), page 5-38

Field Reference

Table C-18 *Server Properties Dialog Box*

Element	Description
Type	The type of server managing the device. Click the arrow to select one of the following options: <ul style="list-style-type: none"> • Auto Update Server—Select this option if the device you are adding is managed by an Auto Update Server. • Configuration Engine—Select this option if the device you are adding is managed by a Configuration Engine.
Server Name	The hostname of the server.
Domain Name	The domain name of the server.
IP Address	The IP address of the server.
Display Name	The name that is displayed for the server.
Username	The username for the server.
Password	The password for accessing the server. In the Confirm field, enter the password again.

Table C-18 **Server Properties Dialog Box**

Element	Description
Port	The port number that the Auto Update Server or Configuration Engine managed device uses to communicate with the server. Port number is typically 443.
URN	<p>This field is displayed when you select Auto Update Server from the Type field only. It is not displayed when you select CNS-Configuration Engine.</p> <p>The uniform resource name for the Auto Update Server. URN is the name that identifies the resource on the Internet. URN is part of a URL, for example, /autoupdate/AutoUpdateServlet. The full URL could be: https://:<server ip>:443/autoupdate/AutoUpdateServlet</p> <p>where:</p> <ul style="list-style-type: none"> • <server ip> 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.
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

Available Servers Dialog Box

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

Navigation Path

Select **Edit Servers** from the Server field in the Device Information page of the Add New Device wizard. For detailed procedure, see [Editing an Auto Update Server or Configuration Engine When Adding a New Device, page 5-41](#).

Related Topics

- [Server Properties Dialog Box, page C-40](#)
- [Device Information Page—New Device, page C-35](#)
- [Editing an Auto Update Server or Configuration Engine When Adding a New Device, page 5-41](#)

- [Adding an Auto Update Server or Configuration Engine When Adding a New Device, page 5-38](#)

Field Reference

Table C-19 Available Servers Dialog Box

Element	Description
Display Name	The name that is displayed for the server.
Type	The type of server: AUS or CNS.
IP Address	The IP address of the server.
Server Name	The hostname of the server.
Domain Name	The domain name of the server.
Create button	Enables you to add a new server. When clicked, the Server Properties dialog box appears. For a description of the elements, see Server Properties Dialog Box, page C-40 .
Edit button	Enables you to edit the server information. When clicked, the Server Properties dialog box appears. For a description of the elements, see Server Properties Dialog Box, page C-40 .
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

CNS-Configuration Engine Properties Dialog Box

Use the CNS-Configuration Engine Properties dialog box to provide the Configuration Engine properties information.

Navigation Path

Click the **+ Add Configuration Engine...** from the Server field in the Device Information page of the Add New Device wizard.

Related Topics

- [Available Configuration Engines Dialog Box, page C-43](#)
- [Device Information Page—New Device, page C-35](#)

Field Reference

Table C-20 *CNS-Configuration Engine Properties Dialog Box*

Element	Description
Server Name	The hostname of the Configuration Engine.
Domain Name	The domain name of the Configuration Engine.
IP Address	The IP address of the Configuration Engine.
Display Name	The name that is displayed for the Configuration Engine.
Username	The username for the Configuration Engine.
Password	The password for accessing the Configuration Engine. In the Confirm field, enter the password again.
Port	The port number that the CNS managed device uses to communicate with the Configuration Engine. Port number is typically 443.
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

Available Configuration Engines Dialog Box

Use the Available Configuration Engines dialog box to select, edit, or add a Configuration Engine.

Navigation Path

Select **Edit Configuration Engines...** from the Server field in the Device Information page of the Add New Device wizard.

Related Topics

- [CNS-Configuration Engine Properties Dialog Box, page C-42](#)
- [Device Information Page—New Device, page C-35](#)

Field Reference

Table C-21 Available Configuration Engines Dialog Box

Element	Description
Display Name	The name that is displayed for the Configuration Engine.
IP Address	The IP address of the Configuration Engine.
Server Name	The hostname of the Configuration Engine.
Domain Name	The domain name of Configuration Engine.
Create button	Enables you to add a new Configuration Engine. When clicked, the CNS-Configuration Engine Properties dialog box appears. For a description of the elements, see CNS-Configuration Engine Properties Dialog Box, page C-42 .
Edit button	Enables you to edit the Configuration Engine information. When clicked, the CNS-Configuration Engine Properties dialog box appears. For a description of the elements, see CNS-Configuration Engine Properties Dialog Box, page C-42 .
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

Device Credentials Page

For elements in the Device Credentials page, see [Device Credentials Page, page C-15](#).

Device Grouping Page

For elements in the Device Grouping page, see [Device Grouping Page, page C-28](#).

Add Device(s) from DCR Wizard

To add a device from DCR into Security Manager, click **Add** in the Device selector. The New Device - Choose Method wizard page appears with four options. Select **Add Devices from DCR**, then click **Next**.

The following topics describe the pages in the Add Device from DCR wizard:

- [Device Information Page—DCR, page C-45](#)
- [Device Grouping Page, page C-28](#)

Device Information Page—DCR

Use the Device Information page of the Add Device from DCR wizard to add devices from DCR to Security Manager.

The Device Information page displays two panes: the left pane is called DCR List of Devices and the right pane is called Selected Devices. These panes have arrows between them that enable you to move devices from one pane to the other.

Navigation Path

You can access the Device Information page from the Add Device from DCR wizard. Click the **Add** button in the Device selector, select **Add Device from DCR**, then click **Next**.

Related Topics

- [Understanding the Device View, page 5-24](#)
- [Adding Devices to the Security Manager Inventory, page 5-30](#)
- [Device Grouping Page, page C-28](#)
- [Device Validation Error Messages, page C-27](#)
- [Create Filter Dialog Box, page C-3](#)
- [Discovering Policies, page 6-7](#)

Field Reference

Table C-22 Device Information Page in Add Device(s) from DCR Wizard

Element	Description
DCR List of Devices pane	<p>Contains two elements:</p> <ul style="list-style-type: none"> Filter field—Filters and displays a subset of devices based on the filtering criteria you define. For more information, see Create Filter Dialog Box, page C-3. System Defined Groups—Displays device groups and devices that are available in the Device and Credential Repository (DCR) but not in Security Manager. <p>DCR resides in the CiscoWorks Server. DCR is a common repository of devices that stores device attributes and device credential information.</p>
>> button	Moves the selected devices from one pane to the other pane.
<< button	
Selected Devices pane	Displays all the devices that you selected to add from DCR into Security Manager.

Table C-22 *Device Information Page in Add Device(s) from DCR Wizard (continued)*

Element	Description
Discover Device Settings	

Table C-22 Device Information Page in Add Device(s) from DCR Wizard (continued)


Element	Description
Discover	<p>Provides the following discovery options:</p> <ul style="list-style-type: none"> • Policies and Inventory—When selected, discovers policies and interfaces. This is the default option. <p>When policy discovery is initiated, the system analyzes the configuration on the device, then imports the configured service and platform policies into Security Manager to be managed. When inventory discovery is initiated, the system analyzes the interfaces on the device and then imports them into Security Manager to be managed. If the device is a composite device, all the service modules in that device are discovered.</p> <p>If you select this option, the following policies are displayed:</p> <ul style="list-style-type: none"> – Platform Settings—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 6-3. <p>This is the default option. If you do not want these discovered, deselect this check box.</p> <ul style="list-style-type: none"> – Firewall Policies—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, Appendix J, “Firewall Services User Interface Reference.” <p>This is the default option. If you do not want these discovered, deselect this check box.</p> <hr/> <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> <hr/> <ul style="list-style-type: none"> • Inventory Only—When selected, discovers interfaces. If the device is a composite device, all the service modules in that device are discovered. • No Discovery—When selected, Security Manager does not initiate discovery.

Table C-22 *Device Information Page in Add Device(s) from DCR Wizard (continued)*

Element	Description
Back button	Returns to the previous wizard page.
Next button	Advances to the next wizard page.
Finish button	Saves your wizard definitions and closes the wizard. 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. Otherwise, the Task Status page appears, displaying the status of the device import and discovery.
Cancel button	Closes the wizard without saving your changes.
Help button	Opens help for this page.

Device Grouping Page

For elements in the Device Grouping page, see [Device Grouping Page, page C-28](#).

Device Delete Validation Page

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

Navigation Path

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

Related Topics

- [Deleting Devices from the Security Manager Inventory, page 5-56](#)
- [Devices Page, page C-2](#)
- [Device Delete Validation Details Dialog Box, page C-51](#)

Field Reference

Table C-23 Device Delete Validation Page

Element	Description
Severity	<p>Displays one or all of the following:</p> <ul style="list-style-type: none"> • Error icon—A problem was detected. See the Results column for details. • Warning icon—Proceed with caution. See the Results column for details. • Information icon—Information about the problem. See the Results column for details. <p>Note This column is not displayed if the status is Passed and there are no errors, warnings, or informational messages to report.</p>
Device	<p>Displays the name of the device that you are trying to delete.</p> <p>Note This column is not displayed if the status is Passed and there are no errors, warnings, or informational messages to report.</p>
Result	<p>Provides detailed information about the severity. Double click a row to open the Device Delete Validation Details dialog box, or click the Details button. See Device Delete Validation Details Dialog Box, page C-51.</p> <p>Note This column is not displayed if the status is Passed and there are no errors, warnings, or informational messages to report.</p>
Details button	<p>Displays the Device Delete Validation Details page. See Device Delete Validation Details Dialog Box, page C-51.</p>
OK button	<p>Proceeds with deletion.</p> <p>The OK button appears only if the system has not experienced errors. You might see warning messages though. Read the warning message details in the Results column to determine whether to continue the deletion. If you want to continue, click OK to proceed with the deletion.</p>
Cancel button	<p>Closes the dialog box without saving your changes.</p>
Help button	<p>Opens help for this page.</p>

Device Delete Validation Details Dialog Box

Use the Device Delete Validation Details dialog box to view details about the device deletion.

Navigation Path

You can access the Device Delete Validation Details dialog box from the Device Delete Validation page in either of two ways:

- Double-click a row from the Result column in the Device Delete Validation page.
- Click the **Details** button in the Device Delete Validation page.

Related Topics

- [Deleting Devices from the Security Manager Inventory, page 5-56](#)
- [Devices Page, page C-2](#)
- [Device Delete Validation Page, page C-49](#)

Field Reference

Table C-24 *Device Delete Validation Details*

Element	Description
Severity	Displays one or all of the following: <ul style="list-style-type: none"> • Error—A problem was detected. See the Results column for details. • Warning—Proceed with caution. See the Results column for details. • Information—Provides information about the problem. See the Results column for details.
Device	Displays the name of the device that you are trying to delete.
Result	Provides detailed information about the severity.
OK button	Closes the dialog box.

Create a Clone of <device name> Page

Use the Create a Clone of <device name> page to duplicate a device.

Navigation Path

Right-click the device in the Device selector, then select **Clone**.

Related Topics

- [Cloning a Device, page 5-55](#)
- [Copying Policies Between Devices, page 6-23](#)

Field Reference

Table C-25 **Create a Clone Device Page**

Element	Description
IP Type	The device IP type of the cloned device: Static or Dynamic.
Hostname	<p>The DNS hostname for the cloned device.</p> <p>The maximum length is 70 characters. Valid characters are: 0–9; uppercase A–Z; lowercase a–z; and the following characters: -</p> <p>Note This field is not displayed if the device you select for cloning has a dynamic IP address.</p>
Domain Name	<p>The DNS domain name for the cloned device. If you do not provide the domain name, Security Manager will use the default DNS suffix configured on the server.</p> <p>The maximum length is 70 characters. Valid characters are: 0–9; uppercase A–Z; lowercase a–z; and the following characters: . -</p> <p>Note This field is not displayed if the device you select for cloning has a dynamic IP address.</p>

Table C-25 **Create a Clone Device Page**

Element	Description
IP Address	<p>The management IP address of the cloned device.</p> <p>Valid characters are . and 0–9. The IP address must be in the dotted quad format, for example, 192.64.3.8.</p> <p>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.</p> <p>Note This field is not displayed if the device you select for cloning has a dynamic IP address.</p>
Display Name	<p>The unique name for the cloned device.</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>
Device Identity	<p>The string value that uniquely identifies the device in Auto Update Server or Configuration Engine.</p> <p>This field is only displayed if the device is managed by Auto Update Server or Configuration Engine.</p>
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

Device Properties Page

You can open the Device Properties page in three ways:

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

The following topics describe the options in the Device Properties page:

- [General Page, page C-54](#)
- [Credentials Page, page C-57](#)

- [Device Groups Page, page C-59](#)
- [Policy Object Override Pages, page C-60](#)

General Page

Use the General page to add or edit information for the following four elements:

- Identity
- Operating System
- DCS Settings
- Auto Update or CNS-Configuration Engine



Note

- Security Manager does not assume that the DNS hostname that appears on the Device Properties page is the same as the hostname that you configured on the device.
 - When you add a device to Security Manager, you must enter either the management IP address or the DNS hostname. Because it is not possible to determine the management interface and, therefore, the management IP address when you discover from a configuration file, the hostname in the configuration file is used as the DNS hostname. If the hostname is missing in the CLI of the configuration file, the configuration filename is used as the DNS hostname.
 - During live device discovery, the DNS hostname in the Device Properties page is not updated with the hostname configured on the device. Therefore, if you want to specify the DNS hostname for the device, you must specify it manually when you add the device to Security Manager or on the Device Properties page.
 - If the DNS hostname or display name of the security context you are discovering exists in DCR, Security Manager appends it with a `_01`, `_02`, and so on to give it a unique name.
-

**Caution**

Cisco Security Manager 3.1 does not support IOS version 12.4(11)T and later routers that use the Cisco CNS Configuration Engine to manage and deploy configurations.

Navigation Path

Double-click a device in the Device selector, then click **General** from the Device Properties page.

Related Topics

- [Understanding Device Properties, page 5-51](#)
- [Credentials Page, page C-57](#)
- [Device Groups Page, page C-59](#)
- [Policy Object Override Pages, page C-60](#)

Field Reference**Table C-26** **General Page**

Element	Description
Identity	
Device Type	The type of device. For example, if the device is a Firewall device, the type of Firewall, such as PIX or ASA is displayed.
IP Type	Provides two options: Static or Dynamic. Depending on the IP type you select, the displayed fields differ.
Hostname	Displayed for static IP types only. The DNS hostname for the device. The maximum length is 70 characters. Valid characters are: 0–9; uppercase A–Z; lowercase a–z; and the following character: -
Domain Name	Displayed for static IP types only. The DNS domain name for the device. The maximum length is 70 characters. Valid characters are: 0–9; uppercase A–Z; lowercase a–z; and the following characters: . -
IP Address	Displayed for static IP types only. The management IP address of the device. Valid characters are 0–9. The IP address must be in the dotted quad format, for example 192.64.3.8.

Table C-26 General Page (continued)

Element	Description
Display Name	The display name of the device. The maximum length is 70 characters. Valid characters are: 0–9; uppercase A–Z; lowercase a–z; and the following characters: _ - . : and space
Operating System	
OS Type	The family of the operating system running on the device.
Image Name	The name of the image.
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.
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	Displayed if the OS type is an FWSM, ASA, or PIX Firewall version 7.0. The two options are: Single or Multi.
Operational Mode	Displayed if the OS type is an FWSM, ASA, or PIX Firewall 7.0. The options are: Transparent or Routed, or Mixed. (Mixed applies only to FWSM 3.1 when the Contexts is Multi).
DCS Settings	
Transport Protocol	The transport protocol set on the device, such as SSL, SSH, AUS, CNS, or TMS. Security Manager deploys the configuration to the device according to the transport mechanism or protocols you set on the device. For Cisco IOS routers, note the following: <ul style="list-style-type: none"> You can override the global default settings by selecting SSL or SSH. If you select Use Default, the transport protocol set in the Device Communication page (Tools > Security Manager Administration > Device Communication) is used.

Table C-26 General Page (continued)

Element	Description
Auto Update or CNS-Configuration Engine	<p>Depending on device type, this field will be either called Auto Update or CNS-Configuration Engine.</p> <ul style="list-style-type: none"> For PIX Firewall, FWSM, or ASA devices, this field is called Auto Update. For Cisco IOS routers, this field is called CNS-Configuration Engine.
Server	<p>If you selected a server, that server name is displayed in the field.</p> <p>If you want to select another server but it does not appear in the list, you could add it. To do so, 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-40.</p>
Device Identity	The string value that uniquely identifies the device in Auto Update Server or Configuration Engine.
Manage in Cisco Security Manager	<p>If selected when you added the device, this check box remains selected.</p> <p>If you do not want to manage this device in Security Manager, deselect the check box.</p>
Save button	Saves your changes.
Close button	Closes the page.
Help button	Opens help for this page.

Credentials Page

Use the Credentials page to add or edit device credential information. For information about device credentials, see [Understanding Device Credentials, page 5-43](#).



Note

You can use a maximum of 70 characters to define device credentials. Security Manager does not restrict in the types of characters you can use to define them. The only restriction is that you may not add a space in the password.

Navigation Path

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

Related Topics

- [Understanding Device Properties, page 5-51](#)
- [General Page, page C-54](#)
- [Device Groups Page, page C-59](#)
- [Policy Object Override Pages, page C-60](#)
- [Rx-Boot Mode Credentials Dialog Box, page C-17](#)
- [SNMP Credentials Dialog Box, page C-18](#)
- [HTTP Credentials Dialog Box, page C-19](#)

Field Reference**Table C-27** **Credentials Page**

Element	Description
Primary Credentials	Required for all device types.
Username	The username for logging into the device.
Password	The password for logging into the device. In the Confirm field, enter the password again.
Enable Password	The password that activates enable mode on a Cisco IOS device if enable mode is configured on that device. In the Confirm field, enter the enable password again.
Authentication Certificate Thumbprint	Certificate thumbprint available in the certificate data store for the given device. Click the Retrieve from Device button next to the field to fetch the certificate thumbprint from the device. The Certificate Details dialog box appears. Click Accept to add the thumbprint to the Security Manager certificate data store.
SDEE Credentials	Displayed for devices that support Intrusion Prevention Systems (IPS), such as Cisco IOS routers, ASA, and IDS.
Username	The SDEE username.
Password	The SDEE password. In the Confirm field, enter the SDEE password again.
HTTP Credentials	Displayed for devices that support IPS, such as Cisco IOS routers, ASA, and IDS. This information is required for devices that support SDEE.
HTTP Port	Port 80.
HTTPs Port	Port 443.

Table C-27 **Credentials Page (continued)**

Element	Description
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.
Mode	HTTP or HTTPS.
Rx-Boot Mode Credentials Tab	
For more information, see Rx-Boot Mode Credentials Dialog Box, page C-17 .	
SNMP Credentials Tab	
For more information, see SNMP Credentials Dialog Box, page C-18 .	
HTTP Credentials Tab —Displayed for PIX Firewall, FWSM, and Catalyst 6500/7600 devices.	
For more information, see HTTP Credentials Dialog Box, page C-19 .	
Save button	Saves your changes.
Close button	Closes the window.
Help button	Opens help for this page.

Device Groups Page

Use the Device Groups page to assign, edit, or delete groups.

Navigation Path

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

Related Topics

- [Understanding Device Properties, page 5-51](#)
- [General Page, page C-54](#)
- [Credentials Page, page C-57](#)
- [Policy Object Override Pages, page C-60](#)

Field Reference

Table C-28 Device Groups Page

Element	Description
Group Types, such as Department and Location	The group type, for example, Department or Location, into which the device is grouped or will be grouped. Enables you to select an existing group or to create a new group under a group type. To create a new group, click the arrow, then select Edit Groups... The Edit Device Groups page appears. For a description of the fields in this page, see Edit Device Groups Page, page C-66 .
Set values as default	When selected, sets the current values as defaults for adding and editing device groups later.
Save button	Saves your changes.
Close button	Closes the window.
Help button	Opens help for this page.

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 8-196](#).

Navigation Path

Open the [Device Properties Page, page C-53](#). From the selector, select **Policy Object Overrides > [name of object type]**.

Related Topics

- [Policy Object Overrides Window, page F-566](#)
- [Allowing a Global Object to Be Overridden, page 8-197](#)
- [Creating Device-Level Object Overrides, page 8-198](#)
- [Deleting Device-Level Object Overrides, page 8-201](#)

Field Reference

Table C-29 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 8-48 .
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 8-197 .
Description	Displays an icon if a description is defined for the object. Point at the icon to display a tooltip with the text of the description. Tip Double-click the icon to display the text of the description in a popup window.
Create Override button	Opens the dialog box for that object type. From here you can create an override object.
Edit Override button	Opens the dialog box for that object type. From here you can edit the selected override object.
Delete Override button	Deletes the selected override object and restores the global object definition.

**Note**

For information about the columns specific to each object type, see [Policy Object Manager User Interface Reference, page F-1](#), then click the link for the relevant object page.

Device Shortcut Menu Options

Use the device shortcut menu options to access several tasks, such as device properties, containment, cloning device, showing devices in a map, discovering policies on a device, and so on.

Navigation Path

Select a device in the Device selector, then right-click the device to display a list of menu options.

Related Topics

- [Understanding the Device View, page 5-24](#)

Field Reference

Table C-30 *Devices Shortcut Menu Options*

Element	Description
Device Properties	Displays device properties for the selected device. Valid properties are: General, Credentials, Device Groups, and Policy Object Overrides. See Device Properties Page, page C-53 .
Show Containment	<p>Displays information about composite devices.</p> <p>Note This option is available only for Catalyst 6500/7600 devices, FWSM, PIX Firewall 7.0, and ASA devices.</p> <p>If you select this option, the containment of a device, that is service modules and security contexts supported on the selected device, is displayed:</p> <ul style="list-style-type: none"> • For Catalyst 6500/7600 devices, displays the IDSM and FWSM service modules, and the security contexts supported by the FWSM. • For FWSMs, displays security contexts supported by the FWSM. • For PIX Firewalls, displays security contexts supported by the PIX Firewall. • For ASA devices, displays security contexts supported by the ASA device. <p>For information about security contexts, see Configuring Security Contexts on Firewall Devices, page 15-105.</p>

Table C-30 **Devices Shortcut Menu Options (continued)**

Element	Description
Health and Status	Enables you to view the health and status of FWSM and PIX Firewall devices. Note This option is available only for FWSM and PIX Firewall devices.
Show in Map View	Displays your network topology on a map. See Displaying Your Network on the Map , page 4-16.
Clone Device	Clones (duplicates) a device. The cloned device shares the configurations and properties of the source device. See Cloning a Device , page 5-55. Note This option is not available for Catalyst 6500/7600 devices.
Copy Policies Between Devices	Copies policies from one device to another or to a group of devices of the same type. See Copying Policies Between Devices , page 6-23. Note This option is not available for Catalyst 6500/7600 devices.
Share Policies Between Devices	Makes a private policy assigned to a single device available for assignment to multiple devices. See Sharing a Local Policy , page 6-28. Note This option is not available for Catalyst 6500/7600 devices.
Preview Configuration	Enables you to preview the complete proposed configuration that will be on the device after deployment, including the configuration changes you made using Security Manager and the existing configuration. See Preview Config Dialog Box , page O-8.
Delete Device	Deletes a selected device. See Deleting Devices from the Security Manager Inventory , page 5-56.
Discover Policies on Device	Initiates policy discovery for a selected device or a device group. See Discovering Policies , page 6-7.

Policy Selector Shortcut Menu Options

Right-click a policy type in the Policy selector to display a shortcut menu for performing actions on the selected policy. The available options depend on whether the policy type:

- Is unassigned.
- Contains a local policy for that specific device.
- Contains a shared policy that may be assigned to multiple devices.

Policy Selector Shortcut Menu Options

The current status of each policy type is indicated by the icon displayed next to the policy name. See [Policy Status Icons, page 6-22](#).

Navigation Path

Right-click a policy in the Policy selector to display a list of menu options.

Related Topics

- [Policy Menu General Reference, page D-1](#)
- [Understanding the Device View, page 5-24](#)

Field Reference

Table C-31 *Policy Selector Options*

Menu Command	Description
Unassigned policy options	
Assign Shared Policy	Assigns an existing shared policy to the selected device. See Assign Shared Policy Dialog Box, page D-3 .
Local policy options	
Share Policy	Shares the local policy so that it can be assigned to other devices. See Share Policy Dialog Box, page D-2 .
Assign Shared Policy	Replaces the local policy assigned to the device with a shared policy of the same type. See Assign Shared Policy Dialog Box, page D-3 .
Unassign Policy	Unassigns the policy from the device. When deployed, the configuration that corresponds to the settings defined in this policy is removed from the device.
Shared policy options	
Unshare Policy	Creates a local copy of the shared policy and assigns it to the device in place of the shared policy. See Unsharing a Policy, page 6-32 .
Assign Shared Policy	Replaces the shared policy assigned to the device with a different shared policy of the same type. See Assign Shared Policy Dialog Box, page D-3 .
Unassign Policy	Unassigns the policy from the device. When deployed, the configuration that corresponds to the settings defined in this policy is removed from the device.

Table C-31 Policy Selector Options (continued)

Menu Command	Description
Edit Policy Assignments	Enables you to assign and unassign the shared policy from the devices in your network. See Shared Policy Assignments Dialog Box, page D-11 .
Save Policy As	Saves a new instance of the selected shared policy under a different name. Use this option to create a new policy with the same definition as the policy from which it was created. See Save Policy As Dialog Box, page D-13 .
Rename Policy	Renames the selected policy. See Rename Policy Dialog Box, page D-14 .

Device Group Shortcut Menu Options

Use the device group shortcut menu options to access several grouping tasks, such as add device group, edit device group information, add devices to device group, and add a device to Security Manager.

Navigation Path

Right-click a group in the Device selector to display a list of menu options.

Related Topics

- [Understanding the Device View, page 5-24](#)

Field Reference

Table C-32 Device Grouping Shortcut Menu Options

Element	Description
New Device	Opens the New Device - Choose Method wizard page from which you can select the method for adding a device to the Security Manager inventory.
Edit Device Groups	Enables you to perform device group editing tasks, including, add a group type, add a device group, modify the device group name, and delete a device group.

Table C-32 *Device Grouping Shortcut Menu Options (continued)*

Element	Description
New Device Group	Enables you to add a new device group.
Add Devices to Group	Enables you to add devices to a a selected device group.

Edit Device Groups Page

Use the Edit Device Groups page to edit device groups, create new device group types and device groups, create subgroups under existing device groups, and delete device groups or subgroups.

Navigation Path

Do one of the following:

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

Related Topics

- [Understanding Device Grouping, page 5-57](#)
- [Working With Device Groups, page 5-59](#)

Field Reference

Table C-33 *Edit Device Groups Page*

Element	Description
Groups	Displays device group types, device groups, and subgroups.
Add Type button	Creates a new device group type.
Add button	Creates a device group or subgroup.
Delete button	Deletes a device group type, device group, or subgroup.
OK button	Saves your changes and closes the page.

Table C-33 *Edit Device Groups Page*

Element	Description
Cancel button	Closes the page without saving your changes.
Help	Opens help for this page.

Add Devices to Group Page

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

Navigation Path

Do one of the following:

- Right-click a device group or subgroup in the Device selector, then select **Add Devices to Group**.
- Select **File > Add Devices to Group...**

Related Topics

- [Understanding Device Grouping, page 5-57](#)
- [Device Group Shortcut Menu Options, page C-65](#)

Field Reference

Table C-34 Add Devices to Group Page

Element	Description
Available Devices pane	Contains two elements: <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-3. Device Groups—Displays device group types, device groups, and devices that are available in Security Manager.
>> button	Moves the selected devices from one pane to the other pane.
<< button	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. 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.
Selected Devices pane	Displays all the devices that you selected to add to a group.
OK button	Saves your changes and closes the page.
Cancel button	Closes the page without saving your changes.
Help button	Opens help for this page.

Add Group Dialog Box

Use the Add Group dialog box to create a group.

Navigation Path

Right-click a device group or device group type in the Device selector, then select **New Device Group**.

Related Topics

- [Understanding Device Grouping, page 5-57](#)

- [Device Group Shortcut Menu Options, page C-65](#)

Field Reference

Table C-35 *Add Devices to Groups Page*

Element	Description
Group Name	A unique name for the group.
OK button	Saves your changes and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

Add Group Dialog Box