



CHAPTER 6

Managing the Device Inventory

Before you can manage devices in Security Manager, you must prepare the devices for management, then add those devices to the Security Manager device inventory. After you add the devices, you can view and edit device information, configure policies on devices, copy and share policies, clone devices, and so on. The following topics describe how to manage the device inventory:

- [Understanding the Device Inventory, page 6-1](#)
- [Working with the Device Inventory, page 6-6](#)
- [Working with Device Groups, page 6-28](#)

Understanding the Device Inventory

Security Manager maintains an inventory of the devices that it manages. The inventory includes the information required to locate and log into the device, so that your policies can be deployed to the devices. The following topics describe some general concepts related to the device inventory:

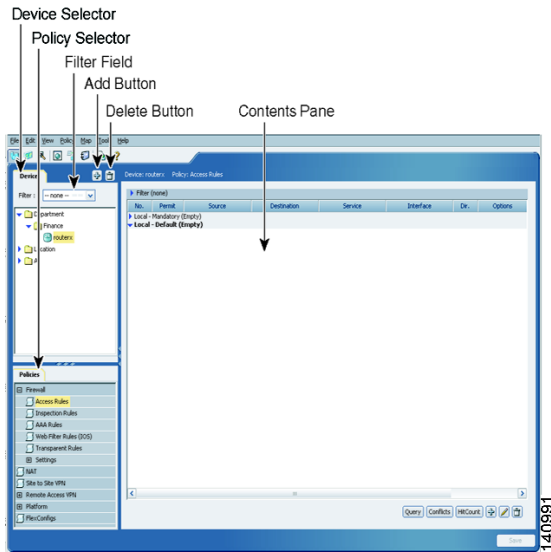
- [Understanding the Device View, page 6-1](#)
- [Understanding Device Names and What Is Considered a Device, page 6-3](#)
- [Understanding Device Credentials, page 6-4](#)
- [Understanding Device Properties, page 6-5](#)
- [Understanding Device Policies, page 6-6](#)

Understanding the Device View

The Device View button opens the Devices page, from which you can add and delete devices from the Security Manager inventory and manage device policies, properties, and interfaces centrally.

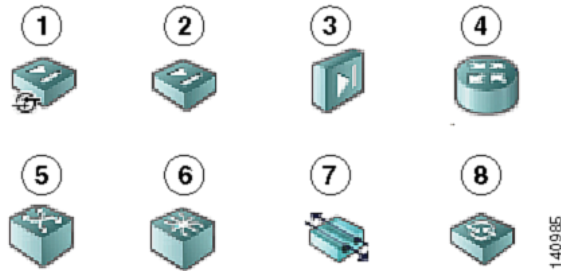
This is a device-centric view in which you can see all devices that you are managing and you can select specific devices to view their properties and define their settings and policies. You can define security policies locally on specific devices. You can then share those policies to make them globally available to be assigned to other devices.

The Devices page contains two panes. The left pane contains two elements: the Device selector, located in the top left pane, and the Policy selector, located in the bottom left pane. The right pane is the main content area. [Figure 6-1](#) shows the Devices page.

Figure 6-1 *Devices Page*

Device selector—Contains the following:

- Add and Delete buttons—Enables you to add and delete devices from the Security Manager inventory.
- Filter field—Enables you to display a subset of devices based on the filtering criteria you define. For details, see [Filtering Items in Selectors, page 3-14](#).
- Device tree—Lists the device groups and devices that exist in the system. Each device type is represented by an icon. For information about the icons, see [Figure 6-2](#).

Figure 6-2 *Device Icons*

1	Adaptive Security Appliances (ASA)	5	Catalyst Switch
2	PIX Firewall	6	Catalyst 7600 Series Router
3	Firewall Services Module (FWSM)	7	VPN 3000 Concentrator
4	Cisco IOS Router	8	Intrusion Prevention System (IPS)

- Shortcut menu options—When you right-click a device or device group, you get a menu of commands related to that device or group. These commands are shortcuts to commands available in the regular menus.

Policy selector—Contains the following:

- Policy groups—Lists the policy groups that are supported on the selected device type. The policy groups that are displayed are dependent on four factors:
 - The type of device selected in the Device selector.
 - The operating system running on the device.
 - The target operating system version selected for determining which commands will be available for generated configurations.
 - Whether the device contains supported service modules.

For details, see [Understanding Device Policies, page 6-6](#).

- Shortcut menu options—When you right-click a policy, you get a menu of commands related to that policy. These commands are shortcuts to commands available in the regular menus.

Contents pane—The main content area.

The information displayed in this area depends on the device you select from the Device selector and the option you select from the Policy selector.

Understanding Device Names and What Is Considered a Device

Besides managing traditional devices, you can use Security Manager to manage virtual devices that you can define on some types of security devices. These virtual devices are treated as separate devices in the device inventory, and they appear as separate entries in the device selectors. Because these virtual devices actually reside on a host physical device, many actions, such as deployment, will have to include the host device as well as the virtual device.

All physical devices appear in the device selectors. In addition, these are the types of virtual devices that appear in the device selectors:

- Security Contexts—You can define security contexts on PIX Firewall, FWSM, and ASA devices. Security contexts act as virtual firewalls. By default, security contexts appear in the device selectors using this naming convention: *host-display-name_context-name*, where *host-display-name* is the display name of the device on which the context is defined, and *context-name* is the name of the security context. For example, the admin security context on the device named firewall12 would be called firewall12_admin.



Tip

You can control whether the display name is added to the context name using the **Prepend Device Name when Generating Security Context Names** property on the Discovery settings page (see [Discovery Page, page A-16](#)). However, if you do not add the display name, it is very difficult to determine the hosting device for a context, and the context names are not sorted with the host device (they do not appear in a folder attached to the host device). If you do not add the display name, Security Manager adds a numeric suffix to the context name if more than one context of the same name is added to the inventory (for example, admin_01, admin_02), and these numbers are not related to the host device.

- Virtual Sensors—You can define virtual sensors on IPS devices. Virtual sensors appear in device selectors using the *host-display-name_virtual-sensor-name* naming convention, and there is not a discovery setting to control this convention.

**Tip**

You can always change the display name for a virtual sensor, security context, or other type of device in the device's properties.

Besides the naming conventions for virtual devices, you also need to understand the relationship between various types of device names:

- **Display name**—The display name is simply the name that appears within Security Manager in device selectors. This name does not have to be related to any name actually defined on the device. When you add devices to the inventory, a display name is suggested based on the DNS name or IP address you enter, but you can use whatever naming convention you want to use.
- **DNS name**—The DNS name you define for a device must be resolvable by the DNS server configured for the Security Manager server.
- **IP address**—The IP address you define for a device should be the management IP address for the device.
- **Hostname**—When you discover a device, the hostname property that is shown in the device properties is taken from the device's configuration. If you add devices using configuration files, and a file does not contain a hostname command, the initial hostname is the name of the configuration file.

However, the hostname device property is not updated if you change the hostname on the device. There is a Hostname policy in the device platform policy area, and it is this Hostname policy that determines the hostname that is defined on the device.

Understanding Device Credentials

Security Manager requires credentials for logging in to devices. The credentials can be used by other applications that you start from Security Manager, such as Resource Manager Essentials (RME) or Monitoring Center for Performance (Performance Monitor). For this reason, the Device Credentials page includes a wider range of optional fields for credentials that you might want to store for possible use by these other applications, or ignore if not required for your purposes.

You can provide device credentials in two ways:

- When you add a device manually or from network discovery. For more information, see these topics:
 - [Adding Devices from the Network, page 6-8](#)
 - [Adding Devices by Manual Definition, page 6-11](#)
- By editing the device properties. For more information, see [Viewing or Changing Device Properties, page 6-17](#).

You can provide the following device credentials:

- **Primary Credentials**—The username and password for logging into the device using SSH or Telnet. This information is required for device communication.
- **HTTP Credentials**—Some devices allow HTTP or HTTPS connections, and some devices (such as IPS devices) require it. By default, Security Manager uses the primary credentials for HTTP/HTTPS access, but you can configure unique HTTP/HTTPS credentials.
- **RX-Boot Mode**—(Optional) Some Cisco routers are designed to run from flash memory where they boot only from the first file in flash. This means that you must run an image other than the one in flash to upgrade the flash image. That image is a reduced command-set image referred to as RX-Boot (a ROM-based image).

- **SNMP Credentials—(Optional)** The Simple Network Management Protocol (SNMP) facilitates the exchange of management information between network devices. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Rather than using device-based credentials, you can configure Security Manager to use the credentials you use when you log into Security Manager. You can then use the AAA server's accounting facilities to track configuration changes by user. Using user login credentials is suitable only if your environment is configured according to these standards:

- You use TACACS+ or RADIUS for change auditing. User-login credentials will be reflected in these accounting records. If you use device credentials, all changes made through Security Manager will come from the same account, regardless of which user made the change.
- User accounts are configured in the AAA server, and they have appropriate device-level access to perform configuration changes.
- You configure Security Manager and the managed devices to use the AAA server for authorization. For information on configuring Security Manager to use AAA, see [Integrating Security Manager with Cisco Secure ACS, page 2-21](#).
- You do not use one-time passwords.

If your network setup supports using user-login credentials, you can configure Security Manager to use them by selecting **Tools > Security Manager Administration**. Select **Device Communication** from the table of contents, and select **Security Manager User Login Credentials** in the **Connect to Device Using** field. The default is to use device credentials for all device access.

Related Topics

- [Device Credentials Page, page C-17](#)
- [Adding Devices to the Device Inventory, page 6-7](#)
- [Device Communication Page, page A-11](#)

Understanding Device Properties

You define device properties when you add devices to Security Manager. Device properties are general information about the device, credentials, the group the device is assigned to, and policy overrides. You must provide some device property information, such as device identity and primary credentials, when you add the device, but you can add or edit the properties from the Device Properties dialog box.

To view the device properties, do one of the following in the Device selector:

- Double-click a device.
- Right-click a device and select **Device Properties**.
- Select a device and select **Tools > Device Properties**.

The Device Properties dialog box has two panes. The left pane contains a table of contents with these items:

- **General**—Contains general information about the device, such as device identity, the operating system running on the device, and device communication settings.
- **Credentials**—Contains device primary credentials (username, password, and enable password), SNMP credentials, Rx-Boot Mode credentials, and HTTP credentials.
- **Device Groups**—Contains the groups to which the device is assigned.

- **Policy Object Overrides**—Contains global settings of certain types of reusable policy objects that you can override for this device.

When you select an item in the table of contents, the corresponding information is displayed in the right pane. For information about the elements in this page, see [Device Properties Page, page C-27](#).

Notes

- 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.
- When you discover a device from the network, 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.

For more information about device properties, see [Viewing or Changing Device Properties, page 6-17](#).

Understanding Device Policies

In Security Manager, a policy is a set of rules or parameters that define a particular aspect of network configuration. You configure your network by defining policies on devices (which includes individual devices, service modules, and security contexts) and VPN topologies (which are made up of multiple devices), and then by deploying the configurations defined by these policies to the devices.

Several policy types might be required to configure a particular solution. For example, to configure a site-to-site VPN, you might need to configure multiple policies, such as IPSec, IKE, GRE, and so forth.

Policies are assigned to one or more devices. After a policy is assigned to a device, any changes to the policy definition change the behavior of the device.

You can use Device view to manage both local policies and shared policies.

For details, see [Managing Policies in Device View, page 7-19](#).

Working with the Device Inventory

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

- [Adding Devices to the Device Inventory, page 6-7](#)
- [Adding, Editing, or Deleting Auto Update Servers or Configuration Engines, page 6-14](#)
- [Testing Device Connectivity, page 6-15](#)
- [Viewing or Changing Device Properties, page 6-17](#)
- [Changing Critical Device Properties, page 6-17](#)
- [Managing Device Communication Settings and Certificates, page 6-21](#)
- [Discovering or Changing the CS-MARS Server for a Device, page 6-23](#)
- [Showing Device Containment, page 6-23](#)

- [Cloning a Device](#), page 6-24
- [Deleting Devices from the Security Manager Inventory](#), page 6-24
- [Viewing Inventory Status](#), page 6-25
- [Exporting the Device Inventory](#), page 6-25
- [Managing the Device Operating System](#), page 6-28

Adding Devices to the Device Inventory

When you add a device to Security Manager, you specify the identifying information for the device, such as its DNS name and IP address. This information is added during device discovery. You can also bring in existing network configurations associated with a device by initiating policy discovery. For complete information on policy discovery, see [Discovering Policies](#), page 7-11. Once you add the device, it appears in the Security Manager device inventory.

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



For PIX Firewalls and FWSM and ASA devices that are configured for failover, add only the active unit to Security Manager. Ensure that the device is configured with a management IP address and use that address for discovery.

The following topics describe the various methods of adding devices:

- To add devices that are currently active on the network, see [Adding Devices from the Network](#), page 6-8. Security Manager connects directly and securely to the device and discovers its identifying information and properties.
 - **Pros**—You need to specify minimal information about a device, and Security Manager obtains the detailed information directly from the device, ensuring accuracy.
 - **Cons**—You can add only one device at a time. You cannot add devices that have dynamic IP addresses, unless you determine the device’s current IP address, add it using that address, and then update the device properties in Security Manager to identify the Configuration Engine that is managing the device.
- To add devices by using a copy of the device configuration files, see [Adding Devices from Configuration Files](#), page 6-10.
 - **Pros**—You can add more than one device at a time.
 - **Cons**—You cannot use this method to add Catalyst 6500/7600 or IPS devices. When adding groups of configuration files, all files must be for the same device type.

Also, you cannot successfully discover policies that require a connection with the device. For example, if a policy points to a file that resides on the device, adding the device using the configuration file will result in a Security Manager configuration that includes the **no** form of the command, because Security Manager cannot retrieve the referenced file from the device. For example, the **svc image** command for web VPNs might be negated.
- To add a device that does not yet exist in the network, so that you can pre-provision it in Security Manager, see [Adding Devices by Manual Definition](#), page 6-11. You can create the device in the system, assign policies to the device, and generate configuration files before installing the device hardware.

- **Pros**—You can pre-provision devices that do not yet exist in the network.
- **Cons**—You must specify more information than that required by any other method. If you create a Catalyst 6500/7600 device, or a router that contains an AIM-IPS module, you should discover its modules by selecting **Policy > Discover Policies on Device**.
- To add devices from an inventory file exported from CiscoWorks Common Services Device Credential Repository (DCR) or Cisco Security Monitoring, Analysis and Response System (CS-MARS), see [Adding Devices from an Export File, page 6-12](#).
 - **Pros**—You can add multiple devices of different types at one time. You can reuse the inventory list from your other network management applications.
 - **Cons**—You cannot use this method to update the properties of devices already defined in the inventory. Also, policy discovery can fail if you attempt to import more than 100 devices at one time, and might fail for even fewer devices. In the case of IPS devices, do not add more than four IPS devices at a time to avoid policy discovery failures.

Adding Devices from the Network

One of the easiest and most reliable ways to add devices to the inventory is to identify devices that are active in the network. By providing the IP address (or DNS hostname) of a device, and the credentials required to log into it, Security Manager can obtain much of the information it needs directly from the device, ensuring the accuracy of the information.

Before You Begin

Before beginning this procedure, ensure the following preparations have been made:

- Prepare the devices to be managed by Security Manager. For more information, see [Chapter 5, “Preparing Devices for Management”](#).
- If you are using ACS for authentication, define the devices in ACS. See [Adding Managed Devices as AAA Clients in Cisco Secure ACS, page 2-25](#).

Related Topics

- [Understanding the Device View, page 6-1](#)
- [Working with Device Groups, page 6-28](#)
- [Viewing or Changing Device Properties, page 6-17](#)

Procedure

-
- Step 1** In Device view, select **File > New Device** or click the **New Device** button in the Device selector. The New Device wizard opens to the Choose Method page.
- Step 2** On the Choose Method page, select **Add Device from Network** and click **Next** to open the Device Information page.
- Step 3** On the Device information page, at minimum fill in the following fields. For a detailed explanation of all fields, see [Device Information Page – Add Device from Network, page C-4](#).
- Enter either a hostname and DNS name, or an IP address (or both).
 - Enter a display name, which is the name that will appear in the Security Manager Device selector.
 - Select the correct operating system and version. If you are configuring a Catalyst switch or a 7600 router, ensure that you select **IOS - Catalyst Switch/7600** rather than one of the other IOS entries.

- Select the transport protocol that should be used to log into the device, if the device is configured to use a protocol that differs from the default defined in Security Manager. The default is set on the Device Communication administration page (see [Device Communication Page, page A-11](#)).

Click **Next**.

- Step 4** On the Device Credentials page, enter the usernames and passwords required to log into the device. Enter at least the primary device credentials, which are the traditional User EXEC mode and Privileged EXEC mode passwords.

For information on the different types of credentials, see [Device Credentials Page, page C-17](#).



Tip When you click Next or Finished from the Device Credentials page, Security Manager tests whether it can connect to the device. You cannot add the device unless the test succeeds. For more information, see [Testing Device Connectivity, page 6-15](#).

- Step 5** (Optional) Click **Next** to open the Device Grouping page, and select the device group to which the imported devices should be added (see [Device Grouping Page, page C-25](#)).

- Step 6** Click **Finish**. Security Manager opens the Discovery Status dialog box where you can view the status of the device discovery and policy analysis (see [Discovery Status Dialog Box, page D-13](#)).



Tip If you are discovering policies while adding a device, carefully read any messages that are presented to you. These messages can contain important recommendations on the next steps you should take. For example, when you add Cisco IOS routers or Catalyst devices, we recommend that you immediately deploy the discovered configuration to a file so that Security Manager can take over ownership of the configuration. For more information about deployment methods, see [Understanding Deployment Methods, page 18-9](#).

- Step 7** If you are adding a device that contains modules, you are notified when the discovery of the device chassis is complete and you are asked if you want to discover the device's modules. When you click **Yes**, you are prompted for this information:

- Catalyst 6500/7600 service modules—The Service Module Credentials dialog box opens prompting for the following information, based on the modules contained in the chassis. For more information, see [Service Module Credentials Dialog Box, page C-22](#).
 - FWSM—The management IP address (recommended), the username and passwords, and the type of discovery you want to perform.
 - IDSM—The username and password and the type of discovery you want to perform.
- AIM-IPS Module—The type of discovery you want to perform, the management IP address, the username and password, and other SSL connection information. For more information, see [AIM-IPS Module Discovery Dialog Box, page C-24](#).

You can skip discovery for any module you do not want to manage in Security Manager.

Click **OK**. You are returned to the Discovery Status dialog box, where you can view the progress of service module discovery.

Adding Devices from Configuration Files

You can add devices to the inventory by having Security Manager process the device configurations without logging into the devices. For each device, you must copy the device configuration to a file and put the file on the Security Manager server.

You cannot use this procedure to add IPS or Catalyst 6500/7600 devices to the inventory.

Before You Begin

Before beginning this procedure, ensure the following preparations have been made:

- Prepare the devices to be managed by Security Manager. For more information, see [Chapter 5, “Preparing Devices for Management”](#).
- If you are using ACS for authentication, define the devices in ACS. See [Adding Managed Devices as AAA Clients in Cisco Secure ACS, page 2-25](#).
- Copy the device configuration files to a directory on the Security Manager server. You cannot use a mounted drive. Use a naming convention that will help you select the correct device type for each configuration.

Related Topics

- [Understanding the Device View, page 6-1](#)
- [Working with Device Groups, page 6-28](#)
- [Viewing or Changing Device Properties, page 6-17](#)

Procedure

-
- Step 1** In Device view, select **File > New Device** or click the **New Device** button in the Device selector. The New Device wizard opens to the Choose Method page.
 - Step 2** On the Choose Method page, select **Add from Configuration File** and click **Next** to open the Device Information page (see [Device Information Page—Configuration File, page C-8](#)).
 - Step 3** Select the device type for the configuration files from the Device Type selector, and select the appropriate system object ID. If you have configuration files for more than one device type, add them in batches based on device type.
 - Step 4** Click **Browse** and select the configuration files that contain the devices (of the specified type) that you want to add.
 - Step 5** Select the appropriate discovery options to indicate which types of policies you want to discover, if any.
 - Step 6** (Optional) Click **Next** and select the device groups to which the new devices should belong.
 - Step 7** Click **Finish**. Security Manager opens the Discovery Status dialog box where you can view the status of the configuration file analysis (see [Discovery Status Dialog Box, page D-13](#)).

**Tip**

If you are discovering policies and get unexpected errors, it might be because the configuration file includes only the major Cisco IOS software version and not the point release information. Some policies defined on the device might use features that became available in a point release, which means that Security Manager might not recognize them as being supported. To resolve the problem, after adding the device, select it in the Device selector, right-click, and select **Device Properties**. On the General page, update the **Target OS Version** field with the software version closest to the one running on the device without being higher than it (you can get the version number using the **show version** command on the device's CLI). You can then rediscover policies by right-clicking and selecting **Discover Policies on Device**.

Adding Devices by Manual Definition

If a device is not yet active on the network, you can add it to Security Manager and preprovision a configuration for the device. In general, you should not use manual definition for a device that exists in the network, because it is much easier to use one of the other techniques for adding devices.

Before You Begin

Before beginning this procedure, ensure the following preparations have been made:

- Prepare the devices to be managed by Security Manager. For more information, see [Chapter 5, “Preparing Devices for Management”](#).
- If you are using ACS for authentication, define the devices in ACS. See [Adding Managed Devices as AAA Clients in Cisco Secure ACS, page 2-25](#).

Related Topics

- [Understanding the Device View, page 6-1](#)
- [Working with Device Groups, page 6-28](#)
- [Viewing or Changing Device Properties, page 6-17](#)

Procedure

-
- Step 1** In Device view, select **File > New Device** or click the **New Device** button in the Device selector. The New Device wizard opens to the Choose Method page.
- Step 2** On the Choose Method page, select **Add New Device** and click **Next** to open the Device Information page.
- Step 3** On the Device Information page, at minimum fill in the following fields. For a detailed explanation of all fields, see [Device Information Page—New Device, page C-10](#).
- Select the device type from the Device Type selector at the left of the page, and select the system object ID at the bottom of the selector.
 - Devices with static IP addresses—If the device you are adding has a static IP address configured on the device:
 - Select **Static** for IP Type.
 - Enter either a DNS hostname and domain name, or an IP address (or both).

- Enter a display name, which is the name that will appear in the Security Manager Device selector.
- Ensure that the correct operating system and version are selected.
- Devices with dynamic IP addresses—If the device you are adding is provided an IP address through DHCP:
 - Select **Dynamic** for IP Type.
 - Enter a display name, which is the name that will appear in the Security Manager Device selector.
 - Ensure that the correct operating system and version are selected.
 - Select the Auto Update Server or Configuration Engine that manages the device and enter the device identity string the server uses for the device. If the correct server is not listed, select **Add Server** and add it to the inventory. For information on adding servers, see [Adding, Editing, or Deleting Auto Update Servers or Configuration Engines, page 6-14](#)

When you are finished filling in the device information, click **Next** to proceed to the Device Credentials page.

- Step 4** (Optional) On the Device Credentials page, enter the usernames and passwords required to log into the device. Typically, you need to enter the primary device credentials, which are the traditional User EXEC mode and Privileged EXEC mode passwords. If you do not enter credentials, you can add them later on the Device Properties page.

For information on the different types of credentials, see [Device Credentials Page, page C-17](#).

Click **Next**.

- Step 5** (Optional) On the Device Grouping page, select the group to which the device should belong, if any. See [Device Grouping Page, page C-25](#)

- Step 6** Click **Finish**. The device is added to the inventory.



Tip If you are adding a PIX, ASA, or FWSM device, you should discover the factory default settings for the device and its security contexts. For more information, see [Discovering Policies on Devices Already in Security Manager, page 7-14](#).

Adding Devices from an Export File

You can add devices from a file you exported from CiscoWorks Common Services Device Credential Repository (DCR) or Cisco Security Monitoring, Analysis and Response System (CS-MARS).

The devices you import cannot be duplicates of devices already in the device inventory. You cannot, for example, update device information in the inventory by reimporting the device.

Before You Begin

Before beginning this procedure, ensure the following preparations have been made:

- Prepare the devices to be managed by Security Manager. For more information, see [Chapter 5, “Preparing Devices for Management”](#).
- If you are using ACS for authentication, define the devices in ACS. See [Adding Managed Devices as AAA Clients in Cisco Secure ACS, page 2-25](#).

- Put the export file you want to use on the Security Manager server. You cannot import devices from a file on your system.
- If you are using a non-standard communication protocol for a type of device, update the global device communication properties to specify the correct protocol. For more information, see [Device Communication Page, page A-11](#).

Related Topics

- [Understanding the Device View, page 6-1](#)
- [Working with Device Groups, page 6-28](#)
- [Viewing or Changing Device Properties, page 6-17](#)

Procedure

-
- Step 1** In Device view, select **File > New Device** or click the **New Device** button in the Device selector. The New Device wizard opens to the Choose Method page.
- Step 2** On the Choose Method page, select **Add Device from File** and click **Next** to open the Device Information page (see [Device Information Page—Add Device from File, page C-15](#)).
- Step 3** Click **Browse** and select the export file that contains the devices that you want to import. Make sure that you select the correct file type to indicate how the file is formatted (either in DCR or CS-MARS export format).

Security Manager evaluates the contents of the export file and displays the list of devices in the import table. All devices that have the status Ready to Import are automatically selected. The list identifies the reasons the unselected devices cannot be imported. You can deselect any devices that you do not want to import.

To see detailed information on a device, select it in the import table. The details are displayed in the bottom pane. You can select different discovery options or transport settings per device.

When you are finished analyzing the list and modifying discovery and transport settings, click **Next** to continue to the optional step of selecting groups, or click **Finish** to complete the wizard. In either case, Security Manager attempts to log into each device and perform the discovery you selected, even if you selected to not perform discovery. Security Manager must be able to log into the device to add it to the inventory. The status is displayed in the Discovery Status dialog box (see [Discovery Status Dialog Box, page D-13](#)).



Tip If you are discovering policies while adding a device, carefully read any messages that are presented to you. These messages can contain important recommendations on the next steps you should take. For example, when you add Cisco IOS routers or Catalyst devices, we recommend that you immediately deploy the discovered configuration to a file so that Security Manager can take over ownership of the configuration. For more information about deployment methods, see [Understanding Deployment Methods, page 18-9](#).

- Step 4** (Optional) On the Device Grouping page, select the device group to which the imported devices should be added (see [Device Grouping Page, page C-25](#)).

Click **Finish**.

- Step 5** If you are adding a device that contains modules, you are notified when the discovery of the device chassis is complete and you are asked if you want to discover the device's modules. When you click **Yes**, you are prompted for this information:

- Catalyst 6500/7600 service modules—The Service Module Credentials dialog box opens prompting for the following information, based on the modules contained in the chassis. For more information, see [Service Module Credentials Dialog Box, page C-22](#).
 - FWSM—The management IP address (recommended), the username and passwords, and the type of discovery you want to perform.
 - IDSM—The username and password and the type of discovery you want to perform.
- AIM-IPS Module—The type of discovery you want to perform, the management IP address, the username and password, and other SSL connection information. For more information, see [AIM-IPS Module Discovery Dialog Box, page C-24](#).

You can skip discovery for any module you do not want to manage in Security Manager.

Click **OK**. You are returned to the Discovery Status dialog box, where you can view the progress of service module discovery.

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

If you want to manage devices that have dynamic IP addresses, that is, a DHCP server supplies an IP address that might not stay constant between device reboots, you must configure the device to use an Auto Update Server or Configuration Engine:

- Auto Update Server (AUS) is a tool for upgrading device configuration files on PIX Firewall and ASA devices that use the auto update feature.
- Cisco Configuration Engine is a tool for upgrading device configuration files on Cisco IOS routers and PIX Firewalls that use the configuration engine feature.

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

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

You can also add these servers if you import them from an inventory file exported from CiscoWorks Common Services Device Credential Repository (DCR). If you import the server, you bypass the procedure described in this section. For more information about importing devices, see [Adding Devices from an Export File, page 6-12](#).

Before You Begin

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

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

Related Topics

- [Adding Devices from the Network, page 6-8](#)
- [Adding Devices by Manual Definition, page 6-11](#)
- [Viewing or Changing Device Properties, page 6-17](#)

Procedure

-
- Step 1** Locate the field that allows you to identify and manage either AUS or Configuration Engine entries in the device inventory:
- a. Select **File > New Device** to open the New Device wizard, select **Add New Device** on the Choose Method page, and click **Next**.
 - b. On the Device Information page, select an ASA device from the Device Type selector, for example, Cisco ASA-5580 Adaptive Security Appliance. The **Server** field in the Auto Update group should include **Add Server** and **Edit Server** in the drop-down list. It will also include **Edit Server** if there are servers already defined. If these entries have specific server types (for example, Add Auto Update Server or Add Configuration Engine), then you will be limited to adding, editing, or deleting that type of server (in this case, select other types of devices to find the appropriate server type).
- Step 2** To add a new AUS or Configuration Engine server, select **Add Server** from the Server drop-down list to open the Server Properties dialog box (see [Server Properties Dialog Box, page C-12](#)).
- Step 3** To edit a server, select **Edit Server** from the Server drop-down list to open the Available Servers dialog box (see [Available Servers Dialog Box, page C-14](#)). You can then select the server and click **Edit**, which opens the Server Properties dialog box where you can make your changes.

From the Available Servers dialog box, you can also:

- Click **Create** to add a server.
 - Select a server and click **Delete** to remove it from the inventory. You are asked to confirm the deletion. Make sure that the server is not being used by a device in the inventory.
-

Testing Device Connectivity

Security Manager must be able to connect to and log into a device in order to manage it. You can test whether Security Manager can use the credentials and transport method you have defined within Security Manager for this purpose.

You can test connectivity only for devices that have static IP addresses. If a device is managed by an Auto Update Server, Token Management Server (TMS) or a Configuration Engine, you cannot test connectivity between Security Manager and the device.

If you add a device from the network or from an export file to the inventory, Security Manager tests connectivity automatically.

You can manually test device connectivity for any device in the inventory or for new devices that you are adding manually. The following procedure describes how to test connectivity for devices that are already in the inventory. When adding devices manually, click **Test Connectivity** on the Device Credentials page of the New Device wizard to perform the test described below. For more information on adding devices manually, see [Adding Devices by Manual Definition, page 6-11](#).

Before You Begin

Security Manager uses the settings on the Device Communication page to determine the connection timeout, how often to retry the connection, the transport protocol, and which credentials to use. To configure these settings, select **Tools > Security Manager Administration** and select **Device Communication** from the table of contents.

Related Topics

- [Understanding the Device View, page 6-1](#)
- [Viewing or Changing Device Properties, page 6-17](#)
- [Device Communication Page, page A-11](#)

Procedure

-
- Step 1** In Device view, do one of the following in the Device selector to open the Device Properties dialog box:
- Double-click a device.
 - Right-click a device and select **Device Properties**.
 - Select a device and select **Tools > Device Properties**.
- Step 2** Select **Credentials** from the table of contents.
- Step 3** Click **Test Connectivity**.

The Device Connectivity Test dialog box opens and displays the progress of the test, including the protocol being used (see [Device Connectivity Test Dialog Box, page C-21](#)). You can abort the test while it is running. When the test is finished, click **Details** to see:

- For successful tests, the output of the **show version** command or the **getVersion** command (for IPS Sensors and Cisco IOS IPS Sensors). You can select the text, press Ctrl+C to copy the text to the clipboard, and then paste it into another file for later analysis.
 - For unsuccessful tests, the error information. Some common problems are:
 - The username or password is incorrect.
 - The wrong protocol is selected. For example, the device might not be configured to respond to the selected protocol.
 - The device is not configured to accept connections correctly. Ensure that at least one supported protocol is configured.
 - The wrong operating system is specified for the device (for example, you specified PIX for an ASA device).
 - If you are using ACS authentication and the connection to the device is completed, you can get errors when Security Manager tries to obtain version information if you do not have Control authorization.
 - There might be general network configuration problems. Test connectivity to the device from outside of Security Manager. Look for hardware, media, and booting errors, excessive traffic causing queues to overflow, duplicate MAC or IP addresses on the device, physical discrepancies, such as link, duplex, and speed mismatch, or logical discrepancies, such as VLAN and VTP inconsistencies or ATM network misconfiguration.
-

Viewing or Changing Device Properties

When you add a device to the inventory, you specify at least some of the device's properties, such as names and credentials. For devices that are in the inventory, you can view and change the device properties.

Related Topics

- [Understanding the Device View, page 6-1](#)
- [Understanding Device Properties, page 6-5](#)
- [Understanding Device Policies, page 6-6](#)
- [Changing Critical Device Properties, page 6-17](#)

Procedure

-
- Step 1** In Device view, do one of the following in the Device selector to open the Device Properties dialog box:
- Double-click a device.
 - Right-click a device and select **Device Properties**.
 - Select a device and select **Tools > Device Properties**.
- Step 2** In the Device Properties dialog box, click these entries in the table of contents in the left pane to view or change the properties. You must click **Save** before moving from one page to another.
- **General**—General information about the device, such as the device identity, the operating system running on the device, and transport settings. For information about the fields, see [General Page, page C-27](#).
 - **Credentials**—The device credentials required to log into the device. For information about the fields, see [Credentials Page, page C-30](#).
 - **Groups**—The groups to which the device belongs. For information about the fields, see [Device Groups Page, page C-32](#).
 - **Policy Object Overrides**—The local overrides to policy objects for the device. Policy Object Overrides is a folder that contains the various policy object types that are available for the device. Click a specific policy object type to view the policy objects of that type used by the device and their overrides, if any. For more information about the fields, see [Policy Object Override Pages, page C-33](#).
-

Changing Critical Device Properties

You must use caution when changing the image version of a device, the device type, or the security context or operational mode of FWSM and ASA devices that are managed by Security Manager. In certain cases, these changes enable a different set of features for the device. As a result, some of the policies that you configured for the device in Security Manager might no longer apply.

The key device changes, their effect on the policies available in Security Manager, and the procedure you should follow to implement these device changes, are described in the following sections:

- [Image Version Changes That Do Not Change the Feature Set in Security Manager, page 6-18](#)
- [Changes That Change the Feature Set in Security Manager, page 6-19](#)

Image Version Changes That Do Not Change the Feature Set in Security Manager

The following image version changes *do not* affect the types of policies available for that device in Security Manager:

- Upgrading from any Cisco IOS version supported by Security Manager to any other Cisco IOS version supported by Security Manager.
- Upgrading from any PIX 6.x image to another PIX 6.x image.
- Upgrading from any PIX 7.x image to another PIX 7.x image, retaining the same security context and mode configuration.
- Upgrading from any ASA 7.x image to another ASA 7.x image, retaining the same security context and mode configuration.
- Upgrading from any ASA 8.x image to another ASA 8.x image, retaining the same security context and mode configuration.
- Upgrading from any FWSM 2.x image to another 2.x FWSM image, retaining the same security context and mode configuration.
- Upgrading from any FWSM 3.x image to another 3.x FWSM image, retaining the same security context and mode configuration.
- Upgrading a Catalyst 6500/7600 chassis from any IOS 12.x image to another IOS 12.x image.
- Upgrading from IPS 4.x to IPS 5.x or downgrading from IPS 5.x to IPS 4.x.



Note

This list applies only to images that are supported by Security Manager. For a list of supported images, see *Supported Devices and Software Versions for Cisco Security Manager* for this version of the product at http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html.

For these cases, use the following procedure to change the image version.

Related Topics

- [Understanding the Device View, page 6-1](#)
- [Understanding Device Properties, page 6-5](#)
- [Understanding Device Policies, page 6-6](#)
- [Changes That Change the Feature Set in Security Manager, page 6-19](#)

Procedure

-
- Step 1** Upgrade the image version on the device.
- Step 2** In Device view, do one of the following in the Device selector to open the Device Properties dialog box:
- Double-click a device.
 - Right-click a device and select **Device Properties**.
 - Select a device and select **Tools > Device Properties**.
- Step 3** In the Device Properties dialog box, change the **Target OS Version** property on the General page to the updated version number and click **Save**.
-

Changes That Change the Feature Set in Security Manager

These are the main types of device changes that affect the policy feature set available for a device:

- Image version changes—The following image version changes affect the types of policies available for that device in Security Manager:
 - Upgrading from a PIX 6.x to a PIX 7.x image or from a 7.x to an 8.x image.
 - Downgrading from a PIX 7.x to a PIX 6.x image or from an 8.x to a 7.x image.
 - Upgrading from an ASA 7.x to an ASA 8.x image.
 - Downgrading from an ASA 8.x to an ASA 7.x image.
 - Upgrading from a FWSM 2.x image to an FWSM 3.x image.
 - Downgrading from a FWSM 3.x image to an FWSM 2.x image.
 - Upgrading from an IOS 12.1 or 12.2 image to an IOS 12.3 or 12.4 image.
 - Downgrading from an IOS 12.3 or 12.4 image to an IOS 12.1 or 12.2 image.

Security Manager prevents you from changing the target OS version of a managed device to a version that changes the types of policies that are available for that device. Therefore, you must first delete the device from Security Manager, perform the image change, then add the device back.

Certain types of policies, such as access rules, are not affected by changes in image version or changes in platform type.

- Security context and operational mode changes—Changes that you make to the security context and operational mode settings on an FWSM or ASA device enable a different set of features on that device. These changes occur if you change the device from:
 - Single context to multiple context (or vice-versa).
 - Routed mode to transparent mode (or vice-versa).

Security Manager prevents you from changing the security context or operational mode settings of a managed device. Therefore, you must first delete the device from Security Manager, change the context or mode, then add the device back.

Certain policy types (for example, Banner, Clock, Console Timeout, and HTTP) are not affected by changes in operational mode. Other policy types (for example, ICMP, SSH, and TFTP, in addition to Banner and Clock) are not affected by changes in security context settings.

- Replacing device hardware—In some cases, you might replace a particular device but retain the original contact information (such as the IP address), for example:
 - Replacing a PIX firewall with a Cisco IOS router.
 - Replacing a PIX 7.x device with an ASA device.
 - Replacing a Cisco IOS router with a firewall device.

In all of these cases, the new device changes the types of policies available for that device in Security Manager. Security Manager prevents you from modifying the hardware model of an existing device. Therefore, you must first delete the device from Security Manager, change the physical device, then add the device back.

Certain policy types (for example, access rules) are not affected by changes in device type.

We recommend that you share the policies configured on your device that will not be affected by the change before you remove it from Security Manager. This provides a useful method for reassigning the policies to the device (with any inheritance and policy object references intact) after you add it back to Security Manager. The following procedure describes how to do this.

Related Topics

- [Understanding the Device View, page 6-1](#)
- [Understanding Device Properties, page 6-5](#)
- [Understanding Device Policies, page 6-6](#)
- [Image Version Changes That Do Not Change the Feature Set in Security Manager, page 6-18](#)

Procedure

-
- Step 1** Submit and deploy all the changes you configured for the device in Security Manager. This ensures that the desired configuration is on the device before the image upgrade.
- Step 2** Share the local policies defined on the device:
- a. Right-click the device in the Device selector, then select **Share Device Policies**. By default, all policies configured on the device (local and shared) are selected for sharing in the Share Policies wizard.
 - b. Deselect the check box next to each existing shared policy, as indicated by the hand in the policy icon. You should do this because there is no need to create a copy of the shared policies that already exist; you will reassign the existing shared policies after the image version upgrade.
 - c. Enter a name for the shared policies. We recommend using the device name as a convenient means of identification. For example, if the device name is MyRouter, each shared policy is given the name MyRouter. Make a note of all the policies you are creating for this purpose.
 - d. Click **Finish**. The selected local policies become shared policies.
- Step 3** Delete the device from Security Manager.
- Step 4** Make the desired change to the device, for example, upgrade the image version, change the operational mode, or replace the device.
- Step 5** Add the device back to Security Manager and perform policy discovery.
- Step 6** Reassign the policies to the device:
- a. Right-click the first policy type displayed in the Device Policies selector, then select **Assign Shared Policy**.
 - b. In the Assign Shared Policy dialog box, do one of the following:
 - If a local policy was previously defined on the device, select the shared policy you created for this procedure and click **OK**.
 - If a shared policy of this type was previously assigned to the device, select it and click **OK**.
 - c. (Local policies only) Right-click the policy type again in the Device Policies selector, then select **Unshare Policy**.
 - d. Repeat the process for each policy type that is relevant to the device's configuration. If a shared policy is not available, this indicates that this is a policy type that was not available for the previous image version.
- Step 7** (Optional) Delete the shared policies created for this procedure from Policy view:
- a. Select **View > Policy View** or click the **Policy View** icon on the toolbar.
 - b. Select one of the policies you want to delete and click the **Assignments** tab in the work area to verify that the policy is not assigned to any devices.
 - c. Click the **Delete Policy** button beneath the Shared Policy selector to delete the policy.

- d. Repeat the process for each policy type that you want to delete.
-

Managing Device Communication Settings and Certificates

If you discover device inventory and policies directly from devices, or deploy configurations to devices rather than to files, you must configure Security Manager to use the transport protocols that your devices use. For some device types, only one transport protocol is supported, so you do not need to make a choice. For other devices, such as Cisco IOS routers, you have options concerning the protocols you use.

Security Manager has default settings for transport protocols that are the most-used protocols for each device type. To change these settings, select **Tools > Security Manager Administration** and select **Device Communication** from the table of contents (see [Device Communication Page, page A-11](#)).

For most users, the communication settings that require management are the certificates used for SSL (HTTPS) connections and the public keys used for SSH connections. You might update the certificates and keys on the device, which would leave Security Manager holding an outdated copy. To managing certificates and keys:

- **SSL certificates**—You can configure Security Manager to automatically replace certificates using the ones obtained from the device on the Device Communication page. If you decide to manually manage the SSL certificate store, see [Manually Adding SSL Certificates for Devices that Use HTTPS Communications, page 6-21](#).
- **SSH Public Keys**—By default, Security Manager replaces public keys with the new ones obtained during SSH connections. If you have problems with SSH communications, see [Troubleshooting SSH Connection Problems, page 6-22](#).

Manually Adding SSL Certificates for Devices that Use HTTPS Communications

When you use SSL (HTTPS) as the transport protocol for communicating with IPS, PIX, ASA, or FWSM devices, or Cisco IOS routers, you can configure Security Manager to automatically retrieve the device authentication certificate when adding the device (see [Device Communication Page, page A-11](#)).



Tip

Having an accurate certificate is required for successful HTTPS communications; Security Manager cannot communicate with the device without the correct certificate, which prevents configuration deployment. When using self-signed certificates, the device might create a new certificate if Security Manager attempts to access it using the wrong certificate. Thus, it is best to configure Security Manager to always retrieve the certificate from the device.

Instead of having Security Manager automatically retrieve the certificates, you can manually add them to increase the level of network security. On the Device Communication page, you would configure the device authentication setting for the device type as **Manually add certificates**.

The easiest way to manually update the certificate for a device is to retrieve it from the device. Right-click the device and select **Device Properties**. Click **Credentials** to open the Credentials page, and then click **Retrieve From Device** to the right of the **Authentication Certificate Thumbprint** field. Security Manager retrieves the certificate and prompts you to accept it. You might need to do this if you encounter certificate problems during configuration deployment.

You can also manually type in, or copy and paste, the certificate thumbprint without having Security Manager log into the device. Use the following procedure to manually enter the SSL certificate thumbprint for a device if you configured that device type to require manually added certificates.

Before You Begin

Obtain the certificate thumbprint (a hexadecimal string) for the device.

**Tip**

If the thumbprint is not readily available, you can copy it from the error message that is displayed when you add the device from the network or from an export file.

Procedure

-
- Step 1** Select **Tools > Security Manager Administration** and select **Device Communication** from the table of contents to open the Device Communication page (see [Device Communication Page, page A-11](#)).
- Step 2** Click **Add Certificate** to open the Add Certificate dialog box (see [Add Certificate Dialog Box, page A-14](#)).
- Step 3** Enter the DNS hostname or IP Address of the device, the certificate thumbprint in hexadecimal format, and click **OK**. The thumbprint is added to the certificate store.

**Tip**

To erase an existing thumbprint, leave the Certificate Thumbprint field empty.

Troubleshooting SSH Connection Problems

For devices that use SSH as the transport protocol, Security Manager automatically detects the appropriate SSH version (1.5 or 2) to use with each device. During SSH version 2 connections, Security Manager automatically negotiates encryption algorithms or ciphers with the device. Security Manager also automatically overwrites the SSH public key for the device if the key changes. Thus, you typically will not run into SSH connection problems.

If you do have SSH connection problems, consider these fixes:

- If the public key on the device changed, and SSH connections are failing due to a key problem, remove the key for the device from the Program Files/CSCOpX/MDC/be/tmp/.ssh/known_hosts file on the Security Manager server and retry the operation.
- Security Manager uses 3DES (Data Encryption Standard) as the default encryption algorithm. If this is not the correct algorithm for your devices, either change the configuration of your devices, or update the Program Files/MDC/athena/config/DCS.properties file to indicate the correct algorithm on the DCS.ssh.encrypt property. (Contact Cisco TAC if you need more help). You must restart the Security Manager daemon manager if you change this file.

Related Topics

- [Chapter 5, “Preparing Devices for Management”](#)
- [Device Communication Page, page A-11](#)
- [Credentials Page, page C-30](#)

Discovering or Changing the CS-MARS Server for a Device

If you use the Cisco Security Monitoring, Analysis and Response System (CS-MARS) servers to monitor devices, you can register them in Security Manager and then view syslogs and events that are related to firewall access or IPS signature rules for individual devices.

Security Manager can automatically discover the CS-MARS servers that monitor a device when you try to view events related to a rule. If more than one server monitors a device, you are prompted to select which server to use.

You can also proactively select the CS-MARS server for a device in its Device Properties window. Similarly, if you ever need to change the CS-MARS server assigned to a device, you can change the selection in its Device Properties window. This procedure explains how to discover or change the CS-MARS server for a device from its Device Properties window.

Before You Begin

The CS-MARS server that monitors the device must already be registered with Security Manager on the CS-MARS administration page (**Tools > Security Manager Administration > CS-MARS**). For more information, see [Registering CS-MARS Servers in Security Manager, page 21-22](#).

Related Topics

- [Understanding the Device View, page 6-1](#)
- [Understanding Device Properties, page 6-5](#)
- [CS-MARS Page, page A-3](#)

Procedure

-
- Step 1** In Device view, do one of the following in the Device selector to open the Device Properties dialog box:
- Double-click a device.
 - Right-click a device and choose **Device Properties**.
 - Select a device and choose **Tools > Device Properties**.
- Step 2** Click **General** in the table of contents to open the General properties page (see [General Page, page C-27](#)).
- Step 3** In the CS-MARS Monitoring group, click **Discover CS-MARS**. Security Manager determines which registered server is monitoring the device, if any. If there are more than one, you are prompted to select which CS-MARS server to use.
-

Showing Device Containment

You can display the service modules, security contexts, and virtual sensors that are contained in devices that include them. Based on the type of device, you can view these contained elements:

- Catalyst 6500/7600 devices—The IDS and FWSM service modules, security contexts, and virtual sensors.
- For FWSM, PIX Firewall 7.0, and ASA devices—The security contexts defined on the device.
- IPS devices—The virtual sensors defined on the device.

For information about security contexts, see [Configuring Security Contexts on Firewall Devices, page 15-84](#).

Procedure

-
- Step 1** Select a Catalyst 6500/7600, PIX Firewall 7.0, FWSM, ASA, or IPS device from the Device selector.
- Step 2** Select **Tools > Show Containment**, or right-click the device and select **Show Containment**.
The Composite View dialog box opens and displays elements contained in the selected device, if any.
-

Cloning a Device

A cloned (duplicate) device shares the configurations and properties of the source device. Cloning a device saves you time because you do not need to re-create configuration and properties on the new device.

The cloned device shares the device operating system version, credentials and grouping attributes with the source device, but it has its own unique identity, such as display name, IP address, hostname, and domain name. You can clone only one device at a time.



Note

You cannot clone a Catalyst switch or a Catalyst 6500/7600 device.

Related Topics

- [Understanding the Device View, page 6-1](#)
- [Copying Policies Between Devices, page 7-21](#)

Procedure

-
- Step 1** In Device view, right-click the device to clone in the Device selector and select **Clone Device**. The Create a Clone of Device dialog box appears (see [Create a Clone of Device Dialog Box, page C-26](#)).
- Step 2** Enter the IP address and names for the clone in the appropriate fields. At minimum, you must enter a new display name.
- Step 3** Click **OK**. A clone of the source device with its unique display name is created in the Device selector.
-

Deleting Devices from the Security Manager Inventory

If you do not want to continue managing a device in Security Manager, you can delete it from the inventory. Deleting a device from Security Manager does not delete it from any other network management program. The deletion also does not change any configuration settings on the device.



Tip

If you delete a device that contains other devices, the contained devices are also deleted. For example, if you added a Catalyst switch and its contained FWSM, if you delete the switch, the FWSM is also deleted. You are warned if contained devices will be deleted.

Procedure

- Step 1** In Device view, select the device to delete from the Device selector.
- Step 2** Click the **Delete** button or select **File > Delete Device**. You are asked to confirm the deletion.
- If problems occur during the deletion, the Device Delete Validation dialog box opens (see [Device Delete Validation Page, page C-25](#)). The problem is described and you can elect to continue with the deletion (if possible) by clicking **OK**.
-

Viewing Inventory Status

You can view a summary of device properties for all devices that you are authorized to view. The summary includes device contact information and all device configurations, indicating which settings are local and which are using a shared policy, and indicating any policy object overrides in effect.

If you are using Performance Monitor to monitor your devices, status information from Performance Monitor can be included in the inventory summary if Security Manager is configured to provide it. You can also view the status of configuration deployment to the device. For information on how to configure the inventory status to show this information, see [Configuring Status Providers, page 21-10](#).

The report is in table format, allowing you to organize information by filtering, sorting, reordering and removing columns. You can also export the table contents to a comma-separated values (CSV) file on the Security Manager server.

Procedure

- Step 1** In Device view, select **Tools > Inventory Status**. The Inventory Status appears (see [Inventory Status Window, page C-37](#)).
- To view a subset of the devices listed, select a filter from the Filter list, or you can create a filter. For more information, see [Filtering Tables, page 3-17](#).
 - To view information for a specific device, use the scroll buttons or click on a row to highlight the device.
 - To export the inventory status report to a CSV file, click **Export**. In the Export Inventory Status dialog box, select the directory where you want to create the file, enter a name for the file, and click **OK**.
- Step 2** Click **Close** to close the Inventory Status window.
-

Exporting the Device Inventory

Exporting the device inventory allows you to import the inventory into other network management applications or to manipulate the output for your own reporting purposes. There are two unrelated methods to export the device inventory:

- Use the **Tools > Export Inventory** command—Using this command, you can export the inventory in a format suitable for importing into the CiscoWorks Common Services Device Credential Repository (DCR) or Cisco Security Monitoring, Analysis and Response System (CS-MARS). For more information, see [Exporting the Device Inventory in DCR or CS-MARS Format, page 6-26](#).
- Use the CSMgrDeviceExport Perl script—Using this Perl script, you can export the inventory without starting the Security Manager client. You can direct the output to the screen or to a comma-separated values (CSV) file. For more information, see [Exporting the Device Inventory from the Command Line, page 6-26](#).

Exporting the Device Inventory in DCR or CS-MARS Format

You can export the Security Manager device inventory and then use the exported file to import the inventory into CiscoWorks Common Services Device Credential Repository (DCR) or Cisco Security Monitoring, Analysis and Response System (CS-MARS).

You can export information on devices to which you have Modify Device permissions.

Before You Begin

If you select a device that uses an AUS or Configuration Engine to obtain its IP address, you must also select the server in the list of devices to export. You can export AUS or Configuration Engine information only in DCR format.

Procedure

-
- Step 1** In Device view, select **Tools > Export Inventory** to open the Export Inventory dialog box (see [Export Inventory Dialog Box, page C-34](#)).
- Step 2** Select the devices you want to include in the export file and click >> to add them to the Selected Devices list. You can select a folder to select all devices in the folder.
- Step 3** Click **Browse** to select the folder on the Security Manager server in which to create the export file and to enter a name for the file. For File Type, select whether you want to export the inventory in DCR or CS-MARS format.
- Click **Save** to return to the Export Inventory dialog box. The Export Inventory To field is updated with the export file information.
- Step 4** Click **OK** to create the export file.

If there are problems during the export, the Issues Encountered dialog box opens explaining the problems for each device. For more detailed information for an issue, select a device and click **Details**.

Exporting the Device Inventory from the Command Line

Security Manager includes a Perl script that you can use to export the device inventory without starting the Security Manager client. You can use this script to automate various offline reporting tasks that your organization might require. You can pipe the output to a comma-separated values (CSV) file or otherwise capture and manipulate the output.

The Perl command is located in \$NMSROOT\bin, which is typically C:\Program Files\CSCSp\bin. The syntax of the command is:

```
perl [path]CSMgrDeviceExport.pl-username [-password] [-s {Dhdoirtg}] [-h] [>filename.csv]
```

Syntax

perl [<i>path</i>] CSMgrDeviceExport.pl	The Perl script command. Include the path to the CSMgrDeviceExport.pl file if the path is not defined in the system path variable.
-u <i>username</i>	A Security Manager username. The data exported is limited by the permissions assigned to this user. The user must have View Device permissions.
-p <i>password</i>	(Optional.) The user's password. If you do not include the password on the command, you are prompted for it.
-s { <i>Dhdoirtg</i> }	(Optional.) The fields you are selecting to include in the output. If you do not specify the -s option, all fields are included. You can specify one or more of the following: <ul style="list-style-type: none"> • D—Display name. • h—Host name. • d—Domain name. • o—Operating system (OS) type. • I—Image name. • r—Running OS version. • t—Target OS version. • g—Device groups.
-h	(Optional.) Display the command line help. If you include this option, all other options are ignored.
> <i>filename.csv</i>	(Optional.) Pipe the output to the specified file. If you do not specify a file, the output is displayed on the screen.

Output Format

The output is in standard comma-separated values (CSV) format, which you can open in spreadsheet programs or process with your own scripts. The first line has column headings. The columns, left to right, are in the order of the fields described for the -s option above.

If there is no value for a particular field, that field is blank in the output.

The device group output field is enclosed in double-quotes and it can contain more than one group name. The group names include the path structure for the group. For example, the following output indicates the device is part of two groups, the East Coast group in the Department folder, and the NewGroup group in the New folder. Groups are separated by a semicolon.

```
"/Department/East Coast; /New/NewGroup"
```

Any error messages generated during the script are written to the output file.

Managing the Device Operating System

Security Manager includes shortcut links to several key features in Resource Manager Essentials (RME). You can use software management to analyze individual device operating system versions (also known as image versions) and generate image analysis reports. You can use the report to import and distribute operating system images to groups of devices. You can also schedule operating system upgrade jobs to ensure up-to-date versions and minimize errors.

To enable the shortcut commands, you must configure Security Manager with the location of the RME server. For information on configuring the RME location, see [Device OS Management Page, page A-15](#).

RME Software Image Management (SWIM) includes the following features:

- **Software Repository**—Determines the images that are missing from the network, imports these images into the software library, keeps the library up-to-date, and periodically synchronizes the library with the images running on the network devices. You can also schedule an image import for a later, more convenient time, as well as download an appropriate image from Cisco.com.

To access the software repository, select **Tools > Device OS Management > Software Repository**.

- **Software Distribution**—Generates upgrade analysis reports that allow you to determine prerequisites for image upgrade. You can either select a set of devices and perform an image upgrade, or select a software image and select a set of devices on which to perform the upgrade.

To manage software distribution, select **Tools > Device OS Management > Software Distribution**.

- **Software Management Jobs**—Allows you to view, edit, stop, or delete scheduled image upgrade jobs.

To manage software management jobs, select **Tools > Device OS Management > Management Jobs**.

For specific information on using these RME features, read the online help included with RME.

Working with Device Groups

You can create device groups to help you organize your devices for more effective device management. The following topics explain device groups and how to use them:

- [Understanding Device Grouping, page 6-28](#)
- [Creating Device Group Types, page 6-30](#)
- [Creating Device Groups, page 6-30](#)
- [Deleting Device Groups or Group Types, page 6-31](#)
- [Adding Devices to or Removing Them From Device Groups, page 6-31](#)

Understanding Device Grouping

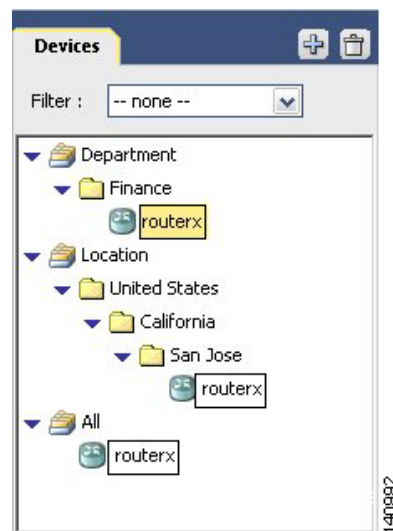
Device groups are simple, arbitrary, organizational collections of devices that you create for more effective network visualization. They are not policy-sharing entities. They are distinct from the various policy object groups (for example AAA server group objects, service group objects, and user group objects). For information on policy objects, see [Introduction to Objects, page 9-2](#).

Device grouping enables you to view a subset of devices in the inventory. The device group hierarchy has two types of folders:

- Device group types—Group types are the highest level in the hierarchy. A group type can contain specific device groups, but it cannot contain devices, except for the All group type, which includes all devices in the inventory. Security Manager comes with the group types Department and Location predefined, but you do not need to use them, and you can delete them. You can create a maximum of 10 group types.
- Device groups—Device groups are subfolders within a group type folder. You can create multiple levels of nested device groups. You can place devices within device groups. However, a device can be in only one group within a group type. For example, in Figure 6-3 under the group type, Location, you can assign routerx to San Jose, but you cannot assign routerx to San Jose and California.

Figure 6-3 shows an example of nested device groups with devices in some of the groups. Notice that an individual device can reside in multiple groups. In this example, routerx is in the Finance group (under the Department group type), and also in the Location > United States > California > San Jose nested group. If you select routerx in any of these places, you are configuring a single device (the configurations are not tied to the grouping).

Figure 6-3 Device Groups



Security Manager lets you create or delete group and group types, and put devices in groups, in many locations in the interface:

- When adding devices to the inventory—The New Device wizard includes a Device Grouping page, where you can create device group types and select a group for the newly-added device. You can also select a default group to which all new devices are added.
- When viewing the device inventory in Device view—The File > Edit Device Groups command opens a dialog box where you can create or delete groups and group types. If you select a group or group type in the Device selector, the File menu and the right-click shortcut menu includes commands for adding groups or adding devices to groups.

To add devices to a group, or remove them from a group, select the group and select **File > Add Devices to Group**.

- When viewing the properties for a device—The Device Grouping page allows you to select the groups to which the device belongs, and to set defaults for devices added to the inventory. This is the only place where you can remove a device from a device group. Double-click a device in the Device selector to open the device properties.

- When using the administration pages—Select **Tools > Security Manager Administration > Device Groups** to open the administration page for device groups, where you can create or delete groups and group types, but you cannot add devices to groups here.

Related Topics

- [Creating Device Group Types, page 6-30](#)
- [Creating Device Groups, page 6-30](#)
- [Deleting Device Groups or Group Types, page 6-31](#)
- [Adding Devices to or Removing Them From Device Groups, page 6-31](#)

Creating Device Group Types

This procedure describes the most direct method to create device group types. For information on other methods of adding group types, see [Understanding Device Grouping, page 6-28](#).

Device group types are the top-level categories in your device group hierarchy. If you want add a device group, see [Creating Device Groups, page 6-30](#)

Related Topics

- [Understanding Device Grouping, page 6-28](#)
- [Deleting Device Groups or Group Types, page 6-31](#)
- [Adding Devices to or Removing Them From Device Groups, page 6-31](#)

Procedure

-
- Step 1** Select **File > Edit Device Groups**.
- The Edit Device Groups page opens (see [Edit Device Groups Dialog Box, page C-34](#)).
- Step 2** Click **Add Type**. A new device group type entry is added to the selector.
- Step 3** Enter a name for the group type and press **Enter**.
- Step 4** Click **OK** to close the Edit Device Groups page.
-

Creating Device Groups

This procedure describes the most direct method to create device groups. For information on other methods of adding groups, see [Understanding Device Grouping, page 6-28](#).

Device groups are the lower-level categories in your device group hierarchy, and are added either within a device group type (top-level) or within another device group. If you would rather add a device type group, see [Creating Device Group Types, page 6-30](#).

Related Topics

- [Understanding Device Grouping, page 6-28](#)
- [Adding Devices to or Removing Them From Device Groups, page 6-31](#)
- [Deleting Device Groups or Group Types, page 6-31](#)

Procedure

-
- Step 1** In the Device selector, right-click the device group type or a device group in which you want to create the group and select **New Device Group**. The Add Group dialog box appears.
- Step 2** Enter a name for the device group and click **OK**. The new device group is added to the Device selector.
-

Deleting Device Groups or Group Types

If you no longer need a device group or group type, you can delete it. The only group type that you cannot delete is the All group.

When you delete a group or group type, you delete any groups that are in it. However, you are not deleting any devices. The devices that are in the group remain in the inventory and can be found in other groups to which they belong (you can find all devices in the All group).

There are many ways to delete device groups and group types. This procedure explains the most direct way. For information on other methods of deleting them, see [Understanding Device Grouping](#), page 6-28.

Procedure

-
- Step 1** In Device view, select **File > Edit Device Groups**. The Edit Device Groups page opens (see [Edit Device Groups Dialog Box](#), page C-34).
- Step 2** Select the group type or group you want to delete and click the **Delete** button. You are asked to confirm the deletion.
-

Adding Devices to or Removing Them From Device Groups

You must create a device group before you add devices to it. To create groups, see [Creating Device Groups](#), page 6-30.

Related Topics

- [Understanding Device Grouping](#), page 6-28

Procedure

-
- Step 1** Select the device group in the Device selector, right-click and select **Add Devices to Group**. The Add Devices to Group page appears.
- Step 2** To add devices to the group, select the devices in the Available Devices selector and click >> to move them to the Selected Devices list.
- To remove devices, select them in the Selected Devices list and click <<.
- Step 3** Click **OK**. The device group membership is adjusted to include the devices that were in the Selected Devices list.
-

