



APPENDIX **D**

Policy User Interface Reference

These topics describe the pages that are accessed from the Policy menu and within the Policy view, or that relate to general policy management. The Policy view is used to globally manage all the shared policies configured with Cisco Security Manager:

- [Policy Menu General Reference, page D-1](#)
- [Policy Discovery Status Page, page D-22](#)
- [Policy View General Reference, page D-25](#)

Policy Menu General Reference

Use the options in the Policy menu to manage local and shared policies in Device view. The options in the Policy menu display the dialog boxes and wizards described in the following topics:

- [Share Policy Dialog Box, page D-2](#)
- [Assign Shared Policy Dialog Box, page D-3](#)
- [Copy Policies Wizard, page D-6](#)
- [Share Policies Wizard, page D-11](#)
- [Shared Policy Assignments Dialog Box, page D-13](#)
- [Save Policy As Dialog Box, page D-15](#)
- [Rename Policy Dialog Box, page D-15](#)

- [Inherit Rules Dialog Box, page D-16](#)
- [Discover Policies On Device Dialog Box, page D-17](#)

Share Policy Dialog Box

Use the Share Policy dialog box to convert a local policy to a shared policy that you can assign to multiple devices or VPNs. For more information, see [Sharing a Local Policy, page 7-28](#).

Navigation Path

In Device view, select a policy from the Device Policies selector, then do one of the following:

- Select **Policy > Share Policy**.
- Right-click the policy, then select **Share Policy**.
- Click the **local device** link in the Assigned To field in the policy banner, then click **Share Policy** in the message dialog box that is opened.

Related Topics

- [Assign Shared Policy Dialog Box, page D-3](#)
- [Shared Policy Assignments Dialog Box, page D-13](#)
- [Inherit Rules Dialog Box, page D-16](#)
- [Policy Menu General Reference, page D-1](#)
- [Using the Policy Banner, page 7-26](#)

Field Reference

Table D-1 Share Policy Dialog Box

Element	Description
Policy Name	The name that identifies the shared policy. Unlike local policies, shared policies require a name so that they can be identified when you assign the policy to devices or VPN topologies. Names can contain up to 255 characters, including spaces and special characters.
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.

Assign Shared Policy Dialog Box

Use the Assign Shared Policy dialog box to assign an existing shared policy to a selected device. For more information, see [Assigning a Shared Policy to a Selected Device](#), page 7-32.



Note

If you use this option to replace a local, rule-based policy, a warning message is displayed that gives you the option to inherit the rules of the shared policy instead of replacing the local policy through assignment. See [Local Policy Will Be Replaced Dialog Box](#), page D-4.

Navigation Path

In Device view, select a policy from the Device Policies selector, then do one of the following:

- Select **Policy > Assign Shared Policy**.
- Right-click the policy in the Device Policies selector, then select **Assign Shared Policy**.
- Click the **local device** link in the Policy Assigned field in the policy banner.

Related Topics

- [Save Policy As Dialog Box](#), page D-15
- [Shared Policy Assignments Dialog Box](#), page D-13

- [Inherit Rules Dialog Box, page D-16](#)
- [Policy Menu General Reference, page D-1](#)
- [Using the Policy Banner, page 7-26](#)

Field Reference

Table D-2 *Assign Shared Policy Dialog Box*

Element	Description
Policy selector	Lists all shared policies defined for the selected policy type. Select the shared policy to assign to the selected device.
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.



Note

You cannot change the policy assigned to the device if the device is locked by another user. Click **Close** to close the dialog box.

Local Policy Will Be Replaced Dialog Box

When working with a rule-based policy such as access rules or AAA rules, use the Local Policy Will Be Replaced dialog box to choose between:

- Assigning a shared policy in place of the existing local policy. If you choose to assign, all local rules are removed and cannot be retrieved.
- Inheriting the rules of the shared policy. If you choose to inherit, the inherited rules are added to the local rules that are already defined.

Navigation Path

The Local Policy Will Be Replaced dialog box is displayed automatically when you do the following:

1. Select a local, rule-based policy (such as Access Rules).

2. Right-click the policy in the Device Policies selector, then select **Assign Shared Policy**.
3. Select a shared policy from the displayed list, then click **OK**.

Related Topics

- [Inheritance vs. Assignment, page 7-51](#)
- [Assign Shared Policy Dialog Box, page D-3](#)
- [Policy Menu General Reference, page D-1](#)

Field Reference

Table D-3 **Local Rules Will Be Replaced Dialog Box**

Element	Description
Assign Policy [name of policy]	Select this option to confirm that you want to replace the local policy defined for the device with the selected shared policy. If you choose this option, the shared policy replaces the local policy, and all rules defined in the local policy are removed.
Inherit from Policy [name of policy]	Select this option to have the local policy inherit the rules defined in the shared policy. If you choose this option, the inherited rules are added to the local rules. Use inheritance instead of assignment when the device needs to maintain the set of local rules already defined for it.
Do not show this again	When selected, Security Manager implements your choice (assignment or inheritance) automatically whenever this situation arises in the future. When deselected, Security Manager displays this dialog box so that you can choose between assignment and inheritance. This is the default. Tip To reset hidden warning messages, select Tools > Security Manager Administration > Customize Desktop , then click Reset 'Do Not Ask' on Warnings .
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.

Copy Policies Wizard

Use the Copy Policies wizard to copy selected policies (both local and shared) to one or more devices that support the selected policies. For example, you can use the Copy Policies wizard to copy a set of firewall service policies and routing policies from one firewall device to fifty other devices with a single operation.

For more information, see [Copying Policies Between Devices, page 7-21](#).

The pages of the Copy Policies wizard are described in the following topics:

- [Copy Policies Wizard—Copy Policies from this Device Page, page D-6](#)
- [Copy Policies Wizard—Select Policies to Copy Page, page D-7](#)
- [Copy Policies Wizard—Copy Policies to these Devices Page, page D-9](#)

Navigation Path

To start the Copy Policies wizard, in Device view, select a device from the Device selector, then do one of the following:

- Select **Policy > Copy Policies Between Devices**. The Copy Policies wizard starts at step 1 (see [Copy Policies Wizard—Copy Policies from this Device Page, page D-6](#)).
- Right-click the device in the Device selector, then select **Copy Policies Between Devices**. The Copy Policies wizard starts at step 2 (see [Copy Policies Wizard—Select Policies to Copy Page, page D-7](#)).

Related Topics

- [Share Policies Wizard, page D-11](#)
- [Policy Menu General Reference, page D-1](#)

Copy Policies Wizard—Copy Policies from this Device Page

Use the Copy Policies from this Device page of the Copy Policies wizard to select the device whose policies will be copied to other devices.

If you start the Copy Policies wizard by right-clicking a specific device, the device you right-clicked is automatically selected as the source device and the wizard starts on the [Copy Policies Wizard—Select Policies to Copy Page, page D-7](#). You can return to the Copy Policies from this Device page by clicking **Back**.

Navigation Path

For information on starting the Copy Policies wizard, see [Copy Policies Wizard, page D-6](#).

Related Topics

- [Copy Policies Wizard, page D-6](#)
- [Copying Policies Between Devices, page 7-21](#)

Field Reference

Table D-4 *Copy Policies Wizard—Copy Policies from this Device Page*

Element	Description
Filter	Selects a filter to apply to the device selector, or enables you to create a new filter. By default, the active filter in Device view is applied to the filter displayed in the wizard. For more information, see Filtering Items in Selectors, page 3-20 . Note If you create a filter while working inside the wizard, it is added to the list of filters available in Device view. The active filter in Device view, however, does not change.
Device selector	Selects the device containing the policies to be copied.
Next button	Advances to the next wizard page. Security Manager evaluates the device and generates a list of the copyable policies defined on the device.

Copy Policies Wizard—Select Policies to Copy Page

Use the Select Policies to Copy page of the Copy Policies wizard to select which policies to copy from the source device to the target devices.

Navigation Path

For information on starting the Copy Policies wizard, see [Copy Policies Wizard, page D-6](#).

Related Topics

- [Copy Policies Wizard, page D-6](#)
- [Copying Policies Between Devices, page 7-21](#)
- [Policy Status Icons, page 7-20](#)

Field Reference**Table D-5** *Copy Policies Wizard—Select Policies to Copy Page*

Element	Description
Policy selector	<p>Selects the policies to copy from the source device to the target devices. Selecting the check box for a policy group selects all of the policies in that group. The selector only includes policies that can be copied; it does not list all policies on the device.</p> <p>Consider the following when selecting policies:</p> <ul style="list-style-type: none"> • When you copy policies between firewall devices (PIX, ASA, FWSM), copying the failover policy automatically copies the interface policy and vice-versa. • It is usually not a good idea to copy interface policies, because these policies can have specific IP addresses. • If you select the security contexts policy (for FWSM, PIX Firewall, or ASA devices), you must submit your changes after copying the devices for the contexts to appear in the device selector. In non-Workflow mode, select File > Submit. In Workflow mode, submit your activity.

Table D-5 Copy Policies Wizard—Select Policies to Copy Page (Continued)

Copy the Global Values of Policy Objects Copy the Overridden Values of Policy Objects	<p>These copy options affect how policies that use policy objects are handled, and they are not mutually exclusive. You can select any combination, and your selection has a significant effect on how the selected policies are copied. These are the possible combinations and their meanings:</p> <ul style="list-style-type: none"> • Select neither option—If a selected policy uses a policy object, and an equivalent policy on the target device uses the same policy object, the policy object's value defined on the target device is preserved. If the target device does not use the policy object, it is copied to the target using the policy object's global value (any overrides on the source device are ignored). • Select Copy the Global Values of Policy Objects, but deselect Copy the Overridden Values of Policy Objects—If the source device includes policies that use policy objects, only policies that use global values for the policy objects are copied. If the target device has an equivalent policy that uses local values for the policy object, the local values are replaced by the policy object's global values. • Deselect Copy the Global Values of Policy Objects, but select Copy the Overridden Values of Policy Objects—If the source device includes policies that use policy objects, only policies that override the policy object's global values are copied. The target devices get the source device's override value for the policy object. • Select both options—The target device will receive the exact same policy object values that exist on the source device.
Back button	Returns to the previous wizard page.
Next button	Advances to the next wizard page. Security Manager evaluates the policies to determine which devices can support all selected policies.

Copy Policies Wizard—Copy Policies to these Devices Page

Use the Copy Policies to these Devices page of the Copy Policies wizard to select the devices to which policies from the source device will be copied.

Navigation Path

For information on starting the Copy Policies wizard, see [Copy Policies Wizard, page D-6](#).

Related Topics

- [Copy Policies Wizard, page D-6](#)
- [Copying Policies Between Devices, page 7-21](#)

Field Reference**Table D-6** Copy Configuration Wizard—Copy Policies to these Devices Page

Element	Description
Filter	<p>Selects a filter to apply to the device selector, or enables you to create a new filter. By default, the active filter in Device view is applied to the filter displayed in the wizard. For more information, see Filtering Items in Selectors, page 3-20.</p> <p>Note If you create a filter while working inside the wizard, it is added to the list of filters available in Device view. The active filter in Device view, however, does not change.</p>
Device selector	<p>Selects the devices to which policies from the source device should be copied. Selecting the check box for a device group selects all of the devices in that group.</p> <p>The device selector displays only those devices that support all of the policies you selected to copy. If you do not see all of the devices to which you want to copy policies, you can return to the policy selection page and deselect the more restrictive policies, and use the wizard a second time to copy the restrictive policies to the subset of devices that support them.</p> <p>The device list is empty if no other device in the inventory can support all selected policies.</p>
Preview button	<p>Click this button to view a summary of the policies that will be copied. The summary shows the selected devices, the policies that will be copied to them, and any overrides that will be created, updated, or deleted due to the copied policies.</p>

Table D-6 Copy Configuration Wizard—Copy Policies to these Devices Page (Continued)

Back button	Returns to the previous wizard page.
Finish Button	Starts the copy operation. Security Manager ensures that the policies are successfully copied to every selected target device. If the copy fails for any target device, the Copy Policy Failed dialog box opens explaining the failures. Security Manager also removes the copied policies from any device to which the copy was successful.

Share Policies Wizard

Use the Share Policies wizard to take the policies configured on a particular device and make them shared policies that you can assign to other devices. For more information, see [Sharing Multiple Policies of a Selected Device, page 7-29](#).

The pages of the Share Policies wizard are described in the following topics:

- [Share Policies Wizard—Share Policies from this Device Page, page D-11](#)
- [Share Policies Wizard—Select Policies to Share Page, page D-12](#)

Navigation Path

In Device view, select a device from the Device selector, then do one of the following:

- Select **Policy > Share Device Policies**.
- Right-click the device in the Device selector, then select **Share Device Policies**.

Related Topics

- [Copy Policies Wizard, page D-6](#)
- [Policy Menu General Reference, page D-1](#)

Share Policies Wizard—Share Policies from this Device Page

Use the Share Policies from this Device page of the Share Policies wizard to select the device whose policies you want to share.

**Note**

When you access the Share Policies wizard by right-clicking a specific device, the device you right-clicked is automatically selected as the source device and you are brought directly to the [Share Policies Wizard—Select Policies to Share Page](#), page D-12. You can return to the Select Source Device page by clicking **Back**.

Navigation Path

In Device view, select a device from the Device selector, then select **Policy > Share Device Policies**.

Related Topics

- [Share Policies Wizard](#), page D-11
- [Sharing Multiple Policies of a Selected Device](#), page 7-29

Field Reference

Table D-7 *Share Configuration Wizard—Share Policies from this Device Page*

Element	Description
Filter	<p>Selects a filter to apply to the device selector, or enables you to create a new filter. By default, the active filter in Device view is applied to the filter displayed in the wizard. For more information, see Filtering Items in Selectors, page 3-20.</p> <p>Note If you create a filter while working inside the wizard, it is added to the list of filters available in Device view. The active filter, however, does not change.</p>
Device selector	Selects the device containing the policies to be shared.
Next button	Advances to the next wizard page.

Share Policies Wizard—Select Policies to Share Page

Use the Select Policies to Share page of the Share Policies wizard to select which policies you want to share.

Navigation Path

Go to the [Share Policies Wizard, page D-11](#), then click **Next** on the Share Policies from this Device page.

Related Topics

- [Share Policies Wizard, page D-11](#)
- [Sharing Multiple Policies of a Selected Device, page 7-29](#)

Field Reference

Table D-8 *Share Policies Wizard—Select Policies to Share Page*

Element	Description
Policy selector	Selects the policies to share. Selecting the check box for a policy group selects all of the devices in that group. By default, all configured policies (local and shared) are selected. Note If you select a policy that is already shared, Security Manager creates a copy of that policy using the name that you define in the wizard.
Save policies as	The name to give to the policies you are sharing.
Back button	Returns to the previous wizard page.
Next button	Advances to the next wizard page.
Finish button	Saves your definitions and close the wizard.

Shared Policy Assignments Dialog Box

Use the Shared Policy Assignments dialog box to modify the list of devices or VPN topologies to which you have assigned a selected shared policy. For more information, see [Modifying Shared Policy Assignments in Device View, page 7-38](#).

You can also modify policy assignments from Policy view. See [Policy View—Assignments Tab, page D-29](#).

Navigation Path

In Device view, select a shared policy from the Device Policies selector, then do one of the following:

- Select **Policy > Edit Policy Assignments**.
- Right-click the policy in the Device Policies selector, then select **Edit Policy Assignments**.
- Click the *n* device link in the Assigned To field in the policy banner.

Related Topics

- [Share Policy Dialog Box, page D-2](#)
- [Shared Policy Assignments Dialog Box, page D-13](#)
- [Inherit Rules Dialog Box, page D-16](#)
- [Policy Menu General Reference, page D-1](#)
- [Using the Policy Banner, page 7-26](#)

Field Reference

Table D-9 **Shared Policy Assignments Dialog Box**

Element	Description
Available Devices/VPNs	Lists all existing devices or VPN topologies. To assign the selected policy to additional devices or VPNs, select one or more items from this list, then click >> to add them to the Selected Devices/VPNs list.
Assigned Devices/VPNs	<p>Lists all devices or VPNs to which the selected policy has been assigned. To remove items from this list, select the item, then click <<.</p> <p>If you unassign a shared, mandatory policy from a VPN (for example, IKE), a default policy is configured automatically in its place. Unassigning a VPN policy that is not mandatory removes the policy completely from the VPN.</p> <p>If you unassign a shared policy from a remote access VPN, an empty policy is configured in its place, even if it is a mandatory policy, such as IKE. In such cases, you must configure a new policy in order to avoid validation errors during deployment.</p> <p>If you unassign a shared policy from a device, the policy type is effectively removed from that device configuration.</p>
OK button	<p>Saves your changes locally on the client and closes the dialog box.</p> <p>Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.</p>

Save Policy As Dialog Box

Use the Save Policy As dialog box to duplicate an existing shared policy under a new name. For more information, see [Copying a Shared Policy, page 7-35](#).

Navigation Path

Select a shared policy in either Device view or Policy view, then do one of the following:

- Select **Policy > Save Policy As**.
- Right-click the shared policy, then select **Save Policy As**.

Related Topics

- [Assign Shared Policy Dialog Box, page D-3](#)
- [Shared Policy Assignments Dialog Box, page D-13](#)
- [Inherit Rules Dialog Box, page D-16](#)
- [Policy Menu General Reference, page D-1](#)

Field Reference

Table D-10 *Save Policy As Dialog Box*

Element	Description
Policy Name	The name that identifies the shared policy. Unlike local policies, shared policies require a name so that they can be identified when you assign the policy to devices or VPN topologies. Names can contain up to 255 characters, including spaces and special characters.
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.

Rename Policy Dialog Box

Use the Rename Policy dialog box to assign a different name to a selected shared policy. For more information, see [Renaming a Shared Policy, page 7-36](#).

Navigation Path

Select a shared policy in either Device view or Policy view, then do one of the following:

- Select **Policy > Rename Policy**.
- Right-click the policy, then select **Rename Policy**.

Related Topics

- [Create a Policy Dialog Box, page D-30](#)
- [Policy View General Reference, page D-25](#)

Field Reference**Table D-11** *Rename Policy Dialog Box*

Element	Description
Policy Name	The new name to assign to the selected shared policy. Names can contain up to 255 characters, including spaces and special characters.
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.

Inherit Rules Dialog Box

Use the Inherit Rules dialog box to have a rule-based policy (such as access rules) inherit the rules of a shared policy of the same type. For more information, see [Inheriting Rules, page 7-52](#).

Navigation Path

Select a shared rule-based policy in either Device view or Policy view, then do one of the following:

- Select **Policy > Inherit Rules**.
- Right-click the policy, then select **Inherit Rules**.
- Click the link in the Inherits From field in the policy banner.

Related Topics

- [Inheritance vs. Assignment, page 7-51](#)
- [Save Policy As Dialog Box, page D-15](#)
- [Assign Shared Policy Dialog Box, page D-3](#)
- [Shared Policy Assignments Dialog Box, page D-13](#)
- [Policy Menu General Reference, page D-1](#)
- [Using the Policy Banner, page 7-26](#)

Field Reference**Table D-12** *Inherit Rules Dialog Box*

Element	Description
Policy selector	Selects the parent policy, that is, the policy whose rules should be inherited. Policies can inherit only from shared policies of the same type. The name of the selected parent policy is displayed below the selector.
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.

Discover Policies On Device Dialog Box

Use the Discover Policies On Device dialog box to have Security Manager discover the policies for a device that is already in the device inventory. You can also discover policies when you add the device to the inventory. For more information about adding devices, see [Adding Devices to the Device Inventory, page 6-8](#).

Navigation Path

In Device view, select a device from the Device selector and do one of the following:

- Select **Policy > Discover Policies on Device**.
- Right-click the device in the Device selector and select **Discover Policies on Device**.

Related Topics

- [Discovering Policies on Devices Already in Security Manager, page 7-10](#)
- [Discovering Policies, page 7-7](#)
- [Viewing Policy Discovery Task Status, page 7-12](#)
- [Selecting or Specifying a File or Directory on the Server File System, page 3-31](#)
- [Discovery Status Dialog Box, page D-19](#)

Field Reference**Table D-13 Discover Policies On Device Dialog Box**

Element	Description
Discovery Task Name	The name assigned to the discovery task. Security Manager automatically generates a name for the task based on the current date and time, but you can modify this name as required.
Discover From Config. File	<p>The source of policy information to be discovered:</p> <ul style="list-style-type: none"> • Live Device—Discover policies directly from the device. • Config File—Discover policies from a configuration file. Specify the location of the file in the Config File field. Click Browse to select the file on the Security Manager server. <p>You can discover policies only from configuration files that were generated from the device (for example, with the show run command). For more information, see Adding Devices from Configuration Files, page 6-13.</p> <ul style="list-style-type: none"> • Factory Default Configuration—Performs discovery on a firewall device using a file containing the factory-default settings for that device. Security Manager automatically chooses the appropriate file for the selected device. For more information, see Default Firewall Configurations, page 16-2.

Table D-13 Discover Policies On Device Dialog Box (Continued)

Discover Policies for Security Contexts	<p>Whether to discover policies for each security context that is configured on a firewall device running in multiple-context mode. This field applies only to PIX, ASA, and FWSM devices.</p> <p>When deselected, Security Manager treats the entire device as having a single set of policies configured in single-context mode.</p> <p>For more information about security contexts, see Configuring Security Contexts on Firewall Devices, page 16-117.</p>
Policies to Discover	<p>The policy types to discover on the selected device:</p> <ul style="list-style-type: none"> • Inventory—Includes device information such as the hostname and domain name, interfaces, and security contexts (for firewall devices running in multiple-context mode). On Cisco IOS routers, this option also discovers all interface-related policies, such as DSL, PPP, and PVC policies. • Platform Settings—Includes all platform-specific policies that can be configured on the selected device. For example, if you are performing policy discovery on a PIX firewall device, this option includes such policies as device administration policies, multicast policies, and routing policies. • Firewall Services—Includes all firewall service policies. For more information, see Chapter 13, “Managing Firewall Services”. • RA VPN Policies—Includes all remote access VPN policies that are configured on the selected device. For more information, see Chapter 11, “Managing Remote Access VPNs”. • IPS—Includes all IPS policies that are configured on the selected device. For more information, see Chapter 18, “Managing IPS Devices” and Chapter 14, “Managing IPS Services”.

Discovery Status Dialog Box

Use the Discovery Status dialog box to view detailed information about the current policy discovery task. The dialog box includes general information about the status of the task, as well as detailed information about any warnings or errors generated by the device being discovered.

The Discovery Status dialog box opens automatically when you initiate a discovery task on existing devices and when you add devices from the network, from a configuration file, or from an export file. For more information about initiating a discovery task, see [Discover Policies On Device Dialog Box](#), page D-17.

Related Topics

- [Viewing Policy Discovery Task Status](#), page 7-12
- [Discovering Policies](#), page 7-7
- [Adding Devices from the Network](#), page 6-10
- [Adding Devices from Configuration Files](#), page 6-13
- [Adding Devices from an Export File](#), page 6-16

Field Reference

Table D-14 **Discovery Status Dialog Box**

Element	Description
Progress bar	Indicates what percentage of the discovery task on the current device has been completed.
Status	The current state of the discovery task.
Devices to be discovered	The total number of devices being discovered during this task. The number includes service modules, security contexts, and virtual sensors.
Devices discovered successfully	The number of devices discovered without errors.
Devices discovered with errors	The number of devices that generated errors during discovery.

Table D-14 **Discovery Status Dialog Box (Continued)**

Discovery Details table	<p>The devices that are being discovered. Select a device to see the messages generated during the discovery of that device in the message list below the summary list. Besides the device name, information in the table includes:</p> <ul style="list-style-type: none"> • Severity—The overall severity level of the discovery task. For example, if the discovery task completed successfully, an Information icon is displayed. If the task failed, an Error icon is displayed. • State—The current state of the policy discovery task for the selected device: <ul style="list-style-type: none"> – Device Added—The device has been added to Security Manager, but policy discovery has not yet started. – Discovery Started—Policy discovery has started. – Reading and Parsing Device Config—The policy discovery task is interpreting the device configuration. – Importing Objects—The policy discovery task is importing objects from the configuration. – Importing Policies—The policy discovery task is importing policies from the configuration. – Discovery Complete—Policy discovery has been completed successfully. – Discovery Failed—Policy discovery failed due to errors. • Discovered From—The source of policy information. For example, when discovering from a configuration file, this field displays the name and path of the file.
Messages list	The messages generated during the discovery for the selected device. Select a message to see detailed information in the fields to the right of the list.
Description	Additional information about the message selected in the message list.

Table D-14 **Discovery Status Dialog Box (Continued)**

Action	The steps you should take to resolve the described problem.
Abort button	<p>Aborts the discovery task.</p> <p>If you abort the task when performing policy discovery on a single device, the result is partial discovery of that device. In such cases, we recommend deleting the information (for example, by discarding the activity) and starting again.</p> <p>If you abort the task when performing policy discovery on multiple devices, Security Manager automatically discards the information for any partially discovered device. Devices for which discovery was completed before you aborted the operation are fully discovered.</p>

Policy Discovery Status Page

Use the Policy Discovery Status page to view the status of previous policy discovery and device addition tasks.

Navigation Path

Select **Tools > Policy Discovery Status**.

Related Topics

- [Viewing Policy Discovery Task Status, page 7-12](#)

Field Reference

Table D-15 Policy Discovery Status Page

Element	Description
Task Table	
<p>The upper portion of the window lists the previous policy discovery or device addition tasks. Select a task to view detailed information about it in the lower portion of the window. The columns in the table provide overall status information for the task.</p> <p>When adding devices that contain security contexts, the context discovery appears as a separate Policy Discovery task.</p>	
Name	The name of the discovery or device addition task. This might be a system generated name or a name you specified when rediscovering device policies.
Type	The type of task, either Policy Discovery (when you rediscover device policies) or Add Device (when you add a device using the New Device wizard and elect to discover policies).
Start Time	The time the task started.
End Time	The time the task stopped.
Status	<p>The overall status of the task. One of the following:</p> <ul style="list-style-type: none"> Completed successfully—The task succeeded. Completed with errors—The task was partially successful. This could occur if all policies were not discovered or if the device was added but no policies were discovered. Completed with warnings—The task was successful but a minor problem occurred. Failed—The task failed. No policies were discovered or no device was added because of errors or because you stopped discovery.
Refresh button	Click this button to refresh the task list to update the information if there are tasks running in the background or if new tasks were created.
Delete button	Click this button to delete the selected task from the database. Deleting old tasks does not affect the related devices or discovered policies.

Table D-15 Policy Discovery Status Page (Continued)**Discovery Details or Import Details Tables**

These tables display the devices included in the selected task. The name differs depending on the type of task (Discovery Details for Policy Discovery tasks, Import Details for Add Device tasks).

Select a device to see the messages generated during the task for that device in the message list below the table.

Device	The name of the device. If the name is followed by (deleted), the device is no longer in the Security Manager inventory.
Config File (Import Details only)	The location of the configuration file. This field is displayed only if you are importing from a configuration file.
Task Type (Import Details only)	One of the following: <ul style="list-style-type: none"> • Import only—Adding devices to Security Manager. • Import and Discover—Adding devices and discovering policies and inventory, or adding devices and discovering policies.
Severity	An icon for one of the following is displayed: <ul style="list-style-type: none"> • Error—The device addition or policy discovery failed. • Information—The device was added successfully or policy discovery was successful.
State Details	These fields have the same meaning, although different names are used in the Discovery Details and Import Details tables. The fields describe the status of the task for the device: <ul style="list-style-type: none"> • Device Added—The device was successfully added to the inventory. • Device Add Failed—The device was not added to the inventory. • Discovery Completed—Discovery succeeded and the discovered policies are added to the Security Manager database. • Discovery Failed—No policies were discovered because errors occurred.
Discovered From (Discovery Details only)	One of the following: <ul style="list-style-type: none"> • Live Device—Security Manager contacted the device to obtain configuration and policy information. • File—Security Manager obtained the configuration and policy information from a configuration file.

Table D-15 **Policy Discovery Status Page (Continued)**

Messages list	The messages generated during the task for the selected device. Select a message to see detailed information in the fields to the right of the list. The severity icons have these meanings: <ul style="list-style-type: none"> • Error—A problem was detected. • Warning—A minor problem occurred during discovery. • Information—An informational message about the selected device.
Description	Additional information about the message selected in the message list.
Action	The steps you should take to resolve the described problem.

Policy View General Reference

Use Policy view to globally manage all the shared policies configured with Cisco Security Manager. Unlike Device view, which you use to manage all the policies configured on a selected device, Policy view enables you to manage all shared policies of a particular type regardless of device.

Policy view enables you to:

- Create new shared policies.
- Edit any policy configuration.
- Modify the list of devices or VPNs to which shared policies are assigned.
- Delete shared policies that are not assigned to any devices or VPNs.

Navigation Path

Click the **Policy View** button on the toolbar or select **View > Policy View**.

Related Topics

- [Policy Menu General Reference, page D-1](#)

Field Reference

Table D-16 Policy View

Element	Description
Policy Type selector	<p>Lists the policy types available in Security Manager, divided by category. Clicking a policy type in the selector displays all the shared policies defined for that type in the Shared Policy selector. See Policy View—Policy Type Selector, page D-27.</p>
Shared Policy selector	<p>Lists the shared policies that are defined for the selected type. Clicking a policy in the selector displays the definition of that policy on the Details tab of the work area. You can modify the definition as required. Changes affect all devices or VPN topologies to which the policy is assigned.</p> <p>Use the Filter list to filter the list of policies displayed in the selector. For more information about creating filters, see Filtering Items in Selectors, page 3-20.</p> <p>The list of devices or VPN topologies to which the policy is assigned is displayed on the Assignments tab. For more information, see Policy View—Assignments Tab, page D-29.</p>
Work area	<p>Contains two tabs:</p> <ul style="list-style-type: none"> • Details—Use this tab to view and edit the definition of the selected policy. Any changes you make to a policy affect every device or VPN to which the policy is assigned. See Policy View—Policy Type Selector, page D-27. • Assignments—Use this tab to view and edit the list of devices or VPNs to which a shared policy is assigned. See Policy View—Assignments Tab, page D-29. <p>The banner at the top of the work area displays the name of the shared policy, the policy type, and the number of devices or VPNs to which the policy is assigned.</p>

Policy View—Policy Type Selector

The Policy Type selector displayed on the upper-left side of Policy view lists each policy type available in Security Manager, divided by domain. Select a policy type to display a list of shared policies that are defined for that type in the Shared Policy selector.

For more information, see [Policy View Selectors, page 7-41](#).

Related Topics

- [Policy View—Policy Type Selector Options, page D-28](#)
- [Policy View—Shared Policy Selector Options, page D-29](#)
- [Policy View General Reference, page D-25](#)

Field Reference

Table D-17 Policy View—Policy Type Selector

Element	Description
Firewall	Lists all policy types for configuring firewall services. See Chapter 13, “Managing Firewall Services” .
NAT (PIX/ASA/FWSM)	Lists all NAT policies configured on PIX/ASA/FWSM devices. See Configuring NAT Policies on Firewall Devices, page 16-24 .
NAT (Router)	Lists all NAT policies configured on Cisco IOS routers. See NAT on Cisco IOS Routers, page 15-5 .
Site-to-Site VPN	Lists all policy types for configuring site-to-site VPNs. See Chapter 10, “Managing Site-to-Site VPNs” .
Remote Access VPN	Lists all policy types for configuring remote-access VPNs. See Chapter 11, “Managing Remote Access VPNs” .
SSL VPN	Lists all policy types for configuring SSL VPNs. See Chapter 11, “Managing Remote Access VPNs” .
Catalyst Platform	Lists all policy types for configuring Catalyst 6500/7600 devices. See Chapter 17, “Managing Cisco Catalyst Switches and Cisco 7600 Series Routers” .
IPS	Lists all policy types for configuring IPS devices. See Chapter 14, “Managing IPS Services” and Chapter 18, “Managing IPS Devices” .

Table D-17 Policy View—Policy Type Selector (Continued)

IPS (Router)	Lists all policy types for configuring IPS policies on IOS routers. See Chapter 14, “Managing IPS Services” and Chapter 18, “Managing IPS Devices” .
PIX/ASA/FWSM Platform	Lists all policy types for configuring PIX/ASA/FWSM platform-specific policies. See Chapter 18, “Managing IPS Devices” .
Router Interfaces	Lists all policy types for configuring interface-related policies on Cisco IOS Routers. See Chapter 14, “Managing IPS Services” .
Router Platform	Lists all policy types for configuring platform-specific Cisco IOS router policies. See Chapter 14, “Managing IPS Services” .
FlexConfigs	Lists all FlexConfig policies. See Chapter 20, “Managing FlexConfigs” .

Policy View—Policy Type Selector Options

Right-click a policy type in the Policy Type selector (see [Policy View—Policy Type Selector, page D-27](#)) to display a shortcut menu for performing functions on the selected policy type.

For more information, see [Policy View Selectors, page 7-41](#).

Related Topics

- [Policy View—Shared Policy Selector Options, page D-29](#)
- [Policy View General Reference, page D-25](#)

Field Reference

Table D-18 Policy Type Selector Options

Menu Command	Description
New [policy type] Policy	Opens the Create a Policy Dialog Box, page D-30 . Use this dialog box to create a shared policy of the selected type.

Policy View—Shared Policy Selector Options

Right-click a policy in the Shared Policy selector of Policy view to display a shortcut menu for performing functions on the selected policy.

For more information, see [Policy View Selectors, page 7-41](#).

Related Topics

- [Policy View—Policy Type Selector Options, page D-28](#)
- [Policy View General Reference, page D-25](#)

Field Reference

Table D-19 **Shared Policy Selector Options**

Menu Command	Description
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-15 .
Rename Policy	Renames the selected policy. See Rename Policy Dialog Box, page D-15 .
Inherit Rules	Applies only to rule-based policies such as access rules. Causes a rule-based policy to inherit the rules of a different shared policy of the same type. See Inherit Rules Dialog Box, page D-16 .
New [policy type] Policy	Opens the Create a Policy Dialog Box, page D-30 . Use this dialog box to create a shared policy of the selected type.
Delete Policy	Deletes a shared policy from Security Manager. Note You can delete only those policies that are not assigned to any devices or VPNs.

Policy View—Assignments Tab

Use the Assignments tab in Policy view to modify the list of devices or VPNs to which the selected shared policy is assigned. For more information, see [Modifying Policy Assignments in Policy View, page 7-44](#).

Navigation Path

In Policy view, select a policy from the Shared Policy selector, then click the **Assignments** tab in the work area.

Related Topics

- [Shared Policy Assignments Dialog Box, page D-13](#)

Field Reference

Table D-20 **Policy View—Assignments Tab**

Element	Description
Available Devices/VPNs	Lists all existing devices or VPN topologies. To assign the selected policy to additional devices or VPNs, select one or more items from this list, then click >> to add them to the Selected Devices list.
Assigned Devices/VPNs	Lists all devices or VPNs to which the selected policy has been assigned. To remove items from this list, select the item, then click <<. <p>If you unassign a shared, mandatory policy from a VPN (for example, IKE), a default policy is configured automatically in its place. Unassigning a VPN policy that is not mandatory removes the policy completely from the VPN.</p> <p>If you unassign a shared policy from a remote access VPN, an empty policy (that is, a policy instance with no values) is configured in its place, even if it is a mandatory policy, such as IKE. In such cases, you must configure a new policy in order to avoid validation errors during deployment.</p> <p>If you unassign a shared policy from a device, an empty policy is assigned in its place.</p>
Save button	Saves your changes to the server but keeps them private. <p>Note To publish your changes, click the Submit button on the toolbar.</p>

Create a Policy Dialog Box

When working in Policy view, use the Create a Policy dialog box to create a new shared policy of a selected type. The new policy is initially not assigned to any devices or VPN topologies. For more information, see [Creating a New Shared Policy, page 7-43](#).



Note See [Policy View—Assignments Tab, page D-29](#) for information about assigning the new policy.

Navigation Path

In Policy view, do one of the following:

- Right-click a policy type in the Policy Types selector, then select **New [name of policy] Policy**.
- Right-click a policy in the Shared Policy selector, then select **New [name of policy] Policy**.

Related Topics

- [Policy View General Reference, page D-25](#)
- [Policy View—Assignments Tab, page D-29](#)

Field Reference

Table D-21 *Create a Policy Dialog Box*

Element	Description
Policy Name	The name to assign to the new shared policy. Names can contain up to 255 characters, including spaces and special characters.
OK button	Saves your changes locally on the client and closes the dialog box. Note To save your changes to the server so that they are not lost when you log out or close your client, click Save on the source page.

