Managing Policies

The following topics describe the concept of policies in Cisco Security Manager and how to use and manage them.

Understanding 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, security contexts, and virtual sensors) and VPN topologies (which are made up of multiple devices), and then deploying the configurations defined by these policies to these devices.

Several types of policies 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.

The following topics describe policies in more detail:

Settings-Based Policies vs. Rule-Based Policies

Security Manager policies are structured as either rule-based policies or settings-based policies.

Rule-Based Policies

Rule-based policies contain one or more rules that govern how to handle traffic on a selected device, such as the access rules and inspection rules defined as part of a firewall service. Rule-based policies can contain hundreds or even thousands of rules arranged in a table, each defining different values for the same set of parameters. The ordering of the rules is very important, as traffic flows are assigned the first rule whose definition matches the flow (known as first matching).

The structure of the rules table depends on whether you configure a local policy or a shared policy (see Local Policies vs. Shared Policies, page 5-3). If you configure a local rule-based policy for a single device, the policy contains a flat table of local rules. If you configure a shared rule-based policy (either in Device view or Policy view), the table is divided into two sections, Mandatory and Default. Mandatory rules always precede the default rules, and cannot be overridden by local or default rules. The Default section contains rules that can be overridden by mandatory and local rules. You can define rules in either the Mandatory or Default section and move rules between sections using cut-and-paste.

When you define certain types of rule-based policies, such as firewall service policies, you can create a policy hierarchy in which rules located at lower levels in the hierarchy acquire properties from the rules located above them. This is known as rule inheritance. For example, you can define a set of inspection rules that apply globally to all firewalls, while supplementing these rules with additional rules that can be applied to a subset of devices. By maintaining common rules in a parent policy, inheritance enables you to reduce the chance of introducing configuration errors that will cause deployment to fail. For more information, see Understanding Rule Inheritance, page 5-4.

Settings-Based Policies

Settings-based policies contain sets of related parameters that together define one aspect of security or device operation. For example, when you configure a Cisco IOS router, you can define a quality of service (QoS) policy that defines which interfaces are included in the policy, the type of traffic on which QoS is applied, and the definition of how this traffic should be queued and shaped. Unlike rule-based policies, which can contain hundreds of rules containing values for the same set of parameters, you can define only one set of parameters for each settings-based policy defined on a device.

Related Topics

- Understanding Policies, page 5-1

Service Policies vs. Platform-Specific Policies

Security Manager policies are divided into several domains, each of which represents a major policy category. These domains can be divided into two categories: service policies and platform-specific policies.

Service policies are divided into the following policy domains:

- Firewall.
- Site-to-site VPN.
- Remote Access VPN.
- IPS service policies.

For example, the firewall policy domain contains policies for access rules, inspection rules, and transparent rules, among others. The site-to-site VPN policy domain contains policies for IKE proposals, IPsec proposals, and preshared keys, among others. Service policies can be applied to any kind of device, regardless of platform, although there may be some variation in policy definition depending on the device type.

Platform-specific policy domains contain policies that configure features that are specific to the selected platform. Not all platform-specific policies are directly related to security. For example, the Router policy domain contains routing policies, identity policies (Network Admission Control and 802.1x), policies related to device administration (DHCP, SNMP, device access), and other policies such as QoS and NAT.

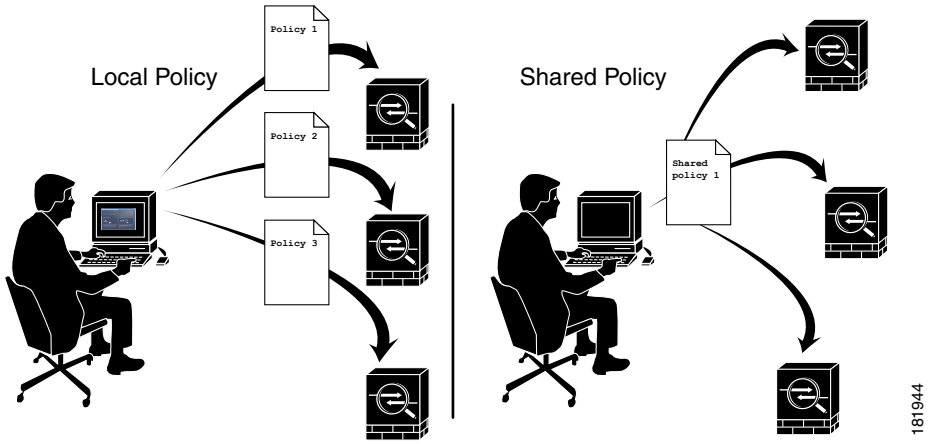
For routers and firewalls (ASA, PIX, FWSM), you can choose which platform-specific policies to manage. For more information, see Customizing Policy Management for Routers and Firewall Devices, page 5-10.

Local Policies vs. Shared Policies

The policies that you configure on devices can either be local or shared. Local policies refer to policies that are defined for a single device. Any changes that you make to a local policy affect only that device. Local policies are well-suited to smaller networks and to devices requiring nonstandard configurations. For example, you might configure a local policy on a router that requires a different OSPF routing policy than the one used by the other routers in your network. For more information about the actions you can perform on local policies, see Performing Basic Policy Management, page 5-30.

As your network grows, maintaining local policies on each device greatly increases the effort required to manage these policies in a comprehensive and efficient manner. To meet this challenge, Security Manager features policy sharing. With policy sharing, you can create a single policy and assign it to multiple devices. For more information, see Sharing a Local Policy, page 5-39.

Figure 5-1 Local vs. Shared Policies



For example, if you want all the Cisco IOS routers in your network to implement the same Network Admission Control (NAC) policy, you need only define a single NAC policy and share it. You can then assign the shared policy to all the routers in your network with a single action. For more information, see Modifying Shared Policy Assignments in Device View or the Site-to-Site VPN Manager, page 5-47.

Any changes that you make to a shared policy are automatically applied to all the devices to which it is assigned. As a result, shared policies both streamline the process of policy creation and help maintain consistency and uniformity in your device configurations.

For more information about the actions you can perform on shared policies, see Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-35.

Tips

- Shared policies can be grouped together to form policy bundles. Policy bundles make managing the assignment of shared policies easier especially when working with a large number of devices. For more information, see Managing Policy Bundles, page 5-54.
- In addition to sharing policies, you can choose to inherit the rules of a rule-based policy when defining another policy of the same type. This makes it possible, for example, to maintain a set of corporate access rules that apply to all firewall devices while providing the flexibility to define additional rules on individual devices as required. For more information, see Understanding Rule Inheritance, page 5-4.
- If you use more than one Security Manager server, you can maintain a consistent set of policies among the servers by regularly exporting shared policies from your master server and importing them into the other servers. You must decide which server to use as the official policy source. For more information, see Exporting Shared Policies, page 10-11 and Importing Policies or Devices, page 10-13

Shared Policies and VPNs

In the same way that shared policies facilitate device configuration, they also facilitate the configuration of VPNs. For example, you can create a shared IPsec proposal policy and assign it to multiple site-to-site VPNs. Any changes that you make to the shared policy affect all the VPNs to which the policy is assigned.

You can assign the shared policies to an existing VPN using the Site-to-Site VPN Manager; right-click a shareable policy and select **Assign Shared Policy**. This is done in much the same way as assigning shared policies in Device view. You can also configure shared policies as the default policies to use in the Create VPN wizard, as described in Understanding and Configuring VPN Default Policies, page 24-12.

Related Topics

- Understanding Policies, page 5-1

Understanding Rule Inheritance

As described in Local Policies vs. Shared Policies, page 5-3, shared policies enable you to configure and assign a common policy definition to multiple devices. Rule inheritance takes this feature one step further by enabling a device to contain the rules defined in a shared policy *in addition to* local rules that are specific to that particular device. Using inheritance, Security Manager can enforce a hierarchy where policies at a lower level (called child policies) inherit the rules of policies defined above them in the hierarchy (called parent policies).

Note If a policy bundle includes a shared policy that inherits from other shared policies, those inherited rules are also applied to any devices on which the policy bundle is applied.

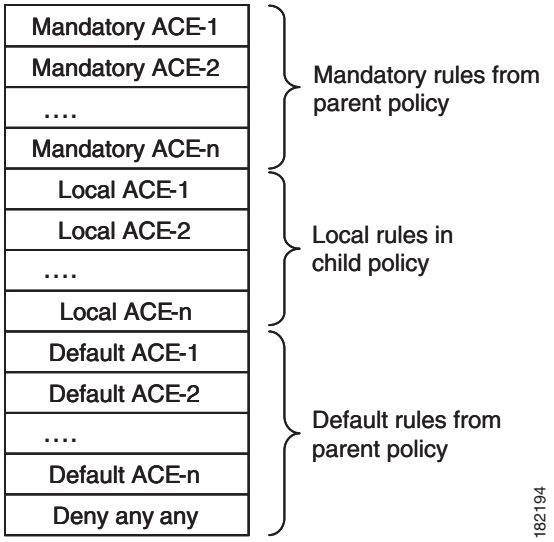
Rule Order When Using Inheritance

As described in Understanding Access Rules, page 16-2, an access list (ACL) consists of rules (also called access control entries or ACEs) arranged in a table. An incoming packet is compared against the first rule in the ACL. If the packet matches the rule, the packet is permitted or denied, depending on the rule. If the packet does not match, the packet is compared against the next rule in the table and so forth, until a matching rule is found and executed.

This first-match system means that the order of rules in the table is of critical importance. When you create a shared access rule policy, Security Manager divides the rules table into multiple sections, Mandatory and Default. The Mandatory section contains rules that cannot be overridden by the local rules defined in a child policy. The Default section contains rules that *can* be overridden by local rules.

Figure 5-2 describes how rules are ordered in the rules table when using inheritance.

Figure 5-2 Order of Rules When Using Inheritance



Benefits of Using Inheritance

The ability to define rule-based policies in a hierarchical manner gives you great flexibility when defining your rule sets, and the hierarchy can extend as many levels as required. For example, you can define an access rule policy for the device at a branch office that inherits rules from a parent policy that determines access at the regional level. This policy, in turn, can inherit rules from a global access rules policy at the top of the hierarchy that sets rules at the corporate level.

In this example, the rules are ordered in the rules table as follows:

```
Mandatory corporate access rules
    Mandatory regional access rules
        Local rules on branch device
    Default regional access rules
Default corporate access rules
```

The policy defined on the branch device is a child of the regional policy and a grandchild of the corporate policy. Structuring inheritance in this manner enables you to define mandatory rules at the corporate level that apply to all devices and that cannot be overridden by rules at a lower level in the hierarchy. At the same time, rule inheritance provides the flexibility to add local rules for specific devices where needed.

Having default rules makes it possible to define a global default rule, such as “deny any any”, that appears at the end of all access rule lists and provides a final measure of security should gaps exist in the mandatory rules and default rules that appear above it in the rules table.

Inheritance Example

For example, you can define a mandatory worm mitigation rule in the corporate access rules policy that mitigates or blocks the worm to all devices with a single entry. Devices configured with the regional access rules policy can inherit the worm mitigation rule from the corporate policy while adding rules that apply at the regional level. For example, you can create a rule that allows FTP traffic to all devices in one region while blocking FTP to devices in all other regions. However, the mandatory rule at the corporate level always appears at the top of the access rules list. Any mandatory rules that you define in a child policy are placed after the mandatory rules defined in the parent policy.

With default rules, the order is reversed—default rules defined in a child policy appear before default rules inherited from the parent policy. Default rules appear after any local rules that are defined on the device, which makes it possible to define a local rule that overrides a default rule. For example, if a regional default rule denies FTP traffic to a list of destinations, you can define a local rule that permits one of those destinations.

IPS Policy Inheritance

Event action filter policies for IPS devices can also use inheritance to add rules defined in a parent policy to the local rules defined on a particular device. The only difference is that although active and inactive rules are displayed together in the Security Manager interface, all inactive rules are deployed last, after the inherited default rules.

Signature policies for IPS devices use a different type of inheritance that can be applied on a per-signature basis. See Configuring Signatures, page 38-4.

Related Topics

- Settings-Based Policies vs. Rule-Based Policies, page 5-2
- Understanding Access Rules, page 16-2
- Understanding Global Access Rules, page 16-3
- Inheritance vs. Assignment, page 5-6
- Inheriting or Uninheriting Rules, page 5-44

Inheritance vs. Assignment

It is important to understand the difference between rule inheritance and policy assignment:

- Inheritance—When you inherit the rules from a selected policy, you do not overwrite the local rules that are already configured on the device. Instead, the inherited rules are *added* to the local rules. If the inherited rules are mandatory rules, they are added before the local rules. If the inherited rules are default rules, they are added *after* the local rules. Any changes that you make to the inherited rules in the parent policy are reflected in the policy that inherits those rules.

  Note Inheritance works differently for IPS signature policies and signature event actions. For more information, see Understanding Signature Inheritance, page 38-3.

- Assignment—When you assign a shared policy to a device, you *replace* whatever was already configured on the device with the selected policy. This holds true whether the device previously had a local policy or a different shared policy of that type.

Therefore, when working with rule-based policies such as access rules, you must use discretion when choosing these options. Use inheritance to supplement the local rules on the device with additional rules from a parent policy. Use assignment to replace the policy on the device with a selected shared policy.

Tip To prevent overwriting your local rules by mistake, Security Manager displays a warning message when you select the Assigned Shared Policy option for a rule-based policy. The message provides you the option of inheriting the rules of the policy instead of assigning it. Choose the inheritance option if you want to preserve your local rules.

Related Topics

- Understanding Rule Inheritance, page 5-4
- Inheriting or Uninheriting Rules, page 5-44
- Local Policies vs. Shared Policies, page 5-3
- Settings-Based Policies vs. Rule-Based Policies, page 5-2

Policy Management and Objects

Objects make it easier to configure policies in Security Manager by providing a set of values with a logical, easy-to-remember name that can be applied wherever it is needed. For example, you can define a network/host object called MyNetwork that contains a set of IP addresses in your network. Whenever you configure a policy requiring these addresses, you can simply refer to the MyNetwork object instead of manually entering the addresses each time.

When you define a policy, you can create objects on the fly by clicking the **Select** button next to any field that accepts an object as a value. For more information, see Selecting Objects for Policies, page 6-2. You can also create and manage objects system-wide from the Policy Object Manager, page 6-4.

Policy objects also are created when you discover policies that already exist on a device. You can discover policies when you add a device to the Security Manager inventory, or you can discover policies on devices that are already in the inventory, as described in Discovering Policies, page 5-12. You can configure Security Manager to reuse already-defined policy objects for newly-discovered policies. For more information on configuring policy object settings for discovery, see Discovery Page, page 11-24.

Certain types of objects enable you to override their predefined values at the device level, which enables you to use an object in a policy while retaining the ability to customize particular values. For more information, see Understanding Policy Object Overrides for Individual Devices, page 6-17.

For more information about objects and how to use them when defining policies, see Chapter 6, "Managing Policy Objects".

Related Topics

- Understanding Policies, page 5-1

Understanding Policy Locking

Security Manager has a policy locking mechanism that is useful in organizations where several people have the authority to make configuration changes. It prevents a potential situation in which two or more people are making changes to the same device, policy, policy assignment, or object at the same time. When a lock is applied, a message is displayed across the top of the work area to other users who access that device or policy.

Tip Security Manager also obtains activity (or configuration session) locks, which are broader in scope than policy locks, when users perform some actions. For more information, see Activities and Locking, page 4-3.

Lock Types

Security Manager uses two different types of locks:

- Policy content locks—Locks the content of a particular policy. The banner displayed above the work area reads:

  This data for this policy is locked by activity/user: <name>.

  The content lock prevents other users from making any changes to the configuration of the locked policy.

- Assignment locks—Locks the assignment of a policy type to a particular device. The banner displayed above the work area reads:

  The assignment of this policy is locked by activity/user: <name>.

  For a local policy, an assignment lock prevents other users from unassigning the policy or assigning a shared policy of the same type in place of the local policy. For a shared policy, an assignment lock prevents other users from assigning a different shared policy of the same type in place of one already assigned.

These locks can either work together or independently of one another, depending on the actions being performed by the user. If both locks are active at the same time, the banner displayed above the work area reads:

This policy is locked by activity/user: <name>.

See Understanding Locking and Policies, page 5-9 for a summary of the effects locking has on the actions you can perform.

Releasing Locks

After is locked is enabled, it remains in place until you either submit your changes (when working in non-Workflow mode) or submit and approve the activity (when working in Workflow mode). If you discard the activity, any locks generated by the activity are also discarded. For more information about workflow modes, see Workflow and Activities Overview, page 1-19.

Keep in mind that:

- Locks are based on the device name, not the IP address of the device. Therefore, we recommend that you avoid defining two devices with different names but the same IP address in Security Manager. Any attempt to deploy to both devices, especially at the same time, leads to unpredictable results.
- In addition, locks do not extend across different operations. For example, locking does not prevent one user from deploying to the same device that is being discovered by a different user.

Additional details about locking can be found in the following sections:

- Understanding Locking and Policies, page 5-9
- Understanding Locking and VPN Topologies, page 5-9
- Understanding Locking and Objects, page 5-10

Understanding Locking and Policies

Table 5-1 on page 5-9 summarizes the effects of policy locks in Security Manager.

Note The ability to modify policies and policy assignments is dependent on the user permissions assigned to the user. See the *Installation Guide for Cisco Security Manager*.

Table 5-1 Locking Summary

If Another User or Activity...	You Cannot...	You Can...
Changes a policy definition	• Modify the policy or assign it to other devices. • Unassign the policy (if it is a local policy)	Unassign the policy from any device (if it is shared).
Changes the definition of a rule-based policy with descendants	• Modify the parent policy or any of the descendants. • Assign the parent policy or any of its descendants to additional devices. • Change the rule inheritance of the parent policy or any of the descendants.	Unassign the policy from any device.
Changes a policy assignment without changing its definition	Modify the policy. **Note** In Policy view, a content lock is placed on the policy. In Device view, an assignment lock is placed on those devices whose assignment is being changed by the other user.	Assign and unassign the policy from other devices.
Changes a policy definition and changes its assignment	Modify the policy or assign it to other devices.	Unassign the policy from any device.

Related Topics

- Understanding Policy Locking, page 5-7
- Understanding Policies, page 5-1

Understanding Locking and VPN Topologies

If you change the device assignment for a VPN topology, or make changes to a specific VPN policy, a lock is placed on the whole VPN topology, and on any other topologies in which the policy is shared. This means that other users cannot make changes to the device assignment, nor can they make changes to any of the VPN policies defined for those VPN topologies.

In order to view and modify site-to-site VPN policies, you must have the required permissions for each device in the VPN topology. You also need permissions to add a device to a VPN topology. If you have different levels of permissions to the devices in the VPN topology, the lowest permission level is applied to the entire topology. For example, if you have read/write permissions to the spokes in a hub-and-spoke topology, but read-only permissions to the device serving as the hub, you are granted read-only permission to the policies and devices in the hub-and-spoke topology. For more information about permissions, see *Installation Guide for Cisco Security Manager*.

Note Unassigning devices from a VPN topology also creates device locks in the VPN topology, which means that these devices cannot be deleted from the inventory. Other users cannot edit the device assignments for the topology until you deploy configurations to all affected devices, including those you remove. The device is not actually removed from the topology until you deploy configurations.

Related Topics

- Understanding Policy Locking, page 5-7
- Chapter 24, "Managing Site-to-Site VPNs: The Basics"

Understanding Locking and Objects

When you create or modify a reusable object, that object is locked to prevent other users from modifying or deleting the same object. Additional rules for object locking include:

- An object lock does not prevent you from modifying the definition or assignment of a policy that uses that object.
- The lock placed on a policy does not prevent you from making changes to an object that is included in the policy definition.
- You can change the definition of any object even if it is part of a policy assigned to a device to which you do *not* have permissions.
- When an object makes use of other objects (such as network/host objects and AAA server group objects), the lock on the object does not prevent another user from modifying those other objects. For example, when you modify a AAA server group object, the lock on that object does not prevent another user from modifying any of the AAA servers that make up the AAA server group.

When an object is locked, users who try to modify that object see a read-only version of the relevant dialog box. When you are working in Workflow mode, a message indicates which activity has locked the object.

Related Topics

- Understanding Policy Locking, page 5-7
- Chapter 6, "Managing Policy Objects"

Customizing Policy Management for Routers and Firewall Devices

When you manage Cisco IOS routers or ASA, PIX, or FWSM firewall devices, you have the option of selecting which policy types to manage with Security Manager and which policy types to leave unmanaged. Managing a policy type means that Security Manager controls the configuration of the policy and considers the information that it stores in its database about that policy to be the desired configuration. Security Manager does not configure unmanaged policy types, nor does it track

configurations of these types that were configured using other methods. For example, if you decide not to manage SNMP policies, any SNMP configurations that you configured using CLI commands are unknown to Security Manager.

Caution If you use AUS or CNS to deploy configurations to ASA or PIX devices, be aware that the device downloads a full configuration from AUS or CNS. Thus, reducing the policies managed by Security Manager actually removes the configurations from the device. If you intend to deselect some ASA/PIX policies for management to use other applications along with Security Manager to configure devices, do not use AUS or CNS.

The ability to customize policy management on routers and firewalls makes it possible, for example, to use Security Manager to manage DHCP and NAT policies while leaving routing protocol policies, such as EIGRP and RIP, unmanaged. These settings, which can be modified only by a user with administrative permissions, affect all Security Manager users.

Unmanaged policies are removed from both Device view and Policy view. Any existing policies of that type, local or shared, are removed from the Security Manager database.

To customize policy management for routers and firewalls, select **Tools > Security Manager Administration > Policy Management** to open the Policy Management Page, page 11-59. The policy types are organized in folders, with router and firewall (which includes all ASA, PIX, and FWSM devices) handled separately. Select or deselect policy types as desired and click **Save**. Subsequent processing depends on whether you are changing a policy type to be managed or unmanaged:

- **Unmanaging a policy type**—If you unmanage a policy type, and any device of that type has that policy configured, you must unassign the policies before unmanaging them. Security Manager displays a list of all devices that have assigned policies of that type, including the policy name, device name, and the user or activity that has a lock on the policy. If you click **Yes** to continue unmanaging the policy, Security Manager obtains the required locks, unassigns the policies, and then unmanages the policy type.

  If a lock could not be obtained for even one device, no policies are unassigned, the policy type is not unmanaged, and you are told of the problem. You can then either manually unassign the policies from the affected devices, or release the user or activity locks, and try again to unmanage the policy type.

  Note Unmanaging a policy has no effect on the active configuration running on the device; Security Manager does not remove the configuration from the device. Instead, unmanaging the policy removes it from the database, and Security Manager no longer considers that part of the device configuration.

- **Managing a previously-unmanaged policy type**—If you start managing a policy type that you previously did not manage using Security Manager, it is possible that the active configuration on the device has commands controlled by the newly-managed policy type. **It is therefore important that you rediscover policies on all devices of that type (either all routers or all ASA, PIX, FWSM devices)**. This ensures that Security Manager has the current configuration for these policies.

  If you do not rediscover policies and leave the newly-managed policies unconfigured, on the next deployment to the device, the existing settings configured on the device are removed. For more information on discovering policies on devices already managed, see Discovering Policies on Devices Already in Security Manager, page 5-15.

Note Features that are unmanaged by Security Manager can still be modified manually with CLI commands or FlexConfigs. For more information about FlexConfigs, see Chapter 7, "Managing FlexConfigs".

Discovering Policies

Policy discovery enables you to bring your existing network configuration into Security Manager to be managed. Policy discovery can be performed by importing the configuration of a live device or by importing a configuration file. If you import a configuration file, the file must have been generated by the device (for example, by using the **show run** command on Cisco IOS Software devices); you cannot discover configuration files in any other format.

You can initiate policy discovery when you add a device by selecting the relevant options in the New Device wizard. For more information, see Adding Devices to the Device Inventory, page 3-6.

You can also initiate policy discovery on existing devices from Device view. For more information, see Discovering Policies on Devices Already in Security Manager, page 5-15.

When you initiate policy discovery on a device, the system analyzes the configuration on the device and then translates this configuration into Security Manager policies and policy objects so that the device can be managed. Warnings are displayed if the imported configuration completes only a partial policy definition. If additional settings are required, you must go to the relevant page in the Security Manager interface to complete the policy definition. Warnings and errors are also displayed if the imported configuration is invalid.

After performing policy discovery, you must submit your changes (or approve your activity when working in Workflow mode) to have the information included in change reports and to make the information available to other users. If you make any changes to the discovered policies, you must deploy the changes to the device for them to take effect. For more information, see Chapter 8, "Managing Deployment".

Tip Use the Security Manager Administration window to configure discovery-related settings that apply to all devices. For more information, see Discovery Page, page 11-24.

Policy Discovery and VPNs

In addition to performing discovery on individual devices, Security Manager allows you to discover the VPNs that are already deployed in your network. How you discover VPNs depends on the type of VPN being discovered:

- Site-to-Site VPNs—A wizard walks you through the discovery procedure step by step. For more information, see Site-To-Site VPN Discovery, page 24-19.

Tip We recommend that you deploy to a file immediately after discovering a Site-to-Site VPN. This enables Security Manager to assume full management of the relevant CLI commands that are configured on the device.

- IPSec and SSL Remote Access VPNs—You can discover IPSec and SSL VPNs when you discover policies on the device, either when you add the device to the inventory or if you discover policies on a device already in the inventory. Policies related to these VPNs are treated as regular device policies. However, when selecting discovery options, you must specifically select to discover RA VPN policies. For more information about remote access VPN policy discovery, see Discovering

Remote Access VPN Policies, page 29-12. For more information about performing policy discovery, see Adding Devices to the Device Inventory, page 3-6 and Discovering Policies on Devices Already in Security Manager, page 5-15.

Note If you add a device using a configuration file, and discover security policies while adding the device, Security Manager cannot successfully discover policies that require that files be downloaded from the discovered device. This especially affects devices that include the **svc image** command in an SSL VPN configuration. Because Security Manager does not have the referenced file in its database, the **no** form of the command is generated for the discovered configuration.

Policy Discovery and Cisco IOS Routers and Catalyst Devices

Security Manager supports a subset of the complete list of commands available in the Cisco IOS software, mostly centered on security-related commands. You can discover all supported Cisco IOS commands. Commands that are not supported are left in place unless they conflict directly with a policy configured in Security Manager. For more information about performing policy discovery on Cisco IOS routers, see Discovering Router Policies, page 58-3. For more information about performing policy discovery on Catalyst devices, see Discovering Policies on Cisco Catalyst Switches and Cisco 7600 Series Routers, page 65-1.

Tip We recommend that you deploy to a file immediately after discovering a Cisco IOS router or Catalyst device. This enables Security Manager to assume full management of the relevant CLI commands that are configured on the device.

Policy Discovery and Firewall Security Contents

When you add a device that has security contexts, you should discover all contexts and policies at the same time; otherwise, you will have to discover policies for each context separately. When you add the device, select **MULTI** for Context and do not select Security Context of Unmanaged Device. (If you select this option, only the admin context is imported, and it has no relationship to other security contexts on the device; select this option only if you want to manage the security context independently from the parent device.) Depending on how you add the device, you might need to select the option to discover security contexts. During discovery, Security Manager identifies each security context and adds it as a separate device to the device list, appending the security context name to the end of the parent's name; for example, if the parent is pix_141, the admin context would be pix_141_admin. (You can control the naming convention for security contexts; for more information, see Discovery Page, page 11-24). You can create new security contexts, or delete existing contexts, as well as create and delete policies for those contexts.

If you create multiple security contexts on FWSM, which are contained in Catalyst 6500 devices, and you are running IOS software on the chassis, add the chassis device using the SSH credentials for the chassis. Then Security Manager can identify each FWSM on the chassis, and give you the option to add each of them. During FWSM discovery, Security Manager discovers the security contexts for each FWSM, including the policies for the FWSM and for each context. However, if you are using the Catalyst OS on the device, you must discover each FWSM individually.

For more information about adding devices to the inventory, see Adding Devices to the Device Inventory, page 3-6.

Policy Discovery and IPS Devices

When you discover policies on an IPS device, the virtual sensors defined on the device are also discovered along with the policies defined for the virtual sensors. If more than one virtual sensor uses the same policy, that policy is created as a shared policy and is assigned to the virtual sensors. Policies defined for a single virtual sensor, or only for the parent device, are created as local policies. You cannot discover policies just for an individual virtual sensor; you can discover policies only on the parent device. If policies are discovered on the parent device that are not assigned to any virtual sensors, those policies are created as shared policies that are not assigned to any device or virtual sensor.

After discovering an IPS device that contains virtual sensors, you must submit your changes to the database for the virtual sensors to appear in the device selector.

Policy Discovery and Object Groups

When you perform policy discovery, any object groups already configured on PIX, ASA, FWSM, and IOS 12.4(20)T+ devices are brought into Security Manager as policy objects. For more information about how Security Manager policy objects are translated into object groups and vice-versa, see How Policy Objects are Provisioned as Object Groups, page 6-92.

In addition, **object network** and **object service** configurations on ASA 8.3+ devices are brought into Security Manager as host, network, or address range network/host objects, or service objects (as opposed to service group objects). The only exception is that address range objects that have the same address for the start and end range are instead created as host network/host objects.

Note For IOS devices, any objects discovered that are used by access control lists that are discovered as ACL objects are subsequently replaced during deployment by the contents of the object. Object groups used with ACL objects are not preserved, although they are discovered as Security Manager policy objects.

Policy Discovery and Security Manager Policy Objects

When you perform policy discovery, Security Manager tries to reuse the policy objects that you have already created in Security Manager. Based on the contents of the device configuration, the following are the possible actions:

- Named policy objects in the configuration—Existing policy objects are reused if their content matches the configuration on the device.

  If the contents of the named policy object does not match, the policy object is reused and a device-level override is created if **Allow Device Override for Discovered Policy Objects** is selected on the Discovery administration page. For more information, see these topics:

  - Understanding Policy Object Overrides for Individual Devices, page 6-17
  - Discovery Page, page 11-24
- Unnamed policy objects in the configuration—Existing policy objects are used if their content matches the configuration on the device. You can control this behavior by changing the value of the **Reuse Policy Objects for Inline Values** setting on the Discovery administration page.
- You can discover objects that have the same definition as existing objects, regardless of the setting you have defined for detecting redundant objects. For more information about this setting, see Policy Objects Page, page 11-61.

For more information on policy objects, see Chapter 6, “Managing Policy Objects”.

Policy Discovery and Access Control Lists

Certain policies in Security Manager support only standard or only extended ACLs, even if both types are supported by the CLI. In such cases, policy discovery works as follows:

- If the Security Manager policy supports only extended ACLs (for example, firewall service policies), any standard ACLs configured on the device for that policy are imported as extended ACLs.
- If the Security Manager policy supports only standard ACLs (for example, SNMP traps on IOS routers), any extended ACLs configured on the device for that policy are imported as standard ACLs.

During the discovery process, Security Manager will show any inactive ACLs that are imported as disabled. If you later deploy these disabled ACLs, they are removed from the device configuration.

Related Topics

- Frequently Asked Questions about Policy Discovery, page 5-26
- Viewing Policy Discovery Task Status, page 5-21
- Understanding Policy Object Overrides for Individual Devices, page 6-17

Discovering Policies on Devices Already in Security Manager

When you add a device to the inventory, you can discover policies at the same time that you add the device. However, you can skip policy discovery and do it later, or rediscover policies after adding the device.

You might initiate policy discovery on existing devices when:

- You discover out-of-band changes in the network, for example, changes to device configurations using CLI commands. In such a situation, you can rediscover existing policies on the device to make sure that the Security Manager database has the most current information. However, we recommend that you enter out-of-band changes in Security Manager rather than perform rediscovery.
- You want to discover a subset of policies (for example, platform-specific settings) that was not discovered when you first added the device to Security Manager.
- You want to import the factory-default configuration of a firewall device. For more information, see Default Firewall Configurations, page 45-2.

Caution If you perform policy discovery on a device *after* configuring policies in Security Manager but before you deploy your changes, the discovered policies overwrite the undeployed changes. For example, if you select the option to discover platform-specific settings, the discovered configuration overwrites any platform-specific undeployed policies you configured in Security Manager. This is true even if the discovered configuration does not include the specific platform policy you configured. For example, discovering platform-specific settings overwrites any routing policies that you have configured for the device in Security Manager, even if the configuration you discover does not contain any routing information. Another result of rediscovery is that any shared policies that were configured on the device are replaced by the local policies that are discovered.

Caution Under certain conditions, Security Manager may fail to discover ASA interfaces in system context. Specifically, if a rediscovery/deployment is done on the system context of a multiple context ASA without checking (selecting) "inventory," then Security Manager may fail to discover the interfaces on other security contexts. This can potentially result in Security Manager altering or altogether deleting interface configurations of other contexts in a subsequent deployment. To avoid this problem, simply be sure to select "inventory" when doing a rediscovery of the system context.

Before You Begin

Ensure that no one is configuring policies on the device or deploying configurations to the device. If you rediscover policies on a device while a deployment job is deploying configurations to the device, you might not be able to see the deployed changes after the rediscovery. Use the Deployment Manager to determine if there are active jobs that include the device before you rediscover policies (select **Manage > Deployments**). If you inadvertently rediscover policies during a deployment job, wait until the deployment job is completed and then discover policies again to ensure that Security Manager is synchronized with the device.

Related Topics

- Viewing Policy Discovery Task Status, page 5-21
- Discovering Policies, page 5-12
- Frequently Asked Questions about Policy Discovery, page 5-26
- Understanding Policies, page 5-1
- Managing Policies in Device View and the Site-to-Site VPN Manager, page 5-29
- Managing Shared Policies in Policy View, page 5-48

Step 1 Decide whether you need to discover policies on a single device or if you want to discover policies on more than one device at a time. Policy discovery options vary based on how you start the discovery process.

- **Single device discovery**—If you need to discover policies related to any of the following, you can do it using only single-device discovery. (Note that single-device discovery is the type of discovery performed when you add a device to the inventory.)
  - Security context configurations for ASA, PIX, and FWSM devices running in multiple context mode.
  - Virtual sensor configurations for IPS devices.
  - Service module information for Catalyst devices.
  - Policy discovery from a configuration file.
  - Policy discovery from the factory default configuration.
- **Bulk rediscovery**—If you need to discover policies for more than one device, you can perform bulk rediscovery. However, bulk rediscovery can be performed only on live devices (that is, devices currently running and accessible in your network), and you cannot discover security context, virtual sensor, or Catalyst service module configurations. (You can discover service modules if you select them directly instead of selecting the device that contains them.)

Step 2 **If you want to perform single-device discovery**, do the following:

a. In device view or map view, ensure that only one device is selected, then right-click and select **Discover Policies on Device**. This opens the Create Discovery Task dialog box.

   Tip: If the dialog box is called Bulk Rediscovery, you need to close the dialog box and try again. Ensure that only a single device is selected and reissue the command. You must use the right-click menu; it is the only way to perform single-device discovery.

b. Modify the discovery task name, if desired, and select the following discovery options. For detailed information, see Create Discovery Task and Bulk Rediscovery Dialog Boxes, page 5-18.

   - **Discover From**—Whether you are discovering from a live device (which is active and accessible in the network), a configuration file (click **Browse** to select the file on the Security Manager server), or factory default configuration (for ASA, PIX, and FWSM devices running

an OS version for which a factory default configuration exists). You can discover the default configuration only for devices that run in single-context mode or for individual security contexts.

Tip: We recommend that you use the Factory Default Configuration settings when you add PIX, ASA, and FWSM devices manually (as described in Adding Devices by Manual Definition, page 3-25). You should discover the default configuration for single-context mode devices and for each security context on a multiple-context mode device. For more information about factory-default policies, see Default Firewall Configurations, page 45-2.

- **Discover Policies for Security Contexts**—Select this option for firewall devices running in multiple-context mode if you want to discover policies for the security contexts defined on them.

c. Select the types of policies you want to discover. For more information about the difference between different types of policies, see Service Policies vs. Platform-Specific Policies, page 5-2.

- Detect ASA-CX Module—Determines if a CX module is installed; see Detecting ASA CX Modules, page 69-21 for more information. Available only with certain ASA 8.4.1+ devices; not displayed here in the Bulk Rediscovery dialog box.
- Inventory—Discovers basic device information (such as hostname and domain name), interfaces, and security contexts on 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—Discovers platform-specific policies, such as routing policies.
- Firewall Services—Discovers firewall services policies, such as access rules and inspection rules, on all platforms.
- NAT Policies—Discovers network address translation (NAT) policies, such as address pools, static translation rules, and dynamic NAT/PAT. Discovery of NAT policies is supported on ASA, ASA-SM, PIX and FWSM devices.
- RA VPN Policies—Discovers IPSec and SSL remote access VPN policies, such as IKE proposals and IPsec proposals.
- IPS—Discovers IPS policies, such as signatures and virtual sensors.

d. Click **OK**. The discovery task is initiated and the Discovery Status dialog box opens so you can view the task status (see Discovery Status Dialog Box, page 5-22). You cannot perform other tasks in Security Manager while discovery is in progress.

Step 3 **If you want to perform bulk rediscovery**, do the following:

a. In device view, do one of the following:

- Select a device group, or multiple devices, then right-click and select **Discover Policies on Device**. Ensure that the Bulk Rediscovery dialog box opens.

Tip: If the dialog box is called Create Discovery Task, you need to close the dialog box and try again. Ensure that a device group or more than one device is selected and reissue the command.

- Select **Policy > Discover Policies on Device**. This opens the Device Selector dialog box. Select the devices you want to discover from the Available Devices list and click **>>** to move them to the Selected Devices list. Click **Next**.

Note If you use the right-click command, Security Manager assumes you have selected the desired devices. You can always click the **Back** button to go to the Device Selector screen and change the device list.

b. Modify the discovery task name, if desired, and select discovery options. For detailed information, see Create Discovery Task and Bulk Rediscovery Dialog Boxes, page 5-18.

   The devices are organized in groups according to device type, with your device groups (if any) shown within each type:

   - To change options for all devices of a given type, select the device type folder and modify the Discover Device Settings options. If the Discover drop-down list shows Multiple Values, then there are different discovery options selected for devices of that type. If you change the value, it changes for all devices. The check boxes for the policy types (explained above for single-device discovery) are available only if you select Policies and Inventory. Only options available for all devices in the selected group are shown, so you might need to select individual devices separately to select the most appropriate set of options.
   - To change options for a single device, click the + icons next to folders to open them until you find the device, select the device, and then select the discovery options.

c. Click **Finish**. The discovery task is initiated and the Discovery Status dialog box opens so you can view the task status (see Discovery Status Dialog Box, page 5-22). You cannot perform other tasks in Security Manager while discovery is in progress.

Create Discovery Task and Bulk Rediscovery Dialog Boxes

Use the Create Discovery Task dialog box to have Security Manager discover the policies for a device that is already in the device inventory. Use the Bulk Rediscovery dialog box to discover policies on more than one device at a time. Your options for policy discover differ based on which dialog box you use. For detailed information on the procedure, including how to get to each of these dialog boxes, see Discovering Policies on Devices Already in Security Manager, page 5-15.

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 3-6.

Navigation Path

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

- Select **Policy > Discover Policies on Device** to perform bulk rediscovery.
- Right-click the device in the Device selector and select **Discover Policies on Device**. If a single device is selected, you get the Create Discovery Task dialog box. Otherwise, you are performing bulk rediscovery.

Tip You can also right click a device in Map view and select **Discover Policies on Device**.

Related Topics

- Discovering Policies, page 5-12
- Viewing Policy Discovery Task Status, page 5-21
- Selecting or Specifying a File or Directory in Security Manager, page 1-49
- Discovery Status Dialog Box, page 5-22

Field Reference

Table 5-2 Create Discovery Task 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 desired.
Selected Devices table (Bulk rediscovery only)	The devices you selected for rediscovery. The devices are organized in groups according to device type, with your device groups (if any) shown within each type: • To change options for all devices of a given type, select the device type folder and modify the Discover Device Settings options. If the Discover drop-down list shows Multiple Values, then there are different discovery options selected for devices of that type. If you change the value, it changes for all devices. The check boxes for the policy types (explained above for single-device discovery) are available only if you select Policies and Inventory. Only options available for all devices in the selected group are shown, so you might need to select individual devices separately to select the most appropriate set of options. • To change options for a single device, click the + icons next to folders to open them until you find the device, select the device, and then select the discovery options. **Tip**: To change which devices are selected for rediscovery, click **Back** to go to the Device Selector dialog box.
Discover From Config. File (Not available for bulk rediscovery)	The source of policy information to be discovered: • 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. 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 3-20. • 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 (shown in the Config File edit box). This option is available only if Security Manager has a default configuration for the OS version running on an ASA, PIX, or FWSM device. You can discover the default configuration only for devices that run in single-context mode or for individual security contexts. For more information, see Default Firewall Configurations, page 45-2.

Table 5-2 Create Discovery Task Dialog Box (Continued)

Element	Description
Discover Policies for Security Contexts (Not available for bulk rediscovery)	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. When deselected, Security Manager treats the entire device as having a single set of policies configured in single-context mode. For more information about security contexts, see Chapter 57, "Configuring Security Contexts on Firewall Devices".

Table 5-2 Create Discovery Task Dialog Box (Continued)

Element	Description
Policies to Discover (for single-device discovery) Discover Device Settings (for bulk rediscovery)	The policy types to discover on the selected device. **Note** For bulk rediscovery, from the Discover drop-down menu, choose **Policies and Inventory** to enable the following options, **Inventory Only** to discover the inventory without discovering other policy types, or **Detect ASA-CX Module** to determine if a CX module is installed without discovering other policies. If the drop-down list has **Multiple Values** selected, this means that the devices in the selected group have different discovery options selected. If you change the selection, your change applies to all the devices in the group. The discovery options are: • Detect ASA-CX Module—Determines if a CX module is installed; see Detecting ASA CX Modules, page 69-21 for more information. Available only with certain ASA 8.4.1+ devices; not displayed here in the Bulk Rediscovery dialog box. • 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. • Firewall Services—Includes all firewall service policies. For more information, see Chapter 12, "Introduction to Firewall Services". • NAT Policies—Includes all network address translation (NAT) policies that are configured on the selected device, such as address pools, static translation rules, and dynamic NAT/PAT. Discovery of NAT policies is supported on ASA, ASA-SM, PIX and FWSM devices. For more information, see Chapter 23, "Configuring Network Address Translation". • RA VPN Policies—Includes all IPSec and SSL remote access VPN policies that are configured on the selected device. This option is disabled if the device does not support remote access VPN configuration. For more information, see Chapter 29, "Managing Remote Access VPNs: The Basics". • IPS Policies—Includes all IPS policies that are configured on the selected device. For more information, see Overview of IPS Configuration, page 35-5 or Overview of Cisco IOS IPS Configuration, page 44-3.

Viewing Policy Discovery Task Status

When you initiate policy discovery a discovery task is created. For each policy discovery initiation, only one task is created regardless of the number of devices being discovered.

You can view the status of the current policy discovery task in the Discovery Status dialog box, which opens automatically when the task is initiated. This dialog box provides updated status information about the discovery task, including summary information about the task and details about each device being discovered.

You can abort a discovery task, if required. When you perform policy discovery on a single device, aborting the task results in partial discovery. In such cases, we recommend deleting the information and starting again. When you perform policy discovery on multiple devices, any devices for which discovery was completed before you aborted the operation are fully discovered. Security Manager automatically discards the information for any partially discovered device.

The Discovery Status dialog box also displays the appropriate warning and error messages if any problems are encountered during the discovery process. For example, if the CLI commands in a configuration file do not define a complete Security Manager policy, a warning message is displayed that you must complete the policy definition in the relevant Security Manager policy page.

For more information, see Discovery Status Dialog Box, page 5-22.

To view information about previous discovery tasks, select **Manage > Policy Discovery Status** to open the Policy Discovery Status window. Select the discovery task in the top pane of the window, and the results of the task are displayed in the lower panes. For more information about using the Policy Discovery Status window, see Policy Discovery Status Page, page 5-24.

Related Topics

- Discovering Policies on Devices Already in Security Manager, page 5-15
- Frequently Asked Questions about Policy Discovery, page 5-26
- Discovering Policies, page 5-12

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 Discovering Policies on Devices Already in Security Manager, page 5-15.

Related Topics

- Viewing Policy Discovery Task Status, page 5-21
- Discovering Policies, page 5-12
- Adding Devices from the Network, page 3-11
- Adding Devices from Configuration Files, page 3-20
- Adding Devices from an Inventory File, page 3-29

Field Reference

Table 5-3 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.
Discovery Details table	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: • 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: – 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.
Action	The steps you should take to resolve the described problem.

Table 5-3 Discovery Status Dialog Box (Continued)

Element	Description
Generate Report button	Click this button to create a discovery status report for this job. The report is a PDF file, saved to your client system, that includes a summary of the job. You can use this report for your own purposes or to aid in troubleshooting a problem with Cisco TAC. For more information, see Generating Deployment or Discovery Status Reports, page 10-28.
Abort button	Aborts the discovery task. 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. 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.

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 **Manage > Policy Discovery Status**.

Related Topics

- Viewing Policy Discovery Task Status, page 5-21

Field Reference

Table 5-4 Policy Discovery Status Page

Element	Description
Task Table 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. When adding devices that contain security contexts, the context discovery appears as a separate Policy Discovery task.	
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.

Table 5-4 Policy Discovery Status Page (Continued)

Element	Description
End Time	The time the task stopped.
Status	The overall status of the task. One of the following: • 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 polices were discovered or no device was added because of errors or because you stopped discovery.
Generate Report button	Click this button to create a discovery status report for the selected job. The report is a PDF file, saved to your client system, that includes a summary of the job. You can use this report for your own purposes or to aid in troubleshooting a problem with Cisco TAC. For more information, see Generating Deployment or Discovery Status Reports, page 10-28.
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.
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: • 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: • Error—The device addition or policy discovery failed. • Information—The device was added successfully or policy discovery was successful.

Table 5-4 Policy Discovery Status Page (Continued)

Element	Description
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: • 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 polices were discovered because errors occurred.
Discovered From (Discovery Details only)	One of the following: • 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.
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: • 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.

Frequently Asked Questions about Policy Discovery

These questions and answers describe how policy discovery processes your device configurations into Security Manager policies.

Question: How does policy discovery work?

Answer: After you select the device whose policies, settings, and interfaces (inventory) you want to discover, Security Manager obtains the running configuration (from live devices) or the supplied configuration (when discovering from configuration files) and translates the CLI into Security Manager policies and objects. The imported configuration is added to the Configuration Archive as the initial configuration for the device. After discovery, you can review the discovered policies and objects and decide whether to commit them to the database. If you dislike them, you can discard them instead. Please note that commit and discard affect all discovered devices as a group and cannot be implemented on a per-device basis.

Question: When should I discover policies?

Answer: Typically, you should discover policies when you add devices to Security Manager. However, if you are creating devices in Security Manager (instead of importing live devices or configuration files), you must perform policy discovery after adding the device. You should also perform policy discovery in order to synchronize Security Manager with any out-of-band changes that have been made to the device, for example through the CLI.

Question: How can I determine the results of the discovery?

Answer: When you initiate a discovery task, a window opens that shows you the discovery status and results. You can also view a history of discovery task results on the Policy Discovery Status page (select **Manage > Policy Discovery Status**).

Question: Does Security Manager show which commands are not discovered, and what can I do about them?

Answer: In the discovery status window, go to the Message Summary section, then select **Commands Not Discovered**. Any undiscovered commands are listed in the Description field. You can either remove the command from the device and repeat the discovery process, or continue. If you continue, Security Manager will remove the unsupported command in the next deployment.

If Security Manager does not support a command found on a device, the discovery is generally not aborted; however, if the device has any access control entries (ACEs) that refer to unsupported object groups, the discovery is aborted. Other error messages, such as **User groups not supported**, might also provide details about undiscovered commands. Read the information in the Action box for suggestions.

Question: How are discovered policies reflected in the user interface?

Answer: Security Manager converts the device commands into policies. There is no difference in appearance between a policy discovered from a device configuration and one defined directly in Security Manager.

Question: I am using Auto Update Server for my PIX or ASA devices. How do I discover policies?

Answer: If a device has a static IP address, you can discover policies from the device. If it has a dynamic IP address, you must discover policies from the device's configuration file (offline).

Question: I am using Cisco Secure ACS to manage authentication and authorization to Security Manager. How does this affect policy discovery?

Answer: You must add all managed devices to Cisco Secure ACS before you can perform policy discovery and manage these devices in Security Manager. This includes security contexts on PIX/ASA/FWSM devices. For more information, see the *Installation Guide for Cisco Security Manager*.

Question: What should I do after discovering VPN or router platform policies?

Answer: Due to the way these features are discovered, Security Manager does not assume management of discovered VPN and router platform policies until after it deploys them. This means that if you discover a router, unassign one of its policies and deploy, no commands are removed from the router's configuration. We recommend, therefore, that you perform deployment to a file immediately after discovering VPN or router platform policies, *before* you make any changes to those policies. After this initial deployment, you can reconfigure these policies and deploy your changes as required.

Question: If I discover policies on a device and then deploy the policies from Security Manager without changing them, what is the difference between the original configuration on the device and the one that exists after the deployment?

Answer: Typically, there will be no differences between the new configuration and your original one, assuming you set up FlexConfigs for any unsupported CLI commands. However, in certain cases minor changes might occur in your ACL or object-group naming schemes. For more information, see How Policy Objects are Provisioned as Object Groups, page 6-92. In addition, any discovered objects that are not being used by a policy are removed from the configuration. There can also be instances where the new configuration is functionally equivalent to the old one but does not use the same commands.

Question: How does Security Manager handle my current CLI naming schemes for ACLs and object groups?

Answer: When you discover policies from a device, Security Manager tries to use the same names you have used. However, depending on your naming scheme, some minor differences might occur between what you defined on your device and the policies created through discovery. Additionally, there is a possibility that a naming conflict can occur between an existing ACL or object on the device and the name required for the new policy or object; in this case, Security Manager generates a different name so as not to misconfigure the device. For example, if the name of a discovered object conflicts with an object of the same type that already exists in Security Manager, a suffix is added to the name of the new object to make it unique or a device-level override is created.

Question: Are all configuration commands discovered and brought into Security Manager?

Answer: No. Security Manager does not discover all device configuration commands. Instead, it discovers security policies. For any configuration commands not discovered, use the FlexConfig feature to include the commands that Security Manager does not support.

Question: If I rediscover policies on a device already in Security Manager, what happens to the policies assigned to the device?

Answer: If you rediscover policies on a device that you are already managing with Security Manager, the newly discovered policies replace the ones assigned to the device. All policies within the selected policy domain (firewall services, platform settings, or both) are replaced, not just the ones that are different on the device compared to the ones in the Security Manager database. If you assigned shared policies to the device, the assignment is removed and the shared policy is left unchanged (so that other devices that use the shared policy are not affected). After policy discovery, all policies assigned to the device are specific to that device; none of them are shared with other devices. If you want to use shared policies with the device, you must redo the assignments after policy discovery.

In addition, any customizations done to local policies are also lost. For example, if you used sections to organize rules-based firewall policies, the sections are removed and the rediscovered policy is a flat list of entries.

Question: Does Security Manager use existing policies and objects during policy discovery?

Answer: During policy discovery, Security Manager uses existing policy objects (ones that you already defined in Security Manager) when creating policies for the device. However, Security Manager does not reuse existing policies; all policies created during discovery are local to the device being discovered. Thus, you might find it beneficial to define your policy objects (such as network objects) before adding devices to Security Manager.

Question: After adding a device and discovering policies, I cannot submit my changes to the database; instead I get warnings such as “Connection Policies Not Set.” What must I do to complete the device addition?

Answer: When you add a device and discover policies (particularly when you add devices from configuration files), Security Manager warns you if the resulting configuration is incomplete in ways that will prevent it from successfully managing the device. Connection policies, for example, are simply the device credentials (user names and passwords) required to log into the device, as well as other connection-related configuration settings (such as HTTP settings). Because these missing settings result in an invalid configuration or prevent Security Manager from contacting and managing the device later, you are prevented from submitting the changes to the database. Ensure that you have complete and valid configurations for these settings, then resubmit your changes to the database.

Question: Why does the AAA policy not show the AAA configuration that I discovered on the device?

Answer: The AAA policy contains the default configurations for authentication, authorization, and accounting. Other AAA commands that specify a particular list name are mapped to the policies that reference them. If the list name is not referenced by a policy, it is not discovered.

Question: Why are parts of the AAA method list definitions configured on my router not discovered?

Answer: Security Manager does not support certain keywords, such as if-needed. Method lists containing these keywords are discovered without the keyword. If the default AAA definitions on the device contain unsupported keywords, the entire command is not discovered.

Question: Can I discover AAA servers on devices running IOS software that were configured using the server-private command?

Answer: Yes, you can discover these servers. However, Security Manager converts them into standard AAA servers that can be used globally or in multiple AAA server groups. The server-private command is not supported.

Question: What do I need to know about discovery and device hostnames?

Answer: When you discover a device, the hostname policy is populated with the hostname discovered on the device. However, the hostname listed in Device Properties is not updated with this value. Ensure that the hostname defined in the device properties is the correct DNS name for the device. For more information, see Understanding Device Properties, page 3-6.

Managing Policies in Device View and the Site-to-Site VPN Manager

You can use Device view or the Site-to-Site VPN Manager to manage both local policies and shared policies, as described in the following sections:

To access Device view, select **View > Device View** or click the **Device View** button on the toolbar. To access the Site-to-Site VPN Manager, select **Manage > Site-to-Site VPNs** or click the **Site-to-Site VPN Manager** button on the toolbar.

Related Topics

- Understanding the Device View, page 3-1
- Managing Shared Policies in Policy View, page 5-48
- Understanding Policies, page 5-1

Policy Status Icons

You can learn the status of any policy in Security Manager at a glance by viewing the icon displayed next to the policy name.

Table 5-5 Policy Status Icons

Icon	Status
	The policy is not configured. Upon deployment, any policy of this type already present on the device is effectively removed.

Table 5-5 Policy Status Icons (Continued)

Icon	Status
	A local policy is configured. The definition of this policy affects only the device or VPN topology on which it is configured.
	A shared policy is configured. Any changes to the definition of this policy affect all of the devices or VPN topologies to which this policy is assigned.
	A policy bundle is configured. Any changes to the definition of this policy affect all of the devices or VPN topologies to which this policy is assigned, whether those policies are assigned using the same policy bundle, another policy bundle that includes the shared policy, or are assigned the shared policy directly and not through a policy bundle.

Related Topics

- Understanding Policies, page 5-1

Performing Basic Policy Management

The following topics describe the operations you can perform on local policies in Device view. Local policies are policies that are specific to the device or VPN topology on which they are configured. They are not shared by other network elements.

- Configuring Local Policies in Device View, page 5-30
- Copying Policies Between Devices, page 5-32
- Unassigning a Policy, page 5-34. (This topic also applies to the Site-to-Site VPN Manager.)

Related Topics

- Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-35
- Managing Shared Policies in Policy View, page 5-48
- Understanding Policies, page 5-1

Configuring Local Policies in Device View

Use Device view to configure local platform and service policies on individual devices. Each policy defines a particular configuration or security task that the device can perform, such as NAT, OSPF routing or inspection rules. Local policies are unnamed and are particular to the individual device on which they have been defined. Any changes that you make to a local policy do not affect other devices that Security Manager is managing.

When you configure a policy, a lock is placed on that policy to prevent other users from making changes to the same policy at the same time. See Understanding Policy Locking, page 5-7.

You can modify any local policy assigned to a particular device provided you have permissions to modify policies and to access that device. For more information about permissions, see the *Installation Guide for Cisco Security Manager*.

After configuring a policy, you must deploy the changes to the device in order to make them active on that device. For more information, see Chapter 8, "Managing Deployment"

Related Topics

- Understanding the Device View, page 3-1
- Managing Policies in Device View and the Site-to-Site VPN Manager, page 5-29
- Copying Policies Between Devices, page 5-32
- Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-35

Step 1 In Device view, select a device from the Device selector, then select a policy for that device from the Device Policies selector. The details of the policy appear in the work area.

Step 2 Modify the definition of the policy as required. Click the Help button to access information specific to the selected policy. For more information, see:

- Chapter 24, "Managing Site-to-Site VPNs: The Basics"
- Chapter 29, "Managing Remote Access VPNs: The Basics"
- Chapter 12, "Introduction to Firewall Services"
- Overview of IPS Configuration, page 35-5
- Overview of Cisco IOS IPS Configuration, page 44-3
- Chapter 58, "Managing Routers"
- Chapter 45, "Managing Firewall Devices"
- Chapter 65, "Managing Cisco Catalyst Switches and Cisco 7600 Series Routers"

Step 3 Click **Save** to save your changes.

If this is the first time you are configuring this policy on this particular device, the icon next to the selected policy changes to indicate that the policy is configured and assigned locally to the device. For more information about policy status icons, see Policy Status Icons, page 5-29.

After you save the policy, the policy is configured but you are the only one who can view the changes. There are additional steps to take to commit your changes and to deploy them to the device. The exact changes depend on whether you are working in Workflow or non-Workflow mode. Before taking the additional steps, configure all of the policies that you want to deploy; you are not required to deploy policy changes one at a time.

Following is a summary of the additional steps you need to take:

- Submit your changes. Submission updates the database on the Security Manager server with your changes.
  - In non-Workflow mode, you submit changes by selecting **File > Submit**. You can also submit your changes and deploy them in a single step by selecting **File > Submit and Deploy**.
  - In Workflow mode, if you are working with an activity approver, you submit your activity, and the changes are committed when the activity is approved. If you are not working with an activity approver, your changes are committed when you approve your own activity. For more information, see Submitting an Activity for Approval (Workflow Mode with Activity Approver), page 4-20 and Approving or Rejecting an Activity (Workflow Mode), page 4-21.

  In both Workflow and non-Workflow mode, policies are validated when you submit them. For more information on validation, see Validating an Activity/Ticket, page 4-18.
- Deploy your changes. Deployment either updates the devices directly with the new configuration, creates configuration files that you can deploy yourself, or copies the configuration files to an intermediate server (Auto Update Server, Configuration Engine, or Token Management Server) from which the device retrieves the updates. The method you use depends on the requirements of

your organization, and you can select different methods for each device. For general information about deployment, see Working with Deployment and the Configuration Archive, page 8-26. For the specific steps based on workflow mode, and information on the deployment methods, see the following topics:

- Deploying Configurations in Non-Workflow Mode, page 8-29
- Deploying Configurations in Workflow Mode, page 8-35
- Deploying Configurations Using an Auto Update Server or CNS Configuration Engine, page 8-42
- Deploying Configurations to a Token Management Server, page 8-43
- Deploying Directly to a Device, page 8-9
- Deploying to a Device through an Intermediate Server, page 8-10
- Deploying to a File, page 8-11

Copying Policies Between Devices

You can streamline device configuration by copying multiple policies, or even a complete set of policies, from one device to other devices that support the selected policies. This makes it easy, for example, to quickly configure a new firewall device with the same policies configured on an existing firewall device.

When you copy policies between devices, those policies that are local on the source device are copied locally to the target device. Shared policies assigned to the source device are copied as shared policies to the target device as well.

Tips

- If your intention is to assign a single shared policy to additional devices, we recommend that you use the assignment feature, rather than copying the policies. For more information about sharing policies in Device view, see Modifying Shared Policy Assignments in Device View or the Site-to-Site VPN Manager, page 5-47.
- To create a new device of the same type that shares the same configuration and properties (including the operating system version, credentials, and grouping attributes) as the source device, use the Clone Device feature. For more information, see Cloning a Device, page 3-54.

Related Topics

- Managing Policies in Device View and the Site-to-Site VPN Manager, page 5-29
- Configuring Local Policies in Device View, page 5-30
- Understanding the Device View, page 3-1
- Policy Status Icons, page 5-29
- Filtering Items in Selectors, page 1-44

Step 1 In Device view, do one of the following:

- Select **Policy > Copy Policies Between Devices**. The Copy Policies wizard starts at step 1, the Copy Policies from this Device page. Select the device that has the policies you want to copy and click **Next**.

- Right-click the device in the Device selector, then select **Copy Policies Between Devices**. The Copy Policies wizard selects the device as the source device and starts at step 2, the Select Policies to Copy page. You can change the source device by clicking **Back**.

Tip You can also right click a device in Map view and select **Copy Policies Between Devices**.

Step 2 Select the policies you want to copy on the Select Policies to Copy page. Initially, most policies from the source device (both local and shared) that can be copied are selected. You can change the selection, however, if you select a policy that depends on another policy, you must select the dependant policies. Security Manager will prompt you if your selections are not valid.

Consider the following when selecting policies:

- Selecting the check box for a policy group selects all of the policies in that group.
- When you copy policies between firewall devices (ASA, PIX, 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. Other types of policies that you should carefully consider before copying them include NAT, routing, or the IPS policy on IOS devices.
- 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.

Step 3 Use the policy object copy options to determine how policy objects are handled. These options are not mutually exclusive, and the combination you select has important implications on how the policies are defined on the target devices.

These are the possible combinations and their meanings:

- To ensure that the target devices have the same policy object settings as the source device, select both **Copy the Global Values of Policy Objects** and **Copy the Overridden Values of Policy Objects**.
- To ensure that if a policy object is used on the target device, its value is not overridden, 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).
- To ensure that any policy objects on the target device use the policy object's global values, 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.
- To ensure that only policy objects with local values on the source device are copied to the target device, 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.

Click **Next**.

Step 4 Select the target devices to which you want to copy policies on the Copy Policies to these Devices page. Selecting the check box for a device group selects all of the devices in that group.

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.

The device list is empty if no other device in the inventory can support all selected policies.

Tip After selecting devices, Click the **Preview** 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.

Step 5 Click **Finish**. You are asked to confirm that you want to copy policies.

The policies are copied to the target devices. If the copy operation fails for any target device, the copy is undone for successful devices, and you are shown a list of reasons why the copy failed for each problem device. Typically, copy failures are because someone else has a lock on a policy or device, or you do not have the required permissions to a device.

Unassigning a Policy

If you unassign a policy that has already been deployed to a device, in most cases the values that are defined for the policy are erased, effectively removing the policy from the device's planned configuration. When you perform deployment, the configuration for this feature that already exists on the device is removed.

The exact behavior depends on the type of policy that you unassign:

- Firewall service policies—If you unassign a policy, Security Manager erases the policy from the device.
- VPN policies:
  - Site-to-site VPN policies—You cannot unassign mandatory site-to-site VPN policies from the devices in the topology. If you unshare a mandatory policy, Security Manager assigns default values to the affected device. If you unassign an optional policy, Security Manager erases the configuration from the device. For more information, see Understanding Mandatory and Optional Policies for Site-to-Site VPNs, page 24-6.
  - IPSec remote access VPN policies—If you unassign a policy, Security Manager erases the policy from the device, even if it is a mandatory policy. In most cases, deployment fails if you do not create a new definition for the mandatory policy. In those cases where deployment does not fail, the device will fail to establish VPN tunnels.
  - SSL VPN policies—If you unassign a policy, Security Manager erases the policy from the device.
- Catalyst 6500/7600 or Catalyst switch policies—Interface and VLAN policies cannot be shared or unassigned. If you unassign a platform policy (such as IDSM settings or VLAN access lists) Security Manager removes the policy from the device.
- IPS policies—For all IPS device and service policies, a default policy is assigned to the device.
- PIX/ASA/FWSM policies—Policies that you cannot share with other devices cannot be unassigned from the device on which they are created. This includes interface, failover, security context, and resource policies. For other policy types (such as timeout policies), Security Manager makes a best effort to restore the system default configuration on the device.

- IOS router policies—Core connectivity policies, such as basic interface settings and accounts and credentials policies cannot be unassigned from the device on which they are created. If you unassign a device access policy that was used to define the password for configuring the device, you might prevent Security Manager from configuring that device in the future. For more information, see User Accounts and Device Credentials on Cisco IOS Routers, page 60-13.

  If you unassign a VTY or console policy, Security Manager restores a default configuration to ensure continued communication with the device. For all other policy types, if you unassign the policy, Security Manager erases the configuration from the device.

Related Topics

- Configuring Local Policies in Device View, page 5-30
- Copying Policies Between Devices, page 5-32
- Managing Policies in Device View and the Site-to-Site VPN Manager, page 5-29

Step 1 Do one of the following:

- (Device view) Select the device that has a policy you want to unassign.
- (Site-to-Site VPN Manager) Select the VPN topology that has a policy you want to unassign.

Step 2 Right-click the local policy and select **Unassign Policy**.

You are asked to confirm that you want to unassign the current policy.

Working with Shared Policies in Device View or the Site-to-Site VPN Manager

Sharing policies makes it possible to configure multiple devices with common policies, which provides greater consistency in your policy definitions and streamlines your management efforts. Any changes to a shared policy affect all the devices and VPN topologies to which the policy is assigned. This makes it easy, for example, to update all of your Cisco IOS routers with new quality of service policies by updating the shared Quality of Service policy assigned to these devices.

When working in Device view or the Site-to-Site VPN Manager, you can take a local policy (such as a policy created during device discovery) and share it. You can then assign the shared policy to as many devices or VPN topologies as you want (provided they are not locked by another user; see Understanding Policy Locking, page 5-7), and you can change these assignments at any time. You can also take these shared policies that were created from the local policy and add them to a policy bundle. For more information on policy bundles, see Managing Policy Bundles, page 5-54.

Tip If you have a device that you are using as a template for the creation of other devices, you can quickly create a policy bundle that can be used for device configuration based on the template device. To do so, first make all policies on the device shared policies (see Sharing Multiple Policies of a Selected Device, page 5-40), then create a policy bundle from those shared policies.

In addition, you can take a shared policy that is assigned to a device or VPN topology and turn it into a local policy for that particular device or topology. This enables you to create a special configuration that affects only that device or topology. Other devices or topologies assigned the shared policy continue to use the shared policy as before.

As an alternative to sharing local policies, you can create new shared policies and manage them at the network level using Policy view. For more information, see Managing Shared Policies in Policy View, page 5-48. After creating the shared policy and assigning it to devices or VPN topologies in Policy view, you can return to Device view or the Site-to-Site VPN Manager and perform additional operations on the policy as described in the sections that follow. Note that all shared policies that you create in Device view or the Site-to-Site VPN Manager automatically appear as shared policies in Policy view.

Tip In Device view or the Site-to-Site VPN Manager, if you edit a shared policy, your changes are applied to all devices or VPN topologies that share the policy. Thus, you do not need to go to Policy view to edit shared policies. You are warned when you try to edit a shared policy that this will happen, to ensure you do not inadvertently make a change to more devices or topologies than what you intend. If you need to change the policy for just one device or topology, you can unshare the policy before editing it, as described in Unsharing a Policy, page 5-41.

The following topics describe how to share policies and the operations that can be performed on them in Device view or the Site-to-Site VPN Manager:

Related Topics

- Importing Policies or Devices, page 10-13
- Understanding Policies, page 5-1
- Managing Policies in Device View and the Site-to-Site VPN Manager, page 5-29

Using the Policy Banner

When you view a device policy in Device view, or a site-to-site VPN policy in the Site-to-Site VPN Manager, there is a banner above the content of the policy in the work area. The banner provides information about whether the policy is local to the device or a shared policy. For shared policies, the banner also indicates the number of devices that use the policy. For policies that allow inheritance, the banner includes information about inheritance.

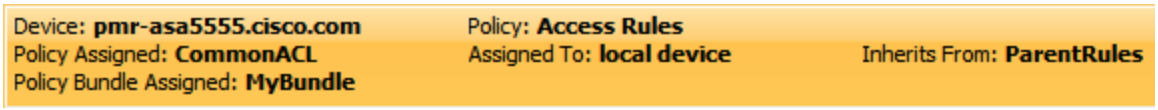
Messages might appear below the banner to indicate the following:

- That the policy is locked by another user. You cannot save changes to the policy until the other user submits (and approves) the changes, cancels an edit, or discards the changes.

- That the shared policy was imported. Imported policies might be re-imported at some point if the policy is managed on a different server. Any changes that you make are eliminated if the policy is imported again. Before editing the policy, ensure that you understand the protocols used in your organization for policy management and importation. You can control whether this message appears using an option on the Tools > Security Manager Administration > Policy Management page (see Policy Management Page, page 11-59).

You can use the links in the banner to create shared policies, assign a shared policy, and configure policy inheritance. The following illustration shows an example of a device policy banner.

Figure 5-3 Policy Banner Example



The fields in the policy banner have the following meanings and uses:

- Policy Assigned—The name of the policy assigned to this device or VPN. If the name has a link, you can assign a shared policy to the element by clicking the link. If there is no link, a shared policy cannot be assigned to this particular type of policy.
  - Local—The policy is a local policy (configured on this device only) rather than a shared policy.
  - Specific policy name—The shared policy is assigned to the device policy.
- Assigned To—If a shared policy is assigned, the number of devices or VPNs to which the policy is assigned. If no shared policy is assigned, **local device** or **this VPN** is indicated. If the name has a link, you can do the following:
  - Local Device or This VPN links—Click the link to create a shared policy from this local policy. You can then assign the shared policy to other devices or VPNs.
  - Number of Devices or VPNs links—Click the link to change the devices or VPNs assigned to the shared policy.
- Inherits From—The name of the policy from which this policy inherits rules. This field appears only for policies that allow inheritance. Click the link to specify a policy or set of policies from which the policy will inherit rules. For more information about inheritance, see Understanding Rule Inheritance, page 5-4.

  The field can contain these entries:
  - None—The policy does not inherit rules from any other policy.
  - Single policy name—The policy inherits rules from this policy.
  - Multiple policy names separated by > signs—The policy inherits rules from the indicated hierarchy of policies.
- Policy Bundle Assigned—The name of the policy bundle assigned to this device or VPN.

Related Topics

- Understanding Policies, page 5-1
- Managing Policies in Device View and the Site-to-Site VPN Manager, page 5-29
- Sharing a Local Policy, page 5-39
- Assigning a Shared Policy to a Device or VPN Topology, page 5-42
- Adding Local Rules to a Shared Policy, page 5-43

- Modifying Shared Policy Definitions in Device View or the Site-to-Site VPN Manager, page 5-46
- Modifying Shared Policy Assignments in Device View or the Site-to-Site VPN Manager, page 5-47
- Inheritance vs. Assignment, page 5-6
- Understanding Policy Locking, page 5-7
- Importing Policies or Devices, page 10-13

Policy Shortcut Menu Commands in Device View and the Site-to-Site VPN Manager

When you right-click a policy in Device view or the Site-to-Site VPN manager, you get a list of commands that you can use on the policy. The shortcut command list includes only those commands available for the selected policy, so the list differs according to your selection.

The available commands depend on whether the policy:

- Is unassigned.
- Contains a local policy for that specific device or VPN topology.
- Contains a shared policy that might be assigned to multiple devices or VPN topologies.
- Can be shared. There are no shortcut commands for policies that cannot be shared between devices or topologies.

The current status of each policy type is indicated by the icon displayed next to the policy name. See Policy Status Icons, page 5-29.

The following table provides a comprehensive list of the possible commands.

Table 5-6 Policy Shortcut Commands

Menu Command	Description
Commands available for both local and shared policies	
Assign Shared Policy	Assigns an existing shared policy to the selected device or VPN topology. If the policy is already assigned a shared policy, your selection assigns a new shared policy, replacing the existing selection. See Assigning a Shared Policy to a Device or VPN Topology, page 5-42.
Inherit Rules	Enables you to identify a shared policy from which to inherit rules, or to remove any inheritance from the child policy. Child policies inherit both the mandatory rules and default rules that are defined in the parent policy. See Inheriting or Uninheriting Rules, page 5-44.
Additional local policy commands	
Share Policy	Shares the local policy so that it can be assigned to other devices or VPN topologies. See Sharing a Local Policy, page 5-39.
Unassign Policy	Unassigns the policy from the device or VPN topology. When deployed, the configuration that corresponds to the settings defined in this policy is removed from the device or the devices in the topology. See Unassigning a Policy, page 5-34.
Additional shared policy commands	
Unshare Policy	Creates a local copy of the shared policy and assigns it to the device or VPN topology in place of the shared policy. See Unsharing a Policy, page 5-41.

Table 5-6 Policy Shortcut Commands (Continued)

Edit Policy Assignments	Enables you to change which devices or VPN topologies are assigned to this policy, not just the device or VPN topology you are currently viewing. See Modifying Shared Policy Assignments in Device View or the Site-to-Site VPN Manager, page 5-47.
Clone Policy	Creates a copy of a policy with a new name. Use this option to create a new policy with the same definition as the policy from which it was created, which you can then edit. See Cloning (Copying) a Shared Policy, page 5-45.
Rename Policy	Renames the selected policy. See Renaming a Shared Policy, page 5-46.

Sharing a Local Policy

As your network grows, you might decide to convert a local policy into a shared policy that you can assign to multiple devices or VPN topologies (see Local Policies vs. Shared Policies, page 5-3). Sharing a policy provides a streamlined management approach that ensures that all devices or topologies assigned to the policy are configured in a consistent manner. For example, if you configure a set of firewall inspection rules on a particular device, sharing that device's inspection rules policy makes it possible to assign that policy to other devices, eliminating the need to configure each device individually. See Assigning a Shared Policy to a Device or VPN Topology, page 5-42.

In addition, having a shared policy enables you to update the configurations of each assigned device or topology at one time, saving time and promoting greater consistency across your set of managed devices.

When you share a policy, you must name the policy. (Local policies do not have names, because they are associated with only a single device or topology.) This enables you to identify this policy when managing shared policies in Policy view.

Related Topics

- Understanding the Device View, page 3-1
- Policy Status Icons, page 5-29
- Using the Policy Banner, page 5-36
- Assigning a Shared Policy to a Device or VPN Topology, page 5-42
- Unsharing a Policy, page 5-41
- Adding Local Rules to a Shared Policy, page 5-43
- Sharing Multiple Policies of a Selected Device, page 5-40
- Inheriting or Uninheriting Rules, page 5-44
- Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-35

Step 1 In Device view or the Site-to-Site VPN Manager, select a policy from the Policies selector, then do one of the following:

- (Device view only) Select **Policy > Share Policy**.
- Right-click the policy and select **Share Policy**.
- Click the **local device/this VPN** link in the Assigned To field in the policy banner. A warning dialog box called Local Policies Cannot Be Assigned to Multiple Devices opens to inform you that you are viewing a local policy. Click **Share Policy** to continue.

The Share Policy dialog box is displayed.

Step 2 Enter a name for the shared policy and click **OK**.

Policy names can contain up to 255 characters, including spaces and special characters.

Sharing Multiple Policies of a Selected Device

With one procedure, you can share multiple policies configured on a particular device. When you perform this procedure, you can choose to share all the policies configured on the device or only some of them. For example, you can take all the firewall service policies defined on an ASA device and share them.

Initially, the resulting shared policies are assigned only to the device from which the procedure was performed. However, you can then assign these shared policies to additional devices as required. See Modifying Shared Policy Assignments in Device View or the Site-to-Site VPN Manager, page 5-47.

This feature provides a convenient way to take the policies configured on a single device and use them as a template for configuring similar devices. For example, after you discover the devices at your branch offices, you can take all the local access rules that you have configured on a similar device and share them with a single procedure so that you can assign them to the branch office devices.

Tip You can use this procedure to make all policies on the device shared policies and then create a policy bundle from those shared policies. This policy bundle can then be used to quickly configure new devices based on the template device.

Tip To create a new device of the same type that shares the same configuration and properties (including device operating system version, credentials, and grouping attributes) as the source device, create a clone of the device. For more information, see Cloning a Device, page 3-54.

Related Topics

- Understanding the Device View, page 3-1
- Copying Policies Between Devices, page 5-32
- Sharing a Local Policy, page 5-39
- Unsharing a Policy, page 5-41
- Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-35
- Filtering Items in Selectors, page 1-44

Step 1 In Device view, do one of the following:

- Select **Policy > Share Device Policies**. The Share Policies wizard opens at the Share Policies from this Device page (step 1). Select the device whose policies you want to share and click **Next**.
- Right-click the device and select **Share Device Policies**. The Share Policies wizard opens at the Select Policies to Share page (step 2); you can click **Back** to go to step 1 and select a different device, if desired.

Tip You can also right click a device in Map view and select **Share Device Policies**.

Step 2 On the Select Policies to Share page, select all policies that you want to share. Initially, all shareable policies configured on the device, whether local or shared, are selected. Deselect the check box next to each policy that you do not want to share.

Following are some tips:

- Local policies that are not checked remain local to the selected device.
- 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.
- Selecting the check box for a policy group selects all of the policies in that group.
- If a policy is configured on the device, but you cannot select it (the check box is solid grey), it is an unshareable policy.

Step 3 Enter a name for the shared policies. All policies are given the same name. You can later rename the individual policies. For more information, see Renaming a Shared Policy, page 5-46.

If you select a policy that is already shared, Security Manager creates a copy of that policy using this name.

Step 4 Click **Finish**. The selected policies become shared policies, which you can then assign to additional devices as needed. For more information, see Modifying Shared Policy Assignments in Device View or the Site-to-Site VPN Manager, page 5-47.

Unsharing a Policy

When you unshare a shared policy assigned to a particular device or VPN topology, you create a copy that becomes a local policy for that device or topology. This means that any subsequent changes made to the local policy affect only this particular device or topology. Other devices or topologies assigned the original shared policy continue to use the shared policy as before.

Note You cannot unshare a policy that is assigned to a device as part of a policy bundle. You must either unassign the policy bundle from the device or remove the shared policy from the policy bundle that is assigned to the device.

For example, Security Manager might be managing a BGP routing policy called MyBGP, which is assigned to 20 routers. If you decide that one of the routers (Router1) requires a variation of this policy, you can select the device, unshare the policy, and make the changes you need for that router. From that point on, Router1 has a local BGP policy while the other 19 routers continue to use the original shared policy, MyBGP.

Related Topics

- Understanding the Device View, page 3-1
- Sharing a Local Policy, page 5-39
- Managing Policies in Device View and the Site-to-Site VPN Manager, page 5-29
- Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-35
- Policy Status Icons, page 5-29

Step 1 In Device view or the Site-to-Site VPN Manager, select a policy from the Policies selector, then do one of the following:

- (Device view only) Select **Policy > Unshare Policy**.
- Right-click the selected shared policy, then select **Unshare Policy**.

Step 2 Click **OK**. The shared policy is converted into a local policy for the selected device or VPN topology. The shared policy icon in the Policies selector is replaced by the local policy icon.

Assigning a Shared Policy to a Device or VPN Topology

You can replace any shareable policy (local or shared) assigned in Device view or the Site-to-Site VPN Manager with an existing shared policy of the same type. For example, if you have a local NAT policy assigned to a Cisco IOS router, you can assign a shared NAT policy in its place. Similarly, if a shared NAT policy was assigned to the router, you can replace it with a different shared NAT policy.

Tip You can use bundle shared policies together to make assigning those policies easier. For more information, see Managing Policy Bundles, page 5-54.

If you are assigning a shared policy to replace a local, rule-based policy (for example, an inspection rules policy), any local rules that you configured are replaced by the rules defined in the shared policy. A warning message gives you the opportunity to preserve the local rules by inheriting the rules of the shared policy instead of assigning the shared policy in place of the local policy. For more information, see Inheritance vs. Assignment, page 5-6.

Tip If you want to use the rules defined in the shared policy and still keep your local rules, we recommend that you select the Inherit Rules option instead of assigning the policy. For more information, see Inheriting or Uninheriting Rules, page 5-44.

Note You can also inherit IPS signature policies and signature event actions, but inheritance works differently than for rules-based policies. For more information, see Understanding Signature Inheritance, page 38-3.

Related Topics

- Understanding the Device View, page 3-1
- Using the Policy Banner, page 5-36
- Unassigning a Policy, page 5-34
- Adding Local Rules to a Shared Policy, page 5-43
- Copying Policies Between Devices, page 5-32
- Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-35

Step 1 In Device view or the Site-to-Site VPN Manager, select a policy from the Policies selector, then do one of the following:

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

The Assign Shared Policy dialog box is displayed if there are any shared policies available for assignment.

Step 2 Select a shared policy from the displayed list to assign to the device or VPN topology and click **OK**. If the policy does not allow inheritance, the shared policy is assigned to the selected device and you are finished.

Step 3 If the policy allows inheritance, you are warned that the shared policy will replace the current policy and given the option to inherit the rules instead with the Local Policy Will Be Replaced dialog box.

Your options are:

- Assign Policy—Assign the shared policy to replace the existing local policy. If you choose to assign, all local rules are removed and they cannot be retrieved.
- Inherit From Policy—Inherit the rules of the shared policy. If you choose to inherit, the inherited rules are added to the local rules that are already defined in the device's local policy. Use inheritance instead of assignment when the device needs to maintain the set of local rules already defined for it.

Tip You can select **Do not show this again** to save your selection and have it applied to all future times that you assign rule-based policies. Otherwise, you are prompted each time you assign policies so that you can make different selections based on the circumstances. If you select this option, you can turn it off by resetting it on the Customize Desktop administration settings page (see Customize Desktop Page, page 11-9).

Adding Local Rules to a Shared Policy

After you assign a shared rule-based policy, such as access rules, to a device, you can define additional rules in the policy that are local to that device. Selecting this option creates an inheritance relationship, where the policy defined on the device inherits rules from the shared policy while adding rules that affect only this particular device. For more information about inheritance, see Understanding Rule Inheritance, page 5-4.

Local rules that you add to a device do not affect the shared policy from which the device inherits its remaining rules. For example, if the shared policy Access_Rules_South is assigned to five devices and you define local rules on one of those devices, the access rules policy on that device consists of the rules defined in Access_Rules_South plus the local rules; the other four devices continue to use only the rules defined Access_Rules_South.

Before You Begin

Assign a shared, rule-based policy to the device as described in Assigning a Shared Policy to a Device or VPN Topology, page 5-42.

Related Topics

- Understanding the Device View, page 3-1
- Cloning (Copying) a Shared Policy, page 5-45
- Assigning a Shared Policy to a Device or VPN Topology, page 5-42

- Unsharing a Policy, page 5-41
- Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-35

Step 1 In Device view, select a device from the Device selector, then select a shared policy assigned to that device from the Device Policies selector. You must select a rule-based policy, such as access rules. The details of the policy appear in the work area.

Step 2 Do one of the following:

- Select **Policy > Add Local Rules**.
- Right-click the policy, then select **Add Local Rules**.

A message is displayed indicating that the policy on this device is now defined as a child policy that inherits rules from the shared policy. If the shared policy in turn inherits rules from a different shared policy, those rules are automatically inherited as well.

Note To change the parent policy from which this policy inherits rules, see Inheriting or Uninheriting Rules, page 5-44.

Step 3 Click **OK** to confirm. In the work area, headings are added for local mandatory and default rules in addition to the mandatory and default rules inherited from the shared policy.

In the Device Policies selector, the status icon changes to the icon for a local policy. For more information, see Policy Status Icons, page 5-29.

Step 4 Define local rules as required.

Tip If you assign a shared policy after adding local rules, both the inherited rules and your local rules are replaced with the selected shared policy.

Inheriting or Uninheriting Rules

This procedure describes how certain types of rule-based policies, such as access rules, can inherit rules from shared policies of the same type. Child policies inherit both the mandatory rules and default rules that are defined in the parent policy.

When working in Device view, you can then define additional rules that are local to the selected device. For more information, see Adding Local Rules to a Shared Policy, page 5-43.

You can edit rule inheritance from either Device view or Policy view.

Related Topics

- Understanding the Device View, page 3-1
- Managing Shared Policies in Policy View, page 5-48
- Assigning a Shared Policy to a Device or VPN Topology, page 5-42
- Understanding Rule Inheritance, page 5-4
- Inheritance vs. Assignment, page 5-6
- Understanding Policies, page 5-1

- Using the Policy Banner, page 5-36

Step 1 Select a local or 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**.
- (Device view only) Click the link in the Inherits From field in the policy banner.

The Inherit Rules dialog box is displayed, containing a list of all shared policies of the selected type, including any inheritance relationships among them.

Step 2 Select the policy from which to inherit rules, or select **No Inheritance** to remove any inheritance from the child policy. The name of the parent policy is displayed below the selector.

For example, if you select an access rules policy called West Coast, your access policy inherits the rules of the West Coast policy. If the West Coast policy is a child policy of another access rules policy called US, your policy inherits the properties of the West Coast policy, which in turn inherits the properties of the US policy.

Step 3 Click **OK** to save your definitions. The work area displays the inherited rules under the name of the parent policy and any local rules, if defined, under the name of the original shared policy.

Cloning (Copying) a Shared Policy

You can clone an existing shared policy. This provides a useful shortcut for creating a new policy that is similar to an existing one; after creating the clone, you can modify it as required.

If you clone a rule-based policy with inheritance, the new policy contains the same inheritance properties as the policy from which it was created. For more information, see Understanding Rule Inheritance, page 5-4.

Tip If you clone a policy in Device view or the Site-to-Site VPN Manager, the new policy is assigned to the selected device or VPN topology. If you want to clone a policy without changing policy assignments, make the clone in Policy view.

Related Topics

- Understanding the Device View, page 3-1
- Managing Shared Policies in Policy View, page 5-48
- Renaming a Shared Policy, page 5-46
- Deleting a Shared Policy, page 5-54

Step 1 Select a shared policy in Device view, Policy view, or the Site-to-Site VPN Manager, then do one of the following:

- (Device or Policy view only) Select **Policy > Clone Policy**.
- Right-click the shared policy, then select **Clone Policy**.

The Clone Policy dialog box is displayed.

Step 2 Enter a name for the new policy and click **OK**.

Names can contain up to 255 characters, including spaces and special characters.

Renaming a Shared Policy

You can rename a shared policy. The new name is immediately reflected in all devices and VPN topologies to which the policy is assigned.

Related Topics

- Understanding the Device View, page 3-1
- Managing Shared Policies in Policy View, page 5-48
- Cloning (Copying) a Shared Policy, page 5-45
- Deleting a Shared Policy, page 5-54

Step 1 Select a shared policy in Device view, Policy view, or the Site-to-Site VPN Manager, then do one of the following:

- (Device or Policy view) Select **Policy > Rename Policy**.
- Right-click the policy, then select **Rename Policy**.

The Rename Policy dialog box is displayed.

Step 2 Enter a new name for the selected policy and click **OK**.

Names can contain up to 255 characters, including spaces and special characters.

Modifying Shared Policy Definitions in Device View or the Site-to-Site VPN Manager

You can modify any shared policy in Device view or the Site-to-Site VPN Manager by selecting one of the devices or VPN topologies to which the policy is assigned, making the necessary changes, and then saving these changes to the Security Manager server. Any changes made to a shared policy in Device view or the Site-to-Site VPN Manager automatically affect all devices to which the shared policy is assigned.

Tip To apply your changes only to the device or VPN topology that you are modifying, you must first unshare the policy (see Unsharing a Policy, page 5-41). This action converts the policy to a local policy and prevents your changes from affecting other devices or topologies.

Related Topics

- Understanding the Device View, page 3-1
- Using the Policy Banner, page 5-36
- Modifying Shared Policy Assignments in Device View or the Site-to-Site VPN Manager, page 5-47
- Configuring Local Policies in Device View, page 5-30
- Managing Policies in Device View and the Site-to-Site VPN Manager, page 5-29

Step 1 Do one of the following:

- (Device view) Select the device that has a shared policy you want to modify.
- (Site-to-Site VPN Manager) Select the VPN topology that has a shared policy you want to modify.

Step 2 Redefine the policy as required.

Step 3 Click **Save**. You are asked to confirm that you want to save your changes, reminding you that the changes you made will be applied to all devices or topologies to which the policy is assigned.

Modifying Shared Policy Assignments in Device View or the Site-to-Site VPN Manager

You can modify the list of devices or VPN topologies assigned a particular shared policy as required. If you remove a device or topology from a policy assignment, that policy is effectively removed from the device's or topology's planned configuration. Upon deployment, any configuration of that type that exists on the device or topology is removed. For more information about the implications of unassigning a policy, see Unassigning a Policy, page 5-34.

Caution Use the policy assignment feature with care, as unassigning a policy removes that configuration from the device or topology and can have unintended consequences. For example, if you unassign a device access policy from a Cisco IOS router and then deploy that change, you might prevent Security Manager from configuring that device in the future (see User Accounts and Device Credentials on Cisco IOS Routers, page 60-13).

Policy assignment can also be modified from Policy view. For more information, see Modifying Policy Assignments in Policy View, page 5-52.

Related Topics

- Understanding the Device View, page 3-1
- Using the Policy Banner, page 5-36
- Assigning a Shared Policy to a Device or VPN Topology, page 5-42
- Unassigning a Policy, page 5-34
- Copying Policies Between Devices, page 5-32
- Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-35
- Inheriting or Uninheriting Rules, page 5-44
- Inheritance vs. Assignment, page 5-6

Step 1 In Device view or the Site-to-Site VPN Manager, select a shared policy from the Policies selector, then do one of the following:

- (Device view only) Select **Policy > Edit Policy Assignments**.
- Right-click the policy and select **Edit Policy Assignments**.
- Click the ***n*** device/VPN link in the Assigned To field in the policy banner.

Step 2 Modify the list of devices or VPN topologies to which the policy is assigned, as follows:

- To assign the selected policy to additional devices or topologies, select them from the Available Devices/VPNs list, then click **>>** to move them to the Assigned Devices list.

- To unassign the selected policy from devices or topologies, select them from the Assigned Devices/VPNs list, then click **<<** to return them to the Available Devices/VPNs list. Devices or topologies that are unassigned from the policy remove this policy from their running configuration during deployment.

Tip To assign a policy to all the devices in a device group, select the name of the device group, then click **>>**.

Step 3 Click **OK** to save your assignment changes.

Managing Shared Policies in Policy View

Use Policy view to globally manage all the shared policies configured in 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.

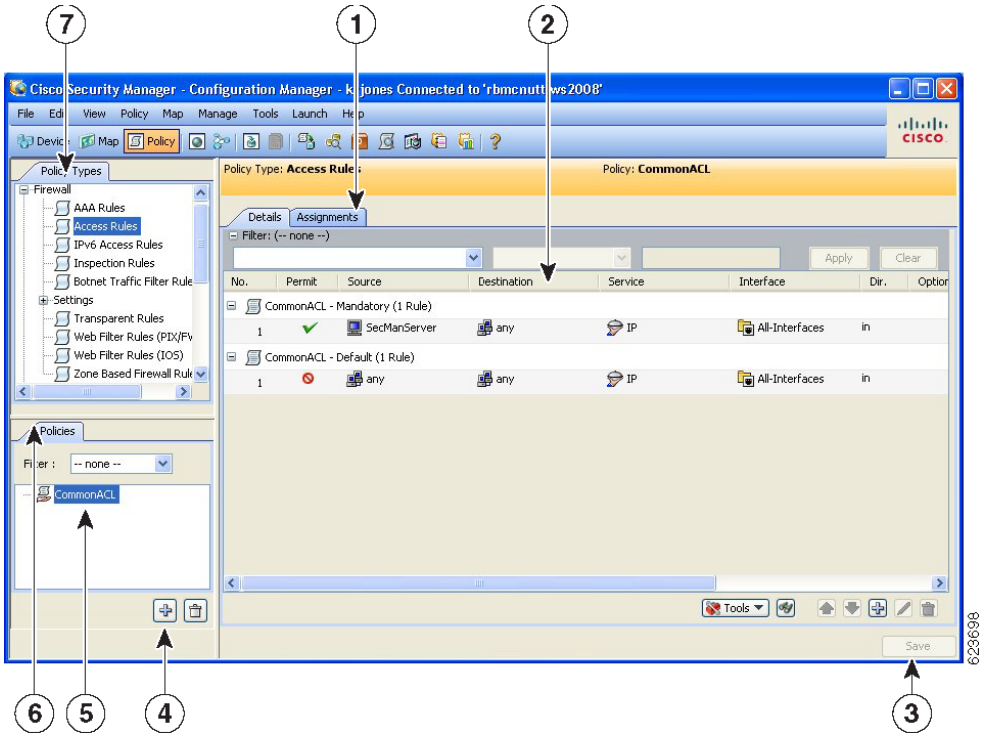
Policy view enables you to:

- 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.

To access Policy view, select **View > Policy View** or click the **Policy View** button on the toolbar.

Figure 5-4 shows the main areas of Policy view.

Figure 5-4 Policy View



1	Assignments tab	5	Shared Policy selector
2	Work area and Details tab	6	Shared Policy filter
3	Save button	7	Policy Type selector
4	Create a Policy and Delete a Policy buttons		

- **(7) Policy Type Selector**—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. To create a new policy, right click the policy type and select **New [policy type] Policy** or click the Create a Policy button in the shared policy selector. For more information, see Policy View Selectors, page 5-50.
- **(4, 5, 6) Shared Policy Selector**—Lists the shared policies that are defined for the selected type. Clicking a policy in the selector displays the definition of the policy and its assignments in the work area. For more information, see Policy View Selectors, page 5-50.

  Right-click a policy in the selector to perform actions on the policy. For more information on the available commands, see Policy View—Shared Policy Selector Options, page 5-51.

  Use the Filter field to filter the list of policies displayed in the selector. For more information about creating filters, see Filtering Items in Selectors, page 1-44.
- **(1, 2, 3) Work Area**—Contains two tabs:
  - Details—Use this tab to view and edit the definition of the selected policy. You can modify the definition as required; click **Save** in the work area to save your changes. Changes affect all devices or VPN topologies to which the policy is assigned. The information displayed on the Details tab is identical to the information displayed in Device view or the Site-to-Site VPN

Manager and can be modified in exactly the same way. See Policy View Selectors, page 5-50.

- Assignments—Use this tab to view and edit the list of devices or VPNs to which a shared policy is assigned. For more information, see Modifying Policy Assignments in Policy View, page 5-52.

Related Topics

- Importing Policies or Devices, page 10-13
- Managing Policies in Device View and the Site-to-Site VPN Manager, page 5-29
- Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-35

Policy View Selectors

Policy view contains two selectors. The upper selector displays all the policy types available for a selected policy domain. The root of the policy type selector is the policy domain name. To display the policy types for a different policy domain, click the root of the tree and select a different domain from the list.

Policy domains include:

- Firewall—Lists all policy types for configuring firewall services. See Chapter 12, "Introduction to Firewall Services".
- NAT (PIX/ASA/FWSM)—Lists all NAT policies configured on PIX, ASA, and FWSM devices. See NAT Policies on Security Devices, page 23-15.
- NAT (Router)—Lists all NAT policies configured on Cisco IOS routers. See NAT Policies on Cisco IOS Routers, page 23-5.
- Site-to-Site VPN—Lists all policy types for configuring site-to-site VPNs. See Chapter 24, "Managing Site-to-Site VPNs: The Basics".
- Remote Access VPN—Lists all policy types for configuring remote-access IPSec and SSL VPNs. See Chapter 29, "Managing Remote Access VPNs: The Basics".
- Catalyst Platform—Lists all policy types for configuring Catalyst switches and 7600 routers. See Chapter 65, "Managing Cisco Catalyst Switches and Cisco 7600 Series Routers".
- IPS—Lists all policy types for configuring IPS devices. See Overview of IPS Configuration, page 35-5.
- IPS (Router)—Lists all policy types for configuring Cisco IOS IPS policies on IOS routers. See Overview of Cisco IOS IPS Configuration, page 44-3.
- PIX/ASA/FWSM Platform—Lists all policy types for configuring PIX/ASA/FWSM platform-specific policies. See Chapter 45, "Managing Firewall Devices".
- Router Interfaces—Lists all policy types for configuring platform-specific Cisco IOS router interface policies. See Chapter 58, "Managing Routers".
- Router Platform—Lists all policy types for configuring platform-specific Cisco IOS router policies. See Chapter 58, "Managing Routers".
- FlexConfigs—Lists all FlexConfig policies. See Chapter 7, "Managing FlexConfigs".

You can expand and collapse the selector as required to view all the available policy types and subtypes. To create a new policy, right click the policy type and select **New [policy type] Policy** or click the Create a Policy button in the shared policy selector.

Selecting a policy type from the Policy Type selector displays all the shared policies of that type in the Shared Policy selector. Local policies configured in Device view are not displayed.

For example, when you select a configuration policy type, such as NAT translation rules, the Shared Policy selector displays a flat list of each shared policy of that type. If you select a rule-based policy type, such as firewall access rules, the Shared Policy selector displays a hierarchical tree of shared policies. This enables you to view the inheritance relationships among the various policies. The Shared Policy selector includes a shortcut menu with options for actions that can be performed on that policy, such as renaming it.

Tip You can create and apply a filter to shorten the list of policies displayed in the Shared Policy selector. For more information about filters, see Filtering Items in Selectors, page 1-44.

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.

Related Topics

- Policy View Selectors, page 5-50
- Managing Shared Policies in Policy View, page 5-48

Field Reference

Table 5-7 Shared Policy Selector Options

Menu Command	Description
Clone Policy	Creates a new shared policy with the same definition as the policy from which it was cloned. See Cloning (Copying) a Shared Policy, page 5-45.
Rename Policy	Renames the selected policy. See Renaming a Shared Policy, page 5-46.
Add to Policy Bundle	Allows you to add the selected shared policy to a policy bundle. See Managing Policy Bundles, page 5-54.
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 Inheriting or Uninheriting Rules, page 5-44.
New [policy type] Policy	Creates a new shared policy of the selected type. See Creating a New Shared Policy, page 5-52.
Delete Policy	Deletes the selected shared policy. See Deleting a Shared Policy, page 5-54

Creating a New Shared Policy

Use Policy view to create a new shared policy. In most cases, the new policy starts out undefined, but in certain cases (for example, many site-to-site VPN policies, such as IPsec proposals and GRE modes) default values are supplied. In all cases, the new policy is not initially assigned to any devices. If the new policy is a rule-based policy that supports inheritance, it can be created as a child of an existing shared policy of the same type. For more information, see Understanding Rule Inheritance, page 5-4.

Tip You can also create shared policies by converting local policies in Device view. For more information, see Sharing a Local Policy, page 5-39.

Related Topics

- Importing Policies or Devices, page 10-13
- Managing Shared Policies in Policy View, page 5-48
- Deleting a Shared Policy, page 5-54

Step 1 In Policy view, select a policy type in the Policy Type selector.

Step 2 Do one of the following:

- Right-click the policy type in the Policy Type selector, then select **New [policy type] Policy**.
- Right-click a policy in the Shared Policy selector, then select **New [policy type] Policy**.
- Click the **Create a Policy** button beneath the Shared Policy selector.

The Create a Policy dialog box is displayed.

Step 3 Enter a name for the new policy. Policy names can contain up to 255 characters, including spaces and special characters.

When creating a Translation Rules policy for NAT rules on security devices (PIX/ASA/FWSM), you must also choose a device software Version: **PIX/ASA 6.3-8.2** or **ASA 8.3 & Later**.

Step 4 Click **OK**. The new policy appears in the Shared Policy selector.

To configure a definition for the new shared policy, click the Help button in the toolbar with the Details tab open to see information specific to the type of policy you are creating. To assign the new shared policy, see Modifying Policy Assignments in Policy View, page 5-52.

Modifying Policy Assignments in Policy View

Use the Assignments tab in Policy view to modify the list of devices or VPN topologies to which you assigned a selected shared policy. The Assignments tab shows a list of all devices that are currently assigned the selected shared policy. It also shows devices that are assigned the policy through inheritance.

Assigning a policy to a device or VPN overwrites any policy of the same type (local or shared) that was previously assigned to the device in Security Manager. When deployed, the newly assigned policy overrides any policy of the same type that is already configured on the device, whether it was configured using Security Manager or using another method, such as the CLI.

When you unassign a shared policy from a device or VPN topology, Security Manager removes the policy from the planned configuration of that device or VPN topology. When the configuration defined by the policy is deployed, any configuration of the same type that is already configured on the device (including the devices in the VPN topology) is removed. For more information, see Unassigning a Policy, page 5-34.

Therefore, if your intention when performing unassign is to assign a different shared policy to a particular device or VPN topology, it is important to select the replacement policy and perform the assignment before performing deployment.

Tip Assigning a replacement policy is particularly important when you use a device access policy to configure the enable password or enable secret password on a Cisco IOS router. If you unassign this policy and fail to define a different password in its place before deployment, Security Manager might be unable to configure this device in the future. For more information, see User Accounts and Device Credentials on Cisco IOS Routers, page 60-13.

Alternatively, you can return to Device view and replace the shared policy assigned to the device with a different shared policy. For more information, see Assigning a Shared Policy to a Device or VPN Topology, page 5-42.

Note If you unassign a mandatory site-to-site VPN policy, such as an IKE proposal policy, Security Manager automatically replaces it with a default policy. If you unassign a mandatory remote access VPN policy, you must manually configure a new policy of that same type or deployment will fail.

Related Topics

- Modifying Shared Policy Assignments in Device View or the Site-to-Site VPN Manager, page 5-47
- Managing Shared Policies in Policy View, page 5-48

Step 1 In Policy view, select a policy type from the Policy Type selector, then select a policy from the Shared Policy selector. For more information about using these selectors, see Policy View Selectors, page 5-50.

Step 2 Click the **Assignments** tab in the work area.

The Assignments tab shows a list of all devices that are currently assigned the selected shared policy. It also shows devices that are assigned the policy through inheritance.

Step 3 Modify the list of devices or VPNs to which the policy is assigned, as follows:

- To assign the selected policy to additional devices or VPNs, select one or more items from the Available Devices/VPNs list, then click **>>** to move them to the Assigned Devices/VPNs list.

  Tip To assign a policy to all the devices in a device group, select the name of the device group, then click **>>**.

- To unassign the selected policy from devices or VPNs, select one or more items from the Assigned Devices/VPNs list, then click **<<** to return them to the Available Devices/VPNs list.

Step 4 Click **Save** to save your assignment changes.

Deleting a Shared Policy

Use Policy view to delete a shared policy from Security Manager.

Before you delete a shared policy, you should unassign it from any devices that use it, and configure replacement policies for those devices. If a shared policy is assigned to a device, when the policy is deleted the device no longer has a policy configured for the deleted shared policy, other than whatever defaults might exist for the policy type. For more information about removing assignments, see Modifying Policy Assignments in Policy View, page 5-52.

Note If a shared policy is part of a policy bundle that is assigned to a device, you must remove the assignment before you can delete the shared policy.

Related Topics

- Creating a New Shared Policy, page 5-52
- Cloning (Copying) a Shared Policy, page 5-45
- Managing Shared Policies in Policy View, page 5-48

Step 1 In Policy view, select a policy type from the Policy Type selector, then select the policy to delete from the Shared Policy selector. For more information about using these selectors, see Policy View Selectors, page 5-50.

Step 2 Do one of the following:

- Right-click the policy, then select **Delete Policy**.
- Click the **Delete a Policy** button beneath the Shared Policy selector.

You are asked to confirm the deletion.

Managing Policy Bundles

Policy bundles are collections of shared policies that can be managed as a group. Policy bundles make managing shared policies easier by allowing you to create the bundle one time and then assign all of the policies in the bundle to a new device at once. The shared policies that are part of the bundle function in the same way as other shared policies and modifying any of the shared policies that are part of a bundle affects all devices that are assigned that policy either directly or through a policy bundle.

When creating a policy bundle, you can only assign one shared policy of each type to the policy bundle. Multiple policy bundles can be assigned to a device as long as the policy types in those policy bundles do not overlap.

When assigning a policy bundle to a device, if local policies on that device are the same policy type as those contained in the policy bundle, you are given the option to inherit or replace the existing policies.

Note When you unassign a policy bundle, all policies that are part of that bundle are removed from the device. Local policies will be lost and cannot be retrieved.

This section contains the following topics:

Creating a New Policy Bundle

You can use the Policy Bundle view to create new policy bundles. When creating a policy bundle, you can only assign one shared policy of each type to the policy bundle.

Related Topics

- Managing Policy Bundles, page 5-54
- Cloning a Policy Bundle, page 5-56
- Renaming a Policy Bundle, page 5-56
- Assigning Policy Bundles to Devices, page 5-57

Step 1 Use one of the following methods to create a policy bundle:

- In Policy Bundle view, do one of the following:
  - From the All Shared Policies view, select the shared policies that you would like to bundle, then right-click on a selected shared policy and select **Create Policy Bundle**.
  - Right-click an existing policy bundle in the Policy Bundle selector, then select **Create Policy Bundle**.
  - Click the **Create a Policy Bundle** button beneath the Policy Bundle selector.
- To create a new policy bundle that includes all of the shared policies on a device, right-click a device in the Device selector in Device view, then select **Create Policy Bundle**.

The Create Policy Bundle dialog box is displayed.

Step 2 Enter a name for the new policy bundle.

Step 3 Click **OK**.

The policy bundle is added to the list of policy bundles in Policy Bundle view.

Step 4 To configure the definition for a policy bundle, do any of the following:

- In Policy Bundle view:
  - To add shared policies to the bundle, select **All Shared Policies** in the Policy Bundle selector and then drag and drop the required shared policies onto the policy bundle.
  - To remove shared policies from the bundle, select the bundle in the Policy Bundle selector. Select the shared policy you want to remove on the Details tab of the Policy Bundle View window, and then click **Delete**.
- In Policy view, right-click the shared policy you want to add to a policy bundle, select **Add to Policy Bundle**, and then select the bundle to which you want to add the shared policy.

Cloning a Policy Bundle

You can use Policy Bundle view to create a new policy bundle by cloning an existing bundle.

Related Topics

- Managing Policy Bundles, page 5-54
- Creating a New Policy Bundle, page 5-55
- Renaming a Policy Bundle, page 5-56
- Assigning Policy Bundles to Devices, page 5-57

Step 1 In Policy Bundle view, right-click an existing policy bundle in the Policy Bundle selector, then select **Clone Policy Bundle**.

The Clone Policy Bundle dialog box is displayed.

Step 2 Enter a name for the new policy bundle.

Step 3 Click **OK**.

The new policy bundle appears in the Policy Bundle selector.

Renaming a Policy Bundle

You can rename existing policy bundles from the Policy Bundle view. Renaming a policy bundle will not affect device assignments.

Related Topics

- Managing Policy Bundles, page 5-54
- Creating a New Policy Bundle, page 5-55
- Cloning a Policy Bundle, page 5-56
- Assigning Policy Bundles to Devices, page 5-57

Step 1 In Policy Bundle view, right-click an existing policy bundle in the Policy Bundle selector, then select **Rename Policy Bundle**.

The Rename Policy Bundle dialog box is displayed.

Step 2 Enter a new name for the policy bundle.

Step 3 Click **OK**.

The policy bundle name is updated in the Policy Bundle selector.

Assigning Policy Bundles to Devices

You can modify the list of devices assigned a particular policy bundle as required. Multiple policy bundles can be assigned to a device as long as the policy types in those policy bundles do not overlap. When assigning a policy bundle to a device, if local policies on that device are the same policy type as those contained in the policy bundle, you are given the option to inherit or replace the existing policies.

Note If any of the policies that are part of a policy bundle are not compatible with the device to which you are assigning it, the bundle cannot be assigned.

If you remove a device from a policy bundle assignment, all policies that are part of that bundle are effectively removed from the device's planned configuration. Local policies will be lost and cannot be retrieved. Upon deployment, any configuration of that type that exists on the device is removed. For more information about the implications of unassigning a policy, see Unassigning a Policy, page 5-34.

Caution Use the policy bundle assignment feature with care, as unassigning a policy bundle removes that configuration from the device and can have unintended consequences. For example, if you unassign a device access policy from a Cisco IOS router and then deploy that change, you might prevent Security Manager from configuring that device in the future (see User Accounts and Device Credentials on Cisco IOS Routers, page 60-13).

Related Topics

- Managing Policy Bundles, page 5-54
- Creating a New Policy Bundle, page 5-55
- Cloning a Policy Bundle, page 5-56
- Renaming a Policy Bundle, page 5-56

Step 1 In Policy Bundle view, select an existing policy bundle in the Policy Bundle selector.

The policy bundle details are displayed in the Policy Bundle main window.

Step 2 Click the **Assignments** tab.

Step 3 Modify the list of devices to which the policy bundle is assigned, as follows:

- To assign the selected policy bundle to additional devices, select them from the Available Devices list, then click **>>** to move them to the Assigned Devices list.
- To unassign the selected policy bundle from devices, select them from the Assigned Devices list, then click **<<** to return them to the Available Devices/VPNs list. Devices or topologies that are unassigned from the policy remove this policy from their running configuration during deployment.

Tip To assign a policy to all the devices in a device group, select the name of the device group, then click **>>**.

Step 4 Click **OK** to save your assignment changes.

The policy bundle name is updated in the Policy Bundle selector.