Managing Policy Objects

Policy objects enable you to define logical collections of elements. They are reusable, named components that can be used by other objects and policies. Objects aid policy definition by eliminating the need to define that component each time you define a policy. When used, an object becomes an integral component of the object or policy. This means that if you change the definition of an object, this change is reflected in all objects and policies that reference the object.

Objects facilitate network updates, because you can identify objects separately but maintain them in a central location. For example, you can identify the servers in your network as a network/host object called MyServers, and the protocols to allow on these servers in a service object. You can then create an access rule that permits the MyServers network/host object to send and receive traffic for the services defined in the service object. If a change is made to these servers, you need only update the network/host or service object and redeploy, instead of trying to locate and edit each rule in which the servers are used.

Objects are defined globally. This means that the definition of an object is the same for every object and policy that references it. However, many object types (for example, interface roles) can be overridden at the device level. Thus, you can create an object that works for most of your devices, yet customize the object to match the configuration of a particular device that has slightly different requirements. For more information, see Understanding Policy Object Overrides for Individual Devices, page 6-18.

This chapter contains the following topics:

- Selecting Objects for Policies, page 6-2
- Policy Object Manager, page 6-4
- Working with Policy Objects—Basic Procedures, page 6-9
- Understanding AAA Server and Server Group Objects, page 6-27
- Creating Access Control List Objects, page 6-53
- Configuring Time Range Objects, page 6-71
- Understanding Interface Role Objects, page 6-73
- Understanding Map Objects, page 6-78
- Understanding Networks/Hosts Objects, page 6-80
- Understanding Pool Objects, page 6-92
- Configuring SAML Identity Provider, page 6-98
- Understanding and Specifying Services and Service and Port List Objects, page 6-100
- How Policy Objects are Provisioned as Object Groups, page 6-106

Selecting Objects for Policies

Modifying Policies using Drag and Drop

If you are modifying an existing policy, you can easily update the policy definition by dragging and dropping objects from the Policy Object Manager onto the applicable field in the policy. You can select a range of objects from the Policy Object Manager window by selecting the first object in the range and then, with the Shift key pressed, selecting the last object in the range. You can select multiple objects by clicking those objects while keeping the Ctrl key pressed. You can also select a range of objects and then add additional objects to your selection by using the Ctrl key method. To drag multiple objects, press and hold the Ctrl key while dragging or drag using the right-mouse button.

Creating Policies using Object Selector

When creating a policy, you often need to select one or more objects to include in the policy definition. For example, firewall policies make use of network/host objects, interface role objects, and service objects.

To include objects in policies, you can manually enter the object name or click the **Select** button to display an object selector dialog box. In certain cases, the object selector is prefiltered to display only the objects that are applicable to the policy that you are configuring. For example, when configuring a policy that requires a subnet, the object selector displays only those network/host objects that represent subnets, not network/host objects that represent single hosts. Object selectors make it easy for you to select which objects to include in a particular policy.

Additionally, object selectors enable you to create and edit objects of that type on the fly. This makes it easy to work with objects without leaving the policy you are defining to open the Policy Object Manager. For example, if when creating a dynamic NAT rule you discover that the ACL object you require does not exist, you can click the Create button to open the dialog box for creating an ACL object. When you finish creating the object, you are returned to the object selector with the new object selected and ready for inclusion in the policy. If you need to modify an existing object before using it, select it, click the Edit button and make your modifications, then click OK to save your changes; this returns you to the object selector.

When you create an object by opening the object editor from within a selector, the new object must conform to the requirements of the field from which the selector was opened. For example, if you open a selector from a field requiring a host and then decide to create a network/host object for that field, you must define the network/host object as a host.

There are two types of objects selectors—a simple list selector for policies that require you to select a single object, and a dual selector for policies that allow you to select multiple objects of a certain type. The following table explains these selectors and how to use them.

Table 6-1 Object Selectors

Element	Description
Type	The type of object to display in the selector, if there is an option. For example: • You can choose between network/host objects and interface roles when configuring sources and destinations in some rule-based policies. • You can choose between standard and extended ACL objects when configuring some ACLs (for example, when configuring VLAN ACLs on Catalyst 6500/7600 devices). **Tip** In some policies, if you select more than one type of object, they are displayed on different tabs within the field.
Available [object type]	Displays all objects that are relevant to the policy or object you are configuring. When selecting interfaces, be aware that there can be interfaces and interface roles with the same name. They can be distinguished by the icon displayed next to the name. For more information, see Specifying Interfaces During Policy Definition, page 6-76. **Tip** You can quickly find an object inside a selector by clicking in the list box and then starting to type the name of the object.
Selected [object type]	Displays the objects that you selected to apply to the policy or object that you are editing.
Multi-Object Selector Buttons	
>> button << button	Moves the selected objects from one list to the other list in the direction indicated. You can select multiple objects by using Ctrl+click. You can also move objects between lists by double-clicking them or by selecting them and pressing Enter.
Up/Down arrow buttons	For a limited number of object types, order matters. If the selector includes **Move Up** and **Move Down** buttons, arrange the objects in priority order. For example, when defining a method list for AAA, use the arrows to determine the order in which different types of AAA server groups are used.
Common Buttons	
Create button	Click this button to create an object of this type. **Tip** In a few cases, such as network/host and service objects, clicking this button opens a list from which you need to select a specific type for the object.
Edit button	Click this button to edit the selected user-defined object. If you try to edit a system-defined object, it is opened in read-only mode.

Related Topics

- Allowing a Policy Object to Be Overridden, page 6-18
- Filtering Items in Selectors, page 1-45

Policy Object Manager

Use the Policy Object Manager to:

- View all available objects grouped by object type.
- Create, copy, edit, and delete policy objects.
- Drag and drop objects onto existing policies to update the policy definition.
- Generate usage reports, which describe how selected objects are being used by other Security Manager objects and policies.

Navigation Path

In Device view or Policy view, click the **Policy Object Manager** button on the toolbar, or choose **Policy Objects** from the **Manage** menu. (The Policy Object Manager cannot be opened from Map view.)

Note When you open the Policy Object Manager, it is initially displayed as a pane in the lower half of the current view to make dragging and dropping objects easier. You can "undock" this pane, making the Policy Object Manager a separate window; you also can "re-dock" the window. See Policy Object Manager: Undocking and Docking, page 6-8 for more information.

Related Topics

- Creating Policy Objects, page 6-9
- Selecting Objects for Policies, page 6-2
- Generating Object Usage Reports, page 6-15
- Managing Object Overrides, page 6-17
- Filtering Tables, page 1-48

Field Reference

Table 6-2 Policy Object Manager Window

Element	Description
Object Type selector, or table of contents (Left pane)	Lists the object types available in Security Manager. When you select an object type, all existing objects of that type are listed in the table in the right pane. The objects are organized into three folders: Favorites, Recent Objects, and All Object Types. Click the arrow to left of a folder name to expand that folder. You can also specify your favorite object types and they will be presented in a separate list so that they can be more easily accessed. To add an object type to your favorites list, right-click the object and then select **Add to Favorites**. To remove an object type from your Favorites list, right-click the object and choose **Remove from Favorites**. Recent Objects is a list of the ten most recently modified objects. Click a recent object to see a summary of the object that includes the name, type, description, and last modified date. You can also access the View Object, Edit Object, and Find Usage buttons for the object. Expand the All Object Types folder to view all types of object available.

Policy Object Table (Right Pane)

The policy object table in the right pane lists existing objects of the type selected in the table of contents. Using this table, you create new objects and work with existing ones. You can use the buttons below the table, or right-click within the table to see additional commands (see Policy Object Manager Shortcut Menu, page 6-8).

Except for the Access Control Lists (ACL) object, there is one table per object type. For ACLs, there are tabs to separate Extended, Standard, Web, and Unified ACL objects. Select the appropriate tab to work with the desired object type.

The columns in the table vary based on the type of object you select. You can alter the columns displayed in the table by right-clicking the table heading and selecting or deselecting columns in the Show Columns command. You can also sort the information by the contents in a column by clicking the column heading; click the heading to toggle between alphabetical and reverse alphabetical sorting.

For detailed information on the settings that are displayed in the table, click the Create or Edit buttons below the table and click Help in the dialog box that is opened. The following section, “Table Columns,” is a description of the columns that you typically see.

Buttons Above Table	
Referenced	Select this option to view reference information for objects. When selected, a "Referenced" column is added to the table to display information on whether an object is being used by any policies or policy objects.
Find Usage	Use the Find Usage feature to view a report on the policies or policy objects that are using the selected object and any device overrides for the object. For more information, see Generating Object Usage Reports, page 6-15.
View Object	When a single object is selected in the table, you can click this button to open the Edit dialog box for that type of object in read-only mode to view the settings for that particular object.

Table 6-2 Policy Object Manager Window (continued)

Element	Description
Export	Use the Export feature to download a CSV file of the object data for the selected object type.
Print	Use the Print feature to print the object data for the selected object type.
Filter	Allows you to filter the rows displayed to help you find items in a large table. For more information, see Filtering Tables, page 1-48.
Table Columns	
*	Indicates the policy object status: • - Policy object has been locked for editing. Hover over the lock icon to see the user and ticket/activity that has the object locked. • - Policy object has been modified in the current ticket/activity but the changes have not been submitted. **Note** You can hover over the status icons to see details about the ticket/activity in which the policy object has been modified/locked and to navigate to that ticket/activity.
Icon (unlabeled field)	The icon displayed for a policy object type identifies objects of that type wherever they appear, such as in rules tables. If the icon includes the image of a pencil, you can edit it.
Name	The name of the policy object.
Content	A summary of the object definition that might not include all defined settings.
Permit	For ACL objects, if the Access Control Entry (ACE) allows traffic, a check mark appears in the Permit column. If the action is deny, a red circle with a slash appears.
Category	The category object that is assigned to the object, if any. Categories help you organize and identify rules and objects. For more information, see Using Category Objects, page 6-13.
Overrides	Whether a user can override the object properties at the device level. A check mark indicates that the object can be overridden. Not all object types are overridable. If an object has been overridden, the Overrides column displays the number of overrides for that object. You can click on the number to see the list of overrides. For more information about device overrides, see Managing Object Overrides, page 6-17.

Table 6-2 Policy Object Manager Window (continued)

Element	Description
Referenced	Whether the object is being used in any policy definitions. You can find out which policies or policy objects are using the selected object and any device overrides for the object using the Find Usage feature (see Generating Object Usage Reports, page 6-15). **Note** To view reference information, make sure the Referenced option is selected on the toolbar above the Policy Object Table. **Note** The Referenced column reports usage based on both committed data and uncommitted data across all activities/tickets, whereas as the Find Usage feature only reports usage based on committed data and data from the current activity/ticket.
Description	The description for the object. If the column is too narrow to display the description, you can double-click the icon to view the description or mouse-over the icon.
Last Ticket(s)	If ticketing is enabled, shows the Ticket ID of the ticket last used to modify the object. You can click on the If ticketing is enabled, shows the ticket(s) associated with last modification to the object. You can click the ticket ID in the Last Ticket(s) column to view details of the ticket and to navigate to the ticket. If linkage to an external ticket management system has been configured, you can also navigate to that system from the ticket details (see Ticket Management Page, page 11-72).
Last Modified Date	Shows the date and time the object was last modified.
Buttons Below Table	
	Click the New Object button to create a new object. The same icon is used for any button that adds an item to a table. **Tip** In a few cases such as Networks/Hosts and Services objects, clicking this button opens a list from which you need to select a specific type for the object. Clicking this button opens a dialog box to create the object. Click the Help button in the dialog box for information on the selected object type. Also, see Creating Policy Objects, page 6-9.
	Click the Edit Object button to edit the selected object. The same icon is used for editing any object in a table. The dialog box used for editing the object is the same as the one used for creating the object. If you try to edit a system-defined default object, you are allowed only to view the object contents. Click the Help button in the dialog box for information on the settings. For more information, see Editing Objects, page 6-12.
	Click the Delete Object button to delete the selected object. You can delete only user-defined objects that are not currently being used in a policy or another policy object. For more information, see Deleting Objects, page 6-16.

Policy Object Manager: Undocking and Docking

Whenever you open the Policy Object Manager, it is initially displayed as a pane in the lower half of the current view to make dragging and dropping objects easier. You can "undock" this pane, making the Policy Object Manager a separate window, you can "re-dock" the window, and you can close the pane or window:

- To undock the Policy Object Manager from the current view in the Configuration Manager window, click the Undock Window button in the upper right corner of the pane's title bar.
- To put the floating window back as a pane in the Configuration Manager window, click the Dock Frame button in the upper right corner of the Policy Object Manager window.
- To close either the pane or the floating window, click the Close button in its upper right corner.

Navigation Path

In Device view or Policy view, click the **Policy Object Manager** button on the toolbar, or choose **Policy Objects** from the **Manage** menu. (The Policy Object Manager cannot be opened from Map view.)

Policy Object Manager Shortcut Menu

Right-clicking inside the policy object table in the Policy Object Manager, page 6-4 displays a shortcut menu for performing various functions on the selected object type.

Field Reference

Table 6-3 Policy Object Manager Shortcut Menu

Menu Command	Description
New Object	Choose this command to create a new policy object. Click Help in the dialog box that is opened for information specific to the object type. Also, see Creating Policy Objects, page 6-9. **Tip** For network/host and service objects, you need to also select an object type from the submenu.
Edit Object	Choose this command to edit the policy object selected in the table. If you select a system-defined default object, you are presented with a view-only look at the object definition. For more information, see Editing Objects, page 6-12.
Delete Object	Choose this command to delete the policy object selected in the table. You can delete only user-defined objects that are not being used in a policy or in another policy object. For more information, see Deleting Objects, page 6-16.
Enable/Disable Device Overrides	Choose the Enable Device Overrides command to enable device overrides on one or more devices on which overrides are disabled. Choose the Disable Device Overrides command to disable device overrides on one or more devices on which overrides are enabled.
Edit Device Overrides	Select this command to change the device-level overrides for this object using the Policy Object Overrides Window, page 6-20. You can create, edit, and delete overrides. For more information, see Managing Object Overrides, page 6-17.

Table 6-3 Policy Object Manager Shortcut Menu (continued)

Menu Command	Description
Clone Object	Select this command to create a copy of the policy object. For more information, see Cloning (Duplicating) Objects, page 6-14.
Copy Object	Choose this command to copy one or more selected objects to the system Clipboard. **Tip** You can also use **Ctrl+C** to copy objects.
Paste Object	Choose this command to paste the object(s) on the system Clipboard into another object. For example, you might add a host-type Networks/Hosts object to an existing group-type Networks/Hosts object. The two object types must be compatible. **Tip** You can also use **Ctrl+V** to paste objects.
Find Usage	Choose this command to generate a usage report for the selected object using the Object Usage dialog box. The usage report tells you where the object is currently being used. for more information, see Generating Object Usage Reports, page 6-15.
View Object	Choose this command to view the definition of the object using a read-only version of the edit dialog box for the object. For more information, see Viewing Object Details, page 6-14.

Working with Policy Objects—Basic Procedures

The following topics describe the actions that you can perform on policy objects. Some tasks are limited to certain types of objects. For example, not all types of object can be overridden, you cannot edit predefined objects, and you cannot import or export all objects.

This section contains the following topics:

- Creating Policy Objects, page 6-9
- Editing Objects, page 6-12
- Using Category Objects, page 6-13
- Cloning (Duplicating) Objects, page 6-14
- Viewing Object Details, page 6-14
- Generating Object Usage Reports, page 6-15
- Deleting Objects, page 6-16
- Managing Object Overrides, page 6-17
- Importing and Exporting Policy Objects, page 6-23

Creating Policy Objects

Security Manager provides predefined policy objects of various types that you can use to define policies. Additionally, you can create your own objects, as required.

You can create objects in one of two ways:

- Using the Policy Object Manager window. This option is best suited for situations where you are defining one or more objects outside of the context of defining a particular policy. See Policy Object Manager, page 6-4.
- Using object selectors. When you define a policy that uses objects, object selectors include buttons for creating and editing objects so you don't have to leave the policy you are defining. This is frequently the best method to use, because during policy creation you are prompted for the specific type of object that applies to the situation, and you are more aware of the settings you need for the policy. See Selecting Objects for Policies, page 6-2.

Tip Your ability to create multiple objects with the same definition depends on a setting on the Policy Objects page in the Security Manager Administration window (select **Tools > Security Manager Administration**). By default, Security Manager warns you when you create an object whose definition is identical to that of an existing object, but it does not prevent you from proceeding. For more information, see Policy Objects Page, page 11-66.

Related Topics

- Chapter 6, "Managing Policy Objects"
- Working with Policy Objects—Basic Procedures, page 6-9

Step 1 Do one of the following:

- Select **Manage > Policy Objects** to open the Policy Object Manager, page 6-4. Select the type of object you want to create from the table of contents, right-click in the table and select **New Object**.
- While configuring a rule, click **Select** next to a field that allows or requires a policy object. In the object selector, click the **Create** button below the available objects list.

Tip In a few cases, such as network/host and service objects, clicking these buttons opens a list from which you need to select a specific type for the object.

The dialog box for adding the selected type of object opens. For more information about the individual types of objects, see the following topics:

- Understanding AAA Server and Server Group Objects, page 6-27
- Creating Access Control List Objects, page 6-53
- Add or Edit As Path Object Dialog Boxes, page 56-154
- ASA Group Policies Dialog Box, page 34-1
- Add or Edit BFD Template Dialog Box
- Using Category Objects, page 6-13
- Add or Edit Community List Object Dialog Box, page 56-156
- Configuring Credentials Policy Objects, page 28-9
- Add and Edit File Object Dialog Boxes, page 34-37
- Understanding FlexConfig Policies and Policy Objects, page 7-2 and Creating FlexConfig Policy Objects, page 7-28 (in Chapter 7, "Managing FlexConfigs")
- Creating Identity User Group Objects, page 13-19
- Configuring IKEv1 Proposal Policy Objects, page 26-10

- Configuring IKEv2 Proposal Policy Objects, page 26-14
- Understanding Interface Role Objects, page 6-73
- Configuring IPSec IKEv1 or IKEv2 Transform Set Policy Objects, page 26-27
- Add and Edit LDAP Attribute Map Dialog Boxes, page 6-46
- Understanding Map Objects, page 6-78
- Understanding Networks/Hosts Objects, page 6-80
- PKI Enrollment Dialog Box, page 26-58
- Add or Edit Policy List Object Dialog Box, page 56-146
- Understanding Pool Objects, page 6-92
- Add or Edit Port Forwarding List Dialog Boxes, page 34-40
- Configuring Port List Objects, page 6-102
- Add or Edit Prefix List Object Dialog Box, page 56-149
- Configuring Risk Rating Policy Objects, page 40-15
- Add or Edit Route Map Object Dialog Boxes, page 56-139
- Creating Security Group Objects, page 14-14
- Creating Cisco Secure Desktop Configuration Objects, page 33-18
- Understanding and Specifying Services and Service and Port List Objects, page 6-100
- Add or Edit Single Sign On Server Dialog Boxes, page 34-42
- Monitoring Service Level Agreements (SLAs) To Maintain Connectivity, page 51-8
- Configuring SSL VPN Bookmark Lists for ASA and IOS Devices, page 31-83
- Configuring ASA Portal Appearance Using SSL VPN Customization Objects, page 31-78
- Add or Edit SSL VPN Gateway Dialog Box, page 34-64
- Add and Edit Smart Tunnel Auto Signon List Dialog Boxes, page 34-71
- Configuring SSL VPN Smart Tunnels for ASA Devices, page 31-85
- Add or Edit Text Object Dialog Box, page 7-32
- Configuring Time Range Objects, page 6-71
- Configuring Traffic Flow Objects, page 58-18
- Add or Edit User Group Dialog Box, page 34-73
- Configuring WINS/NetBIOS Name Service (NBNS) Servers To Enable File System Access in SSL VPNs, page 31-88

Step 2 Enter a name for the object and optionally a description of the object.

Object names are not case-sensitive and are limited to 128 characters. You can begin object names with a letter, a number, or an underscore. You can use a mix of letters, numbers, special characters, and spaces for the remainder of the object name.

Supported special characters include

- hyphens (-),
- underscores (_),
- periods (.), and,

- plus signs (+).

Beginning with version 4.12, Security Manager allows you to use additional special characters including

- exclamation mark (!),
- at sign (@),
- hash sign (#),
- percent sign (%),
- ampersand sign (&), and,
- parentheses or round brackets ().

Security Manager does not support the following characters:

- caret character (^)
- dollar character ($)

Some objects also support the use of colons (:) in the object name; however, objects with a colon in the name are not supported on IPS devices. If you share objects between different device types that include IPS devices, you should avoid using a colon (:) in the object name.

Note Certain object types, such as AAA server groups, ASA user groups, maps, network/host objects, service objects, and traffic flows, have different naming guidelines. For more details, refer to the online help when you are creating each object type.

Step 3 Configure the settings specific to the type of object. Refer to the online help page for the dialog box.

Step 4 (Optional) Under Category, select a category to help you identify this object in the Objects table. See Using Category Objects, page 6-13.

Step 5 (Optional) If the object type provides the option, select **Allow Value Override per Device** to allow the properties of this object to be redefined on individual devices. See Allowing a Policy Object to Be Overridden, page 6-18.

Step 6 Click **OK** to save the object.

Editing Objects

You can edit any user-defined object as required. Changes that you make to the object are reflected in all policies (and other objects) that use the object. However, if an override for the object is already defined for a device, your edits are not reflected in the object used on those devices.

Tips

- You cannot edit predefined objects, but you can copy them to create new objects. See Cloning (Duplicating) Objects, page 6-14.
- Messages appear at the top of the Edit dialog box to indicate the following situations:
  - That you have read-only access to the object. You cannot save changes to these objects.
  - That the policy object was imported using the procedure described in Importing Policies or Devices, page 10-13. Imported objects might be re-imported at some point if the shared policy that uses the object is managed on a different server. Any changes that you make are eliminated if the policy object is imported again. Before editing the object, 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 11-64).

- You can also edit objects when you define policies or objects that use this object type. For more information, see Selecting Objects for Policies, page 6-2.

Before You Begin

Determine if the object is being used, and which policies, objects, and devices would be affected by the changes. You can generate a usage report for this purpose. See Generating Object Usage Reports, page 6-15.

Related Topics

- Creating Policy Objects, page 6-9

Step 1 Select **Manage > Policy Objects** to open the Policy Object Manager, page 6-4.

Step 2 Select the object type from the table of contents.

Step 3 Right-click the object you want to edit and select **Edit Object**.

Step 4 Modify the fields in the Edit dialog box for that object type as required, then click **OK** to save your changes. Click the Help button for information specific to the type of object.

Using Category Objects

Categories provide an intermediate level of detail to objects. By assigning a category to an object, you can look for the name and color of a category to more easily identify rules and objects in rules tables. You can assign a category to a rule or object when you create the rule, or you can edit the rule or object to include category information later. No device configuration commands are generated for category assignments.

The benefits of assigning categories to policy objects are:

- Visibility is improved when you view rules tables using objects that are categorized.
- Objects can be filtered in the rules tables based on category, facilitating rule maintenance.

For example, you might want to create a network/host object and keep track of its use for administrative purposes. When you define this network/host object, you associate it with a category. When you view the access rules table, you can easily identify those rules that use your network/host object. You can also filter the table to display only those items associated with the category.

Security Manager includes a set of predefined categories. Although you cannot change the colors, you can change their names and descriptions. The following procedure explains how to change the name and description.

Step 1 Select **Manage > Policy Objects** to open the Policy Object Manager (see Policy Object Manager, page 6-4).

Step 2 Select **Categories** from the Object Type selector.

Step 3 Click **Edit Object** to open the Category Editor dialog box.

Step 4 Modify the names and descriptions of the predefined category objects as required:

- Label—The color associated with the category.
- Name—The category name. Names can have a maximum of 128 characters, including special characters and spaces.
- Description—Additional information about the object (up to 1024 characters).

Step 5 Click **OK** to save your changes.

Cloning (Duplicating) Objects

An alternative to creating a policy object from scratch is to clone, or duplicate, an existing object. The new object contains all the attributes of the copied object. You can then modify the name and all attributes as required.

Cloning is useful for creating objects that are based on predefined objects that cannot be edited.

Related Topics

- Working with Policy Objects—Basic Procedures, page 6-9

Step 1 Select **Manage > Policy Objects** to open the Policy Object Manager, page 6-4.

Step 2 Select the object type from the table of contents.

Step 3 Right-click the object you want to duplicate and select **Clone Object**.

The dialog box for that object type appears. The Name field contains the following default name for the new object: Copy of *name of copied object*. The remaining fields contain the same values as the copied object.

Step 4 Modify the name of the new object and its configuration, as required. Click the Help button for information specific to that type of object.

Step 5 Click **OK** to save your changes.

Viewing Object Details

You can view contents of an object in read-only mode, even when the object is locked by another activity. This is useful when you need to view complete configuration details for complex objects whose definitions cannot be fully displayed in the Policy Object Manager window or when your user privileges allow you only to view object information.

Related Topics

- Working with Policy Objects—Basic Procedures, page 6-9

Step 1 Select **Manage > Policy Objects** to open the Policy Object Manager, page 6-4.

Step 2 Select the object type from the table of contents.

Step 3 Right-click the object and select **View Object**.

The dialog box for that object appears in read-only mode.

Generating Object Usage Reports

Before you make any changes to a policy object, you should determine if the object is being used. You can do this by viewing the Referenced column in the Policy Object Manager window. Select the Referenced button above the Policy Object Table to enable the Referenced column.

For objects that are referenced, you can generate usage reports that show which policies, objects, VPNs, and devices are using the selected object and would therefore be affected by changes to that object. Usage reports contain any references to the selected object in your current activity as well as references found in the data committed to the database.

Note The Referenced column reports usage based on both committed data and uncommitted data across all activities/tickets, whereas as the Find Usage feature only reports usage based on committed data and data from the current activity/ticket.

You can use either of these methods to generate usage reports:

- Policy Object Manager—Select **Manage > Policy Objects** to open the Policy Object Manager, page 6-4. Select the type of object from the table of contents, right-click the object and select **Find Usage**.
- Firewall rules policies—Left-click an object in a firewall rules table, then right-click and select **Find Usage**.

The usage information is displayed in the Object Usage dialog box. Select the appropriate usage type above the table to view devices, policies, VPNs, or other objects that use the selected object.

For certain policies,

The following table describes the fields in the dialog box.

Table 6-4 Object Usage Dialog Box

Element	Description
Name Type Description	General information about the object for which you are finding usage is displayed at the top of the Object Usage dialog box.
Devices Policies Objects VPN	The type of references you want to view. For example, you can select Objects to view only references to the object from other objects.
Used By	The name of the device, policy, VPN, or object that is referencing the selected object.
Type	The type of item that is referencing the selected object. This can be a device, policy, VPN, or another object.

Table 6-4 Object Usage Dialog Box (continued)

Element	Description
Usage	Indicates how the object is being referenced. For example, if a device is referencing the selected object, this column will indicate that it is a policy assigned to the device that is referencing the object.
Proximity	Indicates the relationship between the selected object and the item that it using it. For example: • A policy that includes a network/host object in its definition has a *direct* relationship with the object and an *indirect* relationship with any other network/host objects contained within the object. • A device on which this policy is assigned references the network/host object *directly* and any other network/host objects contained within the object *indirectly*.
Details Panel	Shows additional details for certain types of references: • **Devices** - For supported policy types, device information is displayed in the Details panel. • **Policies** - For the following supported policy types, the actual rules referencing the object are presented in the Details panel: – AAA Rules – Access Rules – IPv6 Access Rules – Inspection Rules – Translation Rules – Web Filter Rules (PIX/FWSM/ASA) – Zone Based Firewall Rules You can navigate to the rule, export the rule data, or print the rule data from the Details panel. • **Objects** - Details for other objects that are referencing the specified object are presented in the Details panel. You can export the detailed information, print the information, view the object in read-only mode, edit the object, or even find usage for the object from the Details panel in the Object Usage dialog box.

Deleting Objects

You can delete user-defined objects only when they are not being used by policies or other objects. You cannot delete predefined objects. If you delete an object for which device-level overrides are defined, all overrides are also deleted.

Tip You might be prevented from deleting an unused object from the database, if, for example, you replace a local policy that used the object with a shared policy that does not. If object deletion fails, submit or discard all pending changes (in Workflow mode, submit or discard all pending activities), then try again to delete the object. Alternatively, you can leave unused objects in the database, because they will not affect your policies.

Before You Begin

Determine if the object is currently being used and which policies, objects, and devices would be affected by the deletion. You need to remove all references to the object before you can delete it. You can generate a usage report for this purpose. See Generating Object Usage Reports, page 6-15.

Step 1 Select **Manage > Policy Objects** to open the Policy Object Manager, page 6-4.

Step 2 Select the object type from the table of contents.

Step 3 Right-click the object you want to delete and select **Delete Object**, or select the object and click the **Delete Object** button. You are asked to confirm the deletion.

Managing Object Overrides

When you create a policy object, you can elect to allow the object to be overridden. This makes it possible to create a generic object to enable you to create general policies. For individual devices, you override the policy object definition to make the policy apply correctly to the device.

From the Policy Object Manager, page 6-4, you can select a policy object that can be overridden and generate a table of device-level overrides that are defined for that global object. Right-click the object and select **Edit Device Overrides** to generate the table (see Policy Object Overrides Window, page 6-20).

You can create device-level overrides in two places:

- In the Device Properties window of a selected device, which allows you to create and manage overrides for the selected device only. For more information, see Creating or Editing Object Overrides for a Single Device, page 6-19.
- In the Policy Object Manager window, which allows you to create and manage overrides for more than one device at a time. For more information, see Creating or Editing Object Overrides for Multiple Devices At A Time, page 6-19.

Tip If you override any part of the object definition at the device level, any subsequent changes made to the policy definition at the global level do not affect the device on which the object was overridden.

The following topics explain policy object overrides in more detail:

- Understanding Policy Object Overrides for Individual Devices, page 6-18
- Allowing a Policy Object to Be Overridden, page 6-18
- Creating or Editing Object Overrides for a Single Device, page 6-19
- Creating or Editing Object Overrides for Multiple Devices At A Time, page 6-19
- Deleting Device-Level Object Overrides, page 6-21

- Overridable Objects in Security Manager, page 6-22

Understanding Policy Object Overrides for Individual Devices

For many types of policy objects, you can elect to allow an object to be overridden for a particular device. Thus, you can create an object whose definition works for most devices, and then create modifications to the object for the few devices that need slightly different definitions. Or, you can create an object that needs to be overridden for all devices, but which allows you to create a single policy for all devices. Object overrides make it possible for you to create a smaller set of shared policies for use across your devices without giving up the ability to alter policies when needed for individual devices.

For example, you might want to deny ICMP traffic to the different departments in your company, each of which is connected to a different network. You can do this by defining an access rule firewall policy with a rule that includes a network/host object called Departmental Network. By allowing device override for this object, you can then create overrides on each relevant device that specify the actual network to which that device is connected.

Device-level object overrides are especially important when the global object is included in the definition of a VPN policy, which applies to every device in the VPN topology. For example, you select a PKI enrollment object when defining a PKI policy on a site-to-site VPN. If the hub of your VPN uses a different CA server than the spokes, you must use device-level overrides to specify the CA server used by the hub. Although the PKI policy references a single PKI enrollment object, the actual CA server represented by this object will differ for the hub, based on the device-level override you define.

You can quickly tell if an object can be overridden by looking for the Overrides column in the objects table in the Policy Object Manager, page 6-4. A green checkmark indicates that you can create overrides for the object; the presence of the column indicates the object type allows overrides.

Related Topics

- Allowing a Policy Object to Be Overridden, page 6-18
- Creating or Editing Object Overrides for a Single Device, page 6-19
- Creating or Editing Object Overrides for Multiple Devices At A Time, page 6-19
- Deleting Device-Level Object Overrides, page 6-21

Allowing a Policy Object to Be Overridden

To create overrides for an object, the object must allow overrides. Not all object types allow overrides.

For those that do allow overrides, you define the object as allowing overrides by selecting **Allow Value Override per Device** when defining the object. After selecting this option, you must click **OK** to save the object before you can define any overrides. For more information on creating objects, see Creating Policy Objects, page 6-9.

You can also configure Security Manager to create device-level overrides for existing objects when you discover policies on devices that you add to the inventory. During discovery, if Security Manager determines that an existing object applies to a discovered policy, but that it is not a perfect fit, the object is used but a device-level override is created to account for the difference. For example, if you run policy discovery on a device that has an ACL with the same name as an ACL policy object in Security Manager, the name of the discovered policy object is reused, but a device-level override is created for the object. If you do not allow device-level overrides during discovery, a new policy object is created with a number appended to the name; this is the default.

To configure Security Manager to allow device overrides during discovery, select **Tools > Security Manager Administration > Discovery** and select **Allow Device Override for Discovered Policy Objects**.

Note To ensure that a specific policy object will be reused for device-level override during discovery, make sure the **Allow Value Override per Device** check box has been selected for the policy object in Policy Object Manager before policy discovery.

Related Topics

- Understanding Policy Object Overrides for Individual Devices, page 6-18
- Creating or Editing Object Overrides for a Single Device, page 6-19
- Creating or Editing Object Overrides for Multiple Devices At A Time, page 6-19
- Deleting Device-Level Object Overrides, page 6-21

Creating or Editing Object Overrides for a Single Device

You can create or edit device-level object overrides from the Device Properties window.

An override specifies a definition for a global object that affects only the selected device. For example, you can override the definition of a AAA server group object so that the object represents a different group of AAA servers for one device than the group it represents for other devices.

Related Topics

- Understanding Policy Object Overrides for Individual Devices, page 6-18
- Allowing a Policy Object to Be Overridden, page 6-18
- Creating or Editing Object Overrides for Multiple Devices At A Time, page 6-19
- Deleting Device-Level Object Overrides, page 6-21

Step 1 (Device view) Right-click a device in the Device selector and select **Device Properties**.

Step 2 Select the object type you want to override from the **Policy Object Overrides** folder.

The table displays all objects of the selected type that can be overridden at the device level. If an object has an override already defined for the device, the Value Overridden? column contains a check mark.

Step 3 Select the object whose override you want to change and do one of the following:

- Click the **Create Override** button, or right-click and select **Create Override**.
- Click the **Edit Override** button, or right-click and select **Edit Override**.

The dialog box for defining that type of object is displayed with the current properties (either the global properties or the local override).

Step 4 Modify the definition of the object and click **OK** to save the device-level override. In the Device Properties window, a green check mark appears in the Value Overridden? column.

Creating or Editing Object Overrides for Multiple Devices At A Time

You can create or edit device-level object overrides from the Policy Object Manager window.

This method enables you to create overrides on multiple devices at the same time, which is especially useful when creating overrides for several devices that participate in the same VPN topology. For example, if the spokes located in one part of the VPN use a different CA server than the spokes located in a different part of the VPN, you can override the PKI enrollment object that defines the server for these devices. This is a more convenient method than selecting each device individually from Device view and defining the override from the Device Properties window.

Related Topics

- Understanding Policy Object Overrides for Individual Devices, page 6-18
- Allowing a Policy Object to Be Overridden, page 6-18
- Creating or Editing Object Overrides for a Single Device, page 6-19
- Deleting Device-Level Object Overrides, page 6-21

Step 1 Select **Manage > Policy Objects** to open the Policy Object Manager, page 6-4.

Step 2 Select the object type you want to override from the table of contents, and then select the object to override.

Tip Not all types of object allow overrides, and not all objects are defined as overridable. Look for a green check mark in the Overridable column. If the object type allows overrides, but this object does not have a check mark, edit the object to enable object override (see Allowing a Policy Object to Be Overridden, page 6-18).

Step 3 Double-click the checkmark, or right-click the object and select **Edit Device Overrides**, to open the Policy Object Overrides Window, page 6-20. The window contains a table listing each device for which an override is defined for the object.

Tip You can also edit the overridable object and click **Edit** next to the Overrides field.

Step 4 Do one of the following:

- To add an override, click the **Create Override** button, select the devices to which you want to apply the override, and define the override.

  The dialog boxes for creating and editing the override are the same ones used to create the object; click the Help button for information specific to the type of object.

  The override you create applies to all policies on the device that use the object; you cannot override the object for one policy but not for another policy.
- To edit an override, select it and click the **Edit Override** button.

Policy Object Overrides Window

Use the Policy Object Overrides window to view a list of all device-level overrides that are defined for the selected object. The content displayed in the table differs depending on the type of object, but it always includes the device name, object description, and category. Sometimes the content of the object is shown, including the overrides.

- To add an override, click the **Create Override** button. In the Create Overrides for Device window, select the devices from the available list and click **>>** to move them to the selected list. When you click **OK**, you are presented with the dialog box for defining your override, which applies to all newly selected devices. (You are not changing the override of the greyed out devices)

  Note The available devices list shows the devices that have not already had overrides defined for the object. Devices with overrides are shown greyed out in the selected devices list.

  The dialog boxes for creating and editing the override are the same ones used to create the object; click the Help button for information specific to the type of object.

  The override you create applies to all policies on the device that use the object; you cannot override the object for one policy but not for another policy.

- To edit an override, select it and click the **Edit Override** button.
- To delete an override, select it and click the **Delete Override** button.

  Deleting an override does not delete the object or remove the object from its device assignment. When you delete the override, the policies on the device that use the object start using the global definition for the object. This changes the meaning of the policies.

Tip You can also create and edit device-level overrides from the Device Properties window of a selected device. Using the Device Properties windows makes it easy for you to manage the overrides for all objects used by a single device. For more information, see Creating or Editing Object Overrides for a Single Device, page 6-19.

Navigation Path

Open the Policy Object Manager, page 6-4. Select an object type that can be overridden (its object page contains a column called Overrides), then do one of the following:

- Double-click the green checkmark in the Overrides column.
- Right-click the object and select **Edit Device Overrides**.
- Edit the overridable object and click **Edit** next to the Overrides field.

Related Topics

- Understanding Policy Object Overrides for Individual Devices, page 6-18
- Allowing a Policy Object to Be Overridden, page 6-18
- Creating or Editing Object Overrides for Multiple Devices At A Time, page 6-19
- Deleting Device-Level Object Overrides, page 6-21
- Filtering Tables, page 1-48
- Filtering Items in Selectors, page 1-45

Deleting Device-Level Object Overrides

Deleting a device-level override restores the global definition of the object to the selected device. You can delete overrides from the Device Properties window or from the Policy Object Manager window:

- Deleting overrides from Device view—Right-click the device and select **Device Properties**, then select the object type from the **Policy Object Overrides** folder. Select the override you want to delete and click **Delete Override**.
- Deleting overrides from the Policy Object Manager—Select the object type from the table of contents, then right-click the object and select **Edit Device Overrides**. Select the override you want to delete and click **Delete Override**.

Related Topics

- Understanding Policy Object Overrides for Individual Devices, page 6-18
- Allowing a Policy Object to Be Overridden, page 6-18
- Policy Object Override Pages, page 3-52
- Policy Object Overrides Window, page 6-20

Overridable Objects in Security Manager

You can override the following objects in Security Manager:

- **VPN Objects**
  - AAA Server group
  - PKI Enrollment (CA Servcers)
  - WINS Server List
  - SSL VPN Customization
  - SAML Identity Provider
  - Web ACL
  - Port Forwarding List
  - Bookmarks
  - Smart Tunnel List
  - Smart Tunnel Network List
  - Smart Tunnel Auto Sign on List
  - Single Sign on Server
  - Reference Identity
- **Firewall Objects**
  - Identity User Group
  - Networks/Hosts
  - Port Lists
  - Security Group
  - Services
  - Access Control Lists (Extended, Standard, Web, Unified)
  - As Path
  - BFD Template
  - Community List

- Credentials
- Identity Policy (IOS)
- Identity User Group
- Interface Roles
- LDAP Attribute Maps
- LDAP Attribute Maps (IOS)
- Policy List
- Prefix List
- Prefix Lists IPV6
- Risk Rating
- Route Map
- Security Group
- Text Objects
- TLS Proxy
- Pool Objects (DHCP V6,IPV4 Pool,IPV6 Pool, MAC Address Pool, NET Pool)
- MAPs (AVP, Regular Expression Groups, Regular Expressions, TCP Maps)
- Class Maps—Inspect (AOL,DCE/RPC,DIAMETER,DNS,eDonkey,FastTrack,FTP,GunTella,H.323(ASA/PIX/FWSM),H.323(IOS), HTTP(ASA/PIX/FWSM),HTTP(IOS),ICQ,IM,IMAP,Kazaa2,MSN Messenger,POP3,Scansafe,SIP(ASA/PIX/FWSM), SIP(IOS),SMTP,SUN RPC, Windows Messenger, Yahoo Messenger)
- Class Maps—Web Filter (Local,N2H2,Trend,Websense)
- Parameter Maps—Inspect (Inspect Parameters, Protocol Info Parameters)
- Parameter Maps—Web Filter(Loal,N2H2,Trend,URL Filter, URLF Glob parameters, Websense)
- Policy Maps—Inspect (DCE/RPC,DIAMETER,DNS,ESMTP,FTP,GTP,H.323(ASA/PIX/FWSM),H.323(IOS),HTTP ASA7.1.x/PIX7.1.x/FWSM3.x/IOS), HTTP(ASA7.2+/PIX7.2+),HTTP(Zone Based IOS),IM(ASA7.2+/PIX7.2+),IM(IOS),IM(Zone Based IOS),IMAP, IP Options, IPSec Pass Trough,IPV6,LISP,M3UA,NetBIOS,P2P,POP3,Scansafe,Sctp,SIP(ASA/PIX/FWSM), SIP(IOS), Skinny, SMTP, SNMP,SUN RPC)
- Policy Maps—Web Filter (Web Filter)

Importing and Exporting Policy Objects

Security Manager includes a Perl script that you can use to export network/host, service, and port list policy objects so that you can import them into another Security Manager server. The information includes device-level overrides for policy objects that have them.

Note The command works with network/host objects that contain IPv4 addresses only. You cannot use the command to import network/host-IPv6 objects.

You can also manually create a CSV file that you can import. For example, you might obtain a list of IP addresses that identify networks or hosts that should be denied entry to your network. You can create a CSV file that will bulk-load the list as one or more network/host objects if that is easier than manually creating the object in the Policy Object Manager.

Tip Besides using this command, you can use other facilities to export and import policy objects that are assigned to shared policies or configured in local device policies. For more information, see the following topics: Exporting the Device Inventory from the Security Manager Client, page 10-6, Exporting Shared Policies, page 10-12, and Importing Policies or Devices, page 10-13

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

perl [*path*]**PolicyObjectImportExport.pl -u** *username* **-p** *password* **-o {import | export}** [**-a** *activity*] **-t** *object_type* **-f** *filename* [**-c {true | false}**] [**-d {true | false}**] [**-e {true | false}**] [**-g {true | false}**] [**-h**]

Syntax

perl [*path*] **PolicyObjectImportExport .pl**	The Perl script command. Include the path to the PolicyObjectImportExport.pl file if the path is not defined in the system path variable. **Tip** If you forget to include the "perl" command, the system accepts the input but does nothing and provides no feedback on your error. Use Ctrl+Z to return to the command prompt.
-u *username*	A Security Manager username. The data exported is limited by the permissions assigned to this user. The user must have Modify Objects permission for the import or export of policy objects, and additionally the Modify Devices permission for the import or export of device-level overrides. If you are importing objects in non-Workflow mode, you must also have Submit and Approve privileges.
-p *password*	The user's password.
-o {import | export}	The type of operation you are performing, either to import policy objects from an existing file, or to export policy objects to a CSV file. Only committed objects are exported.
-a *activity*	(Optional.) The name of a Workflow activity. If you do not specify a name, a new activity is created with the name username_time.
-t *object_type*	Object type, one of the following: • network—For network/host objects. • service—For service objects. • portlist—For port-list objects.
-f *filename*	The name of the CSV file. When exporting, if the file exists, it is overwritten.

-c {true | false}	(Optional.) When importing objects, whether to enable policy object conflict detection. • false—An object is imported even if an existing object has the same content. • true—If an existing object has the same content as an imported object, the imported object is skipped. You must also select **Enforce** for the **When Redundant Objects Detected** option on the Policy Objects Page, page 11-66.
-d {true | false}	(Optional.) How to handle device-level policy object overrides during either an import or export operation: • true—Include all globally-defined objects and all device-level overrides of the objects. • false—Include only the global definitions of the policy objects. Do not include any device-level policy object override information. This is the default.
-e {true | false}	(Optional.) Whether to "flatten" port-list objects in service objects and service-group objects: • true—The names of any port-list objects found in service objects and service-group objects are replaced with the actual ports from the lists. That is, the two objects, port-list and service, or port-list and service-group, are "flattened" into a single service or service-group. Port-list objects are used in Security Manager to group sets of port definitions, and are used when defining service and service-group objects. However, port-list objects are not supported in PRSM. • false—Port-list objects in service and service-group objects are not flattened. This is the default.
-g {true | false}	(Optional.) Whether to include object and object-group types in the CSV file: • true—The final column in the file will be **Type** and it will indicate "Service" or "Network." • false—The Type column is not included. This is the default.
-h	(Optional.) Display the command line help. If you include this option, all other options are ignored.

Importing Policy Objects

When you are importing objects, if an object refers to another object, that object must already be defined in Security Manager, or it must be defined in the same CSV file that you are importing. If the object is in the same CSV file, it must come before the object that refers to it. (Security Manager automatically sorts objects as required when exporting them.)

If Security Manager already has a policy object of the same name as one you are importing, the object is skipped and not imported. The name conflict can even occur if another user has created an object but not yet committed it for public viewing, so you might not be able to see the conflicting object. Security Manager creates only new objects, it does not update existing objects. Use the -c option to specify whether new objects can be created that have the same content as existing objects.

When you run the command, if there are any errors in the file, only the affected objects are not imported. Error messages indicate these problems as they occur, and Security Manager continues evaluating all records in the file. All correctly defined policy objects are imported, and the objects with errors are skipped. The total count and the names of the policy objects that are not imported are shown in the output screen.

After the import command completes, additional actions depend on the Workflow mode you are using:

- Workflow mode—You must log into Security Manager using the same username and password and submit the activity you specified during the import. The activity must be submitted and approved for the changes to take effect.
- Non-Workflow mode—The imported objects are automatically submitted and approved without action on your part. However, you will receive an error if the username you supplied does not have Submit and Approve privileges, and the import operation will fail.

CSV File Format

All objects in a single file are of the same policy object type. The file is in standard comma-separated values (CSV) format. The first line has column headings. Each row represents a single policy object. The columns, left to right, are:

- Name—(Mandatory.) The name of the object.
- Node—The display name of the device on which an override of the policy object is defined. If the policy object is defined on the global level, the field is empty. When importing objects, if the display name does not match a device already in the Security Manager inventory, the object is skipped and not imported.
- Description—The description of the object, if any.
- Category—The category identifier of the object, if any. The category ID is from 10 to 19.
- Allow Override—Whether the object can be overridden. True if the policy object can be overridden on device level, False (or an empty field) if not.
- Group—The names of other policy objects with the same type referenced by this policy object. If there is more than one object, they are separated by commas. For example, network building block Net1 references network building block Net2 and Net3. The Group field of Net1 would have “Net2,Net3” as its value.
- Data—The content of the object.
- Subtype—The object subtype, if any, for network/host and service objects. For an explanation of network/host and service object types, see Understanding Networks/Hosts Objects, page 6-80 and Understanding and Specifying Services and Service and Port List Objects, page 6-100. Possible values are:
  - Blank, or space—The object is a group object, either network/host or service.
  - NH—(Network/host objects only.) Single host network/host object.
  - NF—(Network/host objects only.) Single fully-qualified domain name (FQDN) network/host object.
  - NN—(Network/host objects only.) Single network address network/host object.
  - NR—(Network/host objects only.) Single Address range network/host object.
  - SO—(Service objects only.) Single-service service object.
- Type—The type of object represented by this entry: “Network” or “Service.”

If there is no value for a particular field, that field is blank in the output. If there are multiple values for a field, the field is enclosed in double quotation marks.

Understanding AAA Server and Server Group Objects

You use AAA server objects to identify the AAA servers used in your network. AAA enables devices to determine who the user is (authentication), what the user is permitted to do (authorization), and what the user actually did (accounting), as described below:

- Authentication—Authentication is the way a user is identified before being allowed access to the network and network services. It controls access by requiring valid user credentials, which are typically a username and password. All authentication methods, except for local, line password, and enable authentication, must be defined through AAA. You can use authentication alone or with authorization and accounting.
- Authorization—After authentication is complete, authorization controls the services and commands available to each authenticated user. Authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database can be located locally on the access server or router or it can be hosted remotely on a RADIUS or TACACS+ security server. Were you not to use authorization, authentication alone would provide the same access to services to all authenticated users. You must use authorization together with authentication.
- Accounting—Accounting is used to track the services users are accessing, as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Accounting information includes when sessions start and stop, usernames, the number of bytes that pass through the device for each session, the service used, and the duration of each session. This data can then be analyzed for network management, client billing, or auditing. You can use accounting alone or together with authentication and authorization.

AAA provides an extra level of protection and control for user access over using access rules (ACLs) alone. For example, you can create an access rule allowing all outside users to attempt to use Telnet on a server on the DMZ network. If you want only some users to actually reach the server (and you might not always know the IP addresses of these users, making it impossible to configure simple access rules), you can enable AAA to allow only authenticated or authorized users to make it through the network device (for example, the ASA or router). Thus, users must authenticate before reaching the Telnet server, where Telnet can also require a separate login.

AAA server objects are collected into AAA server group objects. Policies requiring AAA (such as Easy VPN, Remote Access VPNs, and router platform policies such as Secured Device Provisioning and 802.1x) usually refer to AAA server group objects. These objects contain multiple AAA servers that use the same protocol, such as RADIUS or TACACS+. In essence, AAA server groups represent collections of authentication servers focused on enforcing specific aspects of your overall network security policy. For example, you can group those servers dedicated to authenticating internal traffic, external traffic, or remote dial-in users, as well as servers that authorize the administration of your firewall devices.

The following topics describe how to work with AAA server objects:

- Supported AAA Server Types, page 6-28
- Additional AAA Support on ASA, PIX, and FWSM Devices, page 6-28
- Predefined AAA Authentication Server Groups, page 6-30
- Default AAA Server Groups and IOS Devices, page 6-31
- Creating AAA Server Objects, page 6-32
- Add or Edit AAA Server Dialog Box, page 6-33

- Add and Edit LDAP Attribute Map Dialog Boxes, page 6-46
- Creating AAA Server Group Objects, page 6-48

Supported AAA Server Types

You can use AAA servers that use the RADIUS protocol with all devices, and the TACACS+ and LDAP protocols with all devices except IPS. For ASA, PIX, and FWSM devices, you can also use the protocols described in Additional AAA Support on ASA, PIX, and FWSM Devices, page 6-28

- **RADIUS**—Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco devices and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

  You can use RADIUS with other AAA security protocols, such as TACACS+, Kerberos, and local username lookup, depending on what is supported by a particular device type. RADIUS is supported on all Cisco platforms, but some RADIUS-supported features run only on specified platforms.

  Beginning with Cisco Security Manager 4.17, IPv6 is enabled in RADIUS protocol. This support is applicable only for ASA 9.9.2 devices and above. Users can now configure IPv6 Host Address for Radius authentication in the Add AAA Server dialog box (see, Add or Edit AAA Server Dialog Box). Activity validation is also introduced for unsupported device version.
- **TACACS+**—Terminal Access Controller Access Control System (TACACS+) is a security application that provides centralized validation of users attempting to gain access to a router or network access server. The goal of TACACS+ is to provide a methodology for managing multiple network access points from a single management service.

  TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service independently.
- **LDAP**—Lightweight Directory Access Protocol (LDAP). The use of LDAP servers is specific to certain policies. For example, identity firewall configurations on ASA, VPN configurations on ASA, and ScanSafe configurations on IOS devices. For more information on using LDAP on ASA, see Additional AAA Support on ASA, PIX, and FWSM Devices, page 6-28.

Related Topics

- Additional AAA Support on ASA, PIX, and FWSM Devices, page 6-28
- Creating AAA Server Objects, page 6-32
- Understanding AAA Server and Server Group Objects, page 6-27

Additional AAA Support on ASA, PIX, and FWSM Devices

Note From version 4.17, though Cisco Security Manager continues to support PIX and FWSM features/functionality, it does not support any enhancements.

In addition to supporting RADIUS and TACACS+, ASA, PIX 7.0+, and FWSM 3.1+ devices can support AAA servers running the following protocols. For more information, see the explanation of AAA usage in the configuration guides for the device type and operating system version that interests you.

- **Kerberos**—These devices can use Kerberos servers for authentication. 3DES, DES, and RC4 encryption types are supported.
- **NT**—These devices can use Windows Domain servers for NTLMv1 authentication.
- **SDI Servers**—SecureID servers from RSA Security, Inc. are known as SDI servers. When a user attempts to establish VPN access and the applicable tunnel-group policy specifies an SDI authentication server group, the ASA device sends the username and one-time password to the SDI server. The device then grants or denies user access based on the response from the server. Version 5.0 of SDI introduced the concept of SDI primary and secondary servers that share a single-node secret file (SECURID). As a result, when you configure an SDI server as a AAA server object, you must specify whether the server is version 5.0 or an earlier version.
- **LDAP**—These devices can use Lightweight Directory Access Protocol (LDAP) servers for VPN authorization and user group identification for identity-aware firewall policies. These devices support LDAP version 3 and are compatible with any v3 or v2 directory server. However, password management is supported only on the Sun Microsystems JAVA System Directory Server and the Microsoft Active Directory.

  With any other type of LDAP server (such as Novell or OpenLDAP), all LDAP functions are supported except for password management. Therefore, if someone tries to log in to one of these devices using one of these other servers for authentication and their password has expired, the device drops the connection and a manual password reset is required.

  You can configure Simple Authentication and Security Layer (SASL) mechanisms to authenticate an LDAP client (in this case, the ASA, PIX, or FWSM device) to an LDAP server. These devices and LDAP servers can support multiple mechanisms. If both mechanisms (MD5 and Kerberos) are available, the ASA, PIX, or FWSM device uses the stronger mechanism, Kerberos, for authentication.

  When user authentication for VPN access has succeeded and the applicable tunnel-group policy specifies an LDAP authorization server group, the ASA, PIX, or FWSM device queries the LDAP server and applies the authorizations it receives to the VPN session.
- **HTTP-Form**—These devices can use the HTTP Form protocol for single sign-on (SSO) authentication of WebVPN users only. Single sign-on support lets WebVPN users enter a username and password only once to access multiple protected services and Web servers. The WebVPN server running on the security appliance acts as a proxy for the user to the authenticating server. When a user logs in, the WebVPN server sends an SSO authentication request, including username and password, to the authenticating server using HTTPS. If the server approves the authentication request, it returns an SSO authentication cookie to the WebVPN server. The security appliance keeps this cookie on behalf of the user and uses it to authenticate the user to secure websites within the domain protected by the SSO server.

The following table describes the AAA services that are supported by each protocol:

Table 6-5 AAA Services Supported by ASA, PIX, and FWSM Devices

	Database Type							
AAA Service	**Local**	**RADIUS**	**TACACS +**	**SDI**	**NT**	**Kerberos**	**LDAP**	**HTTP Form**
Authentication of...								
VPN users	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[1]
Firewall sessions	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Administrators	Yes	Yes	Yes	Yes[2]	Yes	Yes	Yes	No

Table 6-5 AAA Services Supported by ASA, PIX, and FWSM Devices (continued)

AAA Service	Database Type							
	Local	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP	HTTP Form
Authorization of...								
VPN users	Yes	Yes	No	No	No	No	Yes	No
Firewall sessions	No	Yes[3]	Yes	No	No	No	No	No
Administrators	Yes[4]	No	Yes	No	No	No	No	No
Accounting of...								
VPN connections	No	Yes	Yes	No	No	No	No	No
Firewall sessions	No	Yes	Yes	No	No	No	No	No
Administrators	No	Yes[5]	Yes	No	No	No	No	No

1. HTTP Form protocol supports single sign-on (SSO) authentication for WebVPN users only.
2. SDI is not supported for HTTP administrative access.
3. For firewall sessions, RADIUS authorization is supported with user-specific ACLs only, which are received or specified in a RADIUS authentication response.
4. Local command authorization is supported by privilege level only.
5. Command accounting is available for TACACS+ only.

Related Topics

- Supported AAA Server Types, page 6-28
- Creating AAA Server Objects, page 6-32
- Understanding AAA Server and Server Group Objects, page 6-27

Predefined AAA Authentication Server Groups

There are several predefined AAA server groups that define an authentication method without specifying particular AAA servers. In policies such as IPSec proposals, you can use these predefined server groups to define the types of AAA authentication to perform and the order in which to perform them.

Table 6-6 on page 6-30 describes the predefined AAA authentication server groups.

Table 6-6 Predefined AAA Authentication Server Groups

Name	Description
Enable	Uses the enable password defined on the device for authentication.
KRB5 KRB5-Telnet	Uses Kerberos 5 for authentication. Use KRB5-Telnet when using Telnet to connect. For Cisco IOS routers, you can use Kerberos 5 client configuration only on selected platforms running IOS Software versions that support this protocol. Server configuration is not supported. The device must include an Advanced series feature set (k9 crypto image).
If-Authenticated	Uses the if-authenticated method, which allows the user to access the requested function if the user is authenticated.

Table 6-6 Predefined AAA Authentication Server Groups (continued)

Name	Description
Line	Uses the line password defined on the device for authentication.
Local Local-case	Uses the local username database (defined on the device) for authentication. Use Local-case if you want the login to be case-sensitive.
None	Uses no authentication.
RADIUS TACACS+	Use RADIUS or TACACS+ authentication. (Does not apply to Cisco IOS routers.) These AAA server groups do not contain any AAA servers. To use one of them when defining a policy, you must create a device-level override and define the AAA servers to associate with the group. For more information, see Creating or Editing Object Overrides for a Single Device, page 6-19.

Related Topics

- Creating AAA Server Group Objects, page 6-48
- Default AAA Server Groups and IOS Devices, page 6-31
- Understanding AAA Server and Server Group Objects, page 6-27

Default AAA Server Groups and IOS Devices

IOS software enables you to define AAA servers either as members of AAA server groups or as individual servers. Security Manager, however, requires all AAA servers to belong to a AAA server group.

Therefore, when you discover an IOS device whose device configuration contains individual AAA servers that do not belong to a AAA server group, Security Manager creates the following server groups to contain these servers:

- For RADIUS: CSM-rad-grp
- For TACACS+: CSM-tac-grp

Both of these special AAA server groups are marked in the Policy Object Manager as the default groups for their protocol. This is indicated by the **Make this Group the Default AAA Server Group** check box.

These groups are created solely for the purpose of management by Security Manager. During deployment, the AAA servers in these special groups are deployed back to the IOS device as individual servers, *not* as part of the group.

You can also create your own default group. The default group can be used in most cases, except when you need to configure multiple AAA server groups that use the same protocol. For example, you might want to define multiple RADIUS groups so that one group can be used for authentication and another group for authorization. Service providers may want to define multiple groups with the same protocol in order to provide customer separation when using VRF.

Note If you use one of these default AAA server groups in a policy defined for a PIX/ASA/FWSM device, the AAA servers are deployed as a group to that device, not as individual servers. This is because all AAA servers on PIX/ASA/FWSM devices must belong to a AAA server group.

Caution We recommend that you use caution when using these default AAA server groups in a policy definition. There are certain commands (for example, **ip radius** and **ip tacacs**, which are configured using the Interface field in the AAA Server dialog box) that can be defined once for each AAA server group and once for all individual AAA servers. Because the AAA servers in the default group are deployed to IOS devices as individual servers, you might inadvertently change the **ip radius** or **ip tacacs** settings for all the individual AAA severs configured on the device, including servers that are not being managed by Security Manager (and whose configurations would otherwise be left undisturbed).

Related Topics

- Predefined AAA Authentication Server Groups, page 6-30
- Creating AAA Server Group Objects, page 6-48
- Understanding AAA Server and Server Group Objects, page 6-27

Creating AAA Server Objects

You can create AAA server objects to populate the AAA server group objects that are referenced by policies such as AAA rules, Easy VPN, and 802.1x. In some cases, AAA server objects are used directly by a policy, such as in AAA policies on IPS devices.

When creating a AAA server object, you must specify the IP address or DNS name of the external AAA server and the protocol used by the server. The other settings required depend on the protocol.

Note On PIX/ASA/FWSM devices, AAA objects in a device configuration that are not referenced by any policies are removed from the device during the next deployment. However, the predefined AAA objects named RADIUS and TACACS+ are never removed from PIX 6.3 devices, even if they are not referenced by any policies.

Related Topics

- Creating Policy Objects, page 6-9
- Supported AAA Server Types, page 6-28
- Additional AAA Support on ASA, PIX, and FWSM Devices, page 6-28
- Understanding AAA Server and Server Group Objects, page 6-27

Step 1 Select **Manage > Policy Objects** to open the Policy Object Manager (see Policy Object Manager, page 6-4).

Step 2 Select **AAA Servers** from the Object Type selector.

Step 3 Right-click in the work area, then select **New Object** to open the Add or Edit AAA Server Dialog Box, page 6-33.

Step 4 Enter a name for the object and optionally a description of the object.

Step 5 Identify the AAA server:

- In the Host field, enter the IP address or for ASA or PIX 7.2+ devices, the host name of the AAA server. You can also enter the name of a network/host object that contains the host IP address, or click **Select** to select the object.

- Optionally, in the Interfaces field, enter the name of an interface or an interface role (which must resolve to a single interface name on the device) whose IP address should be used for all outgoing RADIUS or TACACS+ packets. Do not specify an interface for objects used on an IPS device.
- Optionally, enter the amount of time to wait until a AAA server is considered unresponsive.

Step 6 Select the protocol used by the AAA server and configure protocol-specific properties. You can use RADIUS with all device types, and TACACS+ with all device types except for IPS devices. You can use the Kerberos, LDAP, NT, SDI, and HTTP-FORM protocols only with ASA, PIX 7.x+, and FWSM 3.1+ devices.

For details about the properties, see the following topics:

- RADIUS—See AAA Server Dialog Box—RADIUS Settings, page 6-35.
- TACACS+—See AAA Server Dialog Box—TACACS+ Settings, page 6-38.
- Kerberos—See AAA Server Dialog Box—Kerberos Settings, page 6-39.
- LDAP—See AAA Server Dialog Box—LDAP Settings, page 6-40.
- NT—See AAA Server Dialog Box—NT Settings, page 6-43.
- SDI—See AAA Server Dialog Box—SDI Settings, page 6-43.
- HTTP-FORM—See AAA Server Dialog Box—HTTP-FORM Settings, page 6-44.

Step 7 (Optional) Under Category, select a category to help you identify this object in the Objects table. See Using Category Objects, page 6-13.

Step 8 Click **OK** to save the object.

Add or Edit AAA Server Dialog Box

Use Add or Edit AAA Server dialog box to create, copy, and edit a AAA server object. These objects are collected into AAA server group objects and identify the AAA servers that you want to use when defining various AAA policies. In some cases these objects are used directly in a AAA policy.

For a description of the protocols you can use, see Supported AAA Server Types, page 6-28 and Additional AAA Support on ASA, PIX, and FWSM Devices, page 6-28.

Note You cannot edit the protocol if the object is already included in a AAA server group.

Navigation Path

Select **Manage > Policy Objects**, then select **AAA Servers** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Creating AAA Server Objects, page 6-32
- Understanding AAA Server and Server Group Objects, page 6-27
- Policy Object Manager, page 6-4

Field Reference

Table 6-7 AAA Server Dialog Box—General Settings

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-9.
Description	An optional description of the object.
Host	The address of the AAA server to which authentication requests will be sent. Specify one of the following: • IP Address—The IPv4 or IPv6 address of the AAA server. You can also enter the name of a network/host object that contains the host IP address, or click **Select** to select the object. **Note** AAA- IPV6 hosts are only supported for the LDAP and TACACS+ protocols. Beginning with Cisco Security Manager 4.17, IPv6 hosts for the Radius protocol are supported on ASA 9.9(2) devices onwards. • DNS Name (for PIX/ASA 7.2+ devices only)—The DNS hostname of the AAA server, up to 128 characters. The hostname can contain alphanumeric characters and hyphens, but each element of the hostname must begin and end with an alphanumeric character.
Interface	The interface whose IP address should be used for all outgoing RADIUS or TACACS packets (known as the source interface). Enter the name of an interface or interface role, or click **Select** to select it from a list or to create a new interface role. **Tips** • If you enter the name of an interface, make sure the policy that uses this AAA object is assigned to a device containing an interface with this name. • If you enter the name of an interface role, make sure the role represents a single interface, not multiple interfaces. • Only one source interface can be defined for the AAA servers in a AAA server group. An error is displayed when you submit your changes if different AAA servers in the group use different source interfaces. See Creating AAA Server Group Objects, page 6-48. • You cannot specify an interface name for a AAA server used on an IPS device.

Table 6-7 AAA Server Dialog Box—General Settings (continued)

Element	Description
Timeout	The amount of time to wait for a response to a request until the AAA server is considered unresponsive. If there are other servers in the group, the next server is tried. • Cisco IOS routers—The range is 1-1000 seconds. The default is 5 seconds. • ASA/PIX 7.x+, FWSM 3.1+ devices—The range is 1-300 seconds. The default is 10 seconds. • PIX 6.3 firewalls—The range is 1-512 seconds. The default is 5 seconds. • IPS devices—The range is 1-512 seconds. The default is 3 seconds.
Protocol	The protocol used by the AAA server. The fields below the protocol list change depending on your selection. For specific information about the fields, see the topics indicated. • The following protocols are the most common: – RADIUS—All device types. See AAA Server Dialog Box—RADIUS Settings, page 6-35. – TACACS+—All device types except IPS. See AAA Server Dialog Box—TACACS+ Settings, page 6-38. • The following protocols are supported for ASA/PIX 7.x+ and FWSM 3.1+ devices; LDAP is supported on IOS devices that support ScanSafe policies: – Kerberos—See AAA Server Dialog Box—Kerberos Settings, page 6-39. – LDAP—See AAA Server Dialog Box—LDAP Settings, page 6-40. – NT—See AAA Server Dialog Box—NT Settings, page 6-43. – SDI—See AAA Server Dialog Box—SDI Settings, page 6-43. – HTTP-FORM—See AAA Server Dialog Box—HTTP-FORM Settings, page 6-44.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.

AAA Server Dialog Box—RADIUS Settings

Use the RADIUS settings in the AAA Server dialog box to configure a RADIUS AAA server object.

Navigation Path

Go to the Add or Edit AAA Server Dialog Box, page 6-33 and select **RADIUS** in the Protocol field.

Related Topics

- Creating AAA Server Objects, page 6-32

- Understanding AAA Server and Server Group Objects, page 6-27
- AAA Server Group Dialog Box, page 6-49

Field Reference

Table 6-8 AAA Server Dialog Box—RADIUS Settings

Element	Description
Key Confirm	The shared secret that is used to encrypt data between the network device (client) and AAA server. The key is a case-sensitive, alphanumeric string of up to 127 characters. Special characters are permitted. The key you define in this field must match the key on the RADIUS server. Enter the key again in the Confirm field. Note the following: • A key is required for AAA server objects used in an IPS AAA policy. Otherwise, the key is optional. • Spaces are not permitted on PIX, ASA, or FWSM devices. Otherwise, they are permitted. • If you do not define a key, all traffic between the AAA server and its AAA clients is sent unencrypted.
Authentication/Authorization Port	The port on which AAA authentication and authorization are performed. The default is 1645. **Tip** The default port for IPS devices is 1812, so you need to change this value if you are configuring the object for IPS and you want to use the default port.
Accounting Port	The port on which AAA accounting is performed. The default is 1646.

Table 6-8 AAA Server Dialog Box—RADIUS Settings (continued)

Element	Description
RADIUS Password Confirm (ASA, PIX 7.x+, and FWSM 3.x+ devices only.)	A case-sensitive, alphanumeric keyword of up to 127 characters that is common among users who access this RADIUS authorization server through this device. Enter the password again in the Confirm field. The RADIUS authorization server requires a password and username for each connecting user. The RADIUS server administrator must configure the RADIUS server to associate this password with each user authorizing to the server through this device. Be sure to provide this information to your RADIUS server administrator. If you do not specify a common user password, each user password is the username. Never use a RADIUS authorization server for authentication. Common passwords or usernames as passwords are less secure than assigning unique user passwords. **Tips** • The password applies to authorization servers only, not to authentication servers. For an authentication RADIUS servers, do not configure a common password. • Although the password is required by the RADIUS protocol and the RADIUS server for authorization, users do not need to know it. The device provides the password automatically.
Retry Interval (ASA, PIX 7.x+, and FWSM 3.x+ devices only.)	The interval between attempts to contact the AAA server. Values are: • ASA/FWSM devices—1 to 10 seconds. • PIX devices—1 to 5 seconds.

Table 6-8 AAA Server Dialog Box—RADIUS Settings (continued)

Element	Description
ACL Netmask Convert (ASA, PIX 7.x+, and FWSM 3.x+ devices only.)	The method for handling the netmask expressions that are contained in downloadable ACLs received from the RADIUS server. The ASA/PIX/FWSM expects downloadable ACLs to contain standard netmask expressions whereas devices using Cisco IOS Software expect downloadable ACLs to contain wildcard netmask expressions, which are the reverse of a standard netmask expression. A wildcard mask has ones in bit positions to ignore, zeros in bit positions to match. Translation of wildcard netmask expressions means that downloadable ACLs written for Cisco IOS routers can be used by ASA/PIX/FWSM devices without altering the configuration of the ACLs on the RADIUS server. Select one of the following options: • Standard—The security appliance assumes that all downloadable ACLs received from the RADIUS server contain only standard netmask expressions. No translation from wildcard netmask expressions is performed. This is the default. • Auto-Detect—The security appliance tries to determine the type of netmask expression used in the downloadable ACL. If it detects a wildcard netmask expression, it converts it to a standard netmask expression. This option is useful when you are uncertain how the RADIUS server is configured; however, wildcard netmask expressions with holes in them cannot be unambiguously detected and converted. For example, the wildcard netmask 0.0.255.0 permits anything in the third octet, but the device might not detect this expression as a wildcard netmask. • Wildcard—The security appliance assumes that all downloadable ACLs received from the RADIUS server contain only wildcard netmask expressions, which it converts to standard netmask expressions.

AAA Server Dialog Box—TACACS+ Settings

Use the TACACS+ settings in the AAA Server dialog box to configure a TACACS+ AAA server object.

Navigation Path

Go to the Add or Edit AAA Server Dialog Box, page 6-33 and select **TACACS+** in the Protocol field.

Related Topics

- Creating AAA Server Objects, page 6-32
- Understanding AAA Server and Server Group Objects, page 6-27
- AAA Server Group Dialog Box, page 6-49

Field Reference

Table 6-9 AAA Server Dialog Box—TACACS+ Settings

Element	Description
Key Confirm	The shared secret that is used to encrypt data between the client and the AAA server. The key is a case-sensitive, alphanumeric string of up to 127 characters (U.S. English). Spaces and special characters are permitted. The key you define in this field must match the key on the TACACS+ server. Enter the key again in the Confirm field. Note the following: • Activity validation fails if you try defining a key with a space on a PIX, ASA, or FWSM device. • If you do not define a key, all traffic between the AAA server and its AAA clients is sent unencrypted.
Server Port	The port used for communicating with the AAA server. The default is 49.

AAA Server Dialog Box—Kerberos Settings

Use the Kerberos settings in the AAA Server dialog box to configure a Kerberos AAA server object.

Note This type of AAA server can be configured only on ASA, PIX 7.x+, and FWSM 3.1+ devices.

Navigation Path

Go to the Add or Edit AAA Server Dialog Box, page 6-33 and select **Kerberos** in the Protocol field.

Related Topics

- Creating AAA Server Objects, page 6-32
- Understanding AAA Server and Server Group Objects, page 6-27
- AAA Server Group Dialog Box, page 6-49

Field Reference

Table 6-10 AAA Server Dialog Box—Kerberos Settings

Element	Description
Server Port	The port used for communicating with the AAA server. The default is 88.
Kerberos Realm Name	The name of the realm containing the Kerberos authentication server and ticket granting server (maximum of 64 characters, typically all uppercase). For example, EXAMPLE.COM.
Retry Interval	The interval between attempts to contact the AAA server. Values range from 1 to 10 seconds.

AAA Server Dialog Box—LDAP Settings

Use the LDAP settings in the AAA Server dialog box to configure an LDAP AAA server object.

Note This type of AAA server can be configured only on ASA, PIX 7.x+, FWSM 3.1+, and IOS devices.

Navigation Path

Go to the Add or Edit AAA Server Dialog Box, page 6-33 and select **LDAP** in the Protocol field.

Related Topics

- Creating AAA Server Objects, page 6-32
- Understanding AAA Server and Server Group Objects, page 6-27
- AAA Server Group Dialog Box, page 6-49

Field Reference

Table 6-11 AAA Server Dialog Box—LDAP Settings

Element	Description
Enable LDAP over SSL/Secure Communication	Whether to establish a secure SSL connection between the device and the LDAP server. **Tip** You must select this option when using a Microsoft Active Directory LDAP server in order to enable password management.
No Negotiation (IOS only.)	When selected, this checkbox precludes further negotiation and moves to accept the channels previously established and accepted.
Server Port	The port used for communicating with the AAA server. The default is 389.
Login Directory	The name of the username or directory object in the LDAP hierarchy used for authenticated binding (maximum of 128 characters). Authenticated binding is required by some LDAP servers (including the Microsoft Active Directory server) before other LDAP operations can be performed. This field describes the authentication characteristics of the device. These characteristics should correspond to those of a user with administrator privileges. This string is case-sensitive. Spaces are not permitted in the string, but other special characters are allowed. Typically, this is a username such as DOMAIN\Administrator. However, you can use the more traditional format too, for example, cn=Administrator,OU=Employees,DN=example,DN=com.
Login Password	The case-sensitive, alphanumeric password for accessing the LDAP server (maximum of 64 characters). Spaces are not allowed.
Encrypted (IOS)	Whether the login password is encrypted.

Table 6-11 AAA Server Dialog Box—LDAP Settings (continued)

Element	Description
LDAP Hierarchy Location	The base distinguished name (DN), which is the location in the LDAP hierarchy where the authentication server should being searching when it receives an authorization request. For example, OU=Cisco. The maximum length is 128 characters. The string is case-sensitive. Spaces are not permitted, but other special characters are allowed.
PIX/ASA/FWSM Tab	
LDAP Scope	The extent of the search the server should make in the LDAP hierarchy when it receives an authorization request. The available options are: • onelevel—Searches only one level beneath the base DN. This type of search scope is faster than a subtree search, because it is less comprehensive. This is the default. • subtree—Searches all levels beneath the base DN (that is, searches the entire subtree hierarchy). This option takes more time.
LDAP Distinguished Name	The Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server. Common naming attributes are Common Name (CN), sAMAccountName, userPrincipalName, and User ID (uid). The case-sensitive, alphanumeric string can be up to 128 characters. Spaces are not permitted in the string, but other special characters are allowed.
SASL MD5 Authentication SASL Kerberos Authentication Kerberos Server Group	These options establish a Simple Authentication and Security Layer (SASL) mechanism to authenticate an LDAP client (the ASA/PIX/FWSM device) with an LDAP server. If you do not select one of these options, the simple mechanism is used, and usernames and passwords are transmitted in clear text. You can define one or both SASL authentication mechanisms. When negotiating SASL authentication, the ASA/PIX/FWSM device retrieves the list of SASL mechanisms configured on the LDAP server and selects the strongest mechanism configured on both devices. • SASL MD5 Authentication—Whether to have the device send the LDAP server an MD5 value computed from the username and password. You must configure the LDAP server to store the user passwords in reversible manner, or the LDAP server will not be able to validate the passwords. • SASL Kerberos Authentication—Whether to have the device send the LDAP server the username and realm using the GSSAPI (Generic Security Services Application Programming Interface) Kerberos mechanism. This mechanism is stronger than the MD5 mechanism. If you select Kerberos, you must also enter the name of the Kerberos AAA server group used for SASL authentication. The maximum length is 16 characters.

Table 6-11 AAA Server Dialog Box—LDAP Settings (continued)

Element	Description
LDAP Server Type	The type of LDAP server used for AAA: • Auto-Detect—The ASA/PIX/FWSM device tries to determine the server type automatically. This is the default. • Microsoft—The LDAP server is a Microsoft Active Directory server. **Note** You must configure LDAP over SSL to enable password management with Microsoft Active Directory. • Sun—The LDAP server is a Sun Microsystems JAVA System Directory Server. • OpenLDAP—The server is an Open LDAP server. You can use this only with ASA/PIX 8.0+ devices. • Novell—The server is a Novell LDAP server. You can use this only with ASA/PIX 8.0+ devices.
LDAP Attribute Map	The LDAP attribute configuration to bind to the LDAP server. Enter the name of an LDAP attribute map policy object or click **Select** to select it from a list or to create a new object. LDAP attribute maps take the attribute names that you define and map them to Cisco-defined attributes. For more information, see Add and Edit LDAP Attribute Map Dialog Boxes, page 6-46.
Group Base DN	(Microsoft LDAP AD servers only.) The base designated name (DN) under which all user groups are defined. When the ASA contacts the AD server for user group membership, the search starts at this DN. All groups must reside under this DN in the LDAP directory hierarchy and no group can reside outside of this path, or the group will not be found. Specifying this location can decrease the time required to complete user group searches. The alphanumeric string is case-sensitive and can be up to 128 characters. Spaces are not permitted in the string, but other special characters are allowed. For example: DN=cisco,DN=com **Tip** If you do not specify the group base DN, the LDAP Distinguished Name setting is used as the starting point for group searches.
Group Search Timeout	(Microsoft LDAP AD servers only.) The maximum time to wait for a response from an Active Directory server queried for user group information, in seconds. The default is 10 seconds, the range is 1 to 300 seconds.
IOS Tab	
Secure Cipher	The encryption method to be used.
Attribute Map (IOS)	The name of the IOS attribute map the server employs.
Secure Trust Point	The name of a trust point for certificates.

Table 6-11 AAA Server Dialog Box—LDAP Settings (continued)

Element	Description
Authentication bind-first	You can configure the sequence of search and bind of an authentication request with this option. The default is search first and then bind.
No Authorization Required	No authorization required for authentication requests.
Authentication Compare	Select this checkbox to replace the bind request with compare request for authentication. By default authentication request is performed with bind request.
User Object Filter	Specify the search filter user attribute type to be used in a search request. This helps in filtering out the requested user being searched.

AAA Server Dialog Box—NT Settings

Use the NT settings in the AAA Server dialog box to configure an NT AAA server object.

Note This type of AAA server can be configured only on ASA, PIX 7.x+, and FWSM 3.1+ devices.

Navigation Path

Go to the Add or Edit AAA Server Dialog Box, page 6-33 and select **NT** in the Protocol field.

Related Topics

- Creating AAA Server Objects, page 6-32
- Understanding AAA Server and Server Group Objects, page 6-27
- AAA Server Group Dialog Box, page 6-49

Field Reference

Table 6-12 AAA Server Dialog Box—NT Settings

Element	Description
Server Port	The port used for communicating with the AAA server. The default is 139.
NT Authentication Host	The name of the authentication domain controller hostname (maximum of 16 characters).

AAA Server Dialog Box—SDI Settings

Use the SDI settings in the AAA Server dialog box to configure an SDI AAA server object.

Note This type of AAA server can be configured only on ASA, PIX 7.x+, and FWSM 3.1+ devices.

Navigation Path

Go to the Add or Edit AAA Server Dialog Box, page 6-33 and select **SDI** in the Protocol field.

Related Topics

- Creating AAA Server Objects, page 6-32
- Understanding AAA Server and Server Group Objects, page 6-27
- AAA Server Group Dialog Box, page 6-49

Field Reference

Table 6-13 AAA Server Dialog Box—SDI Settings

Element	Description
Server Port	The port used for communicating with the AAA server. The default is 5500.
Retry Interval	The interval between attempts to contact the AAA server. Values range from 1 to 10 seconds. The default is 10 seconds.
SDI Server Version	The SDI server version: • SDI-pre-5—All SDI versions before version 5.0 • SDI-5—SDI version 5.0 or later.
SDI pre-5 Secondary Server	(Optional) A secondary server to be used for authentication if the primary server fails when using an SDI version prior to 5.0. Enter the IP address or the name of a network/host object, or click **Select** to select an object or create a new one.

AAA Server Dialog Box—HTTP-FORM Settings

Use the HTTP-FORM settings in the AAA Server dialog box to configure an HTTP-Form AAA server object for single sign-on authentication (SSO).

Note This type of AAA server can be configured only on ASA, PIX 7.x+, and FWSM 3.1+ devices.

Navigation Path

Go to the Add or Edit AAA Server Dialog Box, page 6-33 and select **HTTP-FORM** in the Protocol field.

Related Topics

- Creating AAA Server Objects, page 6-32
- Understanding AAA Server and Server Group Objects, page 6-27
- AAA Server Group Dialog Box, page 6-49

Field Reference

Table 6-14 AAA Server Dialog Box—HTTP-Form Settings

Element	Description
Start URL	The URL from which the WebVPN server of the security appliance should retrieve an optional pre-login cookie. The maximum URL length is 1024 characters. The authenticating web server might execute a pre-login sequence by sending a Set-Cookie header along with the login page content. The URL in this field defines the location from which the cookie is retrieved. **Note** The actual login sequence starts after the pre-login cookie sequence.
Action URI	The Uniform Resource Identifier (URI) that defines the location and name of the authentication program on the web server to which the security appliance sends HTTP POST requests for single sign-on (SSO) authentication. The maximum length of the action URI is 2048 characters. **Tip** You can discover the action URI on the authenticating web server by connecting to the web server's login page directly with a browser. The URL of the login web page displayed in your browser is the action URI for the authenticating web server.
Username Parameter	The name of the username parameter included in HTTP POST requests for SSO authentication. The maximum length is 128 characters. At login, the user enters the actual name value, which is entered into the HTTP POST request and passed on to the authenticating web server.
Password Parameter	The name of the password parameter included in HTTP POST requests for SSO authentication. The maximum length is 128 characters. At login, the user enters the actual password value, which is entered into the HTTP POST request and passed on to the authenticating web server.
Hidden Values	The hidden parameters included in HTTP POST requests for SSO authentication. They are referred to as hidden parameters because, unlike the username and password, they are not visible to the user. The maximum length of the hidden parameters is 2048 characters. **Tip** You can discover the hidden parameters that the authenticating web server expects in POST requests by using an HTTP header analyzer on a form received from the web server.
Authentication Cookie Name	The name of the authentication cookie used for SSO by the security appliance. The maximum length is 128 characters. If SSO authentication succeeds, the authenticating web server passes this authentication cookie to the client browser. The client browser then authenticates to other web servers in the SSO domain by presenting this cookie.

Add and Edit LDAP Attribute Map Dialog Boxes

Use the Add and Edit LDAP (Lightweight Directory Access Protocol) Attribute Map dialog boxes to populate the attribute map with name mappings that translate Cisco LDAP attribute names to custom, user-defined attribute names.

If you are introducing a security appliance to an existing LDAP directory, your existing custom LDAP attribute names and values are probably different from the Cisco attribute names and values. Rather than renaming your existing attributes, you can create LDAP attribute maps that map your custom attribute names and values to Cisco attribute names and values. By using simple string substitution, the security appliance then presents you with only your own custom names and values. You can then bind these attribute maps to LDAP servers or remove them as needed. You can also delete entire attribute maps or remove individual name and value entries.

For more information regarding LDAP support on ASA, PIX, and FWSM devices, see Additional AAA Support on ASA, PIX, and FWSM Devices, page 6-28.

Navigation Path

Select **Manage > Policy Objects**, then select **LDAP Attribute Map** from the Object Type selector. Right-click inside the table and select **New Object**, or right-click a row and select **Edit Object**.

Related Topics

- Creating AAA Server Objects, page 6-32
- AAA Server Dialog Box—LDAP Settings, page 6-40

Field Reference

Table 6-15 Add and Edit LDAP Attribute Map Dialog Boxes

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-9.
Description	An optional description of the object.
Attribute Map table	The table shows the mapped values. Each entry shows the customer map name, Cisco map name, and the attribute mapping of customer name to Cisco name. • To add a mapping, click the **Add Row** button to open the Add and Edit LDAP Attribute Map Value Dialog Boxes, page 6-47. • To edit a mapping, select it and click the **Edit Row** button. • To delete a mapping, select it and click the **Delete Row** button.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.

Table 6-15 Add and Edit LDAP Attribute Map Dialog Boxes (continued)

Element	Description
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add and Edit LDAP Attribute Map Value Dialog Boxes

Use the Add and Edit LDAP Attribute Map Value dialog boxes to populate the attribute map with value mappings that apply user-defined attribute values to the custom attribute name and to the matching Cisco attribute name and value.

Navigation Path

From the Add and Edit LDAP Attribute Map Dialog Boxes, page 6-46, click the **Add Row** button to add a new mapping, or select a row and click the **Edit Row** button.

Field Reference

Table 6-16 Add and Edit LDAP Attribute Map Value Dialog Boxes

Element	Description
Customer Map Name	The name of your attribute map that relates to the Cisco map.
Cisco Map Name	The Cisco attribute map name you want to map to the customer map name.
Customer to Cisco Map Value table	The mappings of customer names to Cisco names. • To add a mapping, click the **Add Row** button to open the Add and Edit Map Value Dialog Boxes, page 6-47. • To edit a mapping, select it and click the **Edit Row** button. • To delete a mapping, select it and click the **Delete Row** button.

Add and Edit Map Value Dialog Boxes

Use the Add and Edit Map Value dialog boxes to map a customer LDAP attribute value to a Cisco map value. Enter the value from your LDAP map that you want to equate with a Cisco value.

Navigation Path

From the Add and Edit LDAP Attribute Map Value Dialog Boxes, page 6-47, click the **Add Row** button to add a new mapping, or select a row and click the **Edit Row** button.

Creating AAA Server Group Objects

You can create AAA server group objects for Security Manager policies requiring AAA services, such as authentication and authorization. Each AAA server group object can contain multiple AAA servers, all of which use the same protocol, such as RADIUS or TACACS+. For example, if you want to use RADIUS to authenticate network access and TACACS+ to authenticate CLI access, you must create at least two AAA server group objects, one for RADIUS servers and one for TACACS+ servers.

In addition, only one source interface can be defined for the AAA servers in the group. An error is displayed when you submit your changes if different AAA servers in the group use different source interfaces.

Note The error is triggered by the actual interface defined as the source, not the name of the interface role that represents the interface. That is, two AAA servers can have different interface roles defined as the source interface as long as they both resolve to the same device interface. An error is also displayed if the interface role defined for the source interface matches more than one actual interface on the device.

The number of AAA server group objects that can be created and the number of AAA server objects that can be included in each group object depend on the selected platform. For example, ASA devices support up to 18 single-mode server groups (with up to 16 servers each) and 7 multi-mode server groups (with up to 4 servers each). PIX firewalls support up to 14 server groups, each containing up to 14 servers.

Note Security Manager includes a predefined AAA server group object that you can use when you perform authentication locally inside the Cisco IOS router.

Tip You can also create AAA server group objects when you define policies or objects that use this object type. For more information, see Selecting Objects for Policies, page 6-2.

Related Topics

- Creating Policy Objects, page 6-9
- Predefined AAA Authentication Server Groups, page 6-30
- Default AAA Server Groups and IOS Devices, page 6-31
- Understanding AAA Server and Server Group Objects, page 6-27

Step 1 Select **Manage > Policy Objects** to open the Policy Object Manager (see Policy Object Manager, page 6-4).

Step 2 Select **AAA Server Groups** from the Object Type selector.

Step 3 Right-click inside the work area, then select **New Object** to open the AAA Server Group Dialog Box, page 6-49.

Step 4 Enter a name for the object. The maximum name length is 16 characters if you plan to use this object with ASA, PIX, or FWSM devices and 128 characters for Cisco IOS routers. Spaces are not supported.

Note Cisco IOS routers do not support the following AAA server group names: RADIUS, TACACS, TACACS+. In addition, we do not recommend using an abbreviation of one of these names, such as rad or tac.

Step 5 Select the protocol to be used by the servers in the group.

Step 6 Enter the names of the AAA server policy objects that define the AAA servers to include in the group. Click **Select** to select the objects from a list filtered by the protocol you selected. You can also create new AAA server objects from the selection list. Separate multiple objects with commas.

Step 7 Configure the additional options that you want:

- Make this Group the Default AAA Server Group—For IOS devices only, whether you are using this group as the default group. Use this option if you intend to have a single global server group for this protocol for all policies requiring AAA. For more information, see Default AAA Server Groups and IOS Devices, page 6-31.
- ASA 8.4(2+) devices—If you are creating a RADIUS group containing Active Directory agent servers, select **AD Agent Mode**. This option indicates that the servers in the group are not full-function RADIUS servers but instead provide AD agent functions for identity-aware firewall. Use this group in the Identity Options policy.
- ASA, PIX, FWSM devices—Select options for how to handle AAA servers that stop responding, and for how to send accounting messages. For more information, see AAA Server Group Dialog Box, page 6-49.

Step 8 (Optional) Under Category, select a category to help you identify this object in the Objects table. See Using Category Objects, page 6-13.

Step 9 (Optional) Select **Allow Value Override per Device** to allow the properties of this object to be redefined on individual devices. See Allowing a Policy Object to Be Overridden, page 6-18.

Step 10 Click **OK** to save the object.

AAA Server Group Dialog Box

Use the AAA Server Group dialog box to create, copy, and edit AAA server groups. When defining a policy that uses a AAA server for authentication, authorization, or accounting, you select the server by selecting the server group to which the server belongs.

Navigation Path

Select **Manage > Policy Objects**, then select **AAA Server Groups** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Creating AAA Server Group Objects, page 6-48
- Understanding AAA Server and Server Group Objects, page 6-27
- Creating Policy Objects, page 6-9
- Add or Edit AAA Server Dialog Box, page 6-33
- Policy Object Manager, page 6-4

Field Reference

Table 6-17 AAA Server Group Dialog Box

Element	Description
Name	The object name (up to 16 characters when using this object with firewall devices; up to 128 characters for Cisco IOS routers). Object names are not case-sensitive. Spaces are not supported. Consider the following important points: • Cisco IOS routers do not support AAA server groups named RADIUS, TACACS, or TACACS+. In addition, we do not recommend using an abbreviation of one of these names, such as rad or tac. • If you define this AAA server group as the RADIUS or TACACS+ default group, any name you define here is automatically replaced in the device configuration by the default name (RADIUS or TACACS+) upon deployment.
Description	An optional description of the object.
Protocol	The protocol used by the AAA servers in the group. For more information about these options, see Supported AAA Server Types, page 6-28 and Additional AAA Support on ASA, PIX, and FWSM Devices, page 6-28.
AAA Servers	The AAA server policy objects that comprise the server group. Enter the names of the objects or click **Select** to select them from a list that is filtered to show only those AAA server objects that use the selected protocol. Separate multiple objects with commas. You can also create new objects from the selection list.
Make this Group the Default AAA Server Group (IOS) (IOS devices only.)	Whether to designate this AAA server group as the default group for the RADIUS or TACACS+ protocol. Select this option if you intend to use a single global group for the selected protocol for all policies on a specific device requiring AAA. Do not select this option if you intend to create multiple RADIUS or TACACS+ AAA server groups. Multiple groups can be used to separate different AAA functions (for example, use one group for authentication and a different group for authorization) or to separate different customers in a VRF environment. **Note** When you discover an IOS router, any AAA servers in the device configuration that are not members of a AAA server group are placed in special groups called CSM-rad-grp (for RADIUS) and CSM-tac-grp (for TACACS+), both of which are marked as default groups. These two groups are created solely to enable Security Manager to manage these servers. During deployment, the AAA servers in these special groups are deployed back to the device as individual servers. For more information, see Default AAA Server Groups and IOS Devices, page 6-31.

Table 6-17 AAA Server Group Dialog Box (continued)

Element	Description
AD Agent Mode (ASA 8.4(2+) devices only.)	Whether the servers in the group are Active Directory agents, which are used in identity-aware firewall configurations. You must select this option for an AD agent group to indicate that the group is not a full-function RADIUS server group. Use the AD agent group in the Identity Options policy. For more information, see Identifying Active Directory Servers and Agents, page 13-8.
Dynamic Authorization (ASA 9.2(1+) devices only.)	When using the RADIUS protocol, select the Dynamic Authorization check box to enable the RADIUS Dynamic Authorization Change of Authorization (CoA) services for the AAA server group. Specify the listening port for RADIUS CoA requests in the Port field. The valid range is 1024 to 65535 and the default value is 1700. Once defined, the corresponding RADIUS server group will be registered for CoA notification and the ASA will listen to the port for the CoA policy updates from the Cisco Identity Services Engine (ISE).
Interim Account Update (ASA 9.2(1+) devices only.)	When using the RADIUS protocol, select the Interim Account Update check box to enable the generation of RADIUS interim-accounting-update messages. Currently these messages are only generated when a VPN tunnel connection is added to a clientless VPN session. When this happens the accounting update is generated in order to inform the RADIUS server of the newly assigned IP address. Specify the length, in hours, of the interval between periodic accounting updates in the Interval field. The valid range is 1 to 120 and the default value is 24.
Authorize only (ASA 9.2(1+) devices only.)	When using the RADIUS protocol, select the Authorize only check box to enables authorize-only mode for the RADIUS server group. When this check box is selected, the common password configured for individual AAA servers is not required and does not need to be configured.
Max Failed Attempts (PIX, ASA, FWSM devices only.)	The number of connection failures that will be tolerated for any given server in the server group before that server is deactivated. The default is 3 attempts, the range is 1 to 5.
Internal Realm ID (ASA 9.8(1) and above devices only)	Enter a realm ID that corresponds to the RADIUS or LDAP protocol for the AAA server group policy object. **Note** The realm ID is a unique value in the range of 1-65535; it is only applicable for RADIUS and LDAP protocols.

Table 6-17 AAA Server Group Dialog Box (continued)

Element	Description
Reactivation Mode (PIX, ASA, FWSM devices only.)	The method to use when reactivating failed servers in the group: • Depletion—Reactivate failed servers only after all of the servers in the group are inactive. This is the default. When a server is deactivated, it remains inactive until all other servers in the group are inactive. When and if this occurs, all servers in the group are reactivated. This approach minimizes the occurrence of connection delays due to failed servers. If you configured a fallback method using the local database (for management access only) and all the servers in the group fail to respond, then the group is considered to be unresponsive, and the fallback method is tried. You can configure the Reactivation Deadtime value to determine the number of minutes that will elapse between the disabling of the last server in the group and the subsequent re-enabling of all servers. If you do not have a fallback method, the device continues to retry the servers in the group. • Timed—Reactivate failed servers after 30 seconds of downtime. This option is useful if the first server in the group is the primary server and you prefer that it be used whenever possible rather than the backup servers. This policy breaks down in the case of UDP servers. Because a connection to a UDP server will not fail, even if the server is not present, UDP servers are put back on line blindly. This could lead to slowed connection times or connection failures if a server group contains multiple servers that are not reachable.
Reactivation Deadtime (PIX, ASA, FWSM devices only.)	When you select **Depletion** as the reactivation mode, the number of minutes that should elapse between the deactivation of the last server in the group and the reactivation of all the servers in the group. The default is 10, the range is 0 to 1440 minutes (24 hours).
Group Accounting Mode (PIX, ASA, FWSM devices only.)	When using the RADIUS or TACACS+ protocols, the method for sending accounting messages to the AAA servers in the group: When using the server group for accounting (the protocol must be RADIUS or TACACS+), the method for sending accounting messages to the AAA servers in the group: • Single—Accounting messages are sent to a single server in the group. This is the default. • Simultaneous—Accounting messages are sent to all servers in the group simultaneously. If you select this option, the ASA forces the use of **Timed** as the reactivation mode.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.

Table 6-17 AAA Server Group Dialog Box (continued)

Element	Description
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Creating Access Control List Objects

An Access Control List (ACL) object is made up of one or more access control entries (ACEs), one or more ACL objects, or a combination of both. Each ACE is an individual permit or deny statement within an ACL. You can use ACL policy objects in several other policies and policy objects.

Beginning with Cisco Security Manager version 4.13, if an object group contains VM attribute and if it is applied to any other policies (except Access Rules), the deployment will fail. The VM Attribute Object is only applicable to the devices, which are ASA 9.7.1 or later, and when object-group-search access-control is enabled.

You can create the following types of ACL objects:

- Extended – Extended ACLs enable you to specify source and destination addresses and service (or traffic protocol), and, based on the protocol type, the ports (for TCP or UDP), or the ICMP type (for ICMP) can be specified. For information on extended ACL objects, see Creating Extended Access Control List Objects, page 6-54.
- Standard – Standard ACLs use the source address for matching traffic. For information on standard ACL objects, see Creating Standard Access Control List Objects, page 6-56.
- Web – Web ACLs use destination address and port or a URL filter. For information on Web Type ACL objects, Creating Web Access Control List Objects, page 6-57.
- Unified – Unified ACL objects let you use source networks/hosts, source security groups, users, destination source networks/hosts, destination security groups, and services to match traffic. Further, the network/host specifications can contain IPv4 addresses, IPv6 addresses, or a combination of both. (With the release of Security Manager 4.4 and the ASA 9.0+, the separate IPv4 and IPv6 addressing/objects were “unified.”) See Creating Unified Access Control List Objects, page 6-58 for more information these ACLs.
- Ethertype – EtherType ACLs apply to non-IP layer-2 traffic on bridge group member interfaces only, in routed and transparent modes. You can use these rules to permit or drop traffic based on the EtherType value in the layer-2 packet.With EtherType ACLs, you can control the flow of non-IP traffic across the device. See Configuring Transparent Firewall Rules, page 23-1

For reference information about the dialog boxes used with these objects, see Add or Edit Access List Dialog Boxes, page 6-59.

Creating Extended Access Control List Objects

Extended access control lists allow you to permit or deny traffic from specific IP addresses to specific destination IP address and port, and specify the protocol of the traffic, such as ICMP, TCP, UDP, and so forth. Extended ACLs range from 100 to 199, and for devices running Cisco IOS Software Release 12.0.1 and later, 2000 to 2699.

Extended ACL example:

```
access-list 110 - Applied to traffic leaving the office (outgoing)
access-list 110 permit tcp 10.128.2.0 0.0.0.255 any eq 80
```

ACL 110 permits traffic originating from any address on the 10.128.2.0 network. The "All-IPv4-Addresses" statement means that the traffic is allowed to have any destination address with the limitation of going to port 80. The value of 0.0.0.0/255.255.255.255 can be specified as "All-IPv4-Addresses."

Uses:

- Identifying addresses for NAT (policy NAT and NAT exemption)—Policy NAT lets you identify local traffic for address translation by specifying the source and destination addresses and ports in an extended access list. Regular NAT can only consider local addresses. An access list that is used with policy NAT cannot be configured to deny an access control entry (ACE).
- Identifying addresses for IOS dynamic NAT—For user-defined ACLs, the NAT plug-in generates its own ACL CLIs when deducing NAT traffic from VPN traffic.
- Filtering traffic that will be intercepted by Network Admission Control (NAC).
- Identifying traffic in a traffic class-map for modular policy—Access lists can be used to identify traffic in a class-map, which is used for features that support Modular Policy Framework such as TCP and general connection settings, inspection, IPS, and QoS. You can use one or more access lists to identify specific types of traffic.
- For transparent mode, enabling protocols that are blocked by a routed mode security appliance, including BGP, DHCP, and multicast streams. Because these protocols do not have sessions on the security appliance to allow return traffic, these protocols also require access lists on both interfaces.
- Establishing VPN access—You can use an extended access list in VPN commands to identify the traffic that should be tunneled on the device for an IPsec site-to-site tunnel or to identify the traffic that should be tunneled on the device for a VPN client. Use in conjunction with the policy objects and settings shown in Table 6-18 on page 6-54:

Table 6-18 Policy Objects and Settings

Policy Object	Device	Purpose
VPN Topology	Any	Selecting Protected Networks.
ASA User Group	ASA	Inbound Firewall Policy; Outbound Firewall Policy; Filter ACL.
Traffic Flow	ASA, PIX 7+	Service Policy Rules (MPC). The traffic flow BB (class-map) uses Extended ACL as one of its traffic match types.
User Group	• IOS • Catalyst 6500/7600 • PIX 6.3	For Easy VPN, Split Tunnel ACL and Firewall ACL (IOS devices only).

Related Topics

- Creating Access Control List Objects, page 6-53
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Creating Policy Objects, page 6-9
- Understanding Networks/Hosts Objects, page 6-80
- Understanding and Specifying Services and Service and Port List Objects, page 6-100

Step 1 Choose **Manage > Policy Objects** to open the Policy Object Manager (see Policy Object Manager, page 6-4).

Step 2 From the Object Type selector, select **Access Control Lists**.

The Access Control List page appears. The Extended tab is displayed by default.

Step 3 Right-click inside the work area, then select **New Object**.

The Add Extended Access List dialog box appears (see Add or Edit Access List Dialog Boxes, page 6-59).

Step 4 Enter a name for the object and optionally a description of the object.

Note Make sure that the name of the ACL Object is unique and is not the same name as the Firewall Rules ACL defined in the Firewall ACL Setting. For more information, see Firewall ACL Setting Dialog Box, page 16-26.

Step 5 Right-click inside the table in the dialog box, then select **Add**.

The Add Extended Access Control Entry dialog box appears.

Step 6 Create the access control entry:

- If you choose **Access Control Entry** for Type, specify the characteristics of the traffic that you want to match and whether you are permitting or denying the traffic. Enter the source addresses whence the traffic originates, the destination addresses whither the traffic travels, and the services that define the characteristics of the traffic. Click **Advanced** to define logging options. For detailed information about the fields on the dialog box, see Add and Edit Extended Access Control Entry Dialog Boxes, page 6-61.
- If you choose **ACL Object**, select the object in the available objects list and click **>>** to add it to the list of selected objects.

Step 7 Click **OK** to save your changes.

The dialog box closes and you return to the Add Extended Access List page. The new entry is shown in the table. If necessary, select it and click the up or down buttons to position it at the desired location.

Step 8 (Optional) Under Category, select a category to help you identify this object in the Objects table. See Using Category Objects, page 6-13.

Step 9 Click **OK** to save the object.

Creating Standard Access Control List Objects

A standard access control list allows you to permit or deny traffic from specific IP addresses. The destination of the packet and the ports involved can be anything. Standard IP ACLs range from 1 to 99.

Standard ACL example:

```
access-list 10 permit 192.168.2.0 0.0.0.255
```

Uses:

- Identifying OSPF route redistribution.
- Filtering users of a community string using SNMP.
- Configuring VLAN ACLs for a Catalyst 6500/7600 device.

Related Topics

- Creating Access Control List Objects, page 6-53
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Creating Policy Objects, page 6-9
- Understanding Networks/Hosts Objects, page 6-80

Step 1 Choose **Manage > Policy Objects** to open the Policy Object Manager (see Policy Object Manager, page 6-4).

Step 2 From the Object Type selector, select **Access Control Lists**.

The Access Control List page appears.

Step 3 Click the **Standard** tab.

Step 4 Right-click inside the work area, then select **New Object**.

The Add Standard Access List dialog box appears (see Add or Edit Access List Dialog Boxes, page 6-59).

Step 5 Enter a name for the object and optionally a description of the object.

Note Make sure that the name of the ACL Object is unique and is not the same name as the Firewall Rules ACL defined in the Firewall ACL Setting. For more information, see Firewall ACL Setting Dialog Box, page 16-26.

Step 6 Right-click inside the table, then select **Add**.

The Add Standard Access Control Entry dialog box appears.

Step 7 Create the access control entry:

- If you choose **Access Control Entry** for Type, specify the characteristics of the traffic that you want to match and whether you are permitting or denying the traffic. Enter the source addresses whence the traffic originates and select logging options. For detailed information about the fields on the dialog box, see Add and Edit Standard Access Control Entry Dialog Boxes, page 6-64.
- If you choose **ACL Object**, select the object in the available objects list and click **>>** to add it to the list of selected objects.

Step 8 Click **OK** to save your changes.

The dialog box closes and you return to the Add Standard Access List dialog box. The new entry is shown in the table. If necessary, select it and click the up or down buttons to position it at the desired location.

Step 9 (Optional) Under Category, select a category to help you identify this object in the Objects table. See Using Category Objects, page 6-13.

Step 10 Click **OK** to save the object.

Creating Web Access Control List Objects

Web ACLs, also referred to as WebVPN, let you establish a secure, remote-access VPN tunnel to the security appliance using a web browser. There is no need for either a software or hardware client. WebVPN provides easy access to a broad range of web resources and both web-enabled and legacy applications from almost any computer that can reach HTTPS Internet sites. WebVPN uses Secure Socket Layer Protocol and its successor, Transport Layer Security (SSL/TLS) to provide a secure connection between remote users and specific, supported internal resources that you configure at a central site.

The following table presents examples of Web VPN ACLs.

Table 6-19 Examples of Web VPN ACLs

Action	Filter	Effect
Deny	url http://*.yahoo.com/	Denies access to all of Yahoo!
Deny	url cifs://fileserver/share/directory	Denies access to all files in the specified location.
Deny	url https://www.company.com/directory/file.html	Denies access to the specified file.
Permit	url https://www.company.com/directory	Permits access to the specified location
Deny	url http://*:8080/	Denies HTTPS access to anywhere via port 8080.
Deny	url http://10.10.10.10	Denies HTTP access to 10.10.10.10.
Permit	url any	Permits access to any URL. Usually used after an ACL that denies url access.

Uses:

- As a filter ACL in an ASA User Group policy object (under SSL VPN > Clientless).

Related Topics

- Creating Access Control List Objects, page 6-53
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Creating Policy Objects, page 6-9

Step 1 Choose **Manage > Policy Objects** to open the Policy Object Manager (see Policy Object Manager, page 6-4).

Step 2 From the Object Type selector, select **Access Control Lists**.

The Access Control List page appears.

Step 3 Click the **Web** tab.

Step 4 Right-click inside the work area and select **New Object**.

The Add WebType Access List dialog box appears (see Add or Edit Access List Dialog Boxes, page 6-59).

Step 5 Enter a name for the object and optionally a description of the object.

Note Make sure that the name of the ACL Object is unique and is not the same name as the Firewall Rules ACL defined in the Firewall ACL Setting. For more information, see Firewall ACL Setting Dialog Box, page 16-26.

Step 6 Right-click inside the access control entry table and choose **Add**.

The Add Web Access Control Entry dialog box appears.

Step 7 Create the access control entry:

- If you choose **Access Control Entry** for Type, specify the characteristics of the traffic that you want to match and whether you are permitting or denying the traffic. You can filter based on the network destination of the traffic (Network Filter) or the web address (URL Filter). For detailed information about the fields on the dialog box, see Add and Edit Web Access Control Entry Dialog Boxes, page 6-65.
- If you choose **ACL Object**, select the object in the available objects list and click **>>** to add it to the list of selected objects.

Step 8 Click **OK** to save your changes.

The dialog box closes and you return to the Add WebType Access List page. The new entry is shown in the table. If necessary, select it and click the up or down buttons to position it at the desired location.

Step 9 (Optional) Under Category, select a category to help you identify this object in the Objects table. See Using Category Objects, page 6-13.

Step 10 Click **OK** to save the object.

Creating Unified Access Control List Objects

A unified access control list allows you to permit or deny traffic from specific networks, hosts, security groups, and users, destined for specific networks, hosts and security groups. You also specify the service(s) involved.

Related Topics

- Creating Access Control List Objects, page 6-53
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Creating Policy Objects, page 6-9

- Understanding Networks/Hosts Objects, page 6-80

Step 1 Choose **Manage > Policy Objects** to open the Policy Object Manager (see Policy Object Manager, page 6-4).

Step 2 From the Object Type selector, select **Access Control Lists**.

The Access Control List page appears.

Step 3 Click the **Unified** tab.

Step 4 Right-click inside the work area, then select **New Object**.

The Add Unified Access List dialog box appears (see Add or Edit Access List Dialog Boxes, page 6-59).

Step 5 Enter a name for the object and optionally a description of the object.

Note Make sure that the name of the ACL Object is unique and is not the same name as the Firewall Rules ACL defined in the Firewall ACL Setting. For more information, see Firewall ACL Setting Dialog Box, page 16-26.

Step 6 Right-click inside the table in the dialog box, then choose **Add**.

The Add Unified Access Control Entry dialog box appears.

Step 7 Create the access control entry:

- If you choose **Access Control Entry** for Type, specify the characteristics of the traffic that you want to match and whether you are permitting or denying the traffic. Enter the source addresses whence the traffic originates and select logging options. For detailed information about the fields on the dialog box, see Add and Edit Unified Access Control Entry Dialog Boxes, page 6-67.
- If you choose **ACL Object**, select the object in the available objects list and click **>>** to add it to the list of selected objects.

Step 8 Click **OK** to save your changes.

The dialog box closes and you return to the Add Unified Access List dialog box. The new entry is shown in the table. If necessary, select it and click the up or down buttons to position it at the desired location.

Step 9 (Optional) Under Category, select a category to help you identify this object in the Objects table. See Using Category Objects, page 6-13.

Step 10 Click **OK** to save the object.

Add or Edit Access List Dialog Boxes

Use the Add and Edit Access List dialog boxes to define access control entries (ACEs) for an ACL object. From this page, you can change the order of the ACEs and ACL objects within the table, add or edit ACEs and ACL objects, and delete ACEs and ACL objects.

The title of the dialog box indicates the type of ACL you are creating: Extended, Standard, or Web Type. The dialog boxes are essentially the same, the difference being the columns displayed in the ACE table.

Navigation Path

Select **Manage > Policy Objects**, then select **Access Control Lists** from the Object Type selector. Select the tab for the type of ACL object you want to create, and then right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Creating Access Control List Objects, page 6-53
- Creating Extended Access Control List Objects, page 6-54
- Creating Standard Access Control List Objects, page 6-56
- Creating Web Access Control List Objects, page 6-57
- Contiguous and Discontiguous Network Masks for IPv4 Addresses, page 6-81
- Understanding Networks/Hosts Objects, page 6-80
- Understanding and Specifying Services and Service and Port List Objects, page 6-100

Field Reference

Table 6-20 Add and Edit Access List Dialog Boxes

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-9.
Description	An optional description of the object.

Table 6-20 Add and Edit Access List Dialog Boxes (continued)

Element	Description
Access Control Entry table	The access control entries (ACEs) and ACL objects that are part of the ACL. The table displays the name of the entry or object, description, options, services, and other attributes of the entry. In the Permit column, a green checkmark indicates that the entry permits traffic (typically, the traffic is considered a match for the service you are defining), whereas a red circle with a slash indicates that traffic is denied (typically, the traffic is considered to not match, and the service you are defining is not applied to the denied traffic). The source and, if applicable, destination addresses can be host IP addresses, network addresses, or network/host policy objects. • To add an ACE, click the Add button and fill in the dialog box for the type of ACL you are creating: – Add and Edit Extended Access Control Entry Dialog Boxes, page 6-61 – Add and Edit Standard Access Control Entry Dialog Boxes, page 6-64 – Add and Edit Web Access Control Entry Dialog Boxes, page 6-65 • To edit an ACE, select it and click the Edit button. • To delete an ACE, select it and click the Delete button. • To change the position of an entry, select it and click the Up/Down arrow buttons as required. Entries are evaluated top to bottom, so correct positioning is crucial for you to get the results you intend.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add and Edit Extended Access Control Entry Dialog Boxes

Use the Add or Edit Extended Access Control Entry dialog box to add an access control entry (ACE) or an ACL object to an Extended ACL object.

Navigation Path

From the Add or Edit Access List Dialog Boxes, page 6-59 for Extended ACL objects, click the **Add** button in the ACE table, or select a row and click the **Edit** button.

Related Topics

- Creating Extended Access Control List Objects, page 6-54

- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Understanding Networks/Hosts Objects, page 6-80
- Understanding and Specifying Services and Service and Port List Objects, page 6-100
- Filtering Items in Selectors, page 1-45

Field Reference

Table 6-21 Add and Edit Extended Access Control Entry Dialog Boxes

Element	Description
Type	The type of entry you are adding. The fields on the dialog box change based on your selection. • Access Control Entry—You want to define an ACE. • ACL Objects—You want to include an existing ACL object. You are presented with a list of available ACL objects. Select the objects you want to include and click the >> button to move them to the list of selected objects. You can remove an object by selecting it and clicking <<. You can also edit objects in the selected objects list.
Action	The action to take on traffic defined in the entry: • Permit—The service associated with this ACL is applied to this traffic. That is, the traffic is permitted to use the service. • Deny—The service associated with this ACL is not applied to this traffic. If there are multiple ACLs configured for a service, denied traffic is typically compared to the next ACL in the list; if it matches no permit entry in any ACL for the service, the service is not applied to the traffic. Whether the traffic is dropped from the network depends on the service.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.

Table 6-21 Add and Edit Extended Access Control Entry Dialog Boxes (continued)

Element	Description
Source Destination	The source or destination of the traffic. You can enter more than one value by separating the items with commas. You can enter any combination of the following address types. For more information, see Specifying IP Addresses During Policy Definition, page 6-87. • Network/host object. Enter the name of the object or click **Select** to select it from a list. You can also create new network/host objects from the selection list. (ASA 8.4(2+) only.) You can select FQDN network/host objects to select traffic based on fully-qualified host names. • Host IP address, for example, 10.10.10.100. • Network address, including subnet mask, in either the format 10.10.10.0/24 or 10.10.10.0/255.255.255.0. • A range of IP addresses, for example, 10.10.10.100-10.10.10.200. • An IP address pattern in the format 10.10.0.10/255.255.0.255, where the mask is a discontiguous bit mask (see Contiguous and Discontiguous Network Masks for IPv4 Addresses, page 6-81).
Users	(ASA 8.4(2+) only.) The Active Directory (AD) usernames, user groups, or identity user group objects for the rule, if any. The user specification is conjoined to the source address to limit the match to user addresses within the source address range. You can enter more than one value by separating the items with commas. You can enter any combination of the following values. • Individual user names: NetBIOS_DOMAIN\username • User groups (note the double \): NetBIOS_DOMAIN\\user_group • Identity user group object names. Click **Select** to select objects, users, or user groups from a list or to create new objects. For more information, see: • Selecting Identity Users in Policies, page 13-21 • Configuring Identity-Based Firewall Rules, page 13-21 • Creating Identity User Group Objects, page 13-19
Services	The services that define the type of traffic to act on. You can enter more than one value by separating the items with commas. You can enter any combination of service objects and service types (which are typically a protocol and port combination). If you type in a service, you are prompted as you type with valid values. You can select a value from the list and press Enter or Tab. For complete information on how to specify services, see Understanding and Specifying Services and Service and Port List Objects, page 6-100.

Table 6-21 Add and Edit Extended Access Control Entry Dialog Boxes (continued)

Element	Description
Description	An optional description of the object.
Advanced button	Click this button to define logging options for the entry: • For PIX, ASA, and FWSM devices, you can enable: – Default logging—If a packet is denied, message 106023 is generated. If a packet is permitted, no message is generated. – Per ACE logging—If a packet is denied, message 106100 is generated. You can select the logging severity level for the messages, and the interval (in seconds from 1 to 600) for generating messages. • For IOS devices, when you enable logging, informational messages about packets that match the entry are sent to the console. You can also elect to include the input interface and source MAC address or VC in the logging output.

Add and Edit Standard Access Control Entry Dialog Boxes

Use the Add or Edit Standard Access Control Entry dialog box to add an access control entry (ACE) or an ACL object to a Standard ACL object.

Navigation Path

From the Add or Edit Access List Dialog Boxes, page 6-59 for Standard ACL objects, click the **Add** button in the ACE table, or select a row and click the **Edit** button.

Related Topics

- Creating Standard Access Control List Objects, page 6-56
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Understanding Networks/Hosts Objects, page 6-80
- Understanding and Specifying Services and Service and Port List Objects, page 6-100
- Filtering Items in Selectors, page 1-45

Field Reference

Table 6-22 Add and Edit Standard Access Control Entry Dialog Boxes

Element	Description
Type	The type of entry you are adding. The fields on the dialog box change based on your selection. • Access Control Entry—You want to define an ACE. • ACL Objects—You want to include an existing ACL object. You are presented with a list of available ACL objects. Select the objects you want to include and click the >> button to move them to the list of selected objects. You can remove an object by selecting it and clicking <<. You can also edit objects in the selected objects list.

Table 6-22 Add and Edit Standard Access Control Entry Dialog Boxes (continued)

Element	Description
Action	The action to take on traffic defined in the entry: • Permit—The service associated with this ACL is applied to this traffic. That is, the traffic is permitted to use the service. • Deny—The service associated with this ACL is not applied to this traffic. If there are multiple ACLs configured for a service, denied traffic is typically compared to the next ACL in the list; if it matches no permit entry in any ACL for the service, the service is not applied to the traffic. Whether the traffic is dropped from the network depends on the service.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Source	The source of the traffic. You can enter more than one value by separating the items with commas. You can enter any combination of the following address types. For more information, see Specifying IP Addresses During Policy Definition, page 6-87. • Network/host object. Enter the name of the object or click **Select** to select it from a list. You can also create new network/host objects from the selection list. • Host IP address, for example, 10.10.10.100. • Network address, including subnet mask, in either the format 10.10.10.0/24 or 10.10.10.0/255.255.255.0. • A range of IP addresses, for example, 10.10.10.100-10.10.10.200. • An IP address pattern in the format 10.10.0.10/255.255.0.255, where the mask is a discontiguous bit mask (see Contiguous and Discontiguous Network Masks for IPv4 Addresses, page 6-81).
Description	An optional description of the object.
Log Option	Whether to create log entries when traffic meets the entry criteria. ACL logging generates syslog message 106023 for denied packets. Deny packets must be present to log denied packets.

Add and Edit Web Access Control Entry Dialog Boxes

Use the Add or Edit Web Access Control Entry dialog box to add an access control entry (ACE) or an ACL object to a Web Type ACL object.

Navigation Path

From the Add or Edit Access List Dialog Boxes, page 6-59 for Web Type ACL objects, click the **Add** button in the ACE table, or select a row and click the **Edit** button.

Related Topics

- Creating Web Access Control List Objects, page 6-57
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5

- Understanding Networks/Hosts Objects, page 6-80
- Understanding and Specifying Services and Service and Port List Objects, page 6-100
- Filtering Items in Selectors, page 1-45

Field Reference

Table 6-23 Add and Edit Web Access Control Entry Dialog Boxes

Element	Description
Type	The type of entry you are adding. The fields on the dialog box change based on your selection. • Access Control Entry—You want to define an ACE. • ACL Objects—You want to include an existing ACL object. You are presented with a list of available ACL objects. Select the objects you want to include and click the >> button to move them to the list of selected objects. You can remove an object by selecting it and clicking <<. You can also edit objects in the selected objects list.
Action	The action to take on traffic defined in the entry: • Permit—The service associated with this ACL is applied to this traffic. That is, the traffic is permitted to use the service. • Deny—The service associated with this ACL is not applied to this traffic. If there are multiple ACLs configured for a service, denied traffic is typically compared to the next ACL in the list; if it matches no permit entry in any ACL for the service, the service is not applied to the traffic. Whether the traffic is dropped from the network depends on the service.
Filter Destination	Whether the entry specifies a network filter (host or network address) or a URL filter (web site address). Your selection changes the fields on the dialog box. The fields are described below.
Destination (Network Filter only.)	The destination of the traffic. You can enter more than one value by separating the items with commas. You can enter any combination of the following address types. For more information, see Specifying IP Addresses During Policy Definition, page 6-87. • Network/host object. Enter the name of the object or click **Select** to select it from a list. You can also create new network/host objects from the selection list. • Host IP address, for example, 10.10.10.100. • Network address, including subnet mask, in either the format 10.10.10.0/24 or 10.10.10.0/255.255.255.0. • A range of IP addresses, for example, 10.10.10.100-10.10.10.200. • An IP address pattern in the format 10.10.0.10/255.255.0.255, where the mask is a discontiguous bit mask (see Contiguous and Discontiguous Network Masks for IPv4 Addresses, page 6-81).

Table 6-23 Add and Edit Web Access Control Entry Dialog Boxes (continued)

Element	Description
Ports (Network Filter only.)	The port numbers or port list policy objects that define the port the traffic uses, if you want to use port identification. You can enter more than one value by separating the items with commas. You can enter any combination of the following types: • Port list object. Enter the name of the object or click **Select** to select it from a list. You can also create new port list objects from the selection list. • Port number, for example, 80. • A range of ports, for example, 80-90.
URL Filter (URL Filter only.)	The Universal Resource Locator (URL), or web address, of the traffic. You can use an asterisk as a match-all wildcard. For example, http://*.cisco.com matches all servers on the cisco.com network. You can specify any valid URL.
Logging	The type of logging to use for this entry: • Select Log Disabled to not create log entries. • Select Default to use the default settings on the device. • All other available options enable logging and identify the log level that will be used.
Logging Interval	The interval of time, in seconds, used to generate logging messages, from 1 to 600. The default is 300. You can modify this field only if you select a logging level in the Logging field.
Time Range	The time range policy object that defines the time range associated with the entry. The time range defines the access to the device and relies on the device's system clock. For more information, see Configuring Time Range Objects, page 6-71. Enter the name of the object or click **Select** to select it from a list. You can also create new time range objects from the selection list. **Note** Time range is not supported on FWSM 2.x or PIX 6.3 devices.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Description	An optional description of the object.

Add and Edit Unified Access Control Entry Dialog Boxes

Use the Add or Edit Unified Access Control Entry dialog box to add an access control entry (ACE) or an ACL object to a Unified ACL object.

Navigation Path

From the Add or Edit Access List Dialog Boxes, page 6-59 for Unified ACL objects, click the **Add** button in the ACE table, or select a row and click the **Edit** button.

Related Topics

- Creating Unified Access Control List Objects, page 6-58
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Understanding Networks/Hosts Objects, page 6-80
- Understanding and Specifying Services and Service and Port List Objects, page 6-100
- Filtering Items in Selectors, page 1-45

Field Reference

Table 6-24 Add and Edit Unified Access Control Entry Dialog Boxes

Element	Description
Type	The type of entry; the fields in the dialog box change based on your choice: • Access Control Entry—You want to define an ACE. • ACL Objects—You want to include one or more existing ACL objects. You are presented with a list of available ACL objects. Select the objects you want to include and click the **>>** button to move them to the list of selected objects. You can remove an object by selecting it and clicking **<<**. You can also edit an object in the selected objects list.
Action	The action to take on traffic defined in the entry: • Permit—The Services associated with the ACE are applied to this traffic. That is, the traffic defined by this entry is permitted to use the Services. • Deny—The Services associated with this ACE are not applied to this traffic. If there are multiple ACLs configured for a service, denied traffic is typically compared to the next ACE in the list; if it matches no permit entry in any ACL for the service, the service is not applied to the traffic. Whether the traffic is dropped from the network depends on the service.

Table 6-24 Add and Edit Unified Access Control Entry Dialog Boxes (continued)

Element	Description
Source	Provide traffic sources for this rule; can be networks and hosts. You can enter values or object names, or Select objects, for one or more of the following: • Networks/Hosts – You can specify a various network, host and interface definitions, either individually or as objects. If you Select an interface object as a source, the dialog box displays tabs to differentiate between hosts/networks and interfaces. Enter more than one value in any of these fields by separating the items with commas or ranges. The "All-Address" objects do not restrict the rule to specific hosts, networks, or interfaces. These addresses are IPv4 or IPv6 addresses for hosts or networks, network/host objects, interfaces, or interface roles. **Note** (ASA 8.4.2+ only) You can only specify a fully qualified domain name (FQDN) by providing an FQDN network/host object, or a group object that includes an FQDN object. You cannot directly type in an FQDN. See Understanding Networks/Hosts Objects, page 6-80, Specifying IP Addresses During Policy Definition, page 6-87 and Understanding Interface Role Objects, page 6-73 for additional information about these definitions. **Note** Enter the IPv6 addresses as comma separated values only. Preview configuration displays an error when IPv6 address is provided as a range. All Source, Source SG, and Users specifications area combined to limit traffic matches to only those flows that include all source definitions. For example, specified user traffic originating from within a specified source address range.
Source SG	(ASA 9.0+ only) Enter or Select the name or tag number for one or more source Security Groups for the ACE, if any. For more information about security groups, see: • Selecting Security Groups in Policies, page 14-16 • Configuring TrustSec-Based Firewall Rules, page 14-17 • Creating Security Group Objects, page 14-14

Table 6-24 Add and Edit Unified Access Control Entry Dialog Boxes (continued)

Element	Description
Users	(ASA 8.4.2+ only) Enter or Select the Active Directory (AD) user names, user groups, or identity user group objects for the ACE, if any. The user specification is conjoined to the source address to limit the match to user addresses within the source address range. You can enter more than one value by separating the items with commas. You can enter any combination of the following values: • Individual user names: NetBIOS_DOMAIN\username • User groups (note the double \): NetBIOS_DOMAIN\\user_group • Identity user group object names. For more information, see: • Selecting Identity Users in Policies, page 13-21 • Configuring Identity-Based Firewall Rules, page 13-21 • Creating Identity User Group Objects, page 13-19
Destination	The source or destination of the traffic. You can enter more than one value by separating the items with commas. **Note** Enter the IPv6 addresses as comma separated values only. Preview configuration displays an error when IPv6 address is provided as a range. Provide traffic destinations, and optionally destination security groups (ASA 9.0+ only), for this ACE. As with the source entries, you can enter values or object names, or Select objects, for one or more destinations.
Destination SG	(ASA 9.0+ only) Enter or Select the name or tag number for one or more source Security Groups for the ACE, if any. For more information about security groups, see: • Selecting Security Groups in Policies, page 14-16 • Configuring TrustSec-Based Firewall Rules, page 14-17 • Creating Security Group Objects, page 14-14
Service	The services that define the type of traffic to act on. You can enter more than one value by separating the items with commas. You can enter or Select any combination of service objects and service types (which are typically a protocol and port combination). If you type in a service, you are prompted as you type with valid values. For complete information on how to specify services, see Understanding and Specifying Services and Service and Port List Objects, page 6-100.

Table 6-24 Add and Edit Unified Access Control Entry Dialog Boxes (continued)

Element	Description
Advanced button	Click this button to open the Advanced dialog box and define logging options for the ACE. For PIX, ASA, and FWSM devices, you can enable: • Default logging—If a packet is denied, message 106023 is generated. If a packet is permitted, no message is generated. • Per ACE logging—If a packet is denied, message 106100 is generated. You can select the logging severity level for the messages, and the interval (in seconds from 1 to 600) for generating messages.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Description	An optional description of the object.

Configuring Time Range Objects

Use the Add or Edit Time Range dialog box to create, edit, or copy a time range object.

You can create time range objects for use when creating time-based ACLs and some firewall rules. While similar to extended ACLs in function, time-based ACLs allow for access control based on time considerations. The time range applies to specific rules, and makes those rules active for the specific time period defined in the range. For example, you can implement a rule for typical work hours to allow or prevent certain types of access.

You can also use time range objects when defining ASA user groups to restrict VPN access to specific times during the week. For more information, see ASA Group Policies SSL VPN Settings, page 34-25.

Time range objects can rely on the device's system clock, but they work best when using Network Time Protocol (NTP) synchronization.

Navigation Path

Select **Manage > Policy Objects**, then select **Time Ranges** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Field Reference

Table 6-25 Time Range Dialog Box

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-9.
Description	An optional description of the object (up to 1024 characters).

Table 6-25 Time Range Dialog Box (continued)

Element	Description
Start Time End Time	The overall starting and ending time for the time range object: • Start Now—Defines the time of deployment as the start time. • Never End—Defines no end time for the range. • Start At, End At—Defines a specific start or end date and time. Click the calendar icon to display a tool for selecting the date. Enter the time in the Time field using the 24-hour clock format, HH:MM.
Recurring Ranges	Recurring time periods that happen within the overall start and end times, if any. For example, if you want to create a time range object that defines work hours, you could select Start Now and Never End for the overall range, and enter a recurring range of weekdays from 08:00 to 18:00 hours. • To add a range, click the **New Recurring Range** button and fill in the Recurring Ranges Dialog Box, page 6-72. • To edit a range, select it and click the **Edit Recurring Range** button. • To delete a range, select it and click the **Delete Recurring Range** button.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.

Recurring Ranges Dialog Box

Use the Recurring Ranges dialog box to add or edit recurring time intervals that are defined as part of a time range object. You can define as many recurring ranges as required.

Navigation Path

Go to the Add or Edit Time Range dialog box and click the **New Recurring Range** button under Recurring Ranges, or select a range and click **Edit Recurring Range**. See Configuring Time Range Objects, page 6-71.

Field Reference

Table 6-26 Recurring Ranges Dialog Box

Element	Description
Specify days of the week and times during which this recurring range will be active	Defines a recurring range that is based on specific days and times of the week. You can select from: • Every day • Weekdays • Weekends • On these days of the week—Select the specific days to include in the range. Also select the starting and ending time during the day. The default is all day.
Specify a weekly interval during which this recurring range will be active	Defines a recurring range for every week. Select the starting and ending day and time. For example, you can start the weekly period on Sunday and end it on Thursday.

Understanding Interface Role Objects

Interface Role objects have the following uses:

- Specifying multiple interfaces— Interface role objects allow you to apply policies to specific interfaces on multiple devices without having to manually define the names of each interface. Because most devices follow a standard naming convention for their interfaces, you can define a naming pattern that describes a particular interface type and then assign a policy to all interfaces matching that pattern.
- Zones—You use interface role objects to define the zones in a zone-based firewall rules policy.

For example, you might define an interface role with a naming pattern of DMZ*. When you include this interface role in a policy, the policy is applied to all interfaces whose name begins with “DMZ” on the selected devices. As a result, you can, for example, assign a policy that enables anti-spoof checking on all DMZ interfaces to all relevant device interfaces with a single action. Interface roles can refer to any of the actual interfaces on the device, including physical interfaces, subinterfaces, and virtual interfaces, such as loopback interfaces.

Interface roles serve as an indirection entity between interfaces on the one hand and policies on the other. This enables you to apply policies to particular device interfaces based on the assigned role. Additionally, if you change the naming convention used for a particular interface type, you do not need to determine which policies are affected by the change. All you do is edit the interface role.

Interface roles are especially useful when you apply policies to new devices. As long as the devices you are adding share the same interface naming scheme as existing devices, the relevant policies can be extended to them without the need to make additional assignments.

Security Manager includes the following predefined interface roles:

- All-Interfaces—Includes every interface defined on a device.
- Internal—Includes only specific interfaces that are meant to be on the inside of a network. See the object definition for a list.

- External—Includes only specific interfaces that are meant to be on the outside of a network. See the object definition for a list.
- Self—Does not include any interfaces. The Self interface role is specific to zone-based firewall rules policies. The Self zone is the router itself. You can use it to identify traffic originating from the router, or traffic directed to the router. It does not include traffic passing through the router.

The following topics describe how to work with interface role objects:

- Creating Interface Role Objects, page 6-74
- Specifying Interfaces During Policy Definition, page 6-76
- Using Interface Roles When a Single Interface Specification is Allowed, page 6-77
- Handling Name Conflicts between Interfaces and Interface Roles, page 6-78
- Chapter 22, "Managing Traffic Zones"

Creating Interface Role Objects

You can create interface role objects that represent one or more interfaces on devices. You can then use these roles when you define policies that require interfaces or zones. When you create an interface role object, you must define the naming pattern of the device interfaces to include in the object. Interface roles can refer to any of the actual interfaces on the device, including physical interfaces, subinterfaces, and virtual interfaces.

Tip You can also create interface role objects when you define policies or objects that use this object type. For more information, see Selecting Objects for Policies, page 6-2.

Related Topics

- Creating Policy Objects, page 6-9
- Specifying Interfaces During Policy Definition, page 6-76
- Understanding Interface Role Objects, page 6-73
- Using Interface Roles When a Single Interface Specification is Allowed, page 6-77
- Managing Object Overrides, page 6-17
- Chapter 22, "Managing Traffic Zones"

Step 1 Select **Manage > Policy Objects** to open the Policy Object Manager (see Policy Object Manager, page 6-4).

Step 2 Select **Interface Roles** from the Object Type selector.

Step 3 Right-click in the work area, then select **New Object**.

The Interface Role dialog box appears.

Step 4 Enter a name for the object and optionally a description of the object. Names can be up to 128 characters, descriptions up to 1024.

Step 5 Enter one or more naming patterns for the interface role object. The names are the complete or partial names of interfaces, subinterfaces, and other virtual interfaces. Separate multiple name patterns with commas.

You can use these wildcards to create name patterns that apply to multiple interfaces:

- Use a period (.) as a wildcard for a single character. To use a period as part of the pattern itself, enter a backslash (\) before the period.
- Use an asterisk (*) as a wildcard for one or more characters at the end of the interface pattern.

  For example, **DMZ*** would include all interfaces whose name begins with “DMZ”, while **DMZ.** would match interfaces such as DMZ1 and DMZ2, but would not match DMZ10.

If the pattern does not include a wildcard, it must match the exact name of the interface. For example, the pattern **FastEthernet** will not match FastEthernet0/1 unless you include an asterisk at the end of the pattern.

Step 6 (Optional) Under Category, select a category to help you identify this object in the Objects table. See Using Category Objects, page 6-13.

Step 7 (Optional) Select **Allow Value Override per Device** to allow the properties of this object to be redefined on individual devices. See Allowing a Policy Object to Be Overridden, page 6-18.

Step 8 Click **OK** to save the object.

Interface Role Dialog Box

Use the Interface Role dialog box to create, copy, or edit an interface role object. Interface Role objects have the following uses:

- Specifying multiple interfaces— Interface role objects allow you to apply policies to specific interfaces on multiple devices without having to manually define the names of each interface.
- Zones—You use interface role objects to define the zones in a zone-based firewall rules policy.

Navigation Path

Select **Manage > Policy Objects**, then select **Interface Roles** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Creating Policy Objects, page 6-9
- Creating Interface Role Objects, page 6-74
- Using Interface Roles When a Single Interface Specification is Allowed, page 6-77
- Specifying Interfaces During Policy Definition, page 6-76
- Understanding Interface Role Objects, page 6-73
- Chapter 22, “Managing Traffic Zones”
- Policy Object Manager, page 6-4

Field Reference

Table 6-27 Interface Role Dialog Box

Element	Description
Name	The name of the policy object. A maximum of 128 characters is allowed.
Description	A description of the policy object. A maximum of 1024 characters is allowed.

Table 6-27 Interface Role Dialog Box (continued)

Element	Description
Interface Name Patterns	The names to include in this interface role. The names are the complete or partial names of interfaces, subinterfaces, and other virtual interfaces. Separate multiple name patterns with commas. **Note** For firewall devices, use the name assigned to the interface (for example, Inside, Outside, or DMZ) and not the hardware port identifier (for example, Ethernet0). You can use these wildcards to create name patterns that apply to multiple interfaces: • Use a period (.) as a wildcard for a single character. To use a period as part of the pattern itself, enter a backslash (\) before the period. • Use an asterisk (*) as a wildcard for one or more characters at the end of the interface pattern. For example, DMZ* would include all interfaces whose name begins with "DMZ", while DMZ. would match interfaces such as DMZ1 and DMZ2, but would not match DMZ10. If the pattern does not include a wildcard, it must match the exact name of the interface. For example, the pattern "FastEthernet" will not match FastEthernet0/1 unless you include an asterisk at the end of the pattern.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Specifying Interfaces During Policy Definition

When you configure policies that require you to identify an interface, you have several options for specifying the interface:

- Enter the name of the interface manually, for example, Ethernet0.

  To manually specify a subinterface as part of a policy definition, you must enter a backslash (\) before the period. For example, Ethernet0\.1.

  If you enter the period without the backslash, Security Manager treats the period as a wildcard for a single character. For example, if you want to define Ethernet1/1.0 as part of an access rule, you need to enter **Ethernet1/1\.0**. If you enter **Ethernet1/1.0** instead, the name matches interfaces named Ethernet1/1.0 and Ethernet1/1/0, because the period on its own is treated as a wildcard.

- Enter the name of an interface role manually. For more information about interface roles, see Understanding Interface Role Objects, page 6-73.

- Select an interface or interface role from a list. By clicking **Select** next to the Interfaces field, you are prompted with a list of valid interface names and interface roles. Subinterfaces appear with a backslash before the period in their names.

  By selecting from a list, you can ensure that your entry is valid. For more information, see Selecting Objects for Policies, page 6-2.

When a policy allows multiple interfaces, separate entries with commas.

In policies and object selectors, icons distinguish between interfaces and interface roles. If you create interface roles with the same name as interfaces, be careful to select exactly what you want. Table 6-28 explains the icons.

Table 6-28 Icons for Interfaces and Interface Roles

Type	Icon
Interface	
Interface role If you can edit the role, a pencil image overlays the icon.	
Global "interface" on ASA 8.3+ devices, used for rules created as global instead of interface-specific.	

Related Topics

- Basic Interface Settings on Cisco IOS Routers, page 62-1
- Configuring Firewall Device Interfaces, page 46-3
- Understanding Interface Role Objects, page 6-73
- Creating Interface Role Objects, page 6-74
- Using Interface Roles When a Single Interface Specification is Allowed, page 6-77

Using Interface Roles When a Single Interface Specification is Allowed

Interface role objects can match a variable number of actual interfaces defined on a device depending on how you define the role. Thus, for a particular device, an interface role might match zero, one, or more than one interface. When you use an interface role in a policy, Security Manager converts the role to commands that configure all interfaces defined on the device that match the role.

Many policies, however, require that you specify a single interface name. If you use an interface role in a situation where the policy allows a single interface name, you should define the interface role so that it matches a single interface. If you use an interface role that matches two or more interfaces on the device, Security Manager selects the first interface on the device that matches the role, which might not be the interface you desire (or that will work properly).

Related Topics

- Specifying Interfaces During Policy Definition, page 6-76
- Understanding Interface Role Objects, page 6-73
- Creating Interface Role Objects, page 6-74

Handling Name Conflicts between Interfaces and Interface Roles

Under normal circumstances, you can configure an interface role that has the same name as an actual interface on the device. If you use object selectors when defining policies (see Selecting Objects for Policies, page 6-2), both the interface and the interface role are listed as available choices, enabling you to select either option. If you type in this common name when you define a policy, Security Manager automatically associates the interface role with the policy, not the interface.

However, a naming conflict can occur under the following circumstances:

1. You type the name of an interface when defining a policy.
2. You later create an interface role that has the same name.
3. You type this name again when defining a policy.
4. You click **Select** to display the object selector, or **Save** to save the policy, or in some cases, **OK** to update the policy.

When this sequence of events occurs, the Interface Name Conflict dialog box opens automatically so that you can select whether you want to specify the interface or the interface role. The dialog box lists only those names for which there are conflicts.

Related Topics

- Specifying Interfaces During Policy Definition, page 6-76
- Understanding Interface Role Objects, page 6-73

Understanding Map Objects

The objects in the Maps folder in the Policy Object Manager allow you to configure class, parameter, and policy maps for inspection rules, zone-based firewall rules, or IPS, QoS and connection rules policies. The types of maps you can use with these policies depends on the operating system running on the device as well as the specific version number, so typically it is best to configure the maps when you are configuring the policies.

Tip Devices enforce unique names for all configured maps. For example, you cannot use the same name for an FTP and DNS class map on the same device. If you select maps with the same name for a device, Security Manager automatically adds a numerical suffix to the duplicate names, for example, dnsmap_1.

The Maps folder contains the following folders. Subfolders organize the maps based on whether they are used for inspection or web content filtering.

- Class Maps—Layer 7 class maps used for identifying traffic that you want to act on.
- Parameter Maps—Parameter maps that configure settings used in zone-based firewall rules policies or other maps.
- Policy Maps—Layer 7 policy maps used for identifying the action to take on selected traffic.

Also included in the Maps folder are entries for TCP Map objects (a Layer 4 object), Regular Expression objects, and Regular Expression Group objects.

The following sections describe the different types of maps in more detail.

Class Maps

Class maps are subordinate to policy maps. You cannot specify a class map directly in a device policy. Instead, you create a policy map to incorporate the class map. The class map itself defines the match conditions for the traffic that you want to target in an inspection rule or zone-based firewall rule.

- ASA/PIX 7.2 and later, and FWSM devices—You can create class maps for the inspection of DNS, FTP, HTTP, IM, and SIP traffic. You also have the option of defining the traffic match directly in the policy map object, but if you create separate class maps, you can reuse them in more than one policy map.
- IOS 12.4(6)T and later devices—You can create class maps for the inspection of IM applications (AOL, ICQ, MSN Messenger, Windows Messenger, and Yahoo Messenger), P2P applications (eDonkey, FastTrack, Gnutella, Kazaa2), H.323, HTTP, IMAP, POP3, SIP, SMTP, Sun RPC. You can also create class maps for filtering web content using the Local, N2H2, Trend, and Websense objects.

  Unlike the class maps used for ASA/PIX/FWSM, you must create separate class maps and refer to them from the related policy maps. You can use these policy maps in zone-based firewall inspection or content filtering rules. For more information, see these topics:

  - Configuring Inspection Maps for Zone-based Firewall Policies, page 21-16
  - Configuring Content Filtering Maps for Zone-based Firewall Policies, page 21-36

To create class maps, see these topics:

- Configuring Class Maps for Inspection Policies, page 17-28
- Configuring Class Maps for Zone-Based Firewall Policies, page 21-19

To create the regular expressions and regular expression groups that you can use in class, parameter, and policy maps, see these topics:

- Add/Edit Regular Expressions, page 17-108
- Configuring Regular Expression Groups, page 17-108

Parameter Maps

Parameter maps define settings that you can use in zone-based firewall inspection or content filtering rules, or in other policy map objects.

- Inspection—You can create Inspection Parameter maps for general zone-based firewall rule parameters, or Protocol Info Parameter maps for use with IM application inspection.
- Content Filtering—You can create the following parameter maps to define web content filtering: Local, N2H2, Trend, URL Filter, URLF Glob, Websense.

Policy Maps

You can configure policy maps to alter the default actions of inspection or to configure web content filtering in zone-based firewall settings policies. Policy maps typically apply to applications that require special handling, perhaps due to embedded IP address information or the fact that the traffic opens secondary channels on dynamically assigned ports.

The policy map identifies the action to take on traffic that matches the conditions identified in the map. For most policy maps, you can specify traffic match conditions by referring to a class map. However, some policy maps require that you specify the match criteria within the policy map.

You can configure these types of policy maps:

- Inspection Rules—When configuring inspection rules, you can use Security Manager to create policy map objects for the following applications: DCE/RPC, DNS, ESMTP, FTP, GTP, H.323, HTTP, IM, IP options, IPsec, NetBIOS, SIP, Skinny, and SNMP. for more information, see Configuring Protocols and Maps for Inspection, page 17-22.
- Zone-Based Firewall Inspection Rules—When configuring zone-based firewall inspection rules, you can use Security Manager to create policy map objects for the following applications: H.323, HTTP, IM (includes AOL, ICQ, MSN Messenger, Windows Messenger, and Yahoo Messenger), IMAP, P2P (includes eDonkey, FastTrack, Gnutella, Kazaa2), POP3, SIP, SMTP, Sun RPC. For more information, see Configuring Inspection Maps for Zone-based Firewall Policies, page 21-16.
- Zone-Based Firewall Content Filtering Rules—When configuring zone-based firewall content filtering rules, you can use Security Manager to create Web Filter policy maps. You can also configure HTTP policy maps to inspect HTTP traffic. For more information, see Configuring Content Filtering Maps for Zone-based Firewall Policies, page 21-36.
- IPS, QoS and Connection Rules—When configuring this service policy, which is specific to PIX 7.x+ and ASA devices, you can customize TCP inspection using a TCP map. For more information, see Configuring TCP Maps, page 58-22 and Chapter 58, "Configuring Service Policy Rules on Firewall Devices".

Understanding Networks/Hosts Objects

Networks/Hosts objects are logical collections of IP addresses that represent networks, hosts, or both.

Note As of Security Manager 4.4, there are no longer separate IPv4 and IPv6 Networks/Hosts objects—there is now a single, unified Networks/Hosts object, which may accept IPv4 addresses, IPv6 addresses, or both (in the case of group objects). However, group objects containing a mixture of IPv4 and IPv6 addresses can be assigned only to policies on ASA 9.0.1 and later devices. See Policy Object Changes in Security Manager 4.4, page 1-10 for more information.

When you create a Networks/Hosts object, you must choose the type of object, which defines and limits the type of addresses the object can contain:

- Group – You can include combinations of any of the following types of addresses:
  - Networks or subnets, specified by IPv4 addresses and subnet masks, or IPv6 prefixes and prefix lengths.
  - Ranges of IPv4 or IPv6 network addresses.
  - Individual hosts, specified by IPv4 or IPv6 addresses (but not a domain name).
  - Other network/host objects, selected from a list of existing Networks/Hosts objects, including fully qualified domain name (FQDN) objects.
- FQDN – (ASA 8.4(2+) only) This object can contain a single host's fully qualified domain name, such as myhost.cisco.com. The device uses DNS to periodically resolve the FQDN to its IP address.
- Host – This object can contain a single host IPv4 or IPv6 address, such as 10.100.10.10 or 2001:DB8::0DB8:800:200C:417A.
- Attribute – This object can contain one or more policy based VM attribute agents, which allow a user to define network objects to filter traffic according to attributes associated with one or more Virtual Machines (VMs) in an VMware ESXi environment managed by VMware vCenter. Each VM attribute agent communicates with a single vCenter server.

- Address Range – This object can contain a single range of IPv4 or IPv6 addresses; the start and end addresses must be different, with the start being lower than the end.
- Network – This object can contain a single IPv4 network address and subnet mask, such as 10.100.10.0/24, or a single IPv6 prefix and prefix length, such as 2001:DB8::/32.

Networks/Hosts group objects make it easier to manage scalable policies. By using the associative capabilities of Networks/Hosts objects, you can expand your policies along with your network. For example, when you make changes to the list of addresses contained in a Networks/Hosts object, the changes propagate to all other Networks/Hosts objects, and to policies that refer to that Networks/Hosts object.

The host, network, and address range objects have special uses when used in policies for an ASA 8.3+ device. On these devices, you can configure object NAT rules in the policy object itself. If you use the object on other types of device, this NAT configuration is ignored.

The following topics describe how to work with Networks/Hosts objects:

- Contiguous and Discontiguous Network Masks for IPv4 Addresses, page 6-81
- Creating Networks/Hosts Objects, page 6-82
- Using Unspecified Networks/Hosts Objects, page 6-86
- Specifying IP Addresses During Policy Definition, page 6-87
- VM Attribute Policies, page 6-89

Contiguous and Discontiguous Network Masks for IPv4 Addresses

A network mask determines which portion of an IPv4 address identifies the network and which portion identifies the host. Like the IP address, the mask is represented by four octets. (An octet is an 8-bit binary number equivalent to a decimal number in the range 0-255.) If a given bit of the mask is 1, the corresponding bit of the IP address is in the network portion of the address, and if a given bit of the mask is 0, the corresponding bit of the IP address is in the host portion.

Standard, or contiguous, network masks start with zero or more 1s followed by zero or more 0s. This kind of network mask is considered contiguous because it represents a network that consists of a contiguous IP address range. For example, the network 192.168.1.0/255.255.255.0 contains all the IP addresses ranging from 192.168.1.0 to 192.168.1.255.

The following table shows different methods of representing commonly used standard network masks:

Table 6-29 Standard Network Masks

Dotted Decimal Notation	Classless Inter-Domain Routing (CIDR) Notation
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.255	/32

For example, 255.255.255.0 indicates that the first three octets of the IP address (24 bits or /24 in CIDR notation) are made up of ones and identify the network; the last octet is made up of zeros and identifies the host.

Discontiguous Network Masks

Nonstandard, or discontiguous, network masks are masks that do not conform to the contiguous format. For example, 10.0.1.1/255.0.255.255 indicates that you want to match an address that matches octets 1, 3, and 4 exactly, but any value in octet 2 is accepted.

Although discontiguous network masks are not typically used for network configurations, they are sometimes used for certain commands, such as filtering commands when defining access control lists (ACLs). Security Manager supports the use of nonstandard network masks in the policies whose CLI commands support them. An error is displayed if you try to define a discontiguous network mask in a policy that does not support them.

Network Masks and Discovery

During discovery, Security Manager attempts to match network/host objects with existing equivalent objects defined in the Policy Object Manager:

- For contiguous network masks—Two network/host objects containing only standard networks are considered equivalent if they consist of the same set of IP addresses.
- For discontiguous network masks—Two network/host objects are considered equivalent only if the standard networks consist of the same set of IP addresses and the nonstandard networks are syntactically equivalent.

How Network Masks are Displayed

Although you can enter both contiguous and discontiguous network masks using dotted decimal notation, all contiguous network masks are converted to CIDR notation. This makes it easier to distinguish them from discontiguous network masks, which are displayed in dotted decimal notation only.

Related Topics

- Creating Networks/Hosts Objects, page 6-82
- Specifying IP Addresses During Policy Definition, page 6-87
- Using Unspecified Networks/Hosts Objects, page 6-86
- Understanding Networks/Hosts Objects, page 6-80

Creating Networks/Hosts Objects

You can create Networks/Hosts objects to represent networks, individual hosts, or groups of both. When you create a Networks/Hosts object, you must choose the type of object (group, host, FQDN, network, attribute, address range). Once created, you cannot change the object type.

Tip You can create Networks/Hosts objects "on the fly" when defining policies or objects that use this object type. For more information, see Selecting Objects for Policies, page 6-2.

You can specify NAT object only if you have the Modify privilege mapped to your role.

Related Topics

- Understanding Networks/Hosts Objects, page 6-80
- Creating Policy Objects, page 6-9
- Contiguous and Discontiguous Network Masks for IPv4 Addresses, page 6-81
- Specifying IP Addresses During Policy Definition, page 6-87

- VM Attribute Policies, page 6-89
- Using Unspecified Networks/Hosts Objects, page 6-86
- How Network/Host, Port List, and Service Objects are Named When Provisioned As Object Groups, page 6-107

Step 1 Choose **Policy Objects** from the **Manage** menu, or click the Policy Object Manager button in the button bar, to open the Policy Object Manager pane in the lower section of the Configuration Manager window; see Policy Object Manager, page 6-4 for more information.

Step 2 Select **Networks/Hosts** in the Object Type selector.

Step 3 Click the New Object button at the bottom of the window and choose one of the following types of Networks/Hosts object to open the Add or Edit Network/Host Dialog Box, page 6-83. You also can right-click in the work area, choose **New Object**, and then choose one of the following options to open the dialog box.

- **Group** – To create an object that has one or more entry. You can include any combination of networks, hosts, address ranges, or other network/host objects (including FQDN objects).
- **FQDN** – (ASA 8.4(2+) only) To create an object with a single host's fully qualified domain name, such as myhost.cisco.com.
- **Host** – To create an object with a single host address, such as 10.100.10.10 or 2001:DB8::12ab:5689.
- **Attribute** – (ASA 9.7.1+ only) To create a network object to filter traffic according to attributes associated with one or more virtual machines (VMs) in a VMware ESXi environment managed by VMware vCenter.
- **Address Range** – To create an object with a single range of addresses, such as 10.100.10.1-10.100.10.255.
- **Network** – To create an object with a single network address, such as 10.100.10.0/24 or 2001:DB8::/32.

Tip Host, network, and address range objects also let you configure object NAT rules for ASA 8.3+ devices. Any NAT configuration is ignored for other devices.

Step 4 Provide the appropriate information in the Add or Edit Network/Host Dialog Box, page 6-83.

Add or Edit Network/Host Dialog Box

Use the Add or Edit Network/Host dialog box to view, create, or edit network/host objects. The title, content and appearance of the dialog box differ slightly based on the type of network/host object you are creating: Group, FQDN, Host, Attribute, Address Range, or Network. FQDN objects require ASA 8.4.2 or later devices. Attribute objects require ASA 9.7.1 or later devices.The Group type lets you enter multiple definitions, so you can have a collection of networks, hosts, and other network/host objects, whereas the other types allow a single definition only.

The Host, Network, and Address Range versions of the dialog box provide two tabbed panels of options: General and NAT. Options on the General panel and the non-tabbed versions of the dialog box are described in the following table; the NAT options are described in Add or Edit Network/Host Dialog Box: NAT Tab, page 24-43.

Note As of Security Manager 4.4, there are no longer separate IPv4 and IPv6 Networks/Hosts objects—there is now a single, unified Networks/Hosts object, which may accept IPv4 addresses, IPv6 addresses, or both (in the case of group objects only). However, group objects containing a mixture of IPv4 and IPv6 addresses can be assigned only to policies on ASA 9.0.1 and later devices.

When you create IPv4-based Host, Network, or Address Range objects for use on ASA 8.3+ devices, or unified Host, Network, or Address Range objects for use on ASA 9.0.1+ devices, you can also configure object NAT rules on the NAT tab of the dialog box. In both cases, you must select **Allow Value Override per Device** to allow object NAT. For reference information on the NAT tab, see Add or Edit Network/Host Dialog Box: NAT Tab, page 24-43.

In addition, you can create an object with no addresses. For this type of object, you must also select **Allow Value Override per Device** and create overrides for every device that uses the object. For more information about using unspecified addresses, see Using Unspecified Networks/Hosts Objects, page 6-86.

Navigation Path

Choose **Policy Objects** from the **Manage** menu, or click the Policy Object Manager button in the button bar, to open the Policy Object Manager pane in the lower section of the Configuration Manager window. Select **Networks/Hosts** from the Object Type Selector. Right-click inside the work area and select **New Object** (and select an object type), or right-click a row and select **Edit Object**; you also can use the related buttons at the bottom of the pane to open either dialog box.

Related Topics

- Creating Networks/Hosts Objects, page 6-82
- Understanding Networks/Hosts Objects, page 6-80
- Policy Object Manager, page 6-4
- How Network/Host, Port List, and Service Objects are Named When Provisioned As Object Groups, page 6-107
- Filtering Items in Selectors, page 1-45

Field Reference

Table 6-30 Network/Host Dialog Box (General Tab)

Element	Description
Name	The object name (up to 64 characters). Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-9.
Description	An optional description of the object.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.

Table 6-30 Network/Host Dialog Box (General Tab) (continued)

Element	Description
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. **Tip** If you configure NAT for host, address range, or network objects, you must select this option. The NAT configuration is created as a device override and is not kept in the object. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.
Group object options	
Available Networks/Hosts Members In Group Type in comma separated IP addresses	The Members In Group list shows the networks, hosts, and other network/host objects that are included in this object. To populate the list, do any combination of the following: • Select one or more Address, Attribute, FQDN, Group, Host, Network objects in the Existing Networks/Hosts list and then click the >> button between the lists. • Type one or more IP addresses in the "Type in comma separated IP addresses" field and then click the >> button between the lists. Separate multiple addresses with commas; they are added as separate lines in the Members list. For IPv4 addresses, you can include host addresses, network addresses (with subnet masks entered after a / character, such as 10.100.10.0/24), or a range of addresses (separate the starting and ending address with a hyphen, and optionally include a subnet mask). For IPv6 addresses, you can include host addresses, network addresses (with prefixes entered after a / character, such as 2001:DB8::/32), or a range of addresses (such as 2001:DB8::1-2001:DB8::100). See Specifying IP Addresses During Policy Definition, page 6-87 for more information. • To remove an item from the Members In Group list, select it and click the appropriate << button to return the item to its source location. You can select and remove multiple items at one time. **Note** Group objects containing a mixture of IPv4 and IPv6 addresses can be assigned only to policies on ASA 9.0.1 and later devices.
FQDN object options	
FQDN FQDN Type	The fully qualified domain name of a single host; for example, somehost.cisco.com. The FQDN Type specifies the type of IP address mapped to the provided domain: IPv4 Only, IPv6 Only, or **Default**, which applies a device-specific default; for all non-ASA and pre-9.0.1 ASA devices, the default is IPv4.

Table 6-30 Network/Host Dialog Box (General Tab) (continued)

Element	Description
Host object options	
IP Address	The IPv4 or IPv6 address of the single host to include in the object.
Attribute object options	
Agent Name Type Value	The VM Attribute Agent name. Select from a list of VM attribute agents or add a new VM Attribute Agent. The VM Attribute Agent Type should not exceed 128 characters. The VM Attribute Agent Value should not exceed 128 characters. **Note** A user can assign custom attribute types and values to a set of VMs in order to apply a common set of policies to a set of VMs with a common user-defined characteristic
Address Range object options	
Start IP Address End IP Address	The first and last IP address that define a range of addresses. The start and end addresses must be different, with the start being lower than the end.
Network object options	
IP Address Net Mask/Prefix	The IPv4 or IPv6 address that represents the network; for example, 10.100.10.0 or 2001:DB8::/32. If you entered an IPv4 address, enter its subnet mask in the Net Mask/Prefix field. You can type a mask in either CIDR format, for example, 24 (without the forward slash), or in dotted decimal format, for example, 255.255.255.0. If you entered an IPv6 address, enter its prefix length in the Net Mask/Prefix field.

Using Unspecified Networks/Hosts Objects

When you define a Networks/Hosts object, you can leave the address fields blank, thereby creating a Networks/Hosts object with an unspecified value. Networks/Hosts objects with unspecified values require that you create overrides for every device that uses them.

The advantage of using a Networks/Hosts object with an unspecified value is that Security Manager displays an error if you submit your changes without creating a device-level override on every device using the object. By contrast, when you define the global object with a placeholder value (such as, 10.10.10.10), that global value could be deployed by mistake if you fail to define an override.

The following procedure describes how to create and implement Networks/Hosts objects with unspecified values.

Related Topics

- Creating Networks/Hosts Objects, page 6-82
- Understanding Policy Object Overrides for Individual Devices, page 6-18
- Contiguous and Discontiguous Network Masks for IPv4 Addresses, page 6-81
- Specifying IP Addresses During Policy Definition, page 6-87

- Understanding Networks/Hosts Objects, page 6-80

Step 1 Create a Networks/Hosts object, making sure to:

- Leave the address fields blank (for example, the Members in Group, IP Address and Net Mask/Prefix, FQDN, or Start and End IP Address).
- Select the **Allow Value Override per Device** check box.

For more information, see Creating Networks/Hosts Objects, page 6-82.

Step 2 Create overrides for each device that will use the object:

a. Click the green checkmark in the Overrides column for the object in the Networks/Hosts table to open the Policy Object Overrides Window, page 6-20.

b. Click the **Create Override** button and select the devices on which you want to create overrides, then define a value in the address field. At this point, this override value applies to all the selected devices. For more information, see Creating or Editing Object Overrides for Multiple Devices At A Time, page 6-19.

c. Double-click each device in the Policy Object Overrides dialog box, then modify the address field for the value required by that device.

Step 3 Define a policy that requires this object. You can use one of two methods:

- Define the policy on a single device in Device view, share the policy, then assign the policy to the other devices. See Sharing a Local Policy, page 5-41 and Modifying Shared Policy Assignments in Device View or the Site-to-Site VPN Manager, page 5-49.
- Create a shared policy in Policy view, then assign the policy to the other devices using the Assignments tab. See Modifying Policy Assignments in Policy View, page 5-54.

Note You can create a Networks/Hosts group object that refers to a Networks/Hosts object with an unspecified value. You do not have to create the device-level overrides before you assign the policy containing the object to devices.

Specifying IP Addresses During Policy Definition

Many policies and policy objects require that you enter an IP address for a host or network. For some policies or objects, you must enter just a host, or just a network. For other policies or objects, you can enter some combination of hosts and networks. You are prevented from entering or selecting addresses that are not appropriate for the circumstances.

The following is a description of all acceptable formats that you can use, both for IPv4 and IPv6 addresses, although a particular policy or object might not allow specific formats (for example, interface roles are allowed as address designations in only a very limited number of policies). If the policy or object allows it, you can enter multiple addresses by separating them with commas.

- Networks/Hosts object. Enter the name of the object or click **Select** to select it from a list. You can also create new Networks/Hosts objects from the selection list.

Note The only way to specify a fully qualified domain name (FQDN) is to use an FQDN Networks/Hosts object, or a group object that includes an FQDN object. You cannot directly type in an FQDN.

- Host IP address, in v4 or v6 format.
  - Complete IPv4 address; for example, 10.10.10.100
  - Complete IPv6 address, showing all eight components. For example, 2001:DB8:0:0:0DB8:800:200C:417A. It is not necessary to include the leading zeros in an individual field. Security Manager converts the address to compressed format if possible.
  - Compressed IPv6 address, where a group of fields is replaced by two colons (::). It is common for IPv6 addresses to contain successive hexadecimal fields of zeros. To make IPv6 addresses less cumbersome, you can use two colons (::) to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address (the colons represent successive hexadecimal fields of zeros). You can use :: at most once in an IPv6 address. For example, 2001:DB8::0DB8:800:200C:417A. The unspecified address, 0:0:0:0:0:0:0:0, can be represented as ::. The loopback address is ::1.
  - IPv6 representation of an IPv4 address. When dealing in mixed IPv4/IPv6 environments, you can represent the IPv4 addresses in an alternate IPv6 format: x:x:x:x:x:x:d.d.d.d, where the Xs are the hexadecimal values of the first 6 fields, and the Ds are the IPv4 address with the octets separated by periods. The first 6 fields are either all zeros, ::FFFF, or 2001:DB8::. For example, 0:0:0:0:0:0:10.1.68.3, which in compressed format is ::10.1.68.3, or 0:0:0:0:0:FFFF:10.1.68.3, or 2001:DB8::10.1.68.3.
- Network address, in either IPv4 or IPv6 format:
  - IPv4 address, including subnet mask, in either CIDR format (10.10.10.0/24), or dotted decimal format (10.10.10.0/255.255.255.0).
  - IPv6 address, including the prefix length in decimal format in a manner similar to CIDR notation for IPv4, for example, /64. The number specifies the number of the left-most contiguous bit of the address that comprise the prefix. For example, 2001:DB8:0:CD30::/60.

    Note You could also enter 2001:DB8:0:CD30::/60 as 2001::CD30:0:0:0:0/60. However, compressing the trailing zeros is the preferred method, and Security Manager will translate the address to 2001:DB8:0:CD30::/60.

    For more detailed information on IPv6 addressing, see the IETF RFC 4291, IP Version 6 Addressing Architecture, at http://www.ietf.org/rfc/rfc4291.txt.
- A range of IP addresses. Separate the beginning and ending addresses with a hyphen. The range does not need to be within a single subnet unless the policy requires it.

  You can also include a prefix or subnet mask in CIDR format; for example, 2001:db8::1 - 2001:db8::2/64, or 10.10.10.100-10.10.10.200/24.
- An IPv4 address pattern in the format 10.10.0.10/255.255.0.255, where the mask is a discontiguous bit mask (see Contiguous and Discontiguous Network Masks for IPv4 Addresses, page 6-81).
- Interface role object (in rare cases). Enter the name of the object or click **Select** to select it from a list (you must select Interface Role as the object type). When you use an interface role, the rule behaves as if you supplied the IP address of the selected interface. This is useful for interfaces that get their address through DHCP, because you do not know what IP address will be assigned to the device. For more information, see Understanding Interface Role Objects, page 6-73.

When you create a network/host object or define IP addresses as part of a policy, Security Manager verifies that the syntax of the address is correct and that a mask or prefix was entered when required. For example, when you define a policy that requires a host, you do not need to enter a mask/prefix. However, when you define a policy that requires a subnet, you must enter the address with the mask/prefix, or select a network/host object that has a mask/prefix defined.

Related Topics

- Creating Networks/Hosts Objects, page 6-82
- Contiguous and Discontiguous Network Masks for IPv4 Addresses, page 6-81
- Using Unspecified Networks/Hosts Objects, page 6-86
- Policy Object Manager, page 6-4
- Understanding Networks/Hosts Objects, page 6-80

VM Attribute Policies

You can define network objects to filter traffic based on attributes associated with one or more virtual machines (VMs) in a VMware ESXi environment. This environment is managed by VMware vCenter. Users can assign attributes to VMs within the ESXi environment and configure an attribute agent; the attribute agent connects to vCenter or to a single ESXi host using HTTPS and requests and retrieves one or more bindings that associate the specific attribute to the primary IP address of the an ESXi VM.

A single ASA can have multiple attribute agents defined; each communicating with a different vCenter, or one or more communicating with the same vCenter.

This enables a user to define access control lists (ACLs) to assign policies to traffic from a group of VMs that share one or more attributes.This feature is referred to as Policy Based on VM Attributes

The VM attributes feature is supported on all hardware platforms, and on all ASAv platforms running on ESXi, KVM, or HyperV hypervisors. VM attributes can only be retrieved from VMs running on an ESXi hypervisor.

Note The ASA uses the term **attribute** or **attribute type** to refer to the characteristic to be monitored. VMWare uses the term **property** for the same characteristic. The terms may be used interchangeably.

Communication between the VM attribute agent and vCenter

There are two types of messages exchanged between the VM attribute agent and the vCenter - Property Request and Binding Update.:

- **Property Request** -This is a HTTPS message sent from the ASA to the IP address of the vCenter Server, indicating the complete list of attribute types currently configured for network objects associated with this attribute agent. attributes that have been configured. This message contains the SSL credentials necessary to authenticate the connection to vCenter. The vCenter responds with a corresponding HTTPS response.
- **Binding Update** - This is a asynchronous HTTPS message sent from the vCenter to the ASA, whenever an attribute changes for one or more VMs. Each binding update is identified by the IP address of the VM reporting the attribute change. If multiple attributes are being monitored by a single agent, a single binding update contains the current value of all monitored attributes for each VM. If a specific attribute being monitored by the agent is not configured on a VM, the binding will contain an empty attribute value for that VM. If a VM has not been configured with any monitored attributes, vCenter does not send a binding update to the ASA.

When an attribute agent issues a property request containing a new attribute type, vCenter responds with a binding update for each VM where the attribute type is configured. After that point, vCenter only issues a new binding when an attribute value is added or changed on a VM.

Attribute Agent States

There are two kinds of attribute agent states - **Connection State** and **Agent State**.

- **Connection State** - This indicates whether or not the attribute agent is currently in contact with vCenter.

Table 6-31 Connection State Table

Connection State	Explanation
No Host Credentials	The user has not entered vCenter host credentials using the **host** subcommand, or the agent has been deleted using the **no attribute source-group** command while there are network objects still using the agent.
Disconnected	The agent has host credentials defined, but is currently not in contact with vCenter. The connection is established when the ASA receives a HTTP 200 response to a keepalive packet.
Connected	The agent has received a response from vCenter to the latest keepalive packet.
Invalid Host Credentials	The agent has attempted to contact vCenter to issue a property request, but the request was rejected because the user name and/or password was incorrect. The agent stays in this state until new credentials are entered, at which point it will move to Disconnected state until a keepalive response is received from vCenter.

- **Agent State** - This indicates whether or not any network objects are configured to monitor attribute types through this agent.

Table 6-32 Agent State Table

Agent State	Explanation
Inactive	The agent currently has no attributes configured.
Active	The agent has one or more attributes configured. An agent can be Active even if there is no connection to vCenter.

Guidelines for Configuring vCenter Virtual Machines

To leverage the VM attributes feature, those attributes must be made available to the vCenter server by the managed virtual machines. As an example, some attributes are:

- **summary.config.name** - The user-defined name associated with the virtual machine - for example, VM-build-machine-1

- **summary.config.guestFullName** - The full name of the guest OS running on the virtual machine - for example, Red Hat Enterprise Linux 7 (64-bit)
- **summary.config.annotation** - The text description field for the virtual machine.

For string attribute values such as **summary.config. annotation**, the value in the network object attribute definition must be an exact match to the value reported to vCenter by the VM. For example, a network object attribute value, 'This is a Build Machine' does not match the VM **summary.config.annotation** value, 'this is a build machine' on the VM. A binding update containing the latter string will not be added to the host-map for the former.

VMs being monitored by the VM attributes feature must have VMware Tools installed. VMware Tools is the software component that reports the IPv4 or IPv6 address of the VM to the vCenter server. Since the function of VM attribute is to bind an IP address to an attribute type/value pair, vCenter will not report any binding information for VMs that are not running VMware Tools.

Within the ESXi environment, VMs are defined by a primary IP address, which roughly corresponds to the management IP address of an ASA. There can only be one primary address per VM, which can be either an IPv4 or IPv6 address. Bindings are always provided between the primary IP address and the attribute type/value pair. If a VM is configured with multiple IP addresses (such as IPv6 link local addresses), vCenter will only send binding updates for the primary address (usually the first address configured).

Note A user can assign custom attribute types and values to a set of VMs in order to apply a common set of policies to a set of VMs with a common user-defined characteristic.

For a comprehensive list of the attributes and related guidelines, refer to the VMware vCenter 5.5/6.0 documentation.

Configuring VM Attribute Policies

There are three steps to configuring a policy based on VM attributes:

Step 1 Configure the Network Object Attribute.

a. Choose **Policy Objects** from the **Manage** menu, or click the Policy Object Manager button in the button bar, to open the Policy Object Manager pane in the lower section of the Configuration Manager window. Select **Networks/Hosts** from the Object Type Selector. Right-click inside the work area and select **New Object > Attribute**; you also can use the **+** button at the bottom of the pane to add a new network object attribute.

Note A Network Attribute Object can be used only if object-group-search is enabled.

b. Select a **VM Attribute Agent**, specify a **VM Attribute Type** and add a value for **VM Attribute Value**.

Step 2 Add a VM Attribute Agent.

a. Specify a **Name** for the VM Attribute Agent and add a **Description** for the VM attribute Agent.

b. By default, the **Agent Type** is esxi.

c. Enter the primary IP address of the vCenter server in the **DNS Host Name/IP Address** field.

d. Specify a **Username** and **Password** to authenticate to the vCenter Server.

e. Specify a duration of time that the connection is kept active while the agent is contacting the vCenter server. The default value of the **Retry Interval** is 30 seconds.

f. Specify the number of times that the agent will attempt to contact the vCenter server before declaring it inactive in the **Retry Count** field. The default value is 3.

g. Click **OK**.

Step 3 Configure an access-list using a VM Attribute. For more information see Creating Access Control List Objects, page 6-53

Note VM Attribute only supports an access-list object.

Understanding Pool Objects

Pool objects have the following uses:

- Specifying pools for use in Layer 3 load balancing for ASA clusters
- Specifying pools for use in Layer 3 EIGRP and OSPFv3 on ASA clusters

The following topics describe how to work with pool objects:

- Add or Edit IPv4 Pool Dialog Box, page 6-92
- Add or Edit IPv6 Pool Dialog Box, page 6-93
- Add or Edit MAC Address Pool Dialog Box, page 6-94
- Add or Edit NET Pool Object Dialog Box, page 6-95
- Add or Edit DHCPv6 Pool Dialog Box, page 6-96

Add or Edit IPv4 Pool Dialog Box

Use the Add or Edit IPv4 Pool dialog box to view, create, or edit IPv4 pool objects.

Navigation Path

Choose **Policy Objects** from the **Manage** menu, or click the Policy Object Manager button in the button bar, to open the Policy Object Manager pane in the lower section of the Configuration Manager window. Select **Pool Objects > IPv4 Pool Object** from the Object Type Selector. Right-click inside the work area and select **New Object** (and select an object type), or right-click a row and select **Edit Object**; you also can use the related buttons at the bottom of the pane to open either dialog box.

Related Topics

- Policy Object Manager, page 6-4
- Selecting Objects for Policies, page 6-2

Field Reference

Table 6-33 Add IPv4 Pool Object Dialog Box

Element	Description
Name	The object name (up to 64 characters). Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-9.
Description	An optional description of the object.
Type	Select whether the pool object is a single IP address or a range of IP addresses.
Address	The IPv4 address of the single host to include in the object.
Start Address End Address	The first and last IP address that define a range of addresses. The start and end addresses must be different, with the start being lower than the end.
Mask	The subnet mask for the IP address or address range.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. **Note** IPv4 Pool objects are always overridable. Clearing this option results in an error. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add or Edit IPv6 Pool Dialog Box

Use the Add or Edit IPv6 Pool dialog box to view, create, or edit IPv6 pool objects.

Navigation Path

Choose **Policy Objects** from the **Manage** menu, or click the Policy Object Manager button in the button bar, to open the Policy Object Manager pane in the lower section of the Configuration Manager window. Select **Pool Objects > IPv6 Pool Object** from the Object Type Selector. Right-click inside the work area and select **New Object** (and select an object type), or right-click a row and select **Edit Object**; you also can use the related buttons at the bottom of the pane to open either dialog box.

Related Topics

- Policy Object Manager, page 6-4
- Selecting Objects for Policies, page 6-2

Field Reference

Table 6-34 Add IPv6 Pool Object Dialog Box

Element	Description
Name	The object name (up to 64 characters). Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-9.
Description	An optional description of the object.
Address	The IPv6 address in address/prefix length format to include in the object.
Count	The number of addresses to be included in the pool. Must be between 1 and 16384.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add or Edit MAC Address Pool Dialog Box

Use the Add or Edit MAC Address Pool dialog box to view, create, or edit MAC Address pool objects.

Navigation Path

Choose **Policy Objects** from the **Manage** menu, or click the Policy Object Manager button in the button bar, to open the Policy Object Manager pane in the lower section of the Configuration Manager window. Select **Pool Objects > MAC Address Pool Object** from the Object Type Selector. Right-click inside the work area and select **New Object** (and select an object type), or right-click a row and select **Edit Object**; you also can use the related buttons at the bottom of the pane to open either dialog box.

Related Topics

- Policy Object Manager, page 6-4
- Selecting Objects for Policies, page 6-2

Field Reference

Table 6-35 Add MAC Address Pool Object Dialog Box

Element	Description
Name	The object name (up to 64 characters). Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-9.
Description	An optional description of the object.

Table 6-35 Add MAC Address Pool Object Dialog Box (continued)

Element	Description
Start MAC Address End MAC Address	The first and last MAC address that define a range of addresses. The start and end addresses must be different, with the start being lower than the end.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add or Edit NET Pool Object Dialog Box

Use the Add or Edit NET Pool Object dialog box to view, create, or edit Network Entity Title Pool objects.

Navigation Path

Choose **Policy Objects** from the **Manage** menu, or click the Policy Object Manager button in the button bar, to open the Policy Object Manager pane in the lower section of the Configuration Manager window. Select **Pool Objects > NET Pool Object** from the Object Type Selector. Right-click inside the work area and select **New Object** (and select an object type), or right-click a row and select **Edit Object**; you also can use the related buttons at the bottom of the pane to open either dialog box.

Related Topics

- Policy Object Manager, page 6-4
- Selecting Objects for Policies, page 6-2

Field Reference

Table 6-36 Add NET Pool Object Dialog Box

Element	Description
Name	The object name (up to 64 characters). Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-9.
Description	An optional description of the object.
Start NET Address End NET Address	The first and last NET address that define a range of addresses. The start and end addresses must be different, with the start being lower than the end.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.

Table 6-36 Add NET Pool Object Dialog Box (continued)

Element	Description
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Add or Edit DHCPv6 Pool Dialog Box

This dialog box is used to add or edit the DHCPv6 Server Pool. For clients that use StateLess Address Auto Configuration (SLAAC) in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information such as the DNS server or domain name when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients.

Navigation Path

- Choose **Policy Objects** from the **Manage** menu, or click the Policy Object Manager button in the button bar, to open the Policy Object Manager pane in the lower section of the Configuration Manager window. Select **Pool Objects > DHCPv6 Pool Object** from the Object Type Selector. Right-click inside the work area and select **New Object** (and select an object type), or right-click a row and select **Edit Object**; you also can use the related buttons at the bottom of the pane to open either dialog box.

OR

- You can access the Add DHCPv6 Pool dialog box from DHCPv6 Pool Selector dialog box: click the Add Row or Edit Row buttons beneath the Available DHCPv6 Pool table. The DHCPv6 Pool Selector dialog box can been accessed from the Server Pool radio button in the Interface IPv6 DHCP section of the IPv6 panel of the Add Interface and Edit Interface dialog box.

Related Topics

- IPv6 Address for Interface Dialog Box, page 46-52
- Add/Edit Interface Dialog Box (PIX 7.0+/ASA/FWSM), page 46-31
- Managing Device Interfaces, Hardware Ports, and Bridge Groups, page 46-26
- Policy Object Manager, page 6-4
- Selecting Objects for Policies, page 6-2

Field Reference

Table 6-37 Add DHCPv6 Pool Dialog Box

Element	Description
Name	The DHCPv6 Pool name should not exceed 200 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-9.

Table 6-37 Add DHCPv6 Pool Dialog Box (continued)

Element	Description
• Configure parameters on one or more tabs, to provide responses to IR messages to clients. • For each of these tabs, specify the following as appropriate: – DNS/SIP/ NIS/ NISP/ SNTP Server: Enter a server name. Make sure that the IPv6 addresses are in the correct format. For more information on IPv6 address format, see http://www.ietf.org/rfc/rfc2373.txt. – DNS/ SIP/NIS/NISP Domain Name: Enter a domain name. Domain names must begin and end with a digit/letter, only letters, digits and hyphen are allowed as internal characters, labels are separated by a dot.Each label must be up to 63 characters and the entire host name has a maximum of 255 characters. For more information on domain names format, see http://www.ietf.org/rfc/rfc1123.txt. **Note** The import command uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface. You can mix and match manually-configured parameters with imported parameters; however, you cannot configure the same parameter manually and in the import command.	
Server tab	(Optional) Specify DNS Server Name and Domain Name.
SIP tab	(Optional) Specify SIP Server Name and SIP Domain Name.
NIS tab	(Optional) Specify NIS Server Name and NIS Domain Name.
NISP tab	(Optional) Specify NISP Server Name and NISP Domain Name.
SNTP tab	(Optional) Specify SNTP Server Name.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Configuring SAML Identity Provider

Beginning with version 4.10, Security Manager enables you to configure Security Assertion Markup Language (SAML) 2.0 based Single-Sign on and Single-Logout for ASA VPN. Single Sign-on Server configuration is no longer supported from ASA version 9.5(2). This has been replaced by SAML Identity Provider.

Security Assertion Markup Language is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. Identity Provider is a service that can assert a user's identity to another resource. An Identity Provider is responsible for authenticating users in an identity management system. Service Provider is a service that the user wants to access (such as a public or a private web application).

Navigation Path

Select **Manage > Policy Objects** and then select **SAML Identity Provider** from the Object Type Selector.

Adding or Editing SAML Identity Provider

Use the Add or Edit SAML Identity Provider dialog box to add a new SAML Identity Provider or edit an existing row.

Navigation Path

Select **Manage > Policy Objects** and then select **SAML Identity Provider** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Field Reference

Table 6-38 Add or Edit SAML Identity Provider

Element	Description
Name	Enter a name for the SAML Identity Provider, between 4 and 256 characters.
Description	(Optional) Enter a description for the SAML Identity Provider.
Sign In URL	This URL is used for signing into the Identity Provider. It must begin with http:// or https:// (not case sensitive) and the length of the Sign In URL must be less than or equal to 500 characters. The Sign In URL field allows only the following special characters: :, /, *, [,],.
Sign Out URL	(Optional) This URL is used for redirecting to when signing out of the Identity Provider. It must begin with http:// or https:// (not case sensitive) and the length of the Sign Out URL must be less than or equal to 500 characters. The Sign Out URL field allows only the following special characters: :, /, *, [,],.

Element	Description
Base URL	(Optional) This is the clientless VPN's base URL. This URL is used in SAML metadata that is provided to third-party identity providers so that they can redirect end users back to the ASA device. If the Base URL is not configured it is retrieved from the ASA device's hostname and domain name. For example, if the host name is ssl-vpn and domain name is xyz, the Base URL used is https://ssl-vpn.xyz.com. The Base URL must begin with http:// or https:// (not case sensitive) and the length of the Base URL must be less than or equal to 500 characters. The Base URL field allows only the following special characters: :, /, *, [,],. **Note** Either Base URL or Domain Name must be configured in the ASA device to configure SAML.
Identity Provider	Select the Identity Provider from the CA Servers Selector Dialog box. Identity Provider is the service that can assert a user's identity to another resource. An Identity Provider is responsible for authenticating users in an identity management system.
Service Provider	(Optional) Select the Service Provider from the CA Servers Selector Dialog box. Service Provider is the service that the user wants to access (such as a public or private web application).
Request Timeout	(Optional) Enter a value between 1 and 7200. By default there is no SAML timeout.
Enable Signature	(Optional) Enable or disable signature in SAML request. If this is enabled, you must configure the Service Provider. Select the cipher suite for the signature in the Authentication Request drop-down. When you enable the signature, the SHA-256 cipher suite is selected by default. You can change the cipher suite in the Authentication Request drop-down. By default, the Signature is disabled and the Authentication Request drop down is hidden. **Note** You can specify an Authentication Request for a SAML signature, only for ASA 9.8.1 and above.
Enable Internal	(Optional) Enable or disable the Internal flag for SAML Identity Provider. When enabled, the Internal flag identifies the Identity Provider in a private network and the SAML Identity Provider can only be accessed through a WebVPN connection. This also implies that the ASA works as a gateway. By default, the Internal flag is disabled and the Identity Provider can be directly accessed.

Element	Description
Enable Force Re-Authentication	(Optional) Enable or disable Force Re-authentication for SAML Identity Provider. When enabled, the identity provider must authenticate the presenter directly rather than rely on a previous security context. By default, the Force Re-authentication flag is enabled.
Category	(Optional) Select a category between CAT-A to CAT-J.
Allow Value Override per Device	(Optional) If the Allow Value Override per device is selected, edit the Overrides.

Understanding and Specifying Services and Service and Port List Objects

Many policies in Security Manager require that you identify a service to which the policy applies. A service is a protocol and port definition that identifies a particular type of traffic. In many cases, you can specify the service directly in the policy. You can also select service policy objects that define the required services, or use a combination of service objects and policy-specific service designations.

Service objects are convenient because you can create objects to represent the composition of a particular application, or you can model them after the logical organizations that exist on your network, such as a development team or corporate department. There are two types of service policy object:

- Service group—Can contain one or more service, including other service objects. This is the type of service object that was available in all Security Manager 3.x releases.
- Service object—Can contain a single service.

When configuring a policy that requires that you identify a service, you can select or create service objects by clicking the **Select** button next to the Services field. To create a new service from the selection dialog box, click the **Add** button beneath the service list and select a type: group or object. You can also create services from the Policy Object Manager by selecting **Services > Services** from the table of contents and clicking the **Add Object** button and selecting group or object. For information on the specific fields available when creating a service object, see Configuring Service Objects, page 6-103.

Security Manager includes a comprehensive collection of predefined service group objects, including ICMP messages and objects for commonly used services such as HTTP, Syslog, POP3, Telnet, and SNMP. Before using a predefined service group object, you should review the object definition to verify that it conforms to your network implementation. If the predefined object does not meet your needs (for example, if you require different destination ports), you can create a new service object from scratch or based on a copy of an existing object. For more information, see Cloning (Duplicating) Objects, page 6-14.

Whether you are creating a service object or specifying services directly in a policy, you can specify services using the following formats. As you type, Security Manager might prompt you with text-completion options related to your entry. You can select a value from the list and press Enter or Tab. You can enter more than one service by separating services with commas.

- *protocol*, where the protocol is 1-255 or a well known protocol name such as tcp, udp, gre, icmp, and so forth. If you enter a number, Security Manager might convert it to the associated name.
- **icmp/***message_type*/*message_code*, where the message type is 1 to 255 or a well-known ICMP message type name such as echo, and the message code is 0 to 255 (for example, **icmp/unreachable/1** or **icmp/echo-reply**).

- **icmp6/***message_type*/*message_code*, where the message type is 1 to 255 or a well-known ICMP message type name such as echo, and the message code is 0 to 255 (for example, **icmp6/unreachable/1** or **icmp6/echo-reply**).
- **{tcp | udp | tcp&udp}/**{*destination_port_number* | *port_list_object*} where the destination port number is 1-65535 or the name of a port list object. You can enter a range of ports using a hyphen, for example, 10-20. The source port number is the Default Range port list object. The Default Range object includes either all ports (1-65535) or all secure ports (1024-65535), depending on the setting you select in the Policy Objects Page, page 11-66 (select **Tools > Security Manager Administration > Policy Objects**).

  For example, defining a service as tcp/10 means that 10 is the destination port and no source port is defined.

  When you specify ports, you can also use the following special keywords: **lt** (less than), **gt** (greater than), **eq** (equal to), and **neq** (not equal to), followed by a number. For example, **lt 440** specifies all ports less than 440.

Tip To create port list objects, select **Services > Port Lists** in the Policy Object Manager and click the **Add Object** button. For more information, see Configuring Port List Objects, page 6-102.

- **{tcp | udp | tcp&udp}/**{*source_port_number* | *port_list_object*}**/** {*destination_port_number* | *port_list_object*}, where the source and destination port numbers are 1-65535 or the name of a port list object. You can enter a range of ports using a hyphen, for example, 10-20.

  For example, defining a service as tcp/10/20 means that 10 is the source port and 20 is the destination port. If you do not want to specify a destination port, use the Default Range port list object, for example, tcp/10/Default Range.
- (Service groups only) *service_object_name*, which is the name of another existing service object. Specifying other objects lets you nest object definitions. Click **Select** to select a service object or to create a new object.

Note The following ICMP message types which are applicable only on IOS devices are automatically replaced with ASA/PIX/FWSM device supported ICMP message types.

- ICMP-Mobile-Redirect
- ICMP-Host-Unreachable
- ICMP-Network-Redirect
- ICMP-Port-Unreachable
- ICMP-Protocol-Unreachable
- ICMP-Reassembly-Timeout
- ICMP-Redirect
- ICMP-protocol-redirect

Related Topics

- Selecting Objects for Policies, page 6-2
- Creating Policy Objects, page 6-9
- Editing Objects, page 6-12

- How Service Objects are Provisioned as Object Groups, page 6-108
- Using Category Objects, page 6-13
- Managing Object Overrides, page 6-17
- Allowing a Policy Object to Be Overridden, page 6-18

Configuring Port List Objects

Use the Port List dialog box to create, edit, or copy a port list object. Each port list object can contain one or more ports or port ranges (for example, 1-1000 and 2000-2500). Additionally, a port list object can include other port list objects.

You typically use port list objects when defining services, but you can also use them in various policies to identify a port rather than typing in the port number. For more information about using port lists in service definitions, see Understanding and Specifying Services and Service and Port List Objects, page 6-100.

Tip The predefined Default Range port list object includes either all ports (1-65535) or all secure ports (1024-65535), depending on the setting you select in the Security Manager Administration window (select **Tools > Security Manager Administration > Policy Objects** and see Policy Objects Page, page 11-66).

Navigation Path

Select **Manage > Policy Objects**, then select **Services > Port Lists** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Understanding and Specifying Services and Service and Port List Objects, page 6-100
- Configuring Service Objects, page 6-103

Field Reference

Table 6-39 Port List Dialog Box

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-9.
Description	An optional description of the object.

Table 6-39 Port List Dialog Box (continued)

Element	Description
Ports	The ports or ranges included in the port list object, for example, 443, or 1-1000. You can define a single port, a range of ports, multiple port ranges, or any combination of single ports and ranges. Separate multiple entries with commas. Port values range from 1 to 65535. You can use the following operators to identify ranges: • **gt**—Greater than. For example, gt 1000. • **lt**—Less than. For example, lt 1000. • **eq**—Equals. For example, eq 1000. However, **eq 1000** has the same meaning as simply entering **1000**. • **neq**—Does not equal. For example, neq 1000. If you use this operator, you can include only the neq value in the Ports field. However, you can include port ranges in the object. Thus, if you want to create an object that specifies all ports from 1000-1200 except for 1150, create a port list object for the 1000-1200 range, and another object that specifies neq 1150 and that includes the other port list object.
Port Lists	The other port list objects included in the object, if any. Enter the name of the port lists or click **Select** to select them from a list or to create new objects. Separate multiple entries with commas.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Configuring Service Objects

Use the Add and Edit Service dialog boxes to create or edit service objects. You can create a service object to describe a type of traffic carried by the devices in your network. When creating a service object, you must specify the protocol used by the service.

When you create a service object, you must choose the object type:

- Service Group—Can contain one or more services, including other service objects. This is the type of service object available in all Security Manager 3.x releases.
- Service object—Can contain a single service.

Security Manager provides many predefined service group objects. Before creating an object, scan the list in the Policy Object Manager to see if an existing object fits your needs. Note that although you can duplicate a predefined object, you cannot edit it.

Cisco Security Manager supports the service objects whose definitions are available in the show running configuration. For the predefined objects, the definition would not be available in the show running configuration. Therefore, any policies configured with these predefined objects in ASA device would not be discovered in Cisco Security Manager.

In order to align with device behavior, in Cisco Security Manager version 4.17, support to these predefined objects was introduced. The ASA predefined objects will be discovered, provided, the device is updated with the object whenever a new predefined service object is added in the ASA. This feature is supported for ASA supporting images across all versions.

Note The PPTP predefined object is not supported.

However, Cisco Security Manager does not support activity validation with respect to ASA versions. Also, the ICMP and ICMPv6 predefined objects of Cisco Security Manager are converted to device predefined objects. Hence, any usage of Cisco Security Manager's predefined objects causes negation and re-creation of that policy.

Navigation Path

Select **Manage > Policy Objects**, then select **Services > Services** from the Object Type Selector. Right-click inside the work area and select **New Object** (and select an object type) or right-click a row and select **Edit Object**.

Related Topics

- Understanding and Specifying Services and Service and Port List Objects, page 6-100
- Policy Object Manager, page 6-4

Field Reference

Table 6-40 Add and Edit Service Dialog Boxes

Element	Description
Name	The object name. If you are using the object for ASA or PIX devices running software version 8.x, limit the length of the name to 64 characters. For other devices the name can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects, page 6-9.
Description	An optional description of the object.

Table 6-40 Add and Edit Service Dialog Boxes (continued)

Element	Description
Services (for groups) Service (for objects)	The services to include in this policy object. When creating a Service Group, you can enter more than one service by separating services with commas. When creating a Service Object, you can enter one service only. You can specify services using the following formats. As you type, Security Manager may prompt you with text-completion options related to your entry. If you enter a service that translates directly to a predefined service object, the entry is converted to the predefined object name; for example, TCP/80 is converted to HTTP. • *protocol*, where the protocol is 1 to 255 or a well known protocol name such as tcp, udp, gre, icmp, and so forth. If you enter a number, Security Manager might convert it to the associated name. • **icmp/***message_type/message_code*, where the message type is 1 to 255 or a well-known ICMP message type name such as echo, and the message code is 0 to 255 (for example, **icmp/unreachable/1** or **icmp/echo-reply**). • **icmp6/***message_type/message_code*, where the message type is 1 to 255 or a well-known ICMP message type name such as echo, and the message code is 0 to 255 (for example, **icmp6/unreachable/1** or **icmp6/echo-reply**).
	• **{tcp | udp | tcp&udp}/**{*destination_port_number* | *port_list_object*} where the destination port number can be 1 to 65535, or the name of a port list object. You can enter a range of ports using a hyphen, for example, 10-20. In this instance, the source port number is the Default Range port list object, which specifies the range 1-65535. (See Configuring Port List Objects, page 6-102 for information about creating and editing port list objects.) Whenever you specify ports, you can also use the following special keywords: **lt** (less than), **gt** (greater than), **eq** (equal to), and **neq** (not equal to), followed by a number. For example, **lt 440** specifies all ports less than 440. • **{tcp | udp | tcp&udp}/**{*source_port_number* | *port_list_object*}**/**{*destination_port_number* | *port_list_object*}, where the source and destination port numbers can be 1 to 65535, or the name of a port list object. You can enter a range of ports using a hyphen, for example, 10-20. • (Service groups only) *service_object_name*, which is the name of another existing service object. Specifying other objects lets you nest object definitions. Click **Select** to select a service object or to create a new object.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.

Table 6-40 Add and Edit Service Dialog Boxes (continued)

Element	Description
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Note The following ICMP message types which are applicable only on IOS devices are automatically replaced with ASA/PIX/FWSM device supported ICMP message types.

- ICMP-Mobile-Redirect
- ICMP-Host-Unreachable
- ICMP-Network-Redirect
- ICMP-Port-Unreachable
- ICMP-Protocol-Unreachable
- ICMP-Reassembly-Timeout
- ICMP-Redirect
- ICMP-protocol-redirect

How Policy Objects are Provisioned as Object Groups

Object groups are a feature of ASA, PIX, FWSM, and IOS 12.4(20)T+ devices that enable you reduce the size of access rules by grouping objects such as IP hosts, networks, protocols, ports, and ICMP message types. Although the functionality of object groups is similar to the functionality of policy objects in Security Manager, there are several important differences in implementation.

As a result, when deploying policies to a device, it is not always possible to create object groups that are an exact copy of the policy objects that you configured in Security Manager. To take one example, policy object names are unique per object type in Security Manager (that is, you can define a network/host object and a service object with the same name), whereas object groups of all types defined on the device share a single naming scheme. Therefore, if you deploy a network/host object whose name matches an existing service object group on the device, a suffix is added to the name of the network/host object to distinguish it from the service object group.

Note For information about the options available when deploying object groups, see Deployment Page, page 11-13.

Similarly, when discovering policies on a device, it is not always possible to create policy objects that are an exact copy of the object groups that are configured on the device. However, Security Manager preserves as much of the original configuration as possible.

Note For IOS devices, any policy objects that are used by access control list 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.

The following sections describe the changes that are made when provisioning policy objects to object groups on the device, or when creating the policy objects when discovering policies on these devices:

- How Network/Host, Port List, and Service Objects are Named When Provisioned As Object Groups, page 6-107
- How Service Objects are Provisioned as Object Groups, page 6-108

How Network/Host, Port List, and Service Objects are Named When Provisioned As Object Groups

In most cases, network/host, port list, and service objects can be provisioned as object groups without changing the object name. Table 6-41 on page 6-107 describes how object names are changed when the names cannot be converted directly to object groups on supported devices.

Note The predefined network/host object **any** is not provisioned as an object group.

Table 6-41 How Network/Host, Port List, and Service Objects are Named as Object Groups

Condition	New Name	Examples
Object name includes a space.	Space is replaced with an underscore.	An object named **my object** is provisioned as an object group named **my_object**.
Object name is longer than 64 characters (the maximum supported by object groups).	Name is truncated so that any suffixes required by the object group (such as _TCP or _UDP, or unique numbers, such as _1) can be added while remaining within the 64-character limit.	
Device already has an object group (Protocol/ICMP/Service) with the same name.	A numeric suffix is added to the name, starting from 1.	If you have a network/host object named **West** and the device already has a TCP service object group named **West**, the name of the object group is changed to **West_1** when deployed.
You have already created a network/host object group with the same name.	A numeric suffix is added to the name, starting from 1.	If you have a network/host object and a port list or service object that are both named **West**, the network/host object is deployed as **West** and the port list is deployed as **West_1**.

Note For ASA software versions 8.2 and earlier, if you create an object of the type Network Object on Security Manager, upon discovering the ASA device with an object of the same object name but of type Network-Object Group, Security Manager does not create a new object. Instead, it reuses the existing objects. However, for ASA software versions 8.3 and later, if you create an object of type Network Object on Security Manager, upon discovering the ASA device with an object of the same object name but of type Network-Object Group, Security Manager creates new objects, say, name_1, name_2, and so on. This implies that for Security Manager managing ASA devices that are running the software version 8.2 or earlier, it creates new objects upon upgrading the ASA to version 8.3 or later.

Related Topics

- Understanding Networks/Hosts Objects, page 6-80
- Understanding and Specifying Services and Service and Port List Objects, page 6-100
- How Service Objects are Provisioned as Object Groups, page 6-108
- How Policy Objects are Provisioned as Object Groups, page 6-106

How Service Objects are Provisioned as Object Groups

The following table describes how Security Manager creates object groups when deploying service objects to supported devices.

Tip For ASA 8.3+ devices, service objects are provisioned using the **object service** command instead of the **object-group** command.

Table 6-42 How Service Objects are Provisioned as Object Groups

Condition	Generated Object Group	Examples

Service object contains the ICMP protocol and ICMP message types.	Generates an ICMP-type object group with the same name as the service object.	Service object service1: **icmp/icmp-echo, 23**
		Object group:
		`object-group icmp-type service1`
		`  icmp-object icmp-echo`
		`  icmp-object 23`

Service object contains only protocols.	Generates a protocol object group with the same name as the service object.	Service object service1: **tcp, gre, 34**
		Object group:
		`object-group protocol service1`
		`  protocol-object tcp`
		`  protocol-object gre`
		`  protocol-object 34`

Service object uses port list objects for both source and destination ports.	Generates service object groups that match the port list objects.	

Table 6-42 How Service Objects are Provisioned as Object Groups (continued)

Condition	Generated Object Group	Examples

Service object contains multiple ports or port ranges, but does not use a port list object for the source ports.	Generates service object group with the name <ObjectName>.src for the source ports.	Service object serv1: **tcp/400,600/23-80**
		Object group:
		`object-group service serv1.src tcp`
		`  port-object eq 400`
		`  port-object eq 600`

Service object contains multiple ports or port ranges, but does not use a port list object for the destination ports.	Generates service object group for the destination ports with the same name as the service object.	Service object serv1: **tcp/400,600/23-80, 566**
		Object group:
		`object-group service serv1 tcp`
		`  port-object range 23 80`
		`  port-object eq 566`
		`object-group service serv1.src tcp`
		`  port-object eq 400`
		`  port-object eq 600`

Service object contains the TCP&UDP protocol and includes defined ports.		Service object serv1: **tcp&udp/400,600/23-80, 566**
		Object group:
		`object-group service serv1 tcp`
		`  port-object range 23 80`
		`  port-object eq 566`
		`object-group service serv1.src tcp`
		`  port-object eq 400`
		`  port-object eq 600`
		`object-group protocol tcp-udp`
		`  protocol-object tcp`
		`  protocol-object udp`

Related Topics

- Understanding and Specifying Services and Service and Port List Objects, page 6-100
- How Network/Host, Port List, and Service Objects are Named When Provisioned As Object Groups, page 6-107
- How Policy Objects are Provisioned as Object Groups, page 6-106