Managing Policies

Policies define the security characteristics and requirements of your network, such as rules on who can access the network, what applications they can use, what web sites they can visit, and so forth. Policies implement your organization’s network security policies.

Depending on whether you are managing multiple devices, or you are directly configuring a CX device, policies can be shared among many devices or local to a single device.

The following topics explain policy basics in more detail.

- Policy Concepts, page 1
- Configuring the Device, page 2
- Policy Basics, page 5

Policy Concepts

You should understand the following basic concepts to effectively use the application and configure your device. Some of these concepts apply to Multiple Device mode only.

Rule-Based Policies versus Configuration Settings

There is a fundamental difference between a rule-based policy, such as access policies, and configuration settings, such as authentication settings.

Rule-based policies are an ordered list of policies. A policy is a single rule that defines some aspect of your firewall security policy. For example, deny access to gambling web sites, or require users to authenticate. Incoming traffic is compared against each rule, starting from the top, until a match is found. When matched, the actions defined in the rule are applied to the traffic. Examples include access, identity, and decryption policies.

Configuration settings are simple. You either configure an option or not, and your settings apply to the device as a whole, or to all traffic as a whole. Examples include authentication settings and decryption settings.

Policy Sets

Rule-based polices are composed of policy sets. A policy set is a named container within which you organize the individual policies or rules. The order of the policies in a policy set matters. In Multiple Device mode, you can share a policy set among devices.
Policy object

A definition of some characteristic that you can use in a policy. For example, you use a URL object to define the URL category that you want to control access to in an access policy. Because policy objects are separate entities, you can reuse them in multiple policies. In Multiple Device mode, the objects are configured on a device only if a policy configured on the device uses the object.

Shared versus Local Policies or Settings

In Single Device mode, all policies and settings are local, that is, they apply to the device you are configuring only.

In Multiple Device mode, you have the option to share a policy or setting among devices. In this case, you can consider “policy” to generically apply to any shareable policy or configuration setting.

When you share a policy, each device to which the policy is assigned gets the same settings. For rule-based policies, you share policy sets, so that each device might use shared policies yet include a different collection of policy sets. For configuration settings, you share the entire page of settings.

You cannot share all types of policy. Some settings are global and apply to all devices. Other settings are always local to a single device. For devices configured as high availability pairs, you share policies based on the pair’s logical name, so that each member device gets the same configuration.

Shared versus Universal Policy Sets

There are two types of shared policy set: shared among specific devices and universal.

Policy sets shared among specific devices are applied to those devices only. Any devices you add to the inventory are not affected.

Universal policy sets are applied to every device (of the correct device type), even devices that you add to the inventory in the future. Thus, you can define a set of policies that should always be enforced (for example, you could always block finger traffic).

Universal policy sets apply to access policies only, and there are two pre-defined ones:

- Universal Top—These policies are always at the top of the ordered list of access policies. Traffic is always compared to the matching rules for these policies before any other shared or local policies.

- Universal Bottom—These policies are always at the bottom of the list. Traffic is not compared to these rules until all other access policies have been evaluated. This would be where you place a Deny All policy to cover any remaining traffic that is not explicitly allowed, for example.

Whenever you edit policies in a Universal policy set, you are editing them for all devices, whether you do it while configuring a specific device in Device view, or you do it in Repository view.

Configuring the Device

To configure most policies and device settings, select Configurations > Policies/Settings.

The Device Configuration page has a tabbed layout, with each tab representing a different rule-based or configuration settings policy. You can open and close tabs as you need them. If a tab is not already open, you can select it from the drop-down menu icon on the right side of the tabs. When you have a lot of tabs open, tab names might be truncated.
Use the **Overview** tab to get a general picture of the device's configuration.

The overall contents of the page itself differs depending on your mode. In Single Device mode, the page contains the tabs only. In Multiple Device mode, the tabs appear under two distinctly separate views.

**Device View**

In Device view, the left column shows the list of devices in the inventory. You select a device to see and edit its configuration. Use the filter box to help you find a device, or change the View By setting to see the inventory organized in different ways.

Mouse over a device in the selector to see details such as device types and model, management addresses, and mode.

**Repository View**

In Repository view, you can see the device inventory with detailed information on the Overview tab. On the policies tabs, you see a list of all policies in the system across all devices. Each policy is a separate expanding/collapsing folder, open it to see the policy contents. From here, you can find and change policies independently of the device, making it easy to change shared policies, or even to make across-the-board changes to a type of policy for many devices.

After making changes in Repository view, you can return to Device view and verify you are getting the desired configuration for each device.

The following graphic explains the various elements of the Device Configuration page. The image shows Multiple Device mode; in Single Device mode, the tabbed area is the entire page.

1. Device/Repository view toggle (Multiple Device mode).
2. Device Selector (Multiple Device mode).
3. Policy action buttons. For rule-based policies, select a rule or policy set to see action buttons related to your selection.
4. Move policy or policy set handle. For rule-based policies, click and hold this icon to drag the policy or policy set to the desired position.
5. Expand All/Collapse All button. For rule-based policies, this opens or closes all policy sets.
6 Notification icons. These identify pending changes, potential user editing conflicts, or other important information. Mouse over for detailed information. Clicking the icon can also provide information, but in the case of the Pending Changes icon, clicking performs an action, taking you to the Pending Changes page.

7 Policy and settings tabs. The Overview tab is always visible. If you have more tabs open than fit, tab scroll arrows appear, allowing you to scroll right and left.

8 Feature status: Shows whether intrusion prevention (Next Generation IPS filtering) and malware protection (web reputation) are on or off for the device. Mouse over the On/Off indication to see details about the device-level profile for each feature. There is an Edit Settings link in the popup to open the settings tab for the feature, where you can change the status and profile.

9 Tab menu. Open tabs from this menu.

The following topics provide an overview of the policies and settings available on the Device Configuration page.

**Device Configuration Policies and Settings**

You can configure the following policies and settings on the Device Configuration page. The available options differ between Single Device mode and Multiple Device mode and by device type.

**Basic Policies**

These policies control traffic passing through the device.

- **Access Policies**—Control access to the network. In Single Device mode, these are CX policies only. In Multiple Device mode, you can configure both CX and ASA access policies.

- **NAT Policies**—(ASA, Multiple Device mode only.) Translate network addresses between internal and external versions.

**Logging**

These policies control device logging.

- **ASA CX Logging**—(CX only.) Controls logging levels for CX devices.

- **Syslog Settings**—Configure syslog servers for ASA and CX, and logging settings for ASA devices. ASA options are available in Multiple Device mode only.
Basic Device Properties

These policies configure functional device settings.

- **Packet Capture**—(CX only.) Set packet capture options and perform global capture of dropped packets.
- **Interfaces**—(ASA, Multiple Device mode only.) Configure device interfaces.
- **High Availability**—(ASA, Multiple Device mode only.) Configure failover between devices to increase network reliability.
- **Traffic Redirection**—(ASA, Multiple Device mode only.) Configure traffic redirection from the ASA to its CX module.
- **Intrusion Prevention**—(CX only.) Enable Next Generation IPS filtering and configure device-level settings.
- **Malware Protection**—(CX only.) Enable web reputation filtering and configure device-level settings.

Decryption

These policies control SSL/TLS decryption.

- **Decryption Settings**—(CX only.) Enable decryption policies and identify the Certificate Authority (CA) certificate that the device will use to managed decrypted traffic flows.
- **Decryption Policies**—(CX only.) Determine whether to decrypt TLS/SSL traffic flows. Decrypting HTTPS and other TLS/SSL traffic flows provides greater visibility into the content of encrypted traffic flows, such as application behaviors, and more detailed threat analysis.

Authentication and Identity

These policies control user and group identification, which enables identity-based access control.

- **AD Agent**—(CX only.) If you are using Active Directory, you can install the Context Directory Agent (CDA) or Active Directory agent to provide passive user-to-IP address mappings based on Windows login authentications.
- **Auth Settings**—(CX only.) Control active authentication timeouts and refresh intervals.
- **Identity Policies**—(CX only.) Determine whether a user must authenticate. The purpose of authentication is to determine the user who is involved in a traffic flow, so that you can apply identity-based access policies to traffic flows.

Policy Basics

The following topics explain how to configure local (single device) or shared (multiple device) policies.
Configuring Policy Sets

Use policy sets to define a segment of a rule-based policy. The policy set appears as a heading row in the policy list, and you can open and close it to show or hide the policies it contains. The policy set header shows the number of policies contained in the set. In Multiple Device mode, you can share policy sets among devices.

Procedure

**Step 1** Select Configurations > Policies/Settings and open the tab for the rule-based policy. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

**Step 2** Select a policy set, then do one of the following:

- To create a new policy set, click the Add Policy Set button. You can also create a new policy set when a policy is selected.
- To edit an existing policy set, click the Edit Policy Set button. You can also click into the policy set fields in the table and type your changes.
- To create a copy of a policy set, click Duplicate Policy Set button. In Multiple Device mode, if you duplicate a Universal policy set, the copy is created as a local policy set.

**Step 3** Fill in the policy set properties:

- **Policy Set Name**—The name of the policy set.
- **Policy Set Type**—The type of policies that will be included in this policy set.
- **Description**—A description of the policy set.
- **Devices**—(Multiple Device mode only.) The devices that should share this policy set. In Device view, this is initially set to include the device you are configuring; in Repository view, it is empty ("not installed"), and the policy set will not be assigned to any device unless you make a selection.
- **Tags**—Words or phrases that help you identify this item. For example, you can assign the same tag to multiple items to make it easy to view them through a search. Tags could identify use case, purpose, or any other characteristic you choose. These tags are for your purposes only, and do not affect how the system or policies function. You can enter (or select) more than one tag.
- **Ticket ID**—A case or ticket identifier from your support system (for example, Remedy). If you are making a change that is related to a network support case, you can enter the ticket ID here for tracking purposes. You can enter new IDs or select from existing IDs that are used in pending changes; specify as many separate IDs as needed. (The list does not show IDs used in already-committed changes.)

**Step 4** Click Save Policy Set.

**Step 5** If necessary, move the policy set so that it is in priority order. Policies are applied on a first-match basis, and the order is defined not only by their order within a policy set but also by the order of the policy sets themselves.
Configuring Rule-Based Policies

Policies define the security characteristics and requirements of your network, such as rules on who can access the network, what applications they can use, what web sites they can visit, and so forth. Policies implement your organization's network security policies.

Policies are grouped into policy sets. Policies are evaluated on a first-match basis; incoming traffic is compared to the match criteria for each policy in a set from top to bottom, and the first policy whose traffic matching criteria is satisfied defines the security policy applied to the traffic. Thus, order within a policy set is critical. If there are multiple policy sets, the sets are evaluated in the same order.

Procedure

Step 1 Select **Configurations > Policies/Settings** and open the tab for the rule-based policy. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

Step 2 Do any of the following:

- To add a new policy, use one of the **Add Policy** buttons. If you select a policy set, you can add the policy at the top or bottom of the set. If you select a policy, you can add the new one above or below it.
- To edit an existing policy, select the policy and click the **Edit Policy** button.
- To base a new policy on a similar existing policy, select the policy and click the **Duplicate Policy** button.

A form opens with the policy properties for the type of policy you are creating or editing. For detailed information about these properties, click the Help link in the form or see the chapter for the policy in this guide.

Step 3 Fill in the policy properties and click **Save Policy**.

Step 4 If necessary, move the policy so that it is in priority order. Policies are applied on a first-match basis, so you must ensure that policies with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

To move a policy set or rule, you click and hold the Move icon (the vertical double-headed arrow on the left margin) and drag it to the policy after which you want to insert it. You can also simply edit the sequence number and change it to the desired value.

Moving Policy Sets and Rules

In rule-based policy sets, the order of the policy rules matters, because they are matched to traffic from top to bottom and the first match determines the policy applied to the traffic. Thus, you need to move policies and policy sets to ensure they are in the right order.

To move a policy set or rule, you click and hold the Move icon (the vertical double-headed arrow on the left margin) and drag it to the policy after which you want to insert it, as illustrated in the following graphic. You can also simply edit the sequence number and change it to the desired value.
You cannot move policies between policy sets. Instead, you must recreate the rule in the desired policy set.

Changing Policy Sharing Status

(Multiple Device mode only.) For policies and policy sets that allow sharing among devices, you can change the sharing settings, converting local policies to shared and vice versa.

In addition to using this procedure, you can adjust the devices that share a policy set when editing the policy set.

When you apply multiple policy sets of a particular type to the same device, they are evaluated in the same order in which they appear on the policy tab. Use Device view to verify the order for a particular device is the desired one.

Procedure

Step 1 Select Configurations > Policies/Settings and open the tab for the rule-based policy.
You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.
Step 2  Click the shared status link for the policy or policy set. The link is named Device Name for unshared policies, or Shared for those already shared. A popup opens with the actions you can implement for this item. The available commands differ based on current sharing and policy type.

Step 3  In the popup, do any of the following:

- To share a local policy, click Shared, then select the devices that should share the policy. The device currently assigned to the policy is already selected, but you can delete it from the list.
- To change the devices for a shared policy, simply change the devices already listed. You can add or delete devices. Any device you remove is assigned a local policy with the same content.
- To make a shared policy local, click Local.

Step 4  Click Apply.

What to Do Next

When you initially share a policy set with a device, the policy set is added to the top of the policy list for the device; in the case of access rules, just below the universal top policy set. You need to go to the policy tab in Device view for each device you add to a policy set, and move the newly-shared policy set to the desired position.

Making Per-Device Exceptions for Shared Policy Sets

(Multiple Device mode only.) For rule-based policies, you can share policy sets among multiple devices so that the devices provide consistent services. However, it is not uncommon that a given device should implement the same policies as a group of other devices yet also have some unique requirements. For example, you might need to add more restrictive access to a network controlled by a certain device.

By creating per-device exceptions, you can share a common policy set among a group of devices yet also create a few device-specific policies within that otherwise shared policy set. These per-device exceptions can be for one device or for a subset of the devices assigned to the policy set. You cannot share these exceptions with devices that are not already sharing the policy set that contains the exception policy.

Note  Per-device exceptions for rule-based policies are possible with ASA or CX access policies only.

Procedure

Step 1  Select Configurations > Policies/Settings and open the Access Policies tab. You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

Step 2  Do any of the following:

- If the policy does not yet exist, create it, and in the Shared/Local field, select the devices that should implement the policy.
• Edit an existing policy and select the devices that should implement the policy in the **Shared/Local** field.

• For existing policies, click the + button in the **Shared/Local** column and select the devices that should implement the policy.

Leave the **Shared/Local** field blank if you want all devices that share the policy set to implement the policy. If this field contains any specific device, the field defines the complete list of devices that will implement the policy.

---

**Editing Rule-Based Policies and Policy Sets**

After creating a policy set or a policy in the set, you can edit it.

**Procedure**

**Step 1** Select **Configurations > Policies/Settings** and open the tab for the rule-based policy. (Multiple Device mode only). You can open the tab for a specific device you select in Device view, or you can open the policy independently of the device in Repository view.

**Step 2** You then have two options for editing a rule-based policy or policy set. Do either of the following:

• **Traditional**—Select the policy or policy set, then click the **Edit Policy** or **Edit Policy Set** button. A window opens where you can make your changes; click the save button when finished.

• **Inline editing**—If a policy supports inline editing, select the policy or policy set, then make changes directly in the table. Mouse over each column in the row to see possible actions. You can click the + button in a field to add to the column, delete items, change the policy action, click in edit fields and type in different text, and so forth. In access policies, if you select an application that supports behaviors, click the **Behaviors** button to configure them.

---

**Disabling or Enabling Rule-Based Policies**

You can disable a rule-based policy if you want to temporarily stop applying it to traffic. You do not need to delete the policy unless you really no longer need it.

You can also easily enable policies you had disabled.

When disabled, a policy is hashed out in the policy table.

**Procedure**

**Step 1** Select **Configurations > Policies/Settings** and open the tab for the rule-based policy.
Managing Policies

Analyzing Shared Policy Assignments

(Multiple Device mode only.) When working in Repository view, you can analyze how your policies are shared among devices. To open Repository view, select Configurations > Policies/Settings, then select Repository above the device selector.

As you select policy tabs, the following links appear in the left pane if they apply to the tab. Use these links to filter and analyze policy assignments:

- **All**—View all policies regardless of assignments.
- **Local**—View only those policies that are local to a device. That is, policies that are not shared.
- **Shared**—View only those policies that are defined as shared, including Universal policy sets. You can click the **Shared** link in the policy heading row to see the list of devices using the policy.
- **Not Installed**—View only those policies that are defined but not yet assigned to any device. You can click the **Not Installed** link in the policy heading row to assign the policy.

Deleting Policies or Policy Sets

Delete policies or policy sets when you no longer need them. However, before you delete a policy or policy set, consider these methods of temporarily disabling them:

- **Policies**—You can temporarily disable a policy by disabling it. When you commit changes, devices assigned the policy will no longer enforce it.

- **Policy Sets**—(Multiple Device mode only.) Unassign the policy set from any device that references it. When you commit changes, the entire policy set is removed from the device and replaced with whatever new policy sets you assigned.

Procedure

Step 1  Select Configurations > Policies/Settings and open the tab for the rule-based policy.

Step 2  Do any of the following:
• To delete a policy, select it and click the **Delete Policy** button.

• To delete a policy set, select it and click the **Delete Policy Set** button.