Policy Management

The following topics describe how to manage policies on the Management Center:

- Policy Deployment, page 1
- Policy Comparison, page 8
- Policy Reports, page 10
- Out-of-Date Policies, page 11
- Policy Warnings, page 12
- Guidelines for Optimizing Access Control Rules, page 13
- Performance Considerations for Limited Deployments, page 15

Policy Deployment

After you use the Firepower Management Center to configure your deployment, and any time you make changes to that configuration, you must deploy the new configuration to affected devices.

This deploy action distributes the following configuration components:

- Access control policies and all associated policies: DNS, file, identity, intrusion, network analysis, SSL
- Any associated rule configurations and objects associated with a policy to be deployed
- Intrusion rule updates
- Device and interface configurations
- Platform settings
- VPN deployments
- Network discovery policy
- NAT policies

You can configure the system to deploy automatically by scheduling a deploy task or by setting the system to deploy when importing intrusion rule updates. Automating policy deployment is especially useful if you allow intrusion rule updates to modify system-provided base policies for intrusion and network analysis. Note
that intrusion rule updates can also modify default values for the advanced preprocessing and performance options in your access control policies.

In a multi-domain deployment:

• You can deploy changes for any domain to which your user account belongs.
• You can deploy changes for all subdomains at the same time if you switch to the Global domain before deploying.
• You can deploy changes for an individual subdomain if you switch to the leaf domain before deploying.

After you initiate a deployment, you can view the deployment status in the Message Center.

### Deploying Configuration Changes

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Approver</td>
</tr>
</tbody>
</table>

The Deploy Policies dialog lists all devices where the system has identified an out-of-date configuration. The Version field at the top of the dialog specifies the time at which you last made configuration changes. The Current Version column in the device table specifies the time of the most recent prior deployment to that device.

⚠️ **Caution**

Deploying configuration changes may cause a short pause in traffic flow and processing as the Snort process restarts, and may also cause a few packets to pass uninspected. On Firepower 7010, 7020, and 7030 managed devices, deploying configuration changes can take up to five minutes. To minimize inconvenience, deploy during a change window.

### Before You Begin

• Review the guidelines for deploying configuration changes; see Guidelines for Deploying Configuration Changes, on page 4.

### Procedure

**Step 1** Click the Deploy button.
The Deploy Policies dialog appears.

**Step 2** Identify the devices where you want to deploy configuration changes. You can:

• Sort — Sort the device list by clicking a column heading.
Filter — Filter the device list. To do so, click on the arrow in the upper, right corner of any column heading in the display; enter text in the Filter text box; and press Enter.

**Step 3** Optionally, expand the device listing to view the configuration changes to be deployed.

The system marks out-of-date policies with an index (◯) icon.

**Step 4** Choose the devices where you want to deploy configuration changes.

**Step 5** Click **Deploy**.

**Step 6** If the system identifies errors or warnings in the changes to be deployed, you have the following choices:

- Click **Proceed** to continue deploying without resolving error or warning conditions. This button is enabled if the system identifies only warnings for the deployment; it is disabled if the system identifies an error in the deployment.
- Click **Cancel** to exit without deploying. Resolve the error and warning conditions, and attempt to deploy the configuration again.

---

**What to Do Next**

- Optionally, monitor the deployment status; see Viewing Deployment Messages.
- If configuration fails to deploy, see Guidelines for Deploying Configuration Changes, on page 4 for possible solutions.

---

**Forcing Deployment to a Device**

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Leaf only</td>
<td>Admin/Network, Admin/Security, Approver</td>
</tr>
</tbody>
</table>

You can deploy configuration settings to a device even if you do not make changes that would typically mark the configuration as out-of-date.

⚠️ **Caution**

Deploying configuration changes may cause a short pause in traffic flow and processing as the Snort process restarts, and may also cause a few packets to pass uninspected. On Firepower 7010, 7020, and 7030 managed devices, deploying configuration changes can take up to five minutes. To minimize inconvenience, deploy during a change window.
### Procedure

**Step 1** Choose Devices > Device Management

**Step 2** Click the edit icon (✏️) next to the device where you want to force deployment. In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

**Step 3** Click the Device tab.

**Step 4** Click the edit icon (✏️) next to the General section heading.

**Step 5** Click the Force Deploy arrow (🗑️).

**Step 6** Optionally, expand the device listing to view the configuration settings to be deployed. The system marks out-of-date policies with an index (🪞) icon.

**Step 7** Click Deploy.

**Step 8** If the system identifies errors or warnings in the configuration settings to be deployed, you have the following choices:

- Click **Proceed** to continue deploying without resolving error or warning conditions. This button is enabled if the system identifies only warnings for the deployment; it is disabled if the system identifies an error in the deployment.

- Click **Cancel** to exit without deploying. Resolve the error and warning conditions, and attempt to deploy the configuration again.

### What to Do Next

- Optionally, monitor the deployment status; see Viewing Deployment Messages.

- If configuration fails to deploy, see Guidelines for Deploying Configuration Changes, on page 4 for possible solutions.

### Guidelines for Deploying Configuration Changes

Keep the following points in mind when deploying configuration changes to managed devices.

#### Important

To minimize inconvenience, deploy during a change window

#### Deployment Consequences

#### Caution

Deploying configuration changes may cause a short pause in traffic flow and processing as the Snort process restarts, and may also cause a few packets to pass uninspected. On Firepower 7010, 7020, and 7030 managed devices, deploying configuration changes can take up to five minutes.
• If you edit interfaces and re-deploy, Snort restarts, which causes a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected for all interface instances on the device, not just those that you edited.

• If you are performing application control but disable required detectors, the system automatically enables the appropriate system-provided detectors upon policy deploy. If none exist, the system enables the most recently modified user-defined detector for the application.

• When you deploy changes to a network discovery policy, the system deletes and then redisCOVERs MAC address, TTL, and hops information from the network map for the hosts in your monitored networks. Also, the affected managed devices discard any discovery data that has not yet been sent to the Firepower Management Center.

Troubleshooting

• Do not apply inline configurations to devices deployed passively, and vice versa.

• Do not exceed the capability of your devices.

Complex access control policies and rules can command significant resources and negatively affect performance. When you deploy an access control policy, the system evaluates all the rules together and creates an expanded set of criteria that target devices use to evaluate network traffic.

If you exceed the maximum number of access control rules or invoked intrusion policies supported by a target device, the system displays a warning. The maximum depends on a number of factors, including policy complexity, physical memory, and the number of processors on the device.

• Verify that the devices are the correct model for the features you configured, and are using the correct licenses and minimum versions of the Firepower System. For example, you cannot target stacked 7000 or 8000 Series devices running different versions of the Firepower System.

Auto-deploying

You can configure the system to deploy automatically as follows:

• After the completion of an intrusion rule update

• Using a scheduled task

Snort® Restarts During Configuration Deployment

The following graphic illustrates how Snort restarts can occur when you enable or disable the Inspect traffic during policy apply advanced access control policy option.

Caution

Restarting the Snort process interrupts traffic. Whether this interruption drops traffic or passes traffic without inspection depends on the model of the managed device and how it handles traffic.
Note the following:

- **When you enable** Inspect traffic during policy apply **:**
  - Certain configurations can require the Snort process to restart.
  - When the configurations you deploy do not require a Snort restart, the system initially uses the currently deployed access control policy to inspect traffic, and switches during deployment to the access control policy you are deploying.

- **When you disable** Inspect traffic during policy apply **,** the Snort process always restarts when you deploy.
  - How a Snort restart affects traffic depends on the interface configuration and the platform.
Table 1: Restart Traffic Effects by Managed Device Model

<table>
<thead>
<tr>
<th>On this managed device model...</th>
<th>Configured as...</th>
<th>Traffic during restart is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>7000 and 8000 Series</td>
<td>inline, Failsafe enabled or disabled</td>
<td>passed without inspection</td>
</tr>
<tr>
<td></td>
<td>inline, tap mode</td>
<td>passed without inspection</td>
</tr>
<tr>
<td></td>
<td>routed, switched, transparent</td>
<td>dropped</td>
</tr>
<tr>
<td></td>
<td>passive</td>
<td>dropped</td>
</tr>
<tr>
<td>ASA Firepower</td>
<td>routed or transparent with fail-open</td>
<td>passed without inspection</td>
</tr>
<tr>
<td></td>
<td>routed or transparent with fail-close</td>
<td>dropped</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>inline, Failsafe enabled or disabled</td>
<td>passed without inspection</td>
</tr>
<tr>
<td></td>
<td>passive</td>
<td>dropped</td>
</tr>
</tbody>
</table>

Configurations and Actions that Restart Snort®

The Snort process always restarts when you deploy any of the configurations or take any of the actions listed below.

Caution

Restarting the Snort process interrupts traffic. Whether this interruption drops traffic or passes traffic without inspection depends on the model of the managed device and how it handles traffic.

Access Control Policy:

- initially deploying an access control policy to a managed device
- changing adaptive profiles to enabled or disabled
- replacing the default value of an access control policy Files and Malware Settings advanced setting
- changing a Security Intelligence list, except the Whitelist Now or Blacklist Now options from the right-click context menu
- associating a custom DNS policy with Security Intelligence
- associating an SSL policy or identity policy with an access control policy, or subsequently dissociating the policy by selecting None
- associating an intrusion policy or file policy with an access control rule, or subsequently dissociating the policy by selecting None
- initially adding a category or reputation URL condition to an access control rule

File Policy:

- enabling or disabling file archiving
• adding a file type or file category to a file rule, or subsequently removing it from the rule
• changing a file rule action to or from Detect Files or Block Malware
• enabling or disabling Store files in a file rule

Identity Policy:
• changing an identity rule action to or from Active Authentication to invoke or end the invocation of a captive portal configuration
• changing a currently deployed captive portal configuration

Network Analysis Policy:
The following changes restart the Snort process when you deploy configuration changes in a custom network analysis policy that you select or deselect as the default network analysis policy, or a network analysis policy that you associate with or dissociate from a network analysis rule.
• changing the value for the IMAP, POP, or SMTP preprocessor Base64 Decoding Depth, 7-Bit/8-Bit/Binary Decoding Depth, Quoted-Printable Decoding Depth, or Unix-to-Unix Decoding Depth

Device Management:
• changing the MTU value for an interface other than the management interface
• adding or modifying a VPN deployment
• modifying a high-availability state sharing option

System Update:
• installing a system update or patch that includes a *binary change
• installing a system update or patch that requires a system reboot for any other reason

*Binary changes can include changes to Snort, a preprocessor, or the vulnerability database (VDB).

Policy Comparison

To review policy changes for compliance with your organization's standards or to optimize system performance, you can examine the differences between two policies or between a saved policy and the running configuration. You can compare the following policy types:

• File
• Health
• Identity
• Intrusion
• Network Analysis
• SSL
The comparison view displays both policies in a side-by-side format. Differences between the two policies are highlighted:

- Blue indicates that the highlighted setting is different in the two policies, and the difference is noted in red text.
- Green indicates that the highlighted setting appears in one policy but not the other.

### Comparing Policies

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>feature dependent</td>
<td>feature dependent</td>
<td>Any</td>
<td>feature dependent</td>
<td>feature dependent</td>
</tr>
</tbody>
</table>

### Procedure

**Step 1** Access the management page for the policy you want to compare:

- File — Policies > Access Control > Malware & File
- Health — System > Health > Policy
- Identity — Policies > Access Control > Identity
- Intrusion — Policies > Access Control > Intrusion
- Network Analysis — Policies > Access Control > Network Analysis Policy or Policies > Access Control > Intrusion, then click Network Analysis Policy

**Note** If your custom user role limits access to the first path listed here, use the second path to access the policy.

- SSL — Policies > Access Control > SSL

**Step 2** Click Compare Policies.

**Step 3** From the Compare Against drop-down list, select the type of comparison you want to make:

- To compare two different policies, select Other Policy.
- To compare two revisions of the same policy, select Other Revision.
- To compare another policy to the currently active policy, select Running Configuration.

**Step 4** Depending on the comparison type you selected, you have the following choices:

- If you are comparing two different policies, select the policies you want to compare from the Policy A and Policy B drop-down lists.
• If you are comparing the running configuration to another policy, select the second policy from the Policy B drop-down list.

**Step 5**  
Click **OK**.

**Step 6**  
Review the comparison results:

- Comparison Viewer — To use the comparison viewer to navigate individually through policy differences, click **Previous** or **Next** above the title bar.
- Comparison Report — To generate a PDF report that lists the differences between the two policies, click **Comparison Report**.

---

**Policy Reports**

For most policies, you can generate two kinds of reports. A report on a single policy provides details on the policy's current saved configuration, while a comparison report lists only the differences between two policies. You can generate a single-policy report for all policy types except health.

---

**Note**

Intrusion policy reports combine the settings in the base policy with the settings of the policy layers, and make no distinction between which settings originated in the base policy or policy layer.

---

**Generating Current Policy Reports**

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>feature dependent</td>
<td>feature dependent</td>
<td>Any</td>
<td>feature dependent</td>
<td>feature dependent</td>
</tr>
</tbody>
</table>

---

**Procedure**

**Step 1**  
Access the management page for the policy for which you want to generate a report:

- Access Control — **Policies > Access Control**
- DNS — **Policies > Access Control > DNS**
- File — **Policies > Access Control > Malware & File**
- Health — **System > Health > Policy**
- Identity — **Policies > Access Control > Identity**
- Intrusion — **Policies > Access Control > Intrusion**
- NAT for 7000 & 8000 Series devices — **Devices > NAT**
• Network Analysis — Policies > Access Control, then click Network Analysis Policy or Policies > Access Control > Intrusion, then click Network Analysis Policy

**Note** If your custom user role limits access to the first path listed here, use the second path to access the policy.

• SSL — Policies > Access Control > SSL

**Step 2** Click the report icon (✓) next to the policy for which you want to generate a report.

---

**Out-of-Date Policies**

The Firepower System marks out-of-date policies with red status text that indicates how many of its targeted devices need a policy update. To clear this status, you must re-deploy the policy to the devices.

Configuration changes that require a policy re-deploy include:

• Modifying an access control policy: any changes to access control rules, the default action, policy targets, Security Intelligence filtering, advanced options including preprocessing, and so on.

• Modifying any of the policies that the access control policy invokes: the SSL policy, network analysis policies, intrusion policies, file policies, identity policies, or DNS policies.

• Changing any reusable object or configuration used in an access control policy or policies it invokes:
  - network, port, VLAN tag, URL, and geolocation objects
  - Security Intelligence lists and feeds
  - application filters or detectors
  - intrusion policy variable sets
  - file lists
  - decryption-related objects and security zones

• Updating the system software, intrusion rules, or the vulnerability database (VDB).

Keep in mind that you can change some of these configurations from multiple places in the web interface. For example, you can modify security zones using the object manager (Objects > Object Management), but modifying an interface type in a device’s configuration (Devices > Device Management) can also change a zone and require a policy re-deploy.

Note that the following updates do **not** require policy re-deploy:

• automatic updates to Security Intelligence feeds and additions to the Security Intelligence global blacklist or whitelist using the context menu

• automatic updates to URL filtering data

• scheduled geolocation database (GeoDB) updates
Policy Warnings

The system uses warning and error icons to mark configurations in policies that could adversely affect traffic analysis and flow. Depending on the issue, the system may also warn you at deploy-time or prevent the policy deploy entirely.

Tip: Hover your pointer over an icon to read the warning, error, or informational text.

Table 2: Policy Error Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
<th>Details</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon" alt="error" /></td>
<td>error</td>
<td>If a rule or configuration has an error, you cannot apply the policy until you correct the issue, even if you disable any affected rules.</td>
<td>A rule that performs URL filtering might be valid until you target a device that does not have a URL Filtering license. At that point, an error icon appears next to the rule, and you cannot apply the policy to that device until you edit or delete the rule, retarget the policy, or enable the appropriate license.</td>
</tr>
<tr>
<td><img src="icon" alt="warning" /></td>
<td>warning</td>
<td>You can apply an access control policy that displays rule or other warnings. However, misconfigurations marked with warnings have no effect. If you disable a rule with a warning, the warning icon disappears. It reappears if you enable the rule without correcting the underlying issue.</td>
<td>Preempted rules or rules that cannot match traffic due to misconfiguration have no effect. This includes conditions using empty object groups, application filters that match no applications, excluded LDAP users, invalid ports, and so on. However, if a warning icon marks a licensing error or model mismatch, you cannot deploy the policy until you correct the issue.</td>
</tr>
<tr>
<td><img src="icon" alt="information" /></td>
<td>information</td>
<td>Information icons convey helpful information about configurations that may affect the flow of traffic. These issues do not prevent you from applying the policy.</td>
<td>With application control and URL filtering, the system may skip matching the first few packets of a connection against some access control rules, until the system identifies the application or web traffic in that connection. This allows connections to be established so that applications and HTTP requests can be identified.</td>
</tr>
</tbody>
</table>
Guidelines for Optimizing Access Control Rules

Properly configuring and ordering access control rules (and, in advanced deployments, network analysis rules) is essential to building an effective deployment. If you do not plan your policy carefully, rules can preempt other rules or contain invalid configurations.

Additionally, when you deploy an access control policy, the system evaluates all the rules together and creates an expanded set of criteria that target devices use to evaluate network traffic. Complex access control policies and rules can command significant resources and negatively affect performance.

Tip
To help ensure that the system handles traffic as you expect, the access control policy interface has a robust feedback system. Icons in the access control policy and rule editors mark warnings and errors.

Guidelines for Ordering Rules

Rules in an access control policy are numbered, starting at 1. The system matches traffic to rules in top-down order by ascending rule number. With the exception of Monitor rules, the first rule that traffic matches is the rule that handles that traffic.

Proper access control rule order reduces the resources required to process network traffic, and prevents rule preemption. Although the rules you create are unique to every organization and deployment, there are a few general guidelines to follow when ordering rules that can optimize performance while still addressing your needs.

Order Rules from Most to Least Critical
First, you must order rules to suit your organization's needs. Place priority rules that must apply to all traffic near the top of the policy. For example, if you want to inspect traffic from a single user for intrusions (using an Allow rule), but trust all other users in the department (using a Trust rule), place two access control rules in that order.

Order Rules from Specific to General
You can improve performance by placing specific rules earlier, that is, rules that narrowly define the traffic they handle. This is also important because rules with broad conditions can match many different types of traffic, and can preempt later, more specific rules.

Consider a scenario where you want to block most social networking sites, but allow access to certain others. For example, you may want your graphic designers to be able to access Creative Commons Flickr and deviantART content, but not access other sites such as Facebook or Google+. You should order your rules as follows:

Rule 1: Allow Flickr, deviantART for the "Design" LDAP user group
Rule 2: Block social networking

If you reverse the rules:

Rule 1: Block social networking
Rule 2: Allow Flickr, deviantART for the "Design" LDAP user group
the first rule blocks all social networking traffic, including Flickr and deviantART. Because no traffic will ever match the second rule, your designers cannot access the content you wanted to make available.

Avoid Rule Preemption
The conditions of an access control rule may preempt a subsequent rule from matching traffic. For example:

Rule 1: allow Admin users
Rule 2: block Admin users

The second rule above will never block traffic because the first rule will have already allowed the traffic. Any type of rule condition can preempt a subsequent rule. For example, the VLAN range in the first rule below includes the VLAN in the second rule, so the first rule preempts the second rule:

Rule 1: allow VLAN 22-33
Rule 2: block VLAN 27

In the following example, Rule 1 matches any VLAN because no VLANs are configured, so Rule 1 preempts Rule 2, which attempts to match VLAN 2:

Rule 1: allow Source Network 10.4.0.0/16
Rule 2: allow Source Network 10.4.0.0/16, VLAN 2

A rule also preempts an identical subsequent rule where all configured conditions are the same. For example:

Rule 1: allow VLAN 1 URL www.example.com
Rule 2: allow VLAN 1 URL www.example.com

A subsequent rule would not be preempted if any condition is different. For example:

Rule 1: allow VLAN 1 URL www.example.com
Rule 2: allow VLAN 2 URL www.example.com

Place Rules That Do Not Invoke Deep Inspection Before Those That Do
Because discovery, intrusion, file, and malware inspection require processing resources, placing rules that do not inspect traffic (Trust, Block) before rules that do (Allow, Interactive Block) can improve performance. This is because Trust and Block rules can divert traffic that the system might otherwise have inspected. All other factors being equal, that is, given a set of rules where none is more critical and preemption is not an issue, consider placing them in the following order:

- Monitor rules that log matching connections, but take no other action on traffic
- Trust and Block rules that handle traffic without further inspection
- Allow and Interactive Block rules that do not inspect traffic further
- Allow and Interactive Block rules that optionally inspect traffic for malware, intrusions, or both

Place Rules That Perform Application and URL Filtering Later

Guidelines for Simplifying Rules
The following guidelines can help you simplify access control rules and improve performance:
• When constructing a rule, use as few individual elements in your conditions as possible. For example, in network conditions, use IP address blocks rather than individual IP addresses. In port conditions, use port ranges. Use application filters and URL categories and reputations to perform application control and URL filtering, and LDAP user groups to perform user control.

Combining elements into objects that you then use in access control rule conditions does not improve performance. For example, using a network object that contains 50 individual IP addresses gives you only an organizational—not a performance—benefit over including those IP addresses in the condition individually.

• Restrict rules by security zones whenever possible. If a device’s interfaces are not in one of the zones in a zone-restricted rule, the rule does not affect performance on that device.

• If one condition is enough to match the traffic you want to handle, do not use two.

Guidelines for Avoiding Intrusion Policy Proliferation

You can use an unlimited number of unique intrusion policies to inspect traffic access control policy: you can associate one intrusion policy with each Allow and Interactive Block rule, as well as with the default action. Every unique pair of intrusion policy and variable set counts as one policy.

However, there is a maximum number of access control rules or intrusion policies that are supported by a target device. The maximum depends on a number of factors, including policy complexity, physical memory, and the number of processors on the device.

If you exceed the maximum supported by your device, you cannot deploy your access control policy and must reevaluate. You may want to consolidate intrusion policies or variable sets so you can associate a single intrusion policy-variable set pair with multiple access control rules.

Performance Considerations for Limited Deployments

Host, application, and user discovery data allow the system to create a complete, up-to-the-minute profile of your network. The system can also act as an intrusion detection and prevention system (IPS), analyzing network traffic for intrusions and exploits and, optionally, dropping offending packets.

Combining discovery and IPS gives context to your network activity and allows you to take advantage of many features, including:

• impact flags and indications of compromise, which can tell you which of your hosts are vulnerable to a particular exploit, attack, or piece of malware
• adaptive profiles and Firepower recommendations, which allow you to examine traffic differently depending on the destination host
• correlation, which allows you to respond to intrusions (and other events) differently depending on the affected host

However, if your organization is interested in performing only IPS, or only discovery, there are a few configurations that can optimize the performance of the system.
Discovery Without Intrusion Prevention

The discovery feature allows you to monitor network traffic and determine the number and types of hosts (including network devices) on your network, as well as the operating systems, active applications, and open ports on those hosts. You can also configure managed devices to monitor user activity on your network. You can use discovery data to perform traffic profiling, assess network compliance, and respond to policy violations.

In a basic deployment (discovery and simple, network-based access control only), you can improve a device’s performance by following a few important guidelines when configuring its access control policy.

**Note**

You must use an access control policy, even if it simply allows all traffic. The network discovery policy can only examine traffic that the access control policy allows to pass.

First, make sure your access control policy does not require complex processing and uses only simple, network-based criteria to handle network traffic. You must implement all of the following guidelines; misconfiguring any one of these options eliminates the performance benefit:

- Do not use the Security Intelligence feature. Remove any populated global whitelist or blacklist from the policy’s Security Intelligence configuration.
- Do not include access control rules with Monitor or Interactive Block actions. Use only Allow, Trust, and Block rules. Keep in mind that allowed traffic can be inspected by discovery; trusted and blocked traffic cannot.
- Do not include access control rules with application, user, URL, ISE attribute, or geolocation-based network conditions. Use only simple network-based conditions: zone, IP address, VLAN tag, and port.
- Do not include access control rules that perform file, malware, or intrusion inspection. In other words, do not associate a file policy or intrusion policy with any access control rule.
- Make sure that the default intrusion policy for the access control policy is set to **No Rules Active**.
- Select **Network Discovery Only** as the policy’s default action. Do not choose a default action for the policy that performs intrusion inspection.

In conjunction with the access control policy, you can configure and deploy the network discovery policy, which specifies the network segments, ports, and zones that the system examines for discovery data, as well as whether hosts, applications, and users are discovered on the segments, ports, and zones.

Intrusion Prevention Without Discovery

The intrusion detection and prevention feature allows you to analyze network traffic for intrusions and exploits and, optionally, drop offending packets. If you want to perform intrusion inspection but do not need to take advantage of discovery data, you can improve a device’s performance by disabling discovery.

**Note**

If you are performing application, user, or URL control, you cannot disable discovery for a performance benefit. Although you can prevent the system from storing discovery data, the system must collect and examine it to implement those features.
To disable discovery, implement all of the following guidelines; misconfiguring any eliminates the performance benefit:

- In your access control policy, do not include rules with application, user, URL, ISE attribute, or geolocation-based network conditions, even if your devices are appropriately licensed. Use only simple network-based conditions: zone, IP address, VLAN tag, and port.
- Delete all rules from your network discovery policy.

After you deploy access control and network discovery policies, new discovery halts on target devices. The system gradually deletes information in the network map according to the timeout periods you specified in the network discovery policy. Alternatively, you can purge all discovery data immediately.