Getting Started with Access Control Policies

The following topics describe how to start using access control policies:

- Introduction to Access Control, on page 1
- Managing Access Control Policies, on page 6
- Creating a Basic Access Control Policy, on page 7
- Editing an Access Control Policy, on page 9
- Managing Access Control Policy Inheritance, on page 10
- Setting Target Devices for an Access Control Policy, on page 14
- Access Control Policy Advanced Settings, on page 14

Introduction to Access Control

Access control is a hierarchical policy-based feature that allows you to specify, inspect, and log (non-fast-pathed) network traffic. Especially useful in multidomain deployments, you can nest access control policies, where each policy inherits the rules and settings from an ancestor (or base) policy. You can enforce this inheritance, or allow lower-level policies to override their ancestors. Each managed device can be targeted by one access control policy.

The data that the policy’s target devices collect about your network traffic can be used to filter and control that traffic based on:

- simple, easily determined transport and network layer characteristics: source and destination, port, protocol, and so on
- the latest contextual information on the traffic, including characteristics such as reputation, risk, business relevance, application used, or URL visited
- realm, user, user group, or ISE attribute
- custom Security Group Tag (SGT)
- characteristics of encrypted traffic; you can also decrypt this traffic for further analysis
- whether unencrypted or decrypted traffic contains a prohibited file, detected malware, or intrusion attempt

Each type of traffic inspection and control occurs where it makes the most sense for maximum flexibility and performance. For example, reputation-based blacklisting uses simple source and destination data, so it can block prohibited traffic early in the process. In contrast, detecting and blocking intrusions and exploits is a last-line defense.
Although you can configure the system without licensing your deployment, many features require that you enable the appropriate licenses before you deploy. Also, some features are only available on certain device models. Warning icons and confirmation dialog boxes designate unsupported features.

For the system to affect traffic, you must deploy relevant configurations to managed devices using routed, switched, or transparent interfaces, or inline interface pairs. Sometimes, the system prevents you from deploying inline configurations to passively deployed devices, including inline devices in tap mode. In other cases, the policy may deploy successfully, but attempting to block or alter traffic using passively deployed devices can have unexpected results. For example, the system may report multiple beginning-of-connection events for each blocked connection, because blocked connections are not blocked in passive deployments.

Access Control Policy Components

A newly created access control policy directs its target devices to handle all traffic using its default action.

In the following graphic, the default action uses the Balanced Security and Connectivity intrusion policy to inspect traffic before allowing it to its final destination.

The following list describes the configurations you can change after you create a simple policy.

You can only edit access control policies that were created in the current domain. Also, you cannot edit settings that are locked by an ancestor access control policy.

Name and Description

Each access control policy must have a unique name. A description is optional.

Inheritance Settings

Policy inheritance allows you to create a hierarchy of access control policies. A parent (or base) policy defines and enforces default settings for its descendants, which is especially useful in multidomain deployments.
A policy's inheritance settings allow you to select its base policy. You can also lock settings in the current policy to force any descendants to inherit them. Descendant policies can override unlocked settings.

**Policy Assignment**

Each access control policy identifies the devices that use it. Each device can be targeted by only one access control policy. In a multidomain deployment, you can require that all the devices in a domain use the same base policy.

**Rules**

Access control rules provide a granular method of handling network traffic. Rules in an access control policy are numbered, starting at 1, including rules inherited from ancestor policies. The system matches traffic to access control rules in top-down order by ascending rule number.

Usually, the system handles network traffic according to the first access control rule where all the rule’s conditions match the traffic. Conditions can be simple or complex, and their use often depends on certain licenses.

**Default Action**

The default action determines how the system handles and logs traffic that is not handled by any other access control configuration. The default action can block or trust all traffic without further inspection, or inspect traffic for intrusions and discovery data.

Although an access control policy can inherit its default action from an ancestor policy, you cannot enforce this inheritance.

**Security Intelligence**

Security Intelligence is a first line of defense against malicious internet content. This feature allows you to blacklist (block) connections based on the latest IP address, URL, and domain name reputation intelligence. To ensure continual access to vital resources, you can override blacklists with custom whitelists.

**HTTP Responses**

When the system blocks a user’s website request, you can either display a generic system-provided response page, or a custom page. You can also display a page that warns users, but also allows them to continue to the originally requested site.

**Advanced Access Control Options**

Advanced access control policy settings typically require little or no modification. Often, the default settings are appropriate. Advanced settings you can modify include traffic preprocessing, SSL inspection, identity, and various performance options.

**Related Topics**

- Rule Management: Common Characteristics

---

**Access Control Policy Default Action**

In a simple access control policy, the default action specifies how target devices handle all traffic. In a more complex policy, the default action handles traffic that:

- is not trusted by Intelligent Application Bypass
- is not blacklisted by Security Intelligence
• is not blocked by SSL inspection (encrypted traffic only)
• matches none of the rules in the policy (except Monitor rules, which match and log—but do not handle or inspect—traffic)

The access control policy default action can block or trust traffic without further inspection, or inspect traffic for intrusions and discovery data.

Note: You **cannot** perform file or malware inspection on traffic handled by the default action. Logging for connections handled by the default action is initially disabled, though you can enable it.

If you are using policy inheritance, the default action for the lowest-level descendant determines final traffic handling. Although an access control policy can inherit its default action from its base policy, you cannot enforce this inheritance.

The following table describes the types of inspection you can perform on traffic handled by each default action.

**Table 1: Access Control Policy Default Actions**

<table>
<thead>
<tr>
<th>Default Action</th>
<th>Effect on Traffic</th>
<th>Inspection Type and Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control: Block All Traffic</td>
<td>block without further inspection</td>
<td>none</td>
</tr>
<tr>
<td>Access Control: Trust All Traffic</td>
<td>trust (allow to its final destination without further inspection)</td>
<td>none</td>
</tr>
<tr>
<td>Intrusion Prevention</td>
<td>allow, as long as it is passed by the intrusion policy you specify</td>
<td>intrusion, using the specified intrusion policy and associated variable set, and discovery, using the network discovery policy</td>
</tr>
<tr>
<td>Network Discovery Only</td>
<td>allow</td>
<td>discovery only, using the network discovery policy</td>
</tr>
<tr>
<td>Inherit from base policy</td>
<td>defined in base policy</td>
<td>defined in base policy</td>
</tr>
</tbody>
</table>

The following diagram illustrates the table.

The following diagrams illustrate the **Block All Traffic** and **Trust All Traffic** default actions.
The following diagrams illustrate the Intrusion Prevention and Network Discovery Only default actions.

**Tip**

The purpose of Network Discovery Only is to improve performance in a discovery-only deployment. Different configurations can disable discovery if you are only interested in intrusion detection and prevention.

**Related Topics**

- Performance Considerations for Limited Deployments
- Logging Connections with a Policy Default Action

**Access Control Policy Inheritance**

Access control uses a hierarchical policy-based implementation. Just as you create a domain hierarchy, you can create a corresponding hierarchy of access control policies. A descendant, or child, access control policy inherits rules and settings from its direct parent, or base, policy. That base policy may have its own parent policy from which it inherits rules and settings, and so on.

An access control policy’s rules are nested between its parent policy’s Mandatory and Default rule sections. This implementation enforces Mandatory rules from ancestor policies, but allows the current policy to write rules that preempt Default rules from ancestor policies.

You can lock the following settings to enforce them in all descendant policies. Descendant policies can override unlocked settings.

- Security Intelligence — Blacklisting and whitelisting connections based on the latest reputation intelligence for IP addresses, URLs, and domain names.
• HTTP Response pages — Displaying a custom or system-provided response page when you block a user's website request.

• Advanced settings — Specifying associated subpolicies, network analysis settings, performance settings, and other general options.

Although an access control policy can inherit its default action from an ancestor policy, you cannot enforce this inheritance.

Policy Inheritance and Multitenancy

Access control's hierarchical policy-based implementation complements multitenancy.

In a typical multidomain deployment, access control policy hierarchy corresponds to domain structure, and you apply the lowest-level access control policy to managed devices. This implementation allows selective access control enforcement at a higher domain level, while lower-level domain administrators can tailor deployment-specific settings. (You must use roles, not policy inheritance and enforcement alone, to restrict administrators in descendant domains.)

For example, as a Global domain administrator for your organization, you can create an access control policy at the Global level. You can then require that all your devices, which are divided into subdomain by function, use that Global-level policy as a base policy.

When subdomain administrators log into the Firepower Management Center to configure access control, they can deploy the Global-level policy as-is. Or, they can create and deploy a descendant access control policy within the boundaries of the Global-level policy.

Note

Although the most useful implementation of access control inheritance and enforcement complements multitenancy, you can create a hierarchy of access control policies within a single domain. You can also assign and deploy access control policies at any level.

Related Topics

Managing Access Control Policy Inheritance, on page 10
Security Intelligence Blacklisting
HTTP Response Pages and Interactive Blocking
Access Control Policy Advanced Settings, on page 14

Managing Access Control 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>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Access Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Network Admin</td>
</tr>
</tbody>
</table>

The Firepower System allows you to edit system-provided access control policies and create custom access control policies. Depending on your devices' initial configurations, system-provided policies can include:

• Default Access Control—Blocks all traffic without further inspection.
• Default Intrusion Prevention—Allows all traffic, but also inspects with the Balanced Security and Connectivity intrusion policy and default intrusion variable set.

• Default Network Discovery—Allows all traffic while inspecting it for discovery data but not intrusions or exploits.

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain.

Procedure

**Step 1** Choose *Policies > Access Control*.

**Step 2** Manage access control policies:

- Copy—Click the copy icon (COPY GRAPHIC).
- Create—Click *New Policy*; see Creating a Basic Access Control Policy, on page 7.
- Delete—Click the delete icon (DELETE GRAPHIC).
- Deploy—Click *Deploy*; see Deploy Configuration Changes.
- Edit—Click the edit icon (EDIT GRAPHIC); see Editing an Access Control Policy, on page 9
- Inheritance—Click the plus icon (INHERITANCE GRAPHIC) next to a policy with descendants to expand your view of the policy's hierarchy.
- Import/Export—Click *Import/Export*; see Configuration Import and Export.
- Report—Click the report icon (REPORT GRAPHIC); see Generating Current Policy Reports.

**Related Topics**

- [Out-of-Date Policies](#)

### Creating a Basic Access Control Policy

<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/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>

When you create a new access control policy, you must, at minimum, choose a default action.

In most cases, logging of connections handled by a default action is initially disabled. An exception occurs if you create a subpolicy in a multidomain deployment. In that case, the system enables connection logging according to the logging configuration of the inherited default action.
Procedure

Step 1  Choose Policies > Access Control.
Step 2  Click New Policy.
Step 3  Enter a unique Name and, optionally, a Description.
Step 4  Optionally, choose a base policy from the Select Base Policy drop-down list.
        If an access control policy is enforced on your domain, this step is not optional. You must choose the enforced policy or one of its descendants as the base policy.

Step 5  Specify the initial Default Action:
        • If you chose a base policy, your new policy inherits its default action. You cannot change it here.
        • Block all traffic creates a policy with the Access Control: Block All Traffic default action.
        • Intrusion Prevention creates a policy with the Intrusion Prevention: Balanced Security and Connectivity default action, associated with the default intrusion variable set.
        • Network Discovery creates a policy with the Network Discovery Only default action.

        Tip  If you want to trust all traffic by default, or if you chose a base policy and do not want to inherit the default action, you can change the default action later.

        Caution  Changing the total number of intrusion policies used by an access control policy restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See Snort® Restart Traffic Behavior for more information. You change the total number of intrusion policies by adding an intrusion policy that is not currently used, or by removing the last instance of an intrusion policy. You can use an intrusion policy in an access control rule, as the default action, or as the default intrusion policy.

Step 6  Optionally, choose the Available Devices where you want to deploy the policy, then click Add to Policy (or drag and drop) to add the selected devices. To narrow the devices that appear, type a search string in the Search field.
        If you want to deploy this policy immediately, you must perform this step.

Step 7  Click Save.

What to do next

• Optionally, further configure the new policy as described in Editing an Access Control Policy, on page 9.

• Deploy configuration changes; see Deploy Configuration Changes.

Related Topics

Access Control Policy Default Action, on page 3
Setting Target Devices for an Access Control Policy, on page 14
Editing an Access Control Policy

<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/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>

Only one person should edit a policy at a time, using a single browser window. If multiple users save the same policy, the last saved changes are retained. For your convenience, the system displays information on who (if anyone) is currently editing each policy. To protect the privacy of your session, a warning appears after 30 minutes of inactivity on the policy editor. After 60 minutes, the system discards your changes.

Procedure

**Step 1** Choose Policies > Access Control.

**Step 2** Click the edit icon (📝) next to the access control policy you want to edit.

If a view icon (🔍) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

**Step 3** Edit your access control policy:

- Name and Description—Click either field and enter new information.
- Default Action—Choose a value from the **Default Action** drop-down list.

**Caution** Changing the total number of intrusion policies used by an access control policy restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See **Snort® Restart Traffic Behavior** for more information. You change the total number of intrusion policies by adding an intrusion policy that is not currently used, or by removing the last instance of an intrusion policy. You can use an intrusion policy in an access control rule, as the default action, or as the default intrusion policy.

- Default Action Variable Set—To change the variable set associated with an **Intrusion Prevention** default action, click the variables icon (💰). In the popup window that appears, select a new variable set and click OK. You can also click the edit icon (📝) to edit the selected variable set in a new window. For more information, see **Managing Variables**.
- Default Action Logging—To configure logging for connections handled by the default action, click the logging icon (🌐); see **Logging Connections with a Policy Default Action**.
- HTTP Responses—To specify what the user sees in a browser when the system blocks a website request, click the **HTTP Responses** tab; see **Choosing HTTP Response Pages**.
- Inheritance: Change Base Policy—To change the base access control policy for this policy, click **Inheritance Settings**; see **Choosing a Base Access Control Policy**, on page 11.
• Inheritance: Lock Settings in Descendants—To enforce this policy’s settings in its descendant policies, click Inheritance Settings; see Locking Settings in Descendant Access Control Policies, on page 12.

• Policy Assignment: Targets—To identify the managed devices targeted by this policy, click Policy Assignment; see Setting Target Devices for an Access Control Policy, on page 14.

• Policy Assignment: Required in Domains—To enforce this policy in a subdomain, click Policy Assignment; see Requiring an Access Control Policy in a Domain, on page 13.

• Rules—To manage access control rules, and to inspect and block malicious traffic using intrusion and file policies, click the Rules tab; see Creating and Editing Access Control Rules.

• Security Intelligence—To immediately blacklist (block) connections based on the latest reputation intelligence, click the Security Intelligence tab; see Configure Security Intelligence.

• Advanced Options—To set preprocessing, SSL inspection, identity, performance, and other advanced options, click the Advanced tab; see Access Control Policy Advanced Settings, on page 14.

• Warnings—To view a list of warnings or errors in your access control policy (and its descendant and associated policies), click Show Warnings. Warnings and errors mark configurations that could adversely affect traffic analysis and flow or prevent the policy from deploying. If there are no warnings, the button does not appear.

Step 4 Click Save.

What to do next
• Deploy configuration changes; see Deploy Configuration Changes.

Related Topics
  Rule and Other Policy Warnings
  About Deep Inspection

Managing Access Control Policy Inheritance

<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/Access Admin</td>
</tr>
</tbody>
</table>

Procedure

Step 1 Edit the access control policy whose inheritance settings you want to change; see Editing an Access Control Policy, on page 9.

Step 2 Manage policy inheritance:
  • Change Base Policy — To change the base access control policy for this policy, click Inheritance Settings and proceed as described in Choosing a Base Access Control Policy, on page 11.
• Lock Settings in Descendants — To enforce this policy's settings in its descendant policies, click **Inheritance Settings** and proceed as described in Locking Settings in Descendant Access Control Policies, on page 12.

• Required in Domains — To enforce this policy in a subdomain, click **Policy Assignment** and proceed as described in Requiring an Access Control Policy in a Domain, on page 13.

• Inherit Settings from Base Policy — To inherit settings from a base access control policy, click the **Security Intelligence**, **HTTP Responses**, or **Advanced** tab and proceed as directed in Inheriting Access Control Policy Settings from the Base Policy, on page 12.

---

**What to do next**

• Deploy configuration changes; see Deploy Configuration Changes.

---

**Choosing a Base Access Control Policy**

<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/Access Admin</td>
</tr>
</tbody>
</table>

You can use one access control policy as the base (parent) for another. By default, a child policy inherits its settings from its base policy, though you can change unlocked settings.

When you change the base policy for the current access control policy, the system updates the current policy with any locked settings from the new base policy.

**Procedure**

**Step 1**  
In the access control policy editor, click **Inheritance Settings**.

**Step 2**  
Choose a policy from the **Select Base Policy** drop-down list.

In a multidomain deployment, an access control policy may be required in the current domain. You can choose only the enforced policy or one of its descendants as the base policy.

**Step 3**  
Click **Save**.

---

**What to do next**

• Deploy configuration changes; see Deploy Configuration Changes.
Inheriting Access Control Policy Settings from the Base Policy

<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/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network Admin</td>
</tr>
</tbody>
</table>

A new child policy inherits many settings from its base policy. If these settings are unlocked in the base policy, you can override them.

If you later reinherit the settings from the base policy, the system displays the base policy's settings and dims the controls. However, the system saves the overrides you made, and restores them if you disable inheritance again.

**Procedure**

**Step 1**
In the access control policy editor, click the **Security Intelligence**, **HTTP Responses**, or **Advanced** tab.

**Step 2**
Check the **Inherit from base policy** check box for each setting you want to inherit.

If the controls are dimmed, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration.

**Step 3**
Click **Save**.

**What to do next**

- Deploy configuration changes; see Deploy Configuration Changes.

Locking Settings in Descendant Access Control 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>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network Admin</td>
</tr>
</tbody>
</table>

Lock a setting in an access control policy to enforce the setting in all descendant policies. Descendant policies can override unlocked settings.

When you lock settings, the system saves overrides already made in descendant policies so that the overrides can be restored if you unlock settings again.

**Procedure**

**Step 1**
In the access control policy editor, click **Inheritance Settings**.

**Step 2**
In the Child Policy Inheritance Settings area, check the settings you want to lock.

If the controls are dimmed, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration.
Step 3  Click **OK** to save the inheritance settings.
Step 4  Click **Save** to save the access control policy.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

### Requiring an Access Control Policy in a Domain

<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/Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

You can require that every device in a domain use the same base access control policy or one of its descendant policies.

**Before you begin**

- Configure at least one domain other than the Global domain.

**Procedure**

**Step 1** In the access control policy editor, click **Policy Assignments**.
**Step 2** Click the **Required on Domains** tab.
**Step 3** Build your domain list:
  - Add — Select the domains where you want to enforce the current access control policy, then click **Add** or drag and drop into the list of selected domains.
  - Delete — Click the delete icon (🗑️) next to a leaf domain, or right-click an ancestor domain and choose **Delete Selected**.
  - Search — Type a search string in the search field. Click the clear icon (❌) to clear the search.
**Step 4** Click **OK** to save the domain enforcement settings.
**Step 5** Click **Save** to save the access control policy.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.
Setting Target Devices for an Access Control Policy

An access control policy specifies the devices that use it. Each device can be targeted by only one access control policy. In multidomain deployments, you can require that all the devices in a domain use the same base policy.

**Procedure**

- **Step 1** In the access control policy editor, click **Policy Assignments**.
- **Step 2** On the **Targeted Devices** tab, build your target list:
  - Add — Select one or more Available Devices, then click Add to Policy or drag and drop into the list of Selected Devices.
  - Delete — Click the delete icon (🗑️) next to a single device, or select multiple devices, right-click, then choose Delete Selected.
  - Search — Type a search string in the search field. Click the clear icon (❌) to clear the search.

Under **Impacted Devices**, the system lists the devices whose assigned access control policies are children of the current policy. Any change to the current policy affects these devices.

- **Step 3** Optionally, click the **Required on Domains** tab to require that all the devices in the subdomains you choose use the same base policy. See Requiring an Access Control Policy in a Domain, on page 13.
- **Step 4** Click **OK** to save your targeted device settings.
- **Step 5** Click **Save** to save the access control policy.

**What to do next**

- Deploy configuration changes; see Deploy Configuration Changes.

Access Control Policy Advanced Settings

Advanced access control policy settings typically require little or no modification. The default settings are appropriate for most deployments. Note that many of the advanced preprocessing and performance options in access control policies may be modified by rule updates as described in Update Intrusion Rules.

If a view icon (💡) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.
See Configurations that Restart the Snort Process When Deployed or Activated for a list of advanced setting modifications that restart the Snort process, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See Snort® Restart Traffic Behavior for more information.

General Settings

To customize the number of characters you store for each URL requested by your users, see Limiting Logging of Long URLs.

To customize the length of time before you re-block a website after a user bypasses an initial block, see Setting the User Bypass Timeout for a Blocked Website.

Disable Retry URL cache miss lookup to allow the system to immediately pass traffic to a URL without a cloud lookup when the category is not cached. The system treats URLs that require a cloud lookup as Uncategorized until the cloud lookup completes with a different category. In passive deployments, the system does not retry the lookup, as it cannot hold packets.

To inspect traffic when you deploy configuration changes unless specific configurations require restarting the Snort process, ensure that Inspect traffic during policy apply is set to its default value (enabled). When this option is enabled, resource demands could result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See Snort® Restart Scenarios for more information.

Associated Policies

Use advanced settings to associate subpolicies (SSL, identity, prefilter) with access control; see Associating Other Policies with Access Control, on page 16.

Network Analysis and Intrusion Policies

Advanced network analysis and intrusion policy settings allow you to:

• Change the access control policy’s default intrusion policy and associated variable set, which are used to initially inspect traffic before the system can determine exactly how to inspect that traffic.

• Change the access control policy’s default network analysis policy, which governs many preprocessing options.

• Use custom network analysis rules and network analysis policies to tailor preprocessing options to specific security zones, networks, and VLANs.

For more information, see Advanced Access Control Settings for Network Analysis and Intrusion Policies.

File and Malware Settings

File and Malware Inspection Performance and Storage Tuning provides information on performance options for file control and AMP for Networks.
Intelligent Application Bypass Settings

Intelligent Application Bypass (IAB) is an expert-level configuration that specifies applications to bypass or test for bypass if traffic exceeds a combination of inspection performance and flow thresholds. For more information, see Intelligent Application Bypass.

Transport/Network Layer Preprocessor Settings

Advanced transport and network preprocessor settings apply globally to all networks, zones, and VLANs where you deploy your access control policy. You configure these advanced settings in an access control policy rather than in a network analysis policy. For more information, see Advanced Transport/Network Preprocessor Settings.

Detection Enhancement Settings

Advanced detection enhancement settings allow you to configure adaptive profiles so you can:

- Use file policies and applications in access control rules.
- Use service metadata in intrusion rules.
- In passive deployments, improve reassembly of packet fragments and TCP streams based on your network’s host operating systems.

For more information, see Adaptive Profiles.

Performance Settings and Latency-Based Performance Settings

About Intrusion Prevention Performance Tuning provides information on improving the performance of your system as it analyzes traffic for attempted intrusions.

For information specific to latency-based performance settings, see Packet and Intrusion Rule Latency Threshold Configuration.

Associating Other Policies with Access Control

<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>feature dependent</td>
<td>feature dependent</td>
<td>Any</td>
<td>Admin/Access Admin/Network Admin</td>
</tr>
</tbody>
</table>

Use an access control policy's advanced settings to associate one of each of the following subpolicies with the access control policy:

- SSL policy—Monitors, decrypts, blocks, or allows application layer protocol traffic encrypted with Secure Socket Layer (SSL) or Transport Layer Security (TLS).

Caution: Adding or removing an SSL policy restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See Snort® Restart Traffic Behavior for more information.
• Identity policy—Performs user authentication based on the realm and authentication method associated with the traffic.
• Prefilter policy—Performs early traffic handling using limited network (layer 4) outer-header criteria.

Procedure

Step 1 In the access control policy editor, click the Advanced tab.

Step 2 Click the edit icon ( ) in the appropriate Policy Settings area.

If a view icon ( ) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck Inherit from base policy to enable editing.

Step 3 Choose a policy from the drop-down list.

If you choose a user-created policy, you can click the edit icon that appears to edit the policy.

Step 4 Click OK.

Step 5 Click Save to save the access control policy.

What to do next

• Deploy configuration changes; see Deploy Configuration Changes.

Related Topics

Snort® Restart Scenarios