



# Getting Started with Access Control Policies

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

- [Introduction to Access Control, page 1](#)
- [Managing Access Control Policies, page 6](#)
- [Creating a Basic Access Control Policy, page 7](#)
- [Editing an Access Control Policy, page 8](#)
- [Managing Access Control Policy Inheritance, page 10](#)
- [Setting Target Devices for an Access Control Policy, page 13](#)
- [Access Control Policy Advanced Settings, 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
- 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.

**Note**

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.

### Simple Access Control Policy

inspects all traffic with a balanced intrusion policy

Identity Policy: None

The screenshot displays the configuration page for a 'Simple Access Control Policy'. At the top, there are tabs for 'Rules', 'Security Intelligence', 'HTTP Responses', and 'Advanced'. Below the tabs, there are buttons for 'Filter by Device', 'Add Rule', 'Add Category', and a search bar. The main area shows two sections: 'Mandatory - Simple Access Control Policy (-)' and 'Default - Simple Access Control Policy (-)', both indicating 'There are no rules in this section'. At the bottom, the 'Default Action' is set to 'Intrusion Prevention: Balanced Security and Connectivity'. The interface also shows 'Inheritance Settings | Policy assignment(0)' and a status bar at the bottom indicating 'Displaying 0 - 0 of 0 rules'.

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

**Note**

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.

## 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.

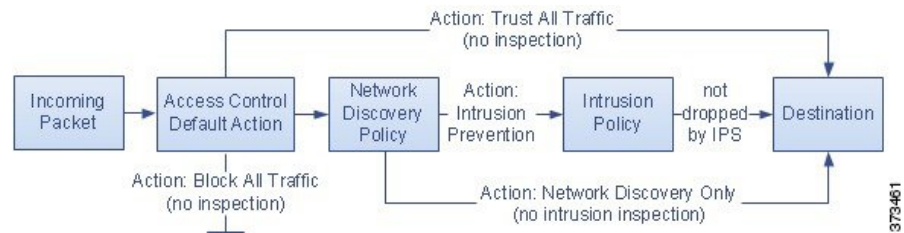
If you are using policy inheritance, the default action for the lowest-level descendant determines final traffic handling. Although an access control policy can inherit its default action from its base policy, you cannot enforce this inheritance.

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

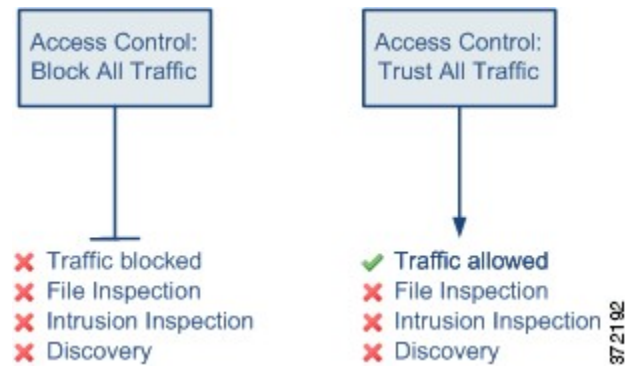
**Table 1: Access Control Policy Default Actions**

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

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.

## Access Control Policy Inheritance

Access control uses a hierarchical policy-based implementation that complements multitenancy. Just as you nest domains, you can nest 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 IP address, URL, and domain name reputation intelligence.
- HTTP Response pages — Displaying a custom or system-provided response page when you block a user's website request.
- Advanced settings — Specifying associated identity and SSL policies, 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

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.

## Managing Access Control Policies

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

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** Select **Policies > Access Control**.

**Step 2** Manage your access control policies:

- **Copy** — Click the copy icon (); see [Editing an Access Control Policy](#), on page 8.
- **Create** — Click **New Policy**; see [Creating a Basic Access Control Policy](#), on page 7.
- **Delete** — Click the delete icon () , then confirm your choice.
- **Deploy** — Click **Deploy**; see [Deploying Configuration Changes](#).
- **Edit** — Click the edit icon (); see [Editing an Access Control Policy](#), on page 8
- **Inheritance** — Click the plus icon () 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 (); see [Generating Current Policy Reports](#).

## Creating a Basic Access Control Policy

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

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.

**Caution**

Initially deploying an access control policy to a managed device restarts the Snort process and interrupts traffic when you deploy configuration changes. Whether this interruption drops traffic or passes traffic without inspection depends on the model of the managed device and how it handles traffic.

**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.

**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 8.
- Deploy configuration changes; see [Deploying Configuration Changes](#).

## Editing an Access Control Policy

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin





Only one person should edit an access control 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** Do **not** use the `Maximum Detection` policy unless instructed to by Support. Cisco uses this policy for testing.
- **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 edit the selected variable set in a new window; click the edit icon () and proceed as described in [Managing Variables](#).
- **Default Action Logging** — To configure logging for connections handled by the default action, click the logging icon () and proceed as described in [Logging Connections Handled by the Access Control 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 and proceed as described in [Configuring an HTTP Response Page](#).
- **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.
- **Inheritance: 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.
- **Policy Assignment: Targets** — To identify the managed devices targeted by this policy, click **Policy Assignment** and proceed as described in [Setting Target Devices for an Access Control Policy](#), on page 13.
- **Policy Assignment: 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.
- **Rules** — To manage access control rules, and to inspect and block malicious traffic using intrusion and file policies, click the **Rules** tab and proceed as described in [Creating and Editing Access Control Rules](#).

- **Security Intelligence** — To immediately blacklist (block) connections based on the latest reputation intelligence, click the **Security Intelligence** tab and proceed as described in [Configuring Security Intelligence](#).
- **Advanced Options** — To set preprocessing, SSL inspection, performance, and other advanced options, click the **Advanced** tab and 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.

**Step 4** Click **Save**.

### What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

## Managing Access Control Policy Inheritance

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

### Procedure

**Step 1** Edit the access control policy whose inheritance settings you want to change; see [Editing an Access Control Policy](#), on page 8.

**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 11.

**What to Do Next**

- Deploy configuration changes; see [Deploying Configuration Changes](#).

## Choosing a Base Access Control Policy

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

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 [Deploying Configuration Changes](#).

## Inheriting Access Control Policy Settings from the Base Policy

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

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 [Deploying Configuration Changes](#).

## Locking Settings in Descendant Access Control Policies

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

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 [Deploying Configuration Changes](#).

## Requiring an Access Control Policy in a Domain



Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

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 [Deploying Configuration Changes](#).

## Setting Target Devices for an Access Control Policy

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

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 all the devices where you can assign this access control policy but that are currently using another policy.
- 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 [Deploying 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 [Intrusion Rule Updates](#).

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.

### 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.

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). Note that when this option is enabled, resource demands could result in a small number of packets dropping without inspection. Disabling this option, or deploying certain specific configurations, automatically restarts the Snort process when you deploy configuration changes. See [Configurations and Actions that Restart Snort®](#) for more information.

**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. See [Snort® Restarts During Configuration Deployment](#) for more information.

### Identity Policy Settings

To choose an identity policy to associate traffic with an identity source and a realm, see [Associating an Identity Policy with an Access Control Policy](#).

**Caution**

Associating an identity policy with an access control policy, or subsequently dissociating the policy by selecting **None**, restarts the Snort process and interrupts traffic when you deploy configuration changes. Whether this interruption drops traffic or passes traffic without inspection depends on the model of the managed device and how it handles traffic. See [Snort® Restarts During Configuration Deployment](#) for more information.

### SSL Policy Settings

To choose an SSL policy to monitor, decrypt, block, or allow application layer protocol traffic encrypted with Secure Socket Layer (SSL) or Transport Layer Security (TLS), see [Associating an SSL Policy with an Access Control Policy](#).

**Caution**

Associating an SSL policy with an access control policy, or subsequently dissociating the policy by selecting **None** restarts the Snort process and interrupts traffic when you deploy configuration changes. Whether this interruption drops traffic or passes traffic without inspection depends on the model of the managed device and how it handles traffic. See [Snort® Restarts During Configuration Deployment](#) for more information.

### 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

Advanced file and malware settings allow you to set performance options for file control and AMP for Firepower. For more information, see [File and Malware Inspection Performance and Storage Tuning](#).



### Caution

Replacing the default value of an access control policy Files and Malware Settings advanced setting restarts the Snort process and interrupts traffic when you deploy configuration changes. Whether this interruption drops traffic or passes traffic without inspection depends on the model of the managed device and how it handles traffic. See [Snort® Restarts During Configuration Deployment](#) for more information.

## Intelligent Application Bypass Settings

Intelligent Application Bypass is an expert-level configuration that you can use to specify applications whose traffic the system can bypass or identify as traffic that would have been bypassed if a configured combination of inspection performance and flow thresholds is exceeded. For more information, see [Access Control Using 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 use adaptive profiles to improve reassembly of packet fragments and TCP streams in passive deployments, based on your network's host operating systems. For more information, see [Adaptive Profiles](#).

## Performance Settings and Latency-Based Performance Settings

[Overview: Intrusion Prevention Performance Tuning](#) provides information on improving the performance of your system as it analyzes traffic for attempted intrusions.