



Access Control Policies

The following topics describe how to work with access control policies:

- [Access control policy components, on page 1](#)
- [Requirements and prerequisites for access control policies, on page 2](#)
- [Managing access control policies, on page 3](#)
- [History for access control policies, on page 29](#)

Access control policy components

Following are the main elements of an 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.

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. You can also assign the policy to device templates.

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 block connections based on the latest IP address, URL, and domain name reputation intelligence. To ensure continual access to vital resources, you can override block list entries with custom do not block list entries.

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.

Logging

Settings for access control policy logging allow you to configure default syslog destinations for the current access control policy. The settings are applicable to the access control policy and all the included decryption, prefilter, and intrusion policies unless the syslog destination settings are explicitly overridden with custom settings in included rules and policies.

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, decryption, identity, and various performance options.

Requirements and prerequisites for access control policies

Model Support

Any

Supported Domains

Any

User Roles

- Admin
- Access Admin
- Network Admin
- You can define custom user roles to differentiate between the intrusion configuration in access control policy and rules and the rest of the access control policy and rules. Using these permissions, you can separate the responsibilities of your network administration team and your intrusion administration teams.

The existing pre-defined user roles that included the Modify Access Control Policy permission support all sub-permissions; you need to create your own custom roles if you want to apply granular permissions. The granular permissions are:

- **Policies > Security policies > Access Control** and choose the **Access Control Policy > Modify Access Control Policy > Modify Threat Configuration** allows the selection of intrusion policy, variable set, and file policy in a rule, the configuration of the advanced options for network analysis and intrusion policies, the configuration of the Security Intelligence policy for the access control policy, and intrusion actions in the policy default action. If a user has this option only, the user can modify no other part of the policy or rule.
- **Modify Remaining Access Control Policy Configuration** controls the ability to edit all other aspects of the policy.

Managing access control policies

You can edit system-provided access control policies and create custom access control policies.

Procedure

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

At the top of the page, there are convenient links to some related features: Object management, Intrusion policies, Network Analysis policies, DNS policies, and policy Import/Export.

Step 2 Manage access control policies:

- **Analyze policy**—Select one or more policy and then click **Analyze Policies** to evaluate access control policies for anomalies such as redundant or shadowed rules, and take action to fix discovered anomalies. The analysis job is sent to the cloud and takes time to complete. See [Identifying and fixing anomalies with Policy Analyzer & Optimizer, on page 22](#).






The Anomalies column shows the results of the analysis. Click the **% Optimizable** link to see the anomalies, or **Re-Analyze** to run the analysis again. The Last Analyzed column shows when Policy Analyzer & Optimizer was last run.

After completing analysis and optimization, you can download the reports by selecting the following options from the **More (⋮)** menu: **Download Last Policy Analysis**, **Remediation History**.

Note

To use the policy analysis feature, you must be using a Cloud-Delivered Firewall Management Center or an connected to Cisco Security Cloud Control (Security Cloud Control). If your setup does not meet requirements, the explanatory dialog that opens when you click this button includes an **Integrate** button to help get you started. Policy Analyzer & Optimizer operates in the cloud only.

- **Create**—Click **Create Policy**; see [Creating a basic access control policy, on page 4](#).
- **Columns**—Click the **Show/Hide Columns** icon above the list of rules to select which information to show in the table. Click **Show All/Hide All** to quickly add or remove all listed columns, excepting name and actions. Click **Default** to undo all of your customizations.

- Inheritance—Vertical lines indicate inheritance relationships between policies.
- Edit—Click **Edit** (); see [Editing an access control policy, on page 5](#)
- Delete—Click **Delete** (). You must remove any device assignments before deleting a policy.
To delete more than one policy at a time, select the check boxes for the policies, then select **Delete Policies** above the table.
- Copy—Select **Clone** from the **More** () menu. Device assignments are not retained in the copy.
- Report—Select **Generate Report** from the **More** () menu.. The report is generated as a background process. Go to the message/notifications center and look in the tasks list. When the report is finished, you can download it from the notification.
- View the audit log—Click **View Audit Log** from the **More** () menu.
- Lock or unlock a policy—See [Locking an access control policy, on page 7](#).

Creating a basic access control policy

When you create a new access control policy, it contains default actions and settings. After creating the policy, you are immediately placed in an edit session so that you can adjust the policy to suit your requirements.

Procedure

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

Step 2 Click **Create Policy**.

Step 3 Enter a unique **Name** and, optionally, a **Description**.

Step 4 Optionally, choose a base policy.

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.

If you select a base policy, the base policy defines the default action and you cannot select a new one in this dialog box. Logging for connections handled by the default action depends on the base policy.

Step 5 When you do not select a base policy, specify the initial **Default Action**:

- **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.

When you select a default action, logging of connections handled by the default action is initially disabled. You can enable it later when you edit the policy.

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 devices to assign to the policy. To narrow the devices that appear, enter a search string. The list includes both devices and device templates.

If you want to deploy this policy immediately, you must perform this step.

Step 7 Click **Save**.

The new policy opens for edit. You can add rules to it and make other changes as needed. See [Editing an access control policy, on page 5](#).

Editing an access control policy

When you edit an access control policy, you should lock it to ensure that your changes do not get overridden by another person who might edit it simultaneously.

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.

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.



Note When you edit a policy and do not lock it, a banner message might indicate that other users are currently editing the policy. When one of these users saves changes, you will be prompted to either merge or discard your changes. You should immediately decide what to do. For more information, see [Concurrent editing and merging changes, on page 8](#).

Procedure

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

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

If **View** (👁) 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.

Tip

You can operate on multiple rules at one time by selecting their checkboxes in the left column, then selecting the action you want to perform from the **Select Bulk Rule Actions** drop-down list next to the search box. Bulk editing is available for enabling and disabling, copying, moving, deleting, and editing rules, or viewing hit counts or related events. You can also remove object overlaps in the selected rules.

You can change the following settings or perform these actions:

- Name and description—Click **Edit** (✎) next to the name, make your changes, and click **Save**.

- **Default action and settings**—Choose a value from the **Default Action** drop-down list, then click **Cog** (⚙️), make your changes to the settings, and click **OK**. For detailed information, see [Setting the access control default action, on page 10](#).
- **Associated policies**—To edit or change policies in the packet flow, click the policy type in the packet flow representation below the policy name. You can select the **Prefilter Rules**, **Decryption**, **Security Intelligence**, and **Identity** policies. When necessary, click **Access Control** to return to the access control rules.
- **Policy assignment**—To identify the managed devices targeted by this policy, or enforce this policy in a subdomain, click the **Assigned: x devices** link. You can assign the policy to devices or device templates.
- **Rules**—To manage access control rules, and to inspect and block malicious traffic using intrusion and file policies, click **Add Rule**, or right-click an existing rule and select **Edit** or another appropriate action. The actions are also available from the **More** (⋮) button for each rule. See [Create and Edit Access Control Rules](#).
- **Layout**—Use the **Grid/Table View** icon above the list of rules to change the layout. Grid view provides color-coded objects in an easy-to-see layout. Table view provides a summary list so that you can see more rules at once. You can freely switch views without impacting the rules.
- **Columns (table view only)**—Click the **Show/Hide Columns** icon above the list of rules to select which information to show in the table. Click **Show/Hide Empty Columns** to quickly add, or remove, all columns that have no information, that is, you are not using those conditions in any rule. Click **Revert to Default** to undo all of your customizations.
- **Analyze rule logic**—You can select the following options from the **Analyze** menu to examine the logic of your rules:
 - **Manage Rule Hit Counts**—To view statistics on how many connections matched each rule. See [Viewing rule hit counts, on page 24](#).
 - **Enable/Disable Rule Conflicts**—Select whether you want to see information on whether rules interfere with each other. You can then view the results using the following commands. See [Analyzing rule conflicts and warnings, on page 26](#)
 - **Show Warnings and Errors**—See whether there are rules with configuration issues that you need to address.
 - **Show Policy Warnings**—See whether there are configuration issues with the policy.
 - **Show Rule Conflicts**—See whether you have redundant or shadowed rules. These conflicts could prevent certain rules from ever being matched by connections, meaning either that you need to fix the match criteria, move the rule, or simply delete the rule.
- **Additional settings**—To change additional settings for the policy, select one of the following options from the **More** drop-down arrow at the end of the packet flow line.
 - **Advanced Settings**—To set preprocessing, decryption, identity, performance, and other advanced options. See [Access control policy advanced settings, on page 15](#).
 - **HTTP Responses**—To specify what the user sees in a browser when the system blocks a website request. See [Choosing HTTP Response Pages](#).

- **Inheritance Settings**—To change the base access control policy for this policy, and to enforce this policy's settings in its descendant policies. See [Choosing a base access control policy, on page 12](#) and [Locking settings in descendant access control policies, on page 12](#).
- **Logging**—To set the default logging options for the policy.

Step 4 Click **Save**.

What to do next

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

Locking an access control policy

You can lock an access control policy to prevent other administrators from editing it. Locking the policy ensures that your changes will not be invalidated if another administrator edits the policy and saves changes before you save your changes. If you do not lock a policy, you might have to merge your changes if another user edits the policy simultaneously and saves changes first. For more information, see [Concurrent editing and merging changes, on page 8](#).

The lock is for the access control policy itself. The lock does not apply to objects used in the policy. For example, another user can edit a network object that is used in a locked access control policy. Your lock remains in place until you explicitly unlock the policy, so you can log out and come back to your edits later.

When locked, other administrators have read-only access to the policy. However, other administrators can assign a locked policy to a managed device.

Before you begin

Any user role that has permission to modify the access control policy has permission to lock it, and to unlock a policy that was locked by another user.

However, the ability to unlock a policy that was locked by another administrator is controlled by the following permission: **Policies > Security policies > Access Control** and choose the **Access Control Policy > Modify Access Control Policy > Override Access Control Policy Lock**.

If you are using custom roles, your organization might have limited your unlocking abilities by not assigning this permission. Without this permission, only the administrator who locks a policy can unlock it.

Procedure

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

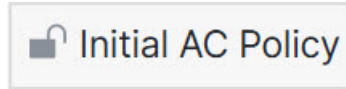
Step 2 Click **Edit** (✎) next to the access control policy you want to lock or unlock.

In the access control policy list:

- A lock icon next to a policy name indicates that the policy is locked. Hover over the icon to see which user locked the policy.

- If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration. Or, it is locked by another user.

Step 3 Click the lock icon next to the policy name to lock or unlock the policy.



If the policy inherits settings from a parent policy, you must choose one of the following options when you click the lock icon.

- **Lock/Unlock this policy**—The locking or unlocking is for this policy only.
- **Lock/Unlock all policies in hierarchy**—This policy and all parent policies are locked or unlocked. If a parent policy is already locked by another administrator, you will see a message and you will not be able to lock that parent policy. When unlocking policies, if you have the Override Access Control Policy Lock permission, all parent policies are unlocked even if they were locked by other users.

Concurrent editing and merging changes

When you allow multiple users to edit an access control policy, you have two choices:

- Have users lock the policy when editing it. This ensures that a single user at a time can make changes. Using locking, you never have to worry about lost or conflicting changes. However, it limits your ability to respond quickly to unexpected events, especially if a user leaves the policy locked while out of the office. For more information about locking policies, see [Locking an access control policy, on page 7](#).
- Allow users to simultaneously edit the policy. If more than one user has made unsaved edits at a given time, the first user who saves the policy gets all of their changes saved. Other users are immediately notified of the save, and must then merge their changes. The rest of this topic explains this approach.



Note If you are using change management, where edits are done within the scope of a ticket, the ticket locks the policy and concurrent editing is not possible.

Before you begin

To limit the amount of merging you have to do, save the policy early and often.

Procedure

Step 1 Determine if other users are also editing the policy.

When you edit an access control policy, look for the following message banner at the top of the page:

User *name* is currently editing this policy.

This message indicates that the named user (there might be more than one) currently have the policy open for edit.

Step 2 Watch for notifications that another user saved changes and take action.

The following banner message indicates another user saved changes and you need to take immediate action:

User *name* modified this policy and saved changes. **Merge Discard.**

Click one of the following links:

- **Merge**—Open a merge window where you can make decisions about which of your changes to keep or to discard, and to identify changes that cannot be merged. See the next step when taking this option.
- **Discard**—Discard all of your changes immediately and start over. If you select this option, the page is refreshed with the latest changes from the other user.

Step 3 Merge changes.

When you click the **Merge** option, a merge window opens with a summary of the total number of observed differences between your edits and the last user's saved edits. No other user's unsaved edits are included. Observations include direct conflicts and informational notifications.

Note

You must complete all merge decisions before you close the window. You cannot wait until later once you click the **Merge** option.

- a) Evaluate each conflict and make a decision for each.

When evaluating the change list, consider the following:

- Initially, all observations are shown, but you can select/deselect the filtering options for **Conflict** and **Info** to limit the displayed information. Conflicts arise when users edit the same rule or setting. Informational items are for edits to different rules or settings.
- If there are no conflicts, your cache is immediately updated with the last saved changes and you can proceed. For example, if you are editing rule 1, and the other user saved changes to rule 2, it is unlikely that there are any conflicts.
- For each conflict (other than rule name), the window shows the version of the element saved by the other user (**Version on Firewall Management Center**), and your changes (**Modified Version**). Changes are color-coded for new (e.g. an option that was not previously defined), edited, or deleted policy elements. You must select either to **Discard** your change, or to **Accept Mine** and overwrite the other user's change. When discarding a change, the rule is refreshed with the other user's saved change and yours is removed.
- Rule conflicts are considered at the rule level, not per element within the rule. For example, if you edit destination networks, and the saved changes are for source networks, either your changes or the other user's changes are retained, not both.
- If the conflict involves the name of a rule, the system tries to create a unique name by adding an underscore and number to the name, such as Rule_1. You can alternatively enter a new name in the edit box provided and click **Save**. If you click **Discard**, the generated rule name is used.
- You cannot skip any conflict. For each conflict, you must make a decision to discard or keep your change.

- If the user who saved changes deleted a rule that you edited, the rule is deleted and you do not have the option to keep the rule.
- If the user who saved changes updated a rule, and your change is to delete the rule, the rule is retained: you cannot merge your deletion.
- For the following options, if your change conflicts with the saved changes, your change is discarded and merging the change is not an option:
 - Other policy assignments: prefilter, Security Intelligence, identity, decryption
 - Changes to advanced settings, policy logging, EVE, HTTP response pages.
 - Policy default action.
 - Inheritance settings.

b) Click **Close**.

Step 4 Once the merger is complete, you can either save the policy immediately or continue editing it. Saving the policy might reduce the impact of future merges.

Setting the access control default action

The default action for an access control policy is applied to any connection that:

- is not fast pathed by the prefilter policy
- is not on a Security Intelligence block list
- is not blocked by the decryption policy (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)

Procedure

Step 1 Edit the access control policy whose inheritance settings you want to change; see [Editing an access control policy, on page 5](#).

Step 2 Select the **Default Action** at the bottom of the rules list.

For detailed information on what each option does, see [Access Control Policy Default Action](#).

Step 3 Click **Cog** (⚙️) to configure the default action settings.

You can configure the following options. Click **OK** when finished.

- Logging options—Whether to log the connection. You can **Log at beginning of connection**, **Log at end of connection**, or both. If you select block as the default action, you can log at the beginning of the connection only.

- **Send connection events to**—If you select one of the logging options, select whether to send events to any combination of the following:
 - **Firewall Management Center**—Send events to the manager.
 - **Syslog server**—Send events to the default syslog server configured for the policy. You can configure overrides to specify a different severity level or syslog server destination.

(Splunk or SIEM syslog server integration) If you have configured Firewall Management Center as the source of connection events in Splunk configuration, choose **Firewall Management Center** under **Send Connection Events to** options. If you have configured Firewall Threat Defense as the connection event source, select at least one syslog destination. For Splunk or any SIEM syslog configuration procedure, see the [Cisco Secure Firewall Management Center Administration Guide](#).

- **SNMP trap**—If you enable logging, you can send SNMP traps to an SNMP server. Select an SNMP configuration, or click + to configure a new one.
- **Default action variable set**—If you selected one of the intrusion prevention default actions, select the variable set that should be used with the intrusion policy you selected.

Step 4 Click **Save**.

Managing access control policy inheritance

Inheritance relates to using another policy as a base policy for an access control policy. This allows you to use one policy to define some baseline characteristics that can be applied to multiple policies. To understand how inheritance works, see [Access Control Policy Inheritance](#).

Procedure

-
- Step 1** Edit the access control policy whose inheritance settings you want to change; see [Editing an access control policy, on page 5](#).
- Step 2** Manage policy inheritance:
- **Change base policy** — To change the base access control policy for this policy, select **Inheritance Settings** from the **More** drop-down arrow at the end of the packet flow line and proceed as described in [Choosing a base access control policy, on page 12](#).
 - **Lock settings in descendants** — To enforce this policy's settings in its descendant policies, select **Inheritance Settings** from the **More** drop-down arrow at the end of the packet flow line and proceed as described in [Locking settings in descendant access control policies, on page 12](#).
 - **Inherit settings from base policy** — To inherit settings from a base access control policy, proceed as directed in [Inheriting access control policy settings from the base policy, on page 13](#).
 - **Required in domains** — To enforce this policy in a subdomain, click the **Assigned: x devices** link and proceed as described in [Requiring an access control policy in a domain, on page 13](#).
-

Choosing a base access control policy

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, select Inheritance Settings from the More drop-down arrow at the end of the packet flow line. |
| Step 2 | Choose a policy from the Select Base Policy drop-down list.
Select None to remove inheritance. |
| Step 3 | Click OK . |
| Step 4 | Click Save to save the access control policy. |
-

What to do next

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

Locking settings in descendant access control policies

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, select Inheritance Settings from the More drop-down arrow at the end of the packet flow line. |
| 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](#).

Inheriting access control policy settings from the base policy

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 **Security Intelligence**, or select **HTTP Responses**, **Logging**, **Encrypted Visibility Engine**, or **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line
- 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](#).

Requiring an access control policy in a domain

You can require that every device in a domain use the same base access control policy or one of its descendant policies. This procedure is relevant in a multi-domain deployment only.

Procedure

-
- Step 1** In the access control policy editor, click the **Assigned: x devices** link.
- Step 2** Click **Required on Domains**.
- 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 **Delete** () 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 **Clear** () 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](#).



Assigning devices to an access control policy

An access control policy specifies the devices that use it. Each device can be assigned to only one access control policy. You can also assign the policy to device templates. Templates are included in the list of available and selected devices.

Procedure

Step 1 In the access control policy editor, click the **Assigned: x devices** link.

Step 2 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 **Delete** () next to a single device, or select multiple devices, right-click, then choose **Delete Selection**.
- Search — Type a search string in the search field. Click **Clear** () 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 Click **OK** to save your targeted device settings.

Step 4 Click **Save** to save the access control policy.

What to do next

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

Logging settings for access control policies

To configure logging settings for an access control policy, select **Logging** from the **More** drop-down arrow at the end of the packet flow line.

You can configure default syslog destinations and syslog alert for the access control policy. The settings are applicable to the access control policy and all the included decryption, prefilter, and intrusion policies unless the syslog destination settings are explicitly overridden with custom settings in included rules and policies.

Logging for connections handled by the default action is initially disabled.

IPS and File and Malware Settings are effective only after you have selected an option at the top of the page for sending syslog messages generally.

Default Syslog Settings

Select the **Syslog Server** option to configure a default syslog server for the policy. Then, select a destination and if required, and alert level. Your options are:

- **Destination > Specific Syslog Alert object**—If you select this option, the events are sent based on the selected syslog alert as configured using the instructions in *Creating a Syslog Alert Response* in the [Cisco Secure Firewall Management Center Administration Guide](#). You can select the syslog alert from the list or add one by specifying the name, logging host, port, facility, and severity. For more information, see *Facilities and Severities for Intrusion Syslog Alerts* in the [Cisco Secure Firewall Management Center Administration Guide](#).

When using this option, the system sends syslog messages to the server using the Management interface. Ensure there is a route from the Management interface to the syslog server, or messages will not arrive at the server.

- **Destination > Use FTD Platform Settings**—If you select this option and select the **Severity**, connection or intrusion events are sent with the selected severity to syslog collectors configured in Platform Settings. Using this option, you can unify the syslog configuration by configuring it in platform settings and reusing the settings in access control policy. Severity selected in this section is applied to all connection and intrusion events. The default severity is ALERT.

Intrusion Settings

- **Send Syslog messages for intrusion (IPS) events**—Send intrusion events as syslog messages. The defaults set above are used unless you override them.
- **Show/Hide Overrides**—If you want to use the default syslog destination and severity, leave these options empty. Otherwise, you can set a different syslog server destination for intrusion events, and change the severity of the events.

File and Malware Settings

- **Send Syslog messages for File and Malware events**—Send file and malware events as syslog messages. The defaults set above are used unless you override them.
- **Show/Hide Overrides**—If you want to use the default syslog destination and severity, leave these options empty. Otherwise, you can set a different syslog server destination for file and malware events, and change the severity of the events.

Access control policy advanced settings

To configure advanced settings for an access control policy, select **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line.

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* in the [Cisco Secure Firewall Management Center Administration Guide](#).

If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings.

**Caution**

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 assigned device handles traffic. See [Snort Restart Traffic Behavior](#) for more information.

Inheriting settings from a parent policy

If the access control policy has a base policy, you can elect to inherit settings from the base policy. Select **Inherit from (base policy)** for each setting group where you want to use the parent policy's settings. If inheritance has been configured so that these settings are locked, you cannot configure unique settings for the policy, these settings are read-only.

If you are allowed to configure unique settings for the policy, you must deselect the option to make your edits.

General settings

Option	Description
Maximum URL characters to store in connection events	To customize the number of characters you store for each URL requested by your users. See <i>Limiting Logging of Long URLs</i> in the Cisco Secure Firewall Management Center Administration Guide for more information.
Allow an Interactive Block to bypass blocking for (seconds)	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 .
Retry URL cache miss lookup	<p>The first time the system encounters a URL that does not have a locally stored category and reputation, it looks up that URL in the cloud and adds the result to the local data store, for faster processing of that URL in the future.</p> <p>This setting determines what the system does when it needs to look up a URL's category and reputation in the cloud.</p> <p>By default, this setting is enabled: The system momentarily delays the traffic while it checks the cloud for the URL's reputation and category, and uses the cloud verdict to handle the traffic.</p> <p>If you disable this setting: When the system encounters a URL that is not in its local cache, the traffic is immediately passed and handled according to the rules configured for Uncategorized and reputationless traffic.</p> <p>In passive deployments, the system does not retry the lookup, as it cannot hold packets.</p>
Enable Threat Intelligence Director	Disable this option to stop publishing TID data to your configured devices.

Option	Description
Enable reputation enforcement on DNS traffic	This option is enabled by default, for improved URL filtering performance and efficacy. For details and additional instructions, see DNS Filtering: Identify URL Reputation and Category During DNS Lookup and subtopics.
Inspect traffic during policy apply	<p>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).</p> <p>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 assigned device handles traffic. See Snort Restart Scenarios for more information.</p>

Associated policies

Use advanced settings to associate subpolicies (decryption, identity, prefilter) with access control; see [Associating other policies with access control](#), on page 21.

TLS server identity discovery

The latest version of the Transport Layer Security (TLS) protocol 1.3, defined by [RFC 8446](#), is the preferred protocol for many web servers to provide secure communications. Because the TLS 1.3 protocol encrypts the server's certificate for additional security, and the certificate is needed to match application and URL filtering criteria in access control rules, the Firepower System provides a way to extract the server certificate *without* decrypting the entire packet.

You can enable this feature, referred to as *TLS server identity discovery*, when you configure advanced settings for an access control policy. Certain features are not supported, such as STARTTLS traffic, the HTTP CONNECT method, and in a network where another device is already decrypting traffic.

If you enable this option, we recommend you also enable the decryption policy's advanced TLS adaptive server identity probe option as well. Together, these options enable more efficient decryption of TLS 1.3 traffic. For more information, see [TLS 1.3 decryption best practices](#).

When a new connection starts that will be affected by TLS server identity discovery, the Firewall Threat Defense holds the original ClientHello packet to determine the identity of the server to which it connects before continuing. The Firewall Threat Defense device sends a specialized connection from the Firewall Threat Defense to the server. The server's response includes the server certificate, the specialized connection is terminated, and the original connection is evaluated as required by the access control policy.

TLS server identity discovery prioritizes the certificate's Common Name (CN) over the [Server Name Indication \(SNI\)](#).

To enable TLS server identity discovery, click the **Advanced** tab, click **Edit** (✎) for the setting, and select **Enhanced application and URL detection**.

TLS Server Identity Discovery

☒ Early application detection and URL categorization

We recommend that you enable early application detection and server identity. Since TLS 1.3 certificates are encrypted, for traffic encrypted with TLS to match access rules that use application or URL filtering, the system must decrypt it. The setting decrypts the certificate only; the connection remains encrypted. Enabling this option is sufficient to decrypt TLS 1.3 certificates; you do not need to create a corresponding SSL decryption rule.

[Revert to Defaults](#)
[Cancel](#)
[OK](#)

TLS Server Identity Discovery

☐ Enhanced application and URL detection

Enables TLS Server Identity Discovery, allowing the firewall to extract certificate details such as Common Name (CN), Organization, or Subject Alternative Names (SANs) even when TLS 1.3 encryption would normally hide them. This improves policy accuracy without requiring a decryption rule; the original client connection remains encrypted.

[Revert to Defaults](#)
[Cancel](#)
[OK](#)

We strongly recommend enabling it for any traffic you want to match on application or URL criteria, especially if you want to perform deep inspection of that traffic. A decryption policy is not required because *traffic is not decrypted* in the process of extracting the server certificate.



Note

- TLS server identity discovery *cannot* be used with any of the following:
 - STARTTLS traffic
 - The HTTP CONNECT method
 - Traffic that is already being decrypted by another device on the network
- Because the certificate is decrypted, TLS server identity discovery can reduce performance depending on the hardware platform.
- TLS server identity discovery is not supported in inline tap mode or passive mode deployments.
- Enabling TLS server identity discovery is not supported on any Secure Firewall Threat Defense Virtual deployed to AWS. If you have any such managed devices managed by the Secure Firewall Management Center, the connection event **PROBE_FLOW_DROP_BYPASS_PROXY** increments every time the device attempts to extract the server certificate.
- TLS Server Identity Discovery also operates on TLS 1.2 sessions.

Network analysis and intrusion policies

Advanced network analysis and intrusion policy settings allow you to:

- Specify the intrusion policy and associated variable set that are used to inspect packets that must pass 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](#).

Threat Defense service policy

You can use the Threat Defense service policy to apply services to specific traffic classes. For example, you can use a service policy to create a timeout configuration that is specific to a particular TCP application, as opposed to one that applies to all TCP applications. This policy applies to Firewall Threat Defense devices only, and will be ignored for any other device type. The service policy rules are applied after the access control rules. For more information, see [Service Policies](#).

File and malware settings

[Tuning File and Malware Inspection Performance and Storage](#) provides information on performance options for file control and malware defense.

Portscan threat detection

Portscan detector is a threat detection mechanism designed to help you detect and prevent portscan activity in all types of traffic to protect networks from eventual attacks. Portscan traffic can be detected efficiently in both allowed and denied traffic. For more information, see [Threat Detection](#).

Elephant flow settings

Elephant flows are large, long duration, and fast flows that can cause duress for Snort cores. There are two actions that can be applied on elephant flows to reduce system stress, CPU hogging, packet drops, and so on. These actions are:

- Bypass any or all applications—This action bypasses flow from Snort inspection.
- Throttle—This action applies dynamic rate limit policy (10% reduction) on elephant flows.

For more information, see the Elephant Flow Detection chapter in the [Cisco Secure Firewall Management Center Snort 3 Configuration Guide](#).

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.

IAB settings are applicable for Snort2 devices or pre 7.2.0 Snort3 devices. 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.

- **Ignore the VLAN header when tracking connections**—Different VLAN tags in traffic traveling in different directions for the same connection can affect traffic reassembly and rule processing. For example, traffic for the same connection could be transmitted over VLAN A and be received over VLAN B. Select this option to configure the system to ignore the VLAN header so packets can be correctly processed for your deployment.
- **Maximum Active Responses**—For a TCP connection that triggers a preprocessor/intrusion rule that is configured to provide an active response, the maximum number of active responses per TCP connection. When additional traffic occurs on a connection where an active response has been initiated, and the traffic occurs more than **Minimum Response Seconds** after a previous active response, the system sends another active response unless the specified maximum has been reached. A setting of 0 disables additional active responses triggered active response rules.
- **Minimum Response Seconds**—Until **Maximum Active Responses** occur, specifies the number of seconds to wait before any additional traffic on a connection where the system has initiated an active response results in a subsequent active response.
- **Session Termination Logging Threshold**—Do not modify this option unless instructed to do so by Cisco Technical Support. This option specifies for the number of bytes that result in a logged message when the session terminates and the specified number was exceeded. Changing the option can affect system performance.

Detection enhancement settings

Detection enhancement settings determine whether adaptive profiles are used for application detection and intrusion rules in the access control policy. Typically, the system uses the static settings in your network analysis policy to preprocess and analyze traffic. With adaptive profile updates, the system can adapt processing behavior using host information either detected by network discovery or imported from a third party.

To enable adaptive profiles in Snort 3, you must select both the **Enable** and **Enable Profile Updates** options.

- **Enable**—You must enable adaptive profiling (its default state) for access control rules to perform application and file control, including malware protection (AMP), and for intrusion rules to use service metadata.
- **Enable Profile Updates**—Profile updates, like the target-based profiles you can configure manually in a network analysis policy, help to defragment IP packets and reassemble streams in the same way as the operating system on the target host. The intrusion rules engine then analyzes the data in the same format as that used by the destination host. Profile updates also compare metadata in an intrusion rule to host information to determine whether a rule should apply for a particular host.
- **Adaptive Profiles – Attribute Update Interval**—When profile updates are enabled, you can control how frequently in minutes network map data is synced from the management center to its managed devices. The system uses the data to determine what profiles should be used when processing traffic. Increasing the value for this option can improve performance in a large network.
- **Adaptive Profiles – Networks**—Optionally, when profile updates are enabled, you can improve performance by constraining profile updates to a comma-separated list of IP addresses, address blocks, and network variables. If you use a network variable, the system uses the variable's value in the variable

set linked to the default intrusion policy for your access control policy. For example, you could enter: 192.168.1.101, 192.168.4.0/24, \$HOME_NET. IPv4 and IPv6 are supported.

The default value (0.0.0.0/0) applies adaptive profile updates to all networks.

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](#).

Encrypted visibility engine

For details about this feature, see the Encrypted Visibility Engine chapter in the [Cisco Secure Firewall Management Center Snort 3 Configuration Guide](#).

Application logging

Enable this feature to enrich connection logs with application data and forward the generated logs to the syslog destinations. Application logging leverages existing deep packet inspection capabilities to extract application data and enables you to enhance network monitoring and gain deeper insights into network traffic. This feature applies to Snort 3 Firewall Threat Defense devices.

For more information about the application logging, see *Application-Aware Event Logging* in the [Cisco Secure Firewall Management Center Administration Guide](#)



Note

Application logging can cause performance drop within network if used without filters configured in the access control rule. Filter specific traffic types using the access control rules to reduce the volume of logged traffic.

Associating other policies with access control

The easiest way to associate the major policies to an access control policy is by clicking the policy's link in the packet flow shown at the top of the access control policy. You can quickly select the associated policy. Alternatively, you can use the policy's advanced settings to associate the policy, as described in this topic. These policies include the following:

- Prefilter policy—Performs early traffic handling using limited network (layer 4) outer-header criteria.
- Decryption policy—Monitors, decrypts, blocks, or allows application layer protocol traffic encrypted with Secure Socket Layer (SSL) or Transport Layer Security (TLS).



Caution

Snort 2 only. Adding or removing a decryption 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 assigned device handles traffic. See [Snort Restart Traffic Behavior](#) for more information.

- Identity policy—Performs user identification based on the realm and authentication method associated with the traffic.

Before you begin

Before associating a decryption policy with an access control policy, review the information about TLS server identity discovery in [Access control policy advanced settings, on page 15](#).

Procedure

-
- Step 1** In the access control policy editor, select **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line.
- Step 2** Click **Edit** (✎) in the appropriate policy settings area.
- If **View** (👁) 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](#).

Identifying and fixing anomalies with Policy Analyzer & Optimizer

You can use the Policy Analyzer & Optimizer to evaluate access control policies for anomalies such as redundant or shadowed rules, and take action to fix discovered anomalies. The Policy Analyzer & Optimizer is hosted in the cloud and is different from the rule analysis available when you are not integrated with the cloud. The non-cloud policy analysis is not available once you integrate with the cloud.

The system automatically performs policy analysis on a daily basis (every 24 hours). You can also manually start an analysis. When you initially enable the service, the system starts an analysis of all existing access control policies.



Note Before optimizing a policy, create a copy of the policy. If you are then dissatisfied with the results of optimization, you can easily reassign the managed devices to the copy and return the system to its starting state.

Before you begin

- You can use Policy Analyzer & Optimizer directly from Security Cloud Control with Firewall Management Center 7.2+, but you can cross-launch the feature starting with 7.6 only. The software version running on the managed devices assigned to the access control policies does not matter. Policy Analyzer & Optimizer is hosted in the cloud only, so whether you run the analysis from within the Firewall Management Center or directly from Security Cloud Control does not make a difference.
- To use the feature, you must select **Enable Policy Analysis & Optimization** when you integrate with the Cisco Security cloud, under **Integrations > Security Cloud Control**.
- If you have enabled change management, Policy Analyzer & Optimizer automatically creates a ticket for the changes, and submits the ticket. The approver must approve the ticket before the changes can be deployed.
- If you are using domains, you cannot click the link in the Anomaly column to see the report. Instead, log into Security Cloud Control and use the feature from that application.
- Policy Analyzer & Optimizer adds rule comments on rules that are updated, disabled, or merged. You can later search on these comments to find optimized rules.
- Changes implemented by Policy Analyzer & Optimizer are reflected in the audit log as API calls under the default name internaladmin.
- After enabling Policy Analyzer & Optimizer, the system evaluates changes every time a rule is added or edited. Users are notified when applying a rule edit if the change will create anomalies such as redundant or shadowed rules.

Procedure

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

If you have already run an analysis, the Anomaly column shows the number of issues with the policy and the percentage the policy can be optimized, and the state of the policy analysis, such as Error or Completed. Last Analyzed shows the date/time when the analysis was run.

Step 2 Select one or more policy, then click **Analyze Policy**.

The analysis runs as a background process in the cloud. When the analysis is complete, the results appear in the Anomaly column.

Notes:

- You can also start an analysis when editing the policy by selecting **Analyze > Policy**. Other options from that menu allow you to show hit counts and warnings.
- If you have not connected to the cloud yet, the explanatory dialog that opens when you click this button includes an **Integrate** button to help get you started. Policy Analyzer & Optimizer operates in the cloud only.

Step 3 When the analysis is complete, click the **% Optimizable** link in the Anomaly column to launch Policy Analyzer & Optimizer in the cloud.

When you have done all the actions you want to take, click **Apply Remediations** (in the cloud). You are shown a confirmation of what will be done. Click **Proceed** to implement the changes.

If the initial analysis ended in an error, you could instead click **Re-analyze** to restart the process.

Step 4 Deploy the policy to complete the changes.

If you have change management enabled, the approver must first approved the ticket that contains the remediations before you can deploy them.

Viewing rule hit counts

Hit count indicates the number of times a policy rule or default action has been matched to a connection. The hit count is incremented only for the first packet of a connection that matches a rule. You can use this information to identify the efficacy of your rules. Hit count information is available only for access control and prefilter rules applied to Firewall Threat Defense devices.



Note

- The count persists through reboots and upgrades.
- Counts are maintained by each unit in an HA pair or cluster separately.
- You will not be able to derive the hit count information from a device when deployment or a task is in progress on the device.
- You can also see rule hit count information in the device CLI using the **show rule hits** command.
- If you have accessed the Hit Count page from the Access Control Policy page, you will not be able to view or edit prefilter rules and vice-versa.
- Hit counts are not available for rules that use the Monitor action.

Before you begin

If you use custom user roles, ensure that the roles include the following privileges:

- View Device, to see the hit counts.
- Modify Device, to refresh the hit counts.

Procedure

Step 1 In the access control policy or prefilter policy editor , click **Analyze > Manage Rule Hit Counts** on the top-right of the page.

Step 2 On the Hit Count page, select the device from the **Select a device** drop-down list.

If it is not the first time that you are generating hit counts for this device, the last fetched hit count information appears next to the drop-down box. Also, verify the **Last Deployed** time to confirm recent policy changes.

Select **All** to see an aggregate of hit counts across all devices assigned to the policy.

Step 3 If necessary, click **Refresh** (🔄) to obtain current hit count data from the selected device.

In the prefilter policy, you might need to click **Fetch Current Hit Count** to get initial hit count data.

You cannot refresh the hit count while deployment to the device is in progress.

Step 4 View and analyze the data.

You can do the following:

- Click **Prefilter** or **Access Control** to switch between the hit counts for these policies.
- Search for a specific rule by entering a search string in the **Filter** box.
- Broadly limit the list to **Hit Rules** or **Never Hit Rules** by selecting these options in the **Filter by** field. When viewing hit rules, you can further limit the list by selecting a time range in the **In Last** field (for example, in the last 1 day).
- (When viewed from the access control policy.) Clear the hit counts for one or more rule by selecting the checkbox for the rule, then clicking **Clear Hit Counts**. When confirming the action, choose **Clear and Reload** to refresh the hit count data. You can clear hit counts for up to 500 rules at a time. You cannot undo clearing hit counts.

Note

Click the checkbox in the table header to select all rules visible in the list. To select a range of rules, select the first rule's checkbox, then Shift+click the last rule's checkbox; all rules in between are also selected.

- (When viewed from the access control policy.) You can do the following with individual rules:
 - Edit the rule by clicking **Edit** from the **More** (⋮) menu.
 - Delete the rule from the policy by clicking **Delete** from the **More** (⋮) menu.
 - Enable or disable the rule by clicking **Enable/Disable Rule** from the **More** (⋮) menu.
 - Clear the hit count (reset it to zero) for the rule by clicking **Clear Hit Count** from the **More** (⋮) menu. You cannot undo this action.
- (When viewed from the prefilter policy.) Change the displayed columns by clicking **Cog** (⚙️) and selecting the columns to show.
- (When viewed from the prefilter policy.) Click on a rule name to edit it, or click **View** (👁️) in the last column to view the rule details. Clicking on the rule name highlights it in the policy page where you can edit it.
- (When viewed from the prefilter policy.) Clear the hit count information (reset it to zero) for a rule by right-clicking the rule and selecting **Clear Hit Count**. You can select multiple rules by using Ctrl+click. You cannot undo this action.
- Generate a comma-separated values report of the details on the page by clicking **Generate CSV** on the bottom-left of the page.

Step 5 Click **Close** to return to the policy page.

Analyzing rule conflicts and warnings



Note The feature described in this topic is available only if you do not integrate with the Cisco Security Cloud. When you integrate with the cloud, the more powerful Policy Analyzer & Optimizer replaces this feature. See [Identifying and fixing anomalies with Policy Analyzer & Optimizer, on page 22](#).

You can view warnings and information about rule conflicts to examine the logic of your access control policy and to identify rules that need changes. When rules overlap, you can end up with unnecessary rules in the policy, and these rules will never be matched to traffic. The analysis can help you delete unnecessary rules, or identify rules that should be moved or modified so they enforce the desired policy.

Policy warnings and errors point out things that you should understand and perhaps address to ensure that your rules provide the desired services.

Rule conflict analysis identifies the following types of problem:

- **Object overlap**—An element in a field of a rule is a subset of one or more elements in the same field of the rule. For example, the source field might include a network object for 10.1.1.0/24, and another object for the host 10.1.1.1. Because 10.1.1.1 is within the network covered by 10.1.1.0/24, the object for 10.1.1.1 is redundant and can be deleted, simplifying the rule and saving device memory.
- **Redundant rule**—Two rules apply the same action to the same type of traffic and removing the base rule would not change the ultimate result. For example, if a rule permitting FTP traffic for a particular network were followed by a rule allowing IP traffic for that same network, and there were no rules in between denying access, then the first rule is redundant and you can delete it.
- **Shadowed rule**—This is the reverse of a redundant rule. In this case, one rule will match the same traffic as another rule such that the second rule will never be applied to any traffic because it comes later in the access list. If the action for both rules is the same, you can delete the shadowed rule. If the two rules specify different actions for traffic, you might need to move the shadowed rule or edit one of the two rules to implement your desired policy. For example, the base rule might deny IP traffic, and the shadowed rule might permit FTP traffic, for a given source or destination.

Before you begin

When doing the analysis:

- Only the first conflict for a given rule is identified. Once you fix the problem, the rule might be identified as having a conflict with another rule in the table. However, a rule might have multiple warnings or errors.
- Rule conflict analysis considers source/destination security zone, network, VLAN, and service/port match conditions and action only. It does not consider other match criteria, so an apparently redundant rule might not be completely redundant.
- FQDN network objects cannot be analyzed for conflict, because the IP address of an FQDN cannot be known prior to DNS lookup.
- Disabled rules are ignored.
- Time range attributes are ignored. Rules for different time periods might be marked as redundant when they are not actually redundant for the time ranges.

- Icons for warnings and errors, and rule conflicts when you enable the feature, are shown in the rules table. For a reference to the icons, see [Rule and Other Policy Warnings](#).

Procedure

-
- Step 1** Choose **Policies > Security policies > Access Control** and edit an access control policy.
- Step 2** Do one of the following to open the rule conflicts and warnings dialog box:
- To view rule conflicts, click the **Analyze** drop-down and click **Enable Rule Conflicts**. When the analysis completes, you see a summary of the conflicts at the top of the page. Then, click **Show Rule Conflicts** from the same menu to see the specific results.
- You must re-enable rule conflict detection each time you open the policy or make a change and save the policy.
- To view rule warnings and errors, click **Analyze > Show Warnings and Errors**.
- After you make a change to the policy, you can refresh the results by clicking the reload icon next to the Analyze button.
- To view policy warnings, click **Analyze > Show Policy Warnings**.
 - If you are finished viewing rule conflicts, click **Analyze > Disable Rule Conflicts**.
- Step 3** In the rule conflicts and warnings dialog box:
- Rule warnings and errors are shown on a separate tab from rule conflicts. There is also a separate tab for policy warnings.
 - Each tab contains sub-tabs to let you examine individual types of problems, such as redundant vs. shadowed or warnings vs. errors. You can also search for an item.
 - **More** (?) next to each rule name provides shortcuts to edit, disable, or delete the rule.
- Step 4** Click **Close** when finished.
-

Searching for rules

You can use search to help you find rules, especially when you have a large number of them.

Procedure

-
- Step 1** When editing an access control policy, build the search string by clicking in the **Search** box.
- For a simple text string search, type the string. The search returns rules that have that string in any column. You cannot do a string search in conjunction with a tag search, such as combining a string search with a source networks search.

- To search on a specific column, start typing the name of the column until the system prompts you with the full name, such as Source Networks, or select the name from the list of searchable fields. When you select the search tag, you can then enter the search string for that tag. For example, **Source Networks 10.1.1.1**.
- When searching for IP addresses within the source/destination columns (but not as a simple text search), you can use the **Search Inside Subnets and Ranges** option to control whether you exactly match the IP address (unchecked) or match any subnet or range that includes the searched address (checked). For example, with the option checked, searching for 10.1.1.1 will include rules for 10.1.1.0/24.
- Searches in the port field return exact match only.
- When entering multiple values, separate the values with commas.
- After your first search, clicking in the search box prompts you with recent searches and tags. You can quickly repeat a search by selecting it, or build similar searches by selecting previous searches or tags and building on them.
- When building a search string with multiple tags, do not include spaces between the tags.
- When you select a tag, you are prompted with values that appear in those columns. Select the values you want to search for.
- You can quickly filter based on some common features by clicking the filter icon to the left of the search box and selecting to show rules with any combination of the following: Allow, Block, Monitor, Intrusion Policy, Time Range, Conflicts, Warnings, Errors, Disabled rules, expired rules, rules that include objects whose definitions overlap..
- To see the rules that apply to a specific device or set of devices, click the filter icon and select the devices. Rules apply to a device if they use security zones that contain at least one interface on the device, or if they do not include security zones.

Step 2 With your cursor at the end of the search string in the search box, press Enter.

The rules that satisfy the search string are highlighted and non-matching rules are hidden. You can deselect **Show Only Matching Rules** to see the entire table, with the highlighted rules within the table. This lets you see the surrounding rules.

Beside the Show Only Matching Rules checkbox is a summary of the total number of rules in the policy compared to the number that match the search string.

Step 3 To close the search and return to the unfiltered and unhighlighted table, click the **X** at the right of the search box. You can also put your cursor at the end of the search string and press the Esc key.

History for access control policies

Table 1:

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Simultaneous editing of access control policies by multiple users.	10.0.0	Any	In previous releases, if two or more users simultaneously edited an access control policy, the first user who saved would retain their changes, and all other users would immediately lose all of their edits. Now, these users have the ability to selectively merge their changes, and changes that do not conflict with the first user's saved changes will automatically be accepted. This improves collaboration between users and reduces the need to lock the policy during edits.
Object group search performance enhancements.	7.6.0	7.6.0	Object group search is now faster and uses fewer CPU resources. New CLI commands: clear asp table network-object , show asp table network-object , debug acl ogs Modified CLI comments (enhanced output): , packet-tracer , show access-list , show object-group
Policy Analyzer & Optimizer for access control.	From mgmt. center: 7.6.0 From Security Cloud Control: 7.2.0	Any	The Policy Analyzer & Optimizer evaluates access control policies for anomalies such as redundant or shadowed rules, and can take action to fix discovered anomalies. You can launch the access control Policy Analyzer & Optimizer directly from a Version 7.6+ Firewall Management Center; this requires Security Cloud Control. For Versions 7.2–7.4 Firewall Management Centers, use Security Cloud Control. New/modified screens: <ul style="list-style-type: none">• To enable: Integration > Cisco Security Cloud > Enable Policy Analyzer & Optimizer• To analyze policies: Policies > Access Control, select policies, click Analyze Policies.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Granular permissions for modifying access control policies and rules.	7.4.0	Any	<p>You can define custom user roles to differentiate between the intrusion configuration in access control policies and rules and the rest of the access control policy and rules. Using these permissions, you can separate the responsibilities of your network administration team and your intrusion administration teams.</p> <p>When defining user roles, you can select the Policies > Access Control > Access Control Policy > Modify Access Control Policy > Modify Threat Configuration option to allow the selection of intrusion policy, variable set, and file policy in a rule, the configuration of the advanced options for Network Analysis and Intrusion Policies, the configuration of the Security Intelligence policy for the access control policy, and intrusion actions in the policy default action. You can use the Modify Remaining Access Control Policy Configuration to control the ability to edit all other aspects of the policy. The existing pre-defined user roles that included the Modify Access Control Policy permission continue to support all sub-permissions; you need to create your own custom roles if you want to apply granular permissions.</p>
New access control policy user interface and rule conflict analysis.	7.3.0	Any	The access control policy user interface introduced in 7.2 is now the default interface. You can also enable rule conflict analysis to help identify redundant rules and objects, and shadowed rules that cannot be matched due to previous rules in the policy.
Access control policy locking.	7.2.0	Any	<p>You can lock an access control policy to prevent other administrators from editing it. Locking the policy ensures that your changes will not be invalidated if another administrator edits the policy and saves changes before you save your changes. Any user who has permission to modify the access control policy has permission to lock it.</p> <p>We added an icon to lock or unlock a policy next to the policy name while editing the policy. In addition, there is a new permission to allow users to unlock policies locked by other administrators: Override Access Control Policy Lock. This permission is enabled by default in the Administrator, Access Admin, and Network Admin roles.</p>
Rule hit counts persist over reboot.	7.2.0	Any	<p>Rebooting a managed device no longer resets access control rule hit counts to zero. Hit counts are reset only if you actively clear the counters. In addition, counts are maintained by each unit in an HA pair or cluster separately. You can use the show rule hits command to see cumulative counters across the HA pair or cluster, or see the counts per node.</p> <p>We modified the following device CLI command: show rule hits.</p>

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Usability improvements for the access control policy.	7.2.0	Any	There is a new user interface available for the access control policy. You can continue to use the legacy user interface, or you can try out the new user interface. The new interface has both a table and a grid view for the rules list, the ability to show or hide columns, enhanced search, infinite scroll, a clearer view of the packet flow related to policies associated with the access control policy, and a simplified add/edit dialog box for creating rules. You can freely switch back and forth between the legacy and new user interfaces while editing an access control policy.
DNS filtering	7.0.0 6.7.0 (experimental)	Any	<p>If URL filtering is enabled and configured, a new option to enhance category and reputation filtering efficacy is enabled by default for each new access control policy.</p> <p>For more information, see DNS Filtering: Identify URL Reputation and Category During DNS Lookup and subtopics.</p> <p>The Advanced tab of access control policy has a new option under General Settings: Enable reputation enforcement on DNS traffic.</p>
TLS server identity discovery	6.7.0	Any	<p>Enable access control policies to evaluate URL and application conditions when a client connects to a TLS 1.3-enabled server. TLS server identity discovery enables these conditions to be evaluated without decrypting traffic.</p> <p>Enabling this feature can impact device performance, depending on model.</p> <p>The Advanced tab page of access control policy has new options:</p> <ul style="list-style-type: none"> Warning is displayed on the Advanced tab; moving the slider to the right enables TLS server identity discovery. New option on the Advanced tab page: TLS Server Identity Discovery.
New Security Intelligence categories	—	Any	<p>The following categories were introduced at about the time of the 6.6 release, but are not specific to 6.6:</p> <ul style="list-style-type: none"> banking_fraud high_risk ioc link_sharing malicious newly_seen spyware

