



## Tune Intrusion Policies Using Rules

---

This chapter provides information on custom rules in Snort 3, intrusion rule action, intrusion event notification filters in an intrusion policy, converting Snort 2 custom rules to Snort 3, and adding rule groups with custom rules to an intrusion policy.

- [Overview of Tuning Intrusion Rules, on page 1](#)
- [Intrusion Rule Types, on page 2](#)
- [Prerequisites for Network Analysis and Intrusion Policies, on page 3](#)
- [Custom Rules in Snort 3, on page 3](#)
- [View Snort 3 Intrusion Rules in an Intrusion Policy, on page 6](#)
- [Intrusion Rule Action, on page 7](#)
- [Intrusion Event Notification Filters in an Intrusion Policy, on page 8](#)
- [Add Intrusion Rule Comments, on page 13](#)
- [Snort 2 Custom Rules Conversion to Snort 3, on page 13](#)
- [Add Custom Rules to Rule Groups, on page 15](#)
- [Add Rule Groups with Custom Rules to an Intrusion Policy, on page 16](#)
- [Manage Custom Rules in Snort 3, on page 17](#)
- [Delete Custom Rules, on page 18](#)
- [Delete Rule Groups, on page 18](#)
- [Intrusion Rule State Options, on page 19](#)

## Overview of Tuning Intrusion Rules

You can configure rule states and other settings for shared object rules, standard text rules, and inspector rules.

You enable a rule by setting its rule state to Alert or to Block. Enabling a rule causes the system to generate events on traffic matching the rule. Disabling a rule stops processing of the rule. You can also set your intrusion policy so that a rule set to Block generates events on, and drops, matching traffic.

You can filter rules to display a subset of rules, enabling you to select the exact set of rules where you want to change rule states or rule settings.

When an intrusion rule or rule argument requires a disabled inspector, the system automatically uses it with its current configuration even though it remains disabled in the network analysis policy's web interface.



**Note** We recommend that you do not modify shared object rules and you only enable or disable these rules for your threat defense device. To create custom Snort rules, contact Cisco support.

## Intrusion Rule Types

An intrusion rule is a specified set of keywords and arguments that the system uses to detect attempts to exploit vulnerabilities in your network. As the system analyzes network traffic, it compares packets against the conditions specified in each rule, and triggers the rule if the data packet meets all the conditions specified in the rule.

An intrusion policy contains:

- *intrusion rules*, which are subdivided into *shared object rules* and *standard text rules*
- *inspector rules*, which are associated with a detection option of the packet decoder or with one of the inspectors included with the system

The following table summarizes attributes of these rule types:

**Table 1: Intrusion Rule Types**

| Type               | Generator ID (GID)                 | Snort ID (SID)     | Source                                              | Can Copy? | Can Edit? |
|--------------------|------------------------------------|--------------------|-----------------------------------------------------|-----------|-----------|
| shared object rule | 3                                  | lower than 1000000 | Cisco Talos Intelligence Group (Talos)              | yes       | limited   |
| standard text rule | 1<br>(Global domain or legacy GID) | lower than 1000000 | Talos                                               | yes       | limited   |
|                    | 1000 - 2000<br>(descendant domain) | 1000000 or higher  | Created or imported by user                         | yes       | yes       |
| preprocessor rule  | decoder- or preprocessor-specific  | lower than 1000000 | Talos                                               | no        | no        |
|                    |                                    | 1000000 or higher  | Generated by the system during option configuration | no        | no        |

You cannot save changes to any rule created by Talos, but you can save a copy of a modified rule as a custom rule. You can modify either variables used in the rule or rule header information (such as source and destination ports and IP addresses). In a multidomain deployment, rules created by Talos belong to the Global domain. Administrators in descendant domains can save local copies of the rules, which they can then edit.

For the rules it creates, Talos assigns default rule states in each default intrusion policy. Most preprocessor rules are disabled by default and must be enabled if you want the system to generate events for preprocessor rules and, in an inline deployment, drop offending packets.

## Prerequisites for Network Analysis and Intrusion Policies

To allow the Snort inspection engine to process traffic for intrusion and malware analysis, you must have the IPS license enabled for the Firewall Threat Defense device.

You must be an Admin user to manage network analysis, intrusion policies, and perform migration tasks.

## Custom Rules in Snort 3

You can create a custom intrusion rule by importing a local rule file. The rule file can either have a `.txt` or `.rules` extension. The system saves the custom rule in the local rule category, regardless of the method you used to create it. A custom rule must belong to a rule group. However, a custom rule can be a part of two or more groups as well.

When you create a custom intrusion rule, the system assigns it a unique rule number, which has the format `GID:SID:Rev`. The elements of this number are:

- **GID**—Generator ID. For custom rules, it is not necessary to specify the GID. The system automatically generates the GID based on whether you are in the Global domain or a sub-domain while uploading the rules. For all standard text rules, this value is 2000 for a Global domain.
- **SID**—Snort ID. Indicates whether the rule is a local rule or a system rule. When you create a new rule, assign a unique SID to the rule.  
  
SID numbers for local rules start at 1000000, and the SID for each new local rule is incremented by one.
- **Rev**—The revision number. For a new rule, the revision number is one. Each time you modify a custom rule the revision number should be incremented by one.

In a custom standard text rule, you set the rule header settings and the rule keywords and arguments. You can use the rule header settings to focus the rule to only match traffic using a specific protocol and traveling to or from specific IP addresses or ports.

To check whether a SID is enabled or disabled, verify the entries in the `snort.lua` file located in the `./file-contents/ngfw/var/sf/detection_engines/<id>/ips/<id>` directory.

- If the SID is disabled by default, no entry will be present in the file.
- If the SID is manually enabled, you will see an entry with **enable:yes**.
- If the SID is disabled after being manually enabled, the entry remains in the file and will display **enable:no**.

**Note**

- Snort 3 custom rules cannot be edited. Ensure that custom rules have a valid classification message for `classtype` within the rule text. If you import a rule without a classification or wrong classification, then delete and recreate the rule.
- You can create custom intrusion rules using Snort 3. However, support for tuning and troubleshooting these rules is not available currently.
- The *classtype* in a Snort rule assigns a classification to the rule indicating the type of attack that is associated with an event. A priority level of 1-4 is also associated with each *classtype*. However, the priority level for certain *classtypes* on the Threat Defense device do not match the open-source Snort *classtype* priority levels that are mentioned in the Snort [documentation](#). For example, *tcp-connection* has a priority of 4 in open-source Snort while a priority of 3 is assigned to it on the Threat Defense device.

**Sensitive Data Detection in Snort 3**

Sensitive data such as social security numbers, credit card numbers, emails, and so on may be leaked onto the internet, intentionally or accidentally. Sensitive data detection is used to detect and generate events on possible sensitive data leakage. Events are generated only if there is a transfer of significant amount of Personally Identifiable Information (PII) data. Sensitive data detection can mask PII in the output of events.

**sd\_pattern Option**

Use the `sd_pattern` IPS option to detect and filter PII. This information includes credit card numbers, U.S. Social Security numbers, phone numbers, and email addresses. A regular expression (regex) syntax is available for defining your own PII.

The `sd_pattern` option has the following settings:

- **Pattern**—An implicit, required setting that specifies the regular expression to look for in the PDU. The regex must be written in PCRE syntax.
- **Threshold**—An explicit, optional setting that specifies the number of matches in the PDU required to generate an event.

The `sd_pattern` as IPS rule option is available in Snort with no requirements for additional inspectors. The rule option's syntax is:

```
sd_pattern: "<pattern>"[, threshold <count>];
```

For example:

```
sd_pattern:"credit_card", threshold 2;
```

**Built-in Patterns**

There are five built-in patterns for sensitive data. To use the built-in patterns in the "pattern" setting, you must specify the name of the PII type that needs to be matched and the necessary regex is substituted for it. The PII name and regex mappings or patterns are described as follows:

- **credit\_card**—  

```
\d{4}\D?\d{4}\D?\d{2}\D?\d{2}\D?\d{3,4}
```
- **us\_social**—

```
[0-8]\d{2}-\d{2}-\d{4}
```

- `us_social_nodashes`—

```
[0-8]\d{8}
```

- `Email`—

```
[a-zA-Z0-9!#$%&'*/=\?^_`{|}~]+(?:\. [a-zA-Z0-9!#$%&'*/=\?^_`{|}~]+)*@(?:[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?
```

- `us_phone`—

```
(?:\+?1[-.\s]?)?(?:([2-9][0-8]\d)\)?[-.\s]([2-9]\d{2})[-.\s](\d{4})
```

| PII Name                        | Pattern                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>credit_card</code>        | <code>\d{4}\D?\d{4}\D?\d{2}\D?\d{2}\D?\d{3,4}</code>                                                                                                                                |
| <code>us_social</code>          | <code>[0-8]\d{2}-\d{2}-\d{4}</code>                                                                                                                                                 |
| <code>us_social_nodashes</code> | <code>[0-8]\d{8}</code>                                                                                                                                                             |
| <code>Email</code>              | <code>[a-zA-Z0-9!#\$%&amp;'*/=\?^_`{ }~]+(?:\. [a-zA-Z0-9!#\$%&amp;'*/=\?^_`{ }~]+)*@(?:[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?</code> |
| <code>us_phone</code>           | <code>(?:\+?1[-.\s]?)?(?:([2-9][0-8]\d)\)?[-.\s]([2-9]\d{2})[-.\s](\d{4})</code>                                                                                                    |

Masking for data matching these patterns only work with system-provided rules or built-in patterns for Credit Cards, U.S. Social Security numbers, emails, and U.S. phone numbers. Masking does not work for custom rules or user-defined PII patterns. Rules are available in the Lightweight Security Package (LSP) for sensitive data, gid:13. By default, they are not enabled in any system-provided policy.

The sensitive data rules in LSP cover all built-in patterns and have the following threshold values:

- `credit_card`: 2
- `us_social`: 2
- `us_social_nodashes`: 20
- `email`: 20
- `us_phone`: 20

You can use the `sd_pattern` option to create custom rules and modify existing rules. To do this, use the Snort 3 intrusion policy interface.

An example of a rule with `sd_pattern` with a custom pattern and threshold:

```
alert tcp (sid: 1000000001; sd_pattern: "[\w-\.]+\@([\w-]+\.)+[\w-]{2,4}", threshold 4; msg: "email, threshold 4")
```

## Examples

An example of custom rules using sensitive data detection:

Rule with built-in pattern:

```
alert tcp (
    msg: "SENSITIVE-DATA Email";
```

```

        flow:only_stream;
        pkt_data;
        sd_pattern:"email", threshold 5;
        service:http, smtp, ftp-data, imap, pop3;
        gid:2000;
        sid:1000001;
    )

```

#### Rule with custom pattern

```

alert tcp (
    msg:"SENSITIVE-DATA US phone numbers";
    flow:only_stream;
    file_data;
    sd_pattern:"+?3?8?(0[\s\.-]\d{2}[\s\.-]\d{3}[\s\.-]\d{2}[\s\.-]\d{2})", threshold
2;

    service:http, smtp, ftp-data, imap, pop3;
    gid:2000;
    sid:1000002;
)

```

Here are some more examples of complete Snort IPS rules with built-in sensitive data patterns:

- alert tcp ( sid:1; msg:"Credit Card"; sd\_pattern:"credit\_card", threshold 2; )
- alert tcp ( sid:2; msg:"US Social Number"; sd\_pattern:"us\_social", threshold 2; )
- alert tcp ( sid:3; msg:"US Social Number No Dashes"; sd\_pattern:"us\_social\_nodashes", threshold 2; )
- alert tcp ( sid:4; msg:"US Phone Number"; sd\_pattern:"us\_phone", threshold 2; )
- alert tcp ( sid:5; msg:"Email"; sd\_pattern:"email", threshold 2; )

Disabling data masking is not supported in the Secure Firewall Management Center and Secure Firewall Device Manager.

For information how to add custom rules to rule groups, see [Add Custom Rules to Rule Groups, on page 15](#).

## View Snort 3 Intrusion Rules in an Intrusion Policy

You can adjust how rules are displayed in the intrusion policy. You can also display the details for a specific rule to see rule settings, rule documentation, and other rule specifics.

### Procedure

- 
- Step 1** Choose **Policies > Security policies > Intrusion**.
  - Step 2** Click **Snort 3 Version** next to the policy.
  - Step 3** While viewing the rules, you can:

- Filter the rules.
- Choose a rule group to see rules related to that group.
- View an intrusion rule's details.
- View rule comments.
- View rule documentation.

See [Edit Snort 3 Intrusion Policies](#) for details on performing these tasks.

## Intrusion Rule Action

Intrusion rule action allows you to enable or disable the rule within an individual intrusion policy, as well as specify which action the system takes if monitored conditions trigger the rule.

The Cisco Talos Intelligence Group (Talos) sets the default action of each intrusion and inspector rule in each default policy. For example, a rule may be enabled in the Security over Connectivity default policy and disabled in the Connectivity over Security default policy. Talos sometimes uses a rule update to change the default action of one or more rules in a default policy. If you allow rule updates to update your base policy, you also allow the rule update to change the default action of a rule in your policy when the default action changes in the default policy you used to create your policy (or in the default policy it is based on). Note, however, that if you have changed the rule action, the rule update does not override your change.

When you create an intrusion rule, it inherits the default actions of the rules in the default policy you use to create your policy.

## Intrusion Rule Action Options

In an intrusion policy, you can set a rule's action to the following values:

### Alert

You want the system to detect a specific intrusion attempt and generate an intrusion event when it finds matching traffic. When a malicious packet crosses your network and triggers the rule, the packet is sent to its destination and the system generates an intrusion event. The malicious packet reaches its target, but you are notified through the event logging.

### Block

You want the system to detect a specific intrusion attempt, drop the packet containing the attack, and generate an intrusion event when it finds matching traffic. The malicious packet never reaches its target, and you are notified through the event logging.

### Disable

You do not want the system to evaluate matching traffic.



**Note** Choosing either the **Alert** or **Block** options enables the rule. Choosing **Disable** disables the rule.

We **strongly** recommend that you **do not** enable all the intrusion rules in an intrusion policy. The performance of your managed device is likely to degrade if all rules are enabled. Instead, tune your rule set to match your network environment as closely as possible.

## Set Intrusion Rule Action

Intrusion rule actions are policy-specific.

## Procedure

**Step 1** Choose **Policies > Security policies > Intrusion**.

**Step 2** Click **Snort 3 Version** next to the policy you want to edit.

**Tip**

This page shows the total number of:

- disabled rules
- enabled rules set to Alert
- enabled rules set to Block
- overridden rules

**Step 3** Choose the rule or rules where you want to set the rule action.

**Step 4** Choose one of the rule actions from the **Rule Action** drop-down list. See [Edit Snort 3 Intrusion Policies](#) for more information about the different rule actions.

**Step 5** Click **Save**.

## What to do next

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

# Intrusion Event Notification Filters in an Intrusion Policy

The importance of an intrusion event can be based on frequency of occurrence, or on source or destination IP address. In some cases you may not care about an event until it has occurred a certain number of times. For example, you may not be concerned if someone attempts to log into a server until they fail a certain number of times. In other cases, you may only need to see a few occurrences to know there is a widespread problem. For example, if a DoS attack is launched against your web server, you may only need to see a few occurrences of an intrusion event to know that you need to address the situation. Seeing hundreds of the same event only overwhelms your system.

## Intrusion Event Thresholds

You can set thresholds for individual rules to limit the number of times the system logs and displays an intrusion event based on how many times the event is generated within a specified time period. This can prevent you from being overwhelmed with a large number of identical events. You can set thresholds per shared object rule, standard text rule, or inspector rule.

## Set Intrusion Event Thresholds

To set a threshold, first specify the thresholding type.

**Table 2: Thresholding Options**

| Option    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Limit     | Logs and displays events for the specified number of packets (specified by the Count argument) that trigger the rule during the specified time period. For example, if you set the type to <b>Limit</b> , the <b>Count</b> to 10, and the <b>Seconds</b> to 60, and 14 packets trigger the rule, the system stops logging events for the rule after displaying the first 10 that occur within the same minute.                                                                                                                                                                                                                                                                                                                                                                        |
| Threshold | Logs and displays a single event when the specified number of packets (specified by the Count argument) trigger the rule during the specified time period. Note that the counter for the time restarts after you hit the threshold count of events and the system logs that event. For example, you set the type to <b>Threshold</b> , <b>Count</b> to 10, and <b>Seconds</b> to 60, and the rule triggers 10 times by second 33. The system generates one event, then resets the Seconds and Count counters to 0. The rule then triggers another 10 times in the next 25 seconds. Because the counters reset to 0 at second 33, the system logs another event.                                                                                                                       |
| Both      | Logs and displays an event once per specified time period, after the specified number (count) of packets trigger the rule. For example, if you set the type to <b>Both</b> , <b>Count</b> to two, and <b>Seconds</b> to 10, the following event counts result: <ul style="list-style-type: none"> <li>• If the rule is triggered once in 10 seconds, the system does not generate any events (the threshold is not met)</li> <li>• If the rule is triggered twice in 10 seconds, the system generates one event (the threshold is met when the rule triggers the second time)</li> <li>• If the rule is triggered four times in 10 seconds, the system generates one event (the threshold is met when the rule triggers the second time, and following events are ignored)</li> </ul> |

Secondly, specify tracking, which determines whether the event threshold is calculated per source or destination IP address.

**Table 3: Thresholding IP Options**

| Option      | Description                                                 |
|-------------|-------------------------------------------------------------|
| Source      | Calculates event instance count per source IP address.      |
| Destination | Calculates event instance count per destination IP address. |

Finally, specify the number of instances and time period that define the threshold.

**Table 4: Thresholding Instance/Time Options**

| Option | Description                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------|
| Count  | The number of event instances per specified time period per tracking IP address required to meet the threshold. |

| Option  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Seconds | The number of seconds that elapse before the count resets. If you set the threshold type to <b>limit</b> , the tracking to <b>Source IP</b> , the <b>count</b> to 10, and the <b>seconds</b> to 10, the system logs and displays the first 10 events that occur in 10 seconds from a given source port. If only 7 events occur in the first 10 seconds, the system logs and displays those; if 40 events occur in the first 10 seconds, the system logs and displays 10, then begins counting again when the 10-second time period elapses. |

Note that you can use intrusion event thresholding alone or in any combination with rate-based attack prevention, the `detection_filter` keyword, and intrusion event suppression.



**Tip** You can also add thresholds from within the packet view of an intrusion event.

## Set Threshold for an Intrusion Rule in Snort 3

You can set a single threshold for a rule from the Rule Detail page. Adding a threshold overwrites any existing threshold for the rule. The threshold you set for an intrusion rule is applied to each packet thread. However, the configuration is fully applied only within the context of a unique flow. There may be more alerts on different network flows, but there will not be fewer alerts than the configured number.

### Procedure

- Step 1** Choose **Policies** > + **Show more** > **Security policies** > **Intrusion Rules**.
  - Step 2** Click **Snort 3 All Rules** tab.
  - Step 3** From an intrusion rule's Alert Configuration column, click the **None** link.
  - Step 4** Click **Edit** (✎).
  - Step 5** In the Alert Configuration window, click the **Threshold** tab.
  - Step 6** From the **Type** drop-down list, choose the type of threshold you want to set:
    - Choose **Limit** to limit notification to the specified number of event instances per time period.
    - Choose **Threshold** to provide notification for each specified number of event instances per time period.
    - Choose **Both** to provide notification once per time period after a specified number of event instances.
  - Step 7** Choose **Source** or **Destination** in the **Track By** field to indicate whether you want the event instances tracked by source or destination IP address.
  - Step 8** Enter the number of event instances you want to use as your threshold in the **Count** field.
  - Step 9** Enter a number that specifies the time period, in seconds, for which event instances are tracked in the **Seconds** field.
  - Step 10** Click **Save**.
- Refer to the video [Snort 3 Suppression and Threshold](#) for additional support and information.

**What to do next**

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

## View and Delete Intrusion Event Thresholds

To view or delete an existing threshold setting for a rule, use the Rules Details view to display the configured settings for a threshold and see if they are appropriate for your system. If they are not, you can add a new threshold to overwrite the existing values.

**Procedure**

- 
- Step 1** Choose **Policies > + Show more > Security policies > Intrusion Rules**.
  - Step 2** Click **Snort 3 All Rules** tab.
  - Step 3** Choose the rule with a configured threshold as shown in the **Alert Configuration** column (the **Alert Configuration** column displays **Threshold** as a link for the rule).
  - Step 4** To remove the threshold for the rule, click **Threshold** link in the **Alert Configuration** column.
  - Step 5** Click **Edit** (✎).
  - Step 6** Click **Threshold** tab.
  - Step 7** Click **Reset**.
  - Step 8** Click **Save**.
- 

**What to do next**

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

## Intrusion Policy Suppression Configuration

You can suppress intrusion event notification when a specific IP address or range of IP addresses triggers a specific rule or inspector. This is useful for eliminating false positives. For example, if you have a mail server that transmits packets that look like a specific exploit, you might suppress event notification for that event when it is triggered by your mail server. The rule triggers for all packets, but you only see events for legitimate attacks.

### Intrusion Policy Suppression Types

Note that you can use intrusion event suppression alone or in any combination with rate-based attack prevention, the `detection_filter` keyword, and intrusion event thresholding.




---

**Tip** You can add suppressions from within the packet view of an intrusion event. You can also access suppression settings by using the **Alert Configuration** column on the intrusion rules editor page (**Policies > + Show more > Security policies > Intrusion Rules**, click **Snort 3 All Rules**).

---

## Set Suppression for an Intrusion Rule in Snort 3

You can set one or more suppressions for a rule in your intrusion policy.

### Before you begin

Ensure you create the required network objects to be added for source or destination suppression.

### Procedure

- 
- Step 1** Choose **Policies** > + **Show more** > **Security policies** > **Intrusion Rules**.
  - Step 2** Click **Snort 3 All Rules** tab.
  - Step 3** Click the **None** link in the intrusion rule's Alert Configuration column.
  - Step 4** Click **Edit** (✎).
  - Step 5** From the **Suppressions** tab, click the add icon **Add** (+) next to any of the following options:
    - Choose **Source Networks** to suppress events generated by packets originating from a specified source IP address.
    - Choose **Destination Networks** to suppress events generated by packets going to a specified destination IP address.
  - Step 6** Select any of the preset networks in the **Network** drop-down list.
  - Step 7** Click **Save**.
  - Step 8** (Optional) Repeat the last three steps if required.
  - Step 9** Click **Save** in the Alert Configuration window.
- 

### What to do next

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

## View and Delete Suppression Conditions

You may want to view or delete an existing suppression condition. For example, you can suppress event notification for packets originating from a mail server IP address because the mail server normally transmits packets that look like exploits. If you then decommission that mail server and reassign the IP address to another host, you should delete the suppression conditions for that source IP address.

### Procedure

- 
- Step 1** Choose **Policies** > + **Show more** > **Security policies** > **Intrusion Rules**.
  - Step 2** Click **Snort 3 All Rules** tab.
  - Step 3** Choose the rule for which you want to view or delete suppressions.
  - Step 4** Click **Suppression** in the **Alert Configuration** column.

- Step 5** Click **Edit** (✎).
- Step 6** Click **Suppressions** tab.
- Step 7** Remove the suppression by clicking **Clear** (✕) next to the suppression.
- Step 8** Click **Save**.
- 

#### What to do next

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

## Add Intrusion Rule Comments

You can add comments to rules in your intrusion policy. Comments added this way are policy-specific; that is, comments you add to a rule in one intrusion policy are not visible in other intrusion policies.

#### Procedure

---

- Step 1** Choose **Policies > Security policies > Intrusion**.
- Step 2** Click **Snort 3 Version** next to the policy you want to edit.
- Step 3** In the right side of the page where all the rules are listed, choose the rule where you want to add a comment.
- Step 4** Click **Comment** (🗨) under the **Comments** column.
- Step 5** In the **Comments** field, enter the rule comment.
- Step 6** Click **Add Comment**.
- Step 7** Click **Save**.

#### Tip

The system displays a **Comment** (🗨) next to the rule in the Comments column.

---

#### What to do next

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

## Snort 2 Custom Rules Conversion to Snort 3

If you are using custom rules, make sure you are prepared to manage that rule set for Snort 3 prior to conversion from Snort 2 to Snort 3. If you are using a rule set from a third-party vendor, contact that vendor to confirm that their rules will successfully convert to Snort 3 or to obtain a replacement rule set written natively for Snort 3. If you have custom rules that you have written yourself, familiarize with writing Snort 3 rules prior to conversion, so you can update your rules to optimize Snort 3 detection after conversion. See the links below to learn more about writing rules in Snort 3.

- <https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html>

- <https://blog.snort.org/2020/10/talos-transition-to-snort-3.html>

You can refer to other blogs at <https://blog.snort.org/> to learn more about Snort 3 rules.



#### Important

Snort 2 network analysis policy (NAP) settings *cannot* be copied to Snort 3 automatically. NAP settings have to be manually replicated in Snort 3.

## Convert all Snort 2 Custom Rules across all Intrusion Policies to Snort 3

### Procedure

**Step 1** Choose **Policies** > + **Show more** > **Security policies** > **Intrusion Rules**.

**Step 2** Click **Snort 3 All Rules** tab.

**Step 3** Ensure **All Rules** is selected in the left pane.

**Step 4** Click the **Tasks** drop-down list and choose:

- **Convert Snort 2 rules and import**—To automatically convert all the Snort 2 custom rules across all the intrusion policies to Snort 3 and import them into Firewall Management Center as Snort 3 custom rules.
- **Convert Snort 2 rules and download**—To automatically convert all the Snort 2 custom rules across all the intrusion policies to Snort 3 and download them into your local system.

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

#### Note

- If you selected **Convert and import** in the previous step, then all the converted rules are saved under a newly created rule group **All Snort 2 Converted Global** under **Local Rules**.
- If you selected **Convert and download** in the previous step, then save the rules file locally. You can review the converted rules in the downloaded file and later upload them by following the steps in [Add Custom Rules to Rule Groups, on page 15](#).

Refer to the video [Converting Snort 2 Rules to Snort 3](#) for additional support and information.

### What to do next

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

## Convert Snort 2 Custom Rules of a Single Intrusion Policy to Snort 3

### Procedure

**Step 1** Choose **Policies > Security policies > Intrusion**.

**Step 2** In the **Intrusion Policies** tab, click **Show Snort 3 Sync status**.

**Step 3** Click the **Sync** icon **Snort out-of-Sync** (🔴) of the intrusion policy.

#### Note

If the Snort 2 and the Snort 3 versions of the intrusion policy are synchronized, then the **Sync** icon is in blue **Snort in-Sync** (🟢). It indicates that there are no custom rules to be converted.

**Step 4** Read through the summary and click the **Custom Rules** tab.

**Step 5** Choose:

- **Import converted rules to this policy**—To convert the Snort 2 custom rules in the intrusion policy to Snort 3 and import them into Firewall Management Center as Snort 3 custom rules.
- **Download converted rules**—To convert the Snort 2 custom rules in the intrusion policy to Snort 3 and download them into your local system. You can review the converted rules in the downloaded file and later upload the file by clicking the upload icon.

**Step 6** Click **Re-Sync**.

### What to do next

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

## Add Custom Rules to Rule Groups

Uploading custom rules in the Firewall Management Center adds the custom rules that you have created locally to the list of all the Snort 3 rules.

### Procedure

**Step 1** Choose **Policies > + Show more > Security policies > Intrusion Rules**.

**Step 2** Click **Snort 3 All Rules** tab.

**Step 3** Click the **Tasks** drop-down list.

**Step 4** Click **Upload Snort 3 Rules**.

**Step 5** Drag and drop the `.txt` or `.rules` file that contains the Snort 3 custom rules that you have created.

**Step 6** Click **OK**.

#### Note

If there are any errors in the selected file, then you cannot proceed further. You can download the error file and **Replace File** link to upload version 2 of the file, after fixing the errors.

**Step 7** Associate rules to a rule group to add the new rules to that group.

You can also create a new custom rule group (by clicking the **Create New Custom Rule Group** link) and then add the rules to the new group.

**Note**

If there are no existing local rule groups, then proceed by clicking **Create New Custom Rule Group to proceed**. Enter a **Name** for the new rule group and click **Save**.

**Step 8** Choose either of the following:

- **Merge Rules** to merge the new rules that you are adding with the existing rules in the rule group.
- **Replace all rules in the group with file contents** to replace all the exiting rules with the new rules that you are adding.

**Note**

If you chose more than one rule group in the previous step, then only the **Merge Rules** option is available.

**Step 9** Click **Next**.

Review the summary to know the new rule IDs that are being added and optionally download it.

**Step 10** Click **Finish**.



**Important**

The rule action of all the uploaded rules is in the disabled state. You have to change them to the required state to ensure the rules are active.

**What to do next**

- Uploading custom rules in the Firewall Management Center adds the custom rules that you have created to the list of all the Snort 3 rules. To enforce these custom rules on the traffic, add and enable these rules in the required intrusion policies. For information on adding rule groups with custom rules to an intrusion policy, see [Add Rule Groups with Custom Rules to an Intrusion Policy, on page 16](#). For information on enabling custom rules, see [Manage Custom Rules in Snort 3, on page 17](#).
- Deploy configuration changes; see [Deploy Configuration Changes](#).

## Add Rule Groups with Custom Rules to an Intrusion Policy

Custom rules that are uploaded in the system have to be enabled in an intrusion policy to enforce those rules on the traffic. After uploading custom rules on Firewall Management Center, add the rule group with the new custom rules in the intrusion policy.

### Procedure

- 
- Step 1** Choose **Policies > Security policies > Intrusion**.
- Step 2** In the **Intrusion Policies** tab, click the **Snort 3 Version** of the intrusion policy.
- Step 3** Click **Add (+)** next to the Rule Groups search bar.
- Step 4** In the **Add Rule Groups** window, click the **Expand Arrow (➤)** icon next to a rule group to expand the local rule group.
- Step 5** Check the check box next to the uploaded custom rules group.
- Step 6** Click **Save**.
- 

### What to do next

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

## Manage Custom Rules in Snort 3

Custom rules that are uploaded in the system have to be added to an intrusion policy and enabled to enforce those rules on the traffic. You can enable the uploaded custom rules across all policies or selectively on individual policies.

Follow the steps to enable custom rules in one or many intrusion policies:

### Procedure

- 
- Step 1** Choose **Policies > + Show more > Security policies > Intrusion Rules**.
- Step 2** Click **Snort 3 All Rules** tab.
- Step 3** Expand **Local Rules**.
- Step 4** Select the required rule group.
- Step 5** Select the rules by checking the check boxes next to them.
- Step 6** Select **Per Intrusion Policy** from the **Rule Actions** drop-down list.
- Step 7** Choose:
- **All Policies**—to have the same rule actions for all the rules to be added.
  - **Per Intrusion Policy**—to have different rule actions for each intrusion policy.
- Step 8** Set the rule actions:
- If you selected **All Policies** in the previous step, then select the required rule action from the **Select Override state** drop-down list.
  - If you selected **Per Intrusion Policy** in the previous step, then select the **Rule Action** against the policy name. To add more policies, click **Add Another**.

**Step 9** Optionally, add a comment in the **Comments** text box.

**Step 10** Click **Save**.

---

#### What to do next

Deploy the changes on the device. See, [Deploy Configuration Changes](#).

## Delete Custom Rules

### Procedure

---

**Step 1** Choose **Policies > + Show more > Security policies > Intrusion Rules**.

**Step 2** Click **Snort 3 All Rules** tab.

**Step 3** Expand **Local Rules** in the left pane.

**Step 4** Check the check boxes of the rules you want to delete.

**Step 5** Ensure that the rule action for all the rules that you select is **Disable**.

If required, follow the steps below to disable the rule action for multiple selected rules:

- a) From the **Rule Actions** drop-down box, select **Per Intrusion Policy**.
- b) Select **All Policies** radio button.
- c) Select **Disable** from the **Select Override state** drop-down list.
- d) Click **Save**.
- e) Check the check boxes of the rules you want to delete.

**Step 6** From the **Rule Actions** drop-down list, select **Delete**.

**Step 7** Click **Delete** in the Delete Rules pop-up window.

---

#### What to do next

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

## Delete Rule Groups

### Before you begin

Exclude the rule group you want to delete from all intrusion policies where you have included it. For steps on excluding a rule group from an intrusion policy, see [Edit Snort 3 Intrusion Policies](#).

## Procedure

- 
- Step 1** Choose **Policies > + Show more > Security policies > Intrusion Rules**.
- Step 2** Click **Snort 3 All Rules** tab.
- Step 3** Expand **Local Rules** in the left pane.
- Step 4** Select the rule group to be deleted.
- Step 5** Ensure the rule action for all the rules in the group is set to **Disable** before proceeding.
- If the rule action for any of the rules is anything other than **Disable**, then you cannot delete the rule group. If required, follow the steps below to disable the rule action for all the rules:
- Check the check box below the **Rule Actions** drop-down list to select all the rules in the group.
  - From the **Rule Actions** drop-down box, select **Per Intrusion Policy**.
  - Select **All Policies** radio button.
  - Select **Disable** from the **Select Override state** drop-down list.
  - Click **Save**.
- Step 6** Click the **Delete** () next to the rule group.
- Step 7** Click **OK** in the Delete Rule Group pop-up window.
- 

## What to do next

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

# Intrusion Rule State Options

In an intrusion policy, you can set a rule's state to the following values:

## Generate Events

You want the system to detect a specific intrusion attempt and generate an intrusion event when it finds matching traffic. When a malicious packet crosses your network and triggers the rule, the packet is sent to its destination and the system generates an intrusion event. The malicious packet reaches its target, but you are notified via the event logging.

## Drop and Generate Events

You want the system to detect a specific intrusion attempt, drop the packet containing the attack, and generate an intrusion event when it finds matching traffic. The malicious packet never reaches its target, and you are notified via the event logging.

Note that rules set to this rule state generate events but do not drop packets in a passive deployment. For the system to drop packets, **Drop when Inline** must also be enabled (the default setting) in your intrusion policy and you must deploy your device inline.

## Disable

You do not want the system to evaluate matching traffic.



**Note** Choosing either the **Generate Events** or **Drop and Generate Events** options enables the rule. Choosing **Disable** disables the rule.

Cisco **strongly** recommends that you **do not** enable all the intrusion rules in an intrusion policy. The performance of your managed device is likely to degrade if all rules are enabled. Instead, tune your rule set to match your network environment as closely as possible.

## Setting Intrusion Rule States

Intrusion rule states are policy-specific.

### Procedure

**Step 1** Choose **Policies > Security policies > Intrusion**.

**Step 2** Click **Snort 2 Version** next to the 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.

#### Tip

This page indicates the total number of enabled rules, the total number of enabled rules set to Generate Events, and the total number set to Drop and Generate Events. Note also that in a passive deployment, rules set to Drop and Generate Events only generate events.

**Step 3** Click **Rules** immediately under **Policy Information** in the navigation panel.

**Step 4** Choose the rule or rules where you want to set the rule state.

**Step 5** Choose one of the following:

- **Rule State > Generate Events**
- **Rule State > Drop and Generate Events**
- **Rule State > Disable**

**Step 6** To save changes you made in this policy since the last policy commit, click **Policy Information** in the navigation panel, then click **Commit Changes**.

If you leave the policy without committing changes, changes since the last commit are discarded if you edit a different policy.

### What to do next

- Deploy configuration changes.