Revised: March 26, 2026

# Custom IPS Signature Sets for SD-Routing Devices

## What's new

*Table 1: What's New*

| Cisco IOS XE release | Feature name | Description | Supported platforms |
|---|---|---|---|
| Cisco IOS XE 26.1 | Unified Threat Defense Support for Cisco Catalyst IR8100 Heavy Duty Series Router | From this release, this feature supports selective activation of Unified Threat Defense (UTD) capabilities. Specifically, the IR8140 supports Intrusion Prevention System (IPS) and Intrusion Detection System (IDS). | Cisco Catalyst IR8140 Heavy Duty Series Router<br>Cisco Catalyst IR8340 Rugged Series Router<br>Cisco Catalyst IR1835 Rugged Router |

## Custom IPS signature sets

Custom Intrusion Prevention System (IPS) signature sets are user-created collections of threat detection rules in Cisco Catalyst SD-WAN Manager. These sets use the Snort3 engine to deliver advanced threat prevention that can be tailored to your network's specific security needs. custom IPS signature sets let you improve and adjust your network protection beyond the standard, built-in rules. This feature allows you to apply flexible security policies designed for your organization's unique risks.

- **Personalized rule sets**: You can create custom rules to detect threats that are specific to your network, industry, or compliance needs. This provides focused protection against the threats that matter most to you.
- **Rule modification and optimization**: With the group overrides feature, you can change how existing IPS rules work. For example, you can disable, increase or decrease the level of groups of rules to match your organization's security policies.
- **Custom groups and organization**: You can organize both custom and existing rules into groups. This makes it easier to manage rules and respond quickly to new threats.
- **Policy alignment**: Custom IPS signature sets help you enforce security policies that fit your business and regulatory requirements. This gives you more control over how your network reacts to different threats.

## Benefits of custom IPS signature sets

The key advantages of leveraging custom IPS signature sets include:

- **Custom IPS signature set creation**: The ability to develop new IPS signature sets tailored to specific security needs and network environments.
- **Rule action overrides**: The flexibility to change the default actions of individual IPS rules within a signature set.
- **Rule group modification**: The ability to customize groups of IPS rules in bulk for streamlined alignment with your organization's security policies.
- **Commenting**: The option to add comments to rules for improved traceability and to facilitate compliance auditing.

# Prerequisites for custom IPS signature sets

This section outlines the requirements for enabling custom IPS signature sets.

- Ensure that Cisco SD-Routing devices are running a minimum software version of Cisco IOS XE Release 17.18.
- Ensure that Cisco Catalyst SD-WAN Manager is running a minimum software version of 20.18.
- Ensure the UTD image is 17.18.1 or higher, and a UTD signature update must have been performed.
- IPS rules will be displayed in Cisco Catalyst SD-WAN Manager only after a UTD image is installed on at least one device.

# Restrictions for custom IPS signature sets

- You can only edit Snort3 IPS signature sets.
- TLS decryption is not supported on the IR8140 router.
- Unified Threat Defense (UTD) is supported only on the Cloud-Low profile.

# Create and apply custom IPS rules

To enhance network security and policy consistency, you can create and apply custom IPS rules by duplicating and modifying existing rules.

You can generate custom IPS rules by duplicating and modifying existing rules. These rules are global, allowing for their reuse across multiple signature sets. The policies incorporating these custom IPS signature sets can then be deployed using Policy Groups, ensuring consistent enforcement of security policies throughout the SD-WAN network.

You can improve network security and keep policies consistent by creating custom IPS rules such as:

- **Custom Rule Creation**: Generate custom IPS rules by duplicating and modifying existing predefined rules

  .
- **Global Reusability**: Custom IPS rules are global objects that can be reused across multiple signature sets.
- **Consistent Policy Enforcement**: Deploy policies containing custom IPS signature sets using Policy Groups to ensure consistent security across the SD-WAN network.

## Create custom IPS signature sets

This section outlines the steps required to create custom IPS profiles by utilizing custom IPS signature sets.

**Step 1** From Cisco Catalyst SD-WAN Manager, go to **Configuration** > **Policy Groups** > **Objects and Profiles** > **Security Objects**.

**Step 2** Select **Signature Set** and click **Add Signature Set**.

**Step 3** Enter a name for the new **Signature Set**.

**Step 4** Choose a **Base Signature Set** from the following options:
**Choose from:**

- **Connectivity**: Delivers basic security by applying fewer rules, prioritizing higher network throughput and performance while offering less restrictive protection.
- **Balanced**: Provides balanced security that actively protects the system while maintaining high network throughput and minimizing false positives, ensuring strong protection without compromising performance.
- **Security**: Provides enhanced security with increased detection capabilities, offering greater protection than the Balanced level. Designed for administrators who are willing to accept some network latency and a low rate of false positives to identify more potential threats.
- **Max-Detect**: This ruleset is designed specifically for use in testing environments and is not optimized for production performance. A higher rate of false positives is anticipated and acceptable for many of the rules included in this policy. As a result, investigations into false positives will generally not be conducted.
- **No-Rules-Active**: No detection rules are enabled. This mode is typically used for testing or troubleshooting and can also serve as the base for creating a completely customized signature set.

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

Custom IPS signature sets is created.

# Manage a custom IPS signature set

This section outlines how to view, modify, and deploy custom IPS signature sets in Cisco Catalyst SD-WAN Manager to enhance network security policies.

**Step 1** From Cisco Catalyst SD-WAN Manager, go to **Configuration** > **Policy Groups** > **Objects and Profiles** > **Security Objects**.

**Step 2** Click the **Pencil icon** adjacent to the name of the **Signature Set** to modify the **Name** and the default Base Signature Set as per your preference.

**Step 3** If you change the signature set's name or base policy, deploy the policy group to apply changes. See Overview of Policy Group Workflows for more information.

If a custom-signature set is already deployed and it is modified, the modifications will be synced to the device at the next UTD signature update interval.Check the UTD Subscribed settings sync timer in Cisco Catalyst SD-WAN Manager by navigating to **Administration** > **Settings** > **UTD Snort Subscriber Signature**.

## Manage a custom IPS signature set for base policy

The **Base Policy** tab provides an overview of the signatures or rules and their actions in the selected base signature-set. For more details, see below:

**View Specific Rule**: Filter the preferred rule using the **Search bar** or the Rule Action drop-down list.

## Manage a custom IPS signature set for group overrides

The **Group Overrides** tab provides a centralized interface for IPS signature security level management. This tab shows all available IPS signature categories, such as local groups, overridden groups, and rule categories, along with their associated rule groups. You can modify the security level for an entire rule category, and you can also change the security level for individual rule groups within a selected category. For more details, see the table below:

| Field Name | Description |
|---|---|
| **Edit Security Level of a Rule Category** | To edit the security level of a rule category, select the rule category and click on the **Pencil icon** adjacent to the preferred rule category for this rule group from the following options:<br>• Connectivity<br>• Balanced<br>• Security<br>• Max-Detect<br>• Disable |
| **Edit Security Level of a Rule Group** | To edit the security level of a rule group, selectthe preferred rule category from the list. Click on the **Pencil icon** adjacent to the to the preferred rule category for this rule group from the following options:<br>• Connectivity<br>• Balanced<br>• Security<br>• Max-Detect<br>• Disable |
| **Undo Rule Category Overrides** | Click the **Diamond icon** for your preferred rule category and select **Revert to default** to undo Rule Overrides to the rule category. |
| **Undo Rule Group Overrides** | Click the **Diamond icon** for your preferred rule group and select **Revert to default** to undo Rule Overrides to the rule group. |

## Manage a custom IPS signature set for rule overrides

Under the **Rule Overrides** tab, you have several options to manage individual IPS signatures. You can view specific rules by filtering them using the search bar or the Rule Action drop-down list. The tab also allows you to edit rule actions for a preferred rule. You can duplicate existing intrusion rules to create custom ones. For more details, see the table below:

| Field Name | Description |
|---|---|
| **View Specific Rule** | Filter the preferred rule using the **Search bar** or the **Rule Action** drop-down list. |

| Field Name | Description |
|---|---|
| **Edit Rule Action** | Click on the drop-down list under the **Rule Action** column for your preferred rule to edit the rule from the below options:<br>• Drop<br>• Alert<br>• Rewrite<br>• Disable |
| **Undo Rule Overrides** | Click the **Diamond icon** for your preferred rule and select **Revert to default** to undo Rule Overrides to the rule. |
| **Add Comment** | Click the **ellipses (...)** adjacent to the preferred rule. Add your comment to track or document changes and **Save**. |

### Duplicate intrusion rule

To create a custom rule by duplicating the existing rule, follow the below steps:

**Step 1** From the **Rule Overrides** tab, click the **ellipses (...)**.

**Step 2** Select **Duplicate** to copy an existing rule.

**Step 3** Assign a **unique ID** to the custom rule. When you duplicate a Talos intrusion rule, you must change the SID to a unique value greater value than 1000000.

**Step 4** Add the custom rule to an existing custom rule group or create a new local rule group using **+ Create new rule group**. Local rule groups appear under **Group Overrides**.

**Step 5** Click **Create New**

You can duplicate only rules with Generator ID (GID) 1. The **Duplicate** option remains disabled for non-GID 1 rules.

A custom rule is created by duplicating an existing rule.

# Troubleshoot custom IPS signature sets

This section outlines the steps required to troubleshoot custom IPS signature sets.

If you encounter the No Rule Available warning message after selecting **Edit Signature Set**, manually populate the IPS signatures by following these steps:

**a.** In Cisco Catalyst SD-WAN Manager, go to **Administration** > **Settings** > **UTD Snort Subscriber Signature**.

**b.** Under the IPS Signature section, select **Local** from the **Download From** option.

**c.** Upload a **UTD signature set**. Version 3.3.5.0 or later is required. For example, you can refer the following link: https://software.cisco.com/download/home/284389362/type/286285292/release/3350.65.s.

**Note** The upload may take several minutes to complete.

**d.** **Save** your changes.

Signature rules should now be available for editing. It is recommended to revert the **Download From** option to its initial value and **Save** your changes.