Migrate from Snort 2 to Snort 3

Starting with Version 7.0, Snort 3 is the default inspection engine for new threat defense deployments with management center. If you are still using the Snort 2 inspection engine, switch to Snort 3 now for improved detection and performance.

Upgrading threat defense to Version 7.2 through 7.6 also upgrades eligible Snort 2 devices to Snort 3. For devices that are ineligible because they use custom intrusion or network analysis policies, manually upgrade to Snort 3 as described here.

Although you can switch individual devices back, you should not. Snort 2 will be deprecated in a future release and will eventually prevent threat defense upgrade.

Snort 3 Inspection Engine

Snort 3 is the default inspection engine for newly registered threat defense devices of version 7.0 and later. However, for threat defense devices of lower versions, Snort 2 is the default inspection engine. When you upgrade a managed threat defense device to version 7.0 or later, the inspection engine remains on Snort 2. To use Snort 3 in upgraded threat defenses of version 7.0 and later, you must explicitly enable it. When Snort 3 is enabled as the inspection engine of the device, the Snort 3 version of the intrusion policy that is applied on the device (through the access control policies) is activated and applied to all the traffic passing through the device.

You can switch Snort versions when required. Snort 2 and Snort 3 intrusion rules are mapped and the mapping is system-provided. However, you may not find a one-to-one mapping of all the intrusion rules in Snort 2 and Snort 3. If you change the rule action for one rule in Snort 2, that change is not retained if you switch to Snort 3 without synchronizing Snort 2 with Snort 3. For more information on synchronization, see Synchronize Snort 2 Rules with Snort 3 , on page 6.

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 Threat Defense device.

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

How to Migrate from Snort 2 to Snort 3

Migrating from Snort 2 to Snort 3 requires you to switch the inspection engine of the threat defense device from Snort 2 to Snort 3.

Depending on your requirements, the tasks to complete the migration of your device from Snort 2 to Snort 3 is listed in the following table:

Step	Task	Links to Procedures
1	Enable Snort 3	• Enable Snort 3 on an Individual Device, on page 3 • Enable Snort 3 on Multiple Devices, on page 3
2	Convert Snort 2 custom rules to Snort 3	• Convert all Snort 2 Custom Rules across all Intrusion Policies to Snort 3, on page 4 • Convert Snort 2 Custom Rules of a Single Intrusion Policy to Snort 3, on page 5
3	Synchronize Snort 2 rules with Snort 3	Synchronize Snort 2 Rules with Snort 3 , on page 6

Prerequisites for Migrating from Snort 2 to Snort 3

The following are the recommended prerequisites that you must consider before migrating your device from Snort 2 to Snort 3.

• Have a working knowledge of Snort. To learn about the Snort 3 architecture, see Snort 3 Adoption.

• Back up your management center. See Backup the Management Center.

• Back up your intrusion policy. See Exporting Configurations.

• Clone your intrusion policy. To do this, you can use an existing policy as the base policy to create a copy of your intrusion policy. In the **Intrusion Policies** page, click **Create Policy** and choose an existing intrusion policy from the **Base Policy** dropdown list.

Enable Snort 3 on an Individual Device

☞

Important During the deployment process, there could be a momentary traffic loss because the current inspection engine needs to be shut down.

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click the device to go to the device home page.

Note The device is marked as Snort 2 or Snort 3, showing the current version on the device.

Step 3 Click the **Device** tab.

Step 4 In the Inspection Engine section, click **Upgrade**.

Note In case you want to disable Snort 3, click **Revert to Snort 2** in the Inspection Engine section.

Step 5 Click **Yes**.

What to do next

Deploy the changes on the device. See, .

The system converts your policy configurations during the deployment process to make them compatible with the selected Snort version.

Enable Snort 3 on Multiple Devices

To enable Snort 3 on multiple devices, ensure all the required threat defense devices are on version 7.0 or later.

☞

Important During the deployment process, there could be a momentary traffic loss because the current inspection engine needs to be shut down.

Step 1 Choose **Devices** > **Device Management**.

Step 2 Select all the devices on which you want to enable or disable Snort 3.

Note The devices are marked as Snort 2 or Snort 3, showing the current version on the device.

Step 3 Click **Select Bulk Action** drop-down list and choose **Upgrade to Snort 3**.

Step 4 Click **Yes**.

What to do next

Deploy the changes on the device. See, Deploy Configuration Changes, on page 7.

The system converts your policy configurations during the deployment process to make them compatible with the selected Snort version.

Convert Snort 2 Custom IPS Rules to Snort 3

If you are using a rule set from a third-party vendor, contact that vendor to confirm that their rules 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.

See the following procedures to convert Snort 2 rules to Snort 3 rules using the system-provided tool.

- Convert all Snort 2 Custom Rules across all Intrusion Policies to Snort 3, on page 4

- Convert Snort 2 Custom Rules of a Single Intrusion Policy to Snort 3, on page 5

☞

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

Step 1   Choose **Objects** > **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 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.

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, on page 7.

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

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

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

Step 3   Click the **Sync** icon ➡ 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 green ➡. 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 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, on page 7.

View Snort 2 and Snort 3 Base Policy Mapping

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

Step 2   Ensure the **Intrusion Policies** tab is selected.

Step 3   Click **IPS Mapping**.

Step 4   In the **IPS Policy Mapping** dialog box, click **View Mappings** to view the Snort 3 to Snort 2 intrusion policy mapping.

Step 5   Click **OK**.

Synchronize Snort 2 Rules with Snort 3

To ensure that the Snort 2 version settings and custom rules are retained and carried over to Snort 3, the management center provides the synchronization functionality. Synchronization helps Snort 2 rule override settings and custom rules, which you may have altered and added over the last few months or years, to be replicated on the Snort 3 version. This utility helps to synchronize Snort 2 version policy configuration with Snort 3 version to start with similar coverage.

If the management center is upgraded from 6.7 or earlier to 7.0 or later version, the system synchronizes the configuration. If the management center is a fresh 7.0 or later version, you can upgrade to a higher version, and the system will not synchronize any content during upgrade.

Before upgrading a device to Snort 3, if changes are made in Snort 2 version, you can use this utility to have the latest synchronization from Snort 2 version to Snort 3 version so that you start with a similar coverage.

Note   On moving to Snort 3, it is recommended that you manage the Snort 3 version of the policy independently and do not use this utility as a regular operation.

Important
- Only the Snort 2 rule overrides and custom rules are copied to Snort 3 and not the other way around. You may not find a one-to-one mapping of all the intrusion rules in Snort 2 and Snort 3.Your changes to rule actions for rules that exist in both versions are synchronized when you perform the following procedure.

- Synchronization *does not* migrate the threshold and suppression settings of any custom or system-provided rules from Snort 2 to Snort 3.

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

Step 2   Ensure the **Intrusion Policies** tab is selected.

Step 3   Click **Show Snort 3 Sync status**.

Step 4   Identify the intrusion policy that is out-of-sync.

Step 5   Click the **Sync** icon ➡.

Note   If the Snort 2 and the Snort 3 versions of the intrusion policy are synchronized, then the **Sync** icon is in green ➡ .

Step 6   Read through the summary and download a copy of the summary if required.

Step 7   Click **Re-Sync**.

Note	• The synchronized settings will be applicable on the Snort 3 intrusion engine only if it is applied on a device, and after a successful deployment.
	• Snort 2 custom rules can be converted to Snort 3 using the system-provided tool. If you have any Snort 2 custom rules click the Custom Rules tab and follow the on-screen instructions to convert the rules. For more information, see Convert Snort 2 Custom Rules of a Single Intrusion Policy to Snort 3, on page 5.

What to do next

Deploy configuration changes; see Deploy Configuration Changes, on page 7.

Deploy Configuration Changes

After you change configurations, deploy them to the affected devices.

Note	This topic covers the basic steps involved in deploying configuration changes. We *strongly* recommend that you refer the *Deploy Configuration Changes* topic in the latest version of the *Cisco Secure Firewall Management Center Configuration Guide* to understand the prerequisites and implications of deploying the changes before proceeding with the steps.

Caution	When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic.

Step 1 On the Secure Firewall Management Center menu bar, click **Deploy** and choose **Deployment**.

The GUI page lists the devices with out-of-date configurations having **Pending**status.

 • The **Modified By** column lists the users who have modified the policies or objects. Expand the device listing to view the users who have modified the policies for each policy listing.

Note	Usernames are not provided for deleted policies and objects.

 • The **Inspect Interruption** column indicates if traffic inspection interruption might occur in the device during deployment.

 If this column is blank for a device, it indicates that there will be no traffic inspection interruptions on that device during deployment.

 • The **Last Modified Time** column specifies the last time you made configuration changes.

 • The **Preview** column allows you to preview the changes for the next deployment.

           • The **Status** column provides the status for each deployment.

Step 2   Identify and choose the devices on which you want to deploy configuration changes.

          • Search—Search for the device name, type, domain, group, or status in the search box.

          • Expand—Click **Expand Arrow** (❯) to view device-specific configuration changes to be deployed.

      When you check a check box adjacent to a device, all the changes made to the device and listed under the device, are pushed for deployment. However, you can use **Policy selection** ( ) to select individual policies or specific configurations to deploy while withholding the remaining changes without deploying them.

Note	• When the status in the **Inspect Interruption** column indicates (**Yes**) that deploying will interrupt inspection, and perhaps traffic, on a threat defense device, the expanded list indicates the specific configurations causing the interruption with the **Inspect Interruption** ( ).
	• When there are changes to interface groups, security zones, or objects, the impacted devices are shown as out-of-date on the management center. To ensure that these changes take effect, the policies with these interface groups, security zones, or objects, also need to be deployed along with these changes. The impacted policies are shown as out-of-date on the **Preview**page on the management center.

Step 3   Click **Deploy**.

Step 4   If the system identifies errors or warnings in the changes to be deployed, it displays them in the **Validation Messages** window. To view complete details, click the arrow icon before the warnings or errors.

      You have the following choices:

          • Deploy—Continue deploying without resolving warning conditions. You cannot proceed if the system identifies errors.
          • Close—Exit without deploying. Resolve the error and warning conditions, and attempt to deploy the configuration again.

What to do next

During deployment, if there is a deployment failure, there is a possibility that the failure may impact traffic. However, it depends on certain conditions. If there are specific configuration changes in the deployment, the deployment failure may lead to traffic being interrupted. For details, see the Deploy Configuration Changes topic in the latest version of the *Cisco Secure Firewall Management Center Configuration Guide*.