



Use Case - Migrate from Snort 2 to Snort 3 In Secure Firewall Management Center

- [Migrate from Snort 2 to Snort 3, on page 1](#)
- [Benefits of Migrating to Snort 3, on page 1](#)
- [Sample Business Scenario, on page 2](#)
- [Best Practices for Migrating from Snort 2 to Snort 3, on page 2](#)
- [Prerequisites, on page 2](#)
- [End-to-End Migration Workflow, on page 2](#)
- [Enable Snort 3 on Threat Defense, on page 3](#)
- [Convert Snort 2 Rules of a Single Intrusion Policy to Snort 3, on page 4](#)
- [Deploy Configuration Changes, on page 9](#)

Migrate from Snort 2 to Snort 3

Snort is an intrusion detection and prevention system that has undergone a significant change from Version 2 to Version 3. To leverage the enhanced features and capabilities of Snort 3, migration of the existing rule sets from Snort 2 becomes crucial. This migration process involves converting and adapting the Snort 2 rules to the Snort 3 rule syntax and optimizing them for improved detection and performance.

In some cases, organizations can have the threat defense devices managed by the Secure Firewall Management Center. Organizations can opt for a hybrid deployment approach during the migration from Snort 2 to Snort 3. This approach allows for a gradual transition and minimizes potential disruptions, if any.

Benefits of Migrating to Snort 3

- **Enhanced protocol support**—Snort 3 provides improved protocol support, allowing you to monitor and detect threats across a wide range of modern protocols, including encrypted traffic.
- **Streamlined rule management**—Snort 3 offers a more user-friendly rule language and rule management system, making it easier to create, modify, and manage rules effectively.
- **Improved performance**—Snort 3 has been optimized to handle higher traffic volumes more efficiently, reducing the risk of performance bottlenecks and ensuring timely threat detection.

Sample Business Scenario

Alice works as a security analyst in a large organization that heavily relies on the Snort inspection engine to monitor and protect their network infrastructure. The organization has been using Snort Version 2 for several years, but they have encountered some limitations and challenges.

Bob, the network administrator, is looking to migrate from Snort 2 to Snort 3 to overcome these issues and enhance his organization's network security capabilities.

This migration will also improve network security monitoring, enhance performance, and streamline rule management.

Best Practices for Migrating from Snort 2 to Snort 3

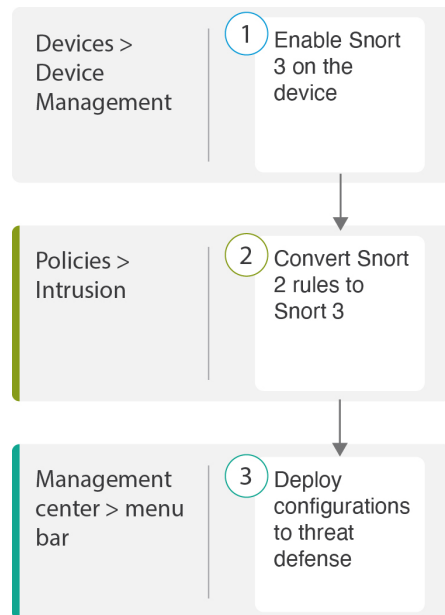
- Back up your intrusion policy before performing the migration. See the Export Configurations task in the [Cisco Secure Firewall Management Center Administration Guide](#).
- Before upgrading a device to Snort 3, if changes are made in Snort 2, use the synchronize utility to include the latest synchronization from Snort 2 to Snort 3 so that you can start with a similar coverage. See [Synchronize Snort 2 Rules with Snort 3](#).
- Snort 2 custom rules are not automatically converted to Snort 3 and must be manually migrated. See [Convert Snort 2 Custom IPS Rules to Snort 3](#).
- Synchronization does not migrate Snort 2 rules with thresholds or suppressions. These rules must be created again in Snort 3.

Prerequisites

- 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](#).

End-to-End Migration Workflow

The following flowchart illustrates the workflow for migrating Snort 2 to Snort 3 in Secure Firewall Management Center.



Step	Description
1	Enable Snort 3 on the device. See Enable Snort 3 on Threat Defense, on page 3 .
2	Convert Snort 2 rules to Snort 3. See Convert Snort 2 Rules of a Single Intrusion Policy to Snort 3, on page 4 .
3	Deploy configuration. See Deploy Configuration Changes .

Enable Snort 3 on Threat Defense

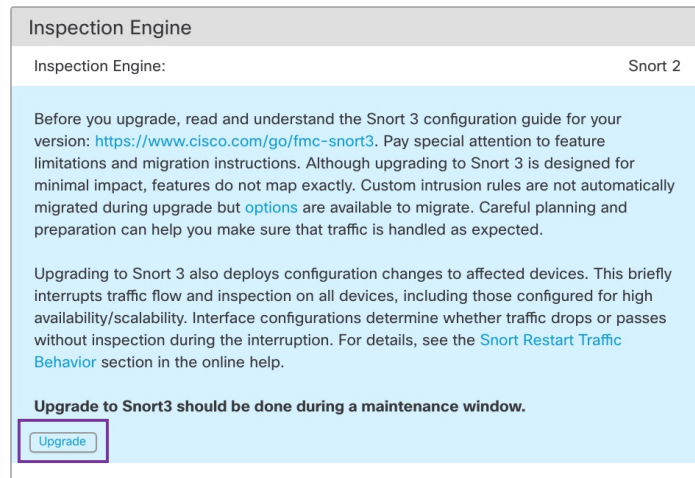


Attention

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

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Click the corresponding device to go to the device home page.
- Step 3** Click the **Device** tab.
- Step 4** In the **Inspection Engine** section, click **Upgrade**.



Step 5 Click **Yes**.

What to do next

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

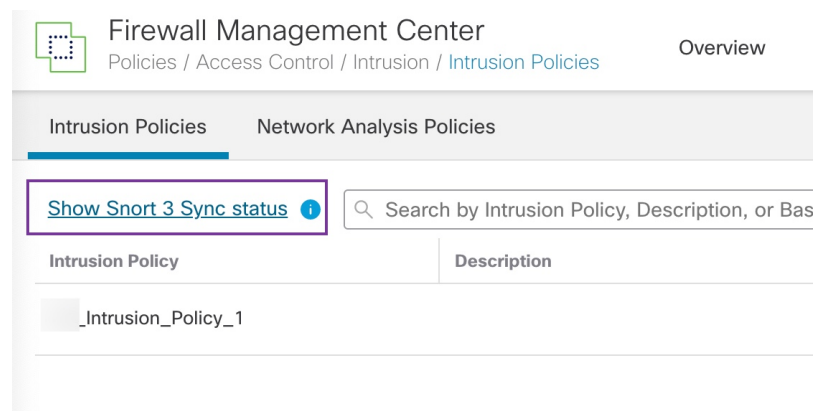
The system converts your policy configurations during the deployment process to make them compatible with the selected Snort version.

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

Procedure

Step 1 Choose **Policies > Access Control heading > Intrusion > Intrusion Policies**.

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



If your policy displays an orange arrow, it indicates that the Snort 2 and the Snort 3 versions of the intrusion policy are not synchronized.

Intrusion Policies Network Analysis Policies	
Hide Snort 3 Sync status ⓘ Search by Intrusion Policy, Description, or Base Policy	
Intrusion Policy	Description

Step 3

Click the orange arrow.

The **Snort 2 to Snort 3 Sync Summary** page displays that the Snort 2 to Snort 3 sync is pending.

Snort 2 to Snort 3 Sync Summary ⓘ

This is a utility to synchronize Snort 2 policy configuration with Snort 3 version to start with a similar coverage.

- Snort 3 policy configuration is synched from Snort 2 version by the system when Firewall Management Center is upgraded from pre-7.0 version.
- 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 similar coverage.

Note: After 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.

[Click here](#) to learn more.

Policy Name:

Used by: 1 Access Control Policy | 1 Device

Re-Sync

Close

Step 4

Click **Re-Sync** to start the synchronization.

Note

When you click **Re-Sync**, the snort2Lua tool converts the rules from Snort 2 to Snort 3.

The **Summary Details** section lists the rules that were migrated or skipped. In our use case, there are 76 custom Snort 2 rules, 17 rules with thresholds, and 15 rules with suppression that were skipped during the sync process. To migrate the custom rules, go to the next step.

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

Policy Name: **_Intrusion_Policy_1**➔ **Snort 3 is partially in sync with Snort 2.** 2023-08-01 05:42:52 EDT

Used by: 1 Access Control Policy | 0 Devices (Snort 2), 1 Devices (Snort 3)

Summary Details**Rule Overrides**

- Based on Talos rule-mapping 18639 Snort 2 rule action overrides migrated to 18635 Snort 3 rules.
- Rules migration skipped for 17 rules with threshold, 15 rules with suppression, as sync of Suppression and Threshold setting(s) are not supported.

Rules migration skipped for 76 custom rules, as sync of Custom Rule setting(s) are not supported. You can manually convert the Snort 2 custom rules to Snort 3 using the snort2Lua tool.

[Download Summary Details](#)Overridden Advanced **Custom Rules**

The custom rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. Use one of the following options to convert the custom rules manually:

To migrate rules with thresholds and suppressions, go to [Step 6](#).Policy Name: **_Intrusion_Policy_1**➔ **Snort 3 is partially in sync with Snort 2.** 2023-08-01 05:42:52 EDT

Used by: 1 Access Control Policy | 0 Devices (Snort 2), 1 Devices (Snort 3)

Summary Details**Rule Overrides**

- Based on Talos rule-mapping 18639 Snort 2 rule action overrides migrated to 18635 Snort 3 rules.
- Rules migration skipped for 17 rules with threshold, 15 rules with suppression, as sync of Suppression and Threshold setting(s) are not supported.
- Rules migration skipped for 76 custom rules, as sync of Custom Rule setting(s) are not supported. You can manually convert the Snort 2 custom rules to Snort 3 using the snort2Lua tool.

[Download Summary Details](#)Overridden Advanced **Custom Rules**

The custom rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. Use one of the following options to convert the custom rules manually:

Step 5

To migrate the 76 custom rules, perform either one of these steps:

- In the **Custom Rules** tab, click the **Import** icon to convert and auto-import the local rules to the Snort 3 version of the policy.

Overridden Advanced **Custom Rules**

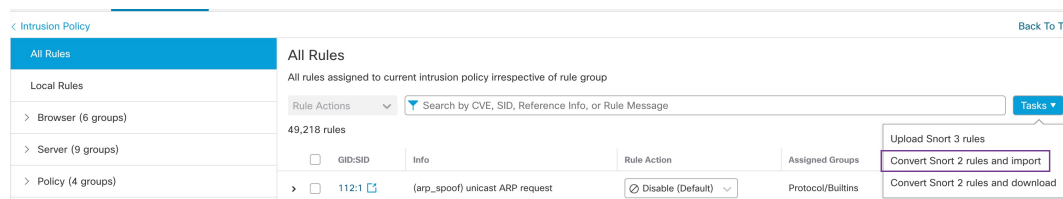
Convert the rules and auto-import them to the Snort 3 version of the policy 

OR

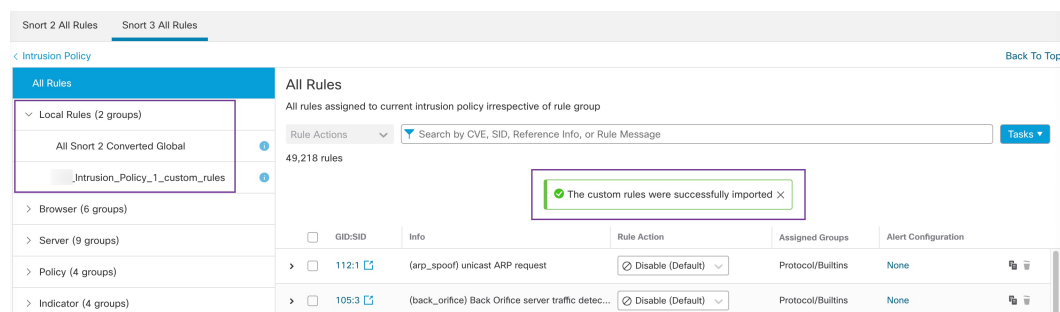
Download converted rules  You can upload the file after you have reviewed the converted rules 

A confirmation message is displayed after the rules are successfully imported.

- Choose **Objects > Intrusion Rules** and click **Snort 3 All Rules**.
 - Click **Local Rules** in the left panel to check if any rules have been migrated. Notice that no custom rules from Snort 2 have been migrated.
 - From the **Tasks** drop-down list, choose **Convert Snort 2 rules and import**.

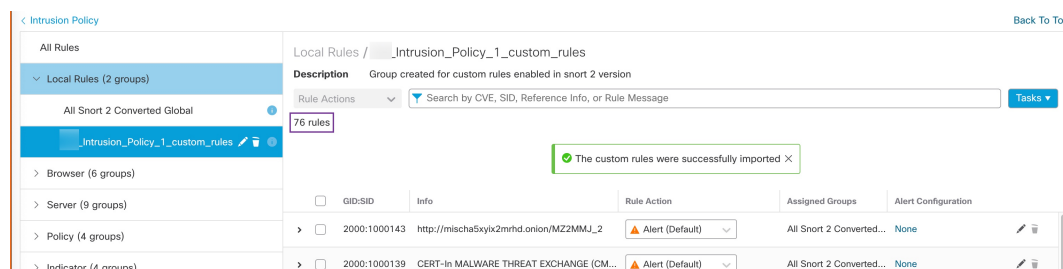


c. Click **OK**.



A newly created rule group (**All Snort 2 Converted Global**) is created under **Local Rules** in the left panel.

Notice that all 76 custom rules have been migrated, as shown in the following figure.



Alternatively, you can select the **Convert Snort 2 rules and download** in the previous step to save the rules file locally. You can review the converted rules in the downloaded file and later upload them using the **Upload Snort 3 rules** option.

Step 6

Click the **Download Summary Details** link to download the rules in .txt format.

The following is a sample of the summary that is displayed.

```
{
  "id": "00505691-15DC-0ed3-0000-004294988561",
  "name": "Intrusion_Policy_1",
  "type": "IntrusionPolicy",
  "syncStatus": {
    "source": {
      "id": "bdce2d6a-1ebe-11ee-8e88-220032eb1fb5",
      "type": "IntrusionPolicy"
    },
    "status": "WARN",
    "description": "Migration is partially successful. Some of the rules are not copied to Snort3.",
    "timestamp": 1690883954814,
    "lastUser": {
      "name": "admin"
    }
  }
}
```

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

```

    },
    "details": [
      {
        "type": "Summary",
        "status": "INFO",
        "description": "Based on Talos rule-mapping 18639 Snort 2 rule action overrides
migrated to 18635 Snort 3 rules."
      },
      {
        "id":
"1:1000156=alert,1:1000114=alert,1:1000160=alert,1:1000135=alert,1:1000115=alert,1:1000118=alert,

1:1000092=alert,1:1000139=alert,1:1000123=alert,1:1000159=alert,1:1000149=disabled,1:1000167=alert,

1:1000133=alert,1:1000095=alert,1:1000143=alert,1:1000106=alert,1:1000153=alert,1:1000097=alert,1:1000141=alert,

1:1000148=alert,1:1000090=alert,1:1000119=alert,1:1000112=alert,1:1000138=alert,1:1000128=alert,1:1000132=alert,

1:1000134=alert,1:1000145=disabled,1:1000110=disabled,1:1000107=alert,1:1000163=alert,1:1000124=alert,1:1000125=alert,

1:1000094=alert,1:1000113=disabled,1:1000147=alert,1:1000161=alert,1:1000105=disabled,1:1000140=alert,1:1000111=alert,

1:1000102=alert,1:1000129=disabled,1:1000108=alert,1:1000144=disabled,1:1000088=alert,1:1000091=alert,1:1000131=alert,

1:1000157=alert,1:1000120=alert,1:1000126=alert,1:1000165=alert,1:1000146=alert,1:1000162=alert,1:1000116=alert,1:1000142=alert,

1:1000170=disabled,1:1000169=alert,1:1000104=alert,1:1000099=disabled,1:1000171=alert,1:1000093=alert,1:1000087=alert,1:1000100=alert,

1:1000137=alert,1:1000158=alert,1:1000103=alert,1:1000098=alert,1:1000127=disabled,1:1000130=alert,1:1000164=alert,1:1000089=alert,

1:1000109=alert,1:1000136=alert,1:1000117=alert,1:1000166=alert,1:1000168=alert",
        "type": "PolicyInfo",
        "description": "Corresponding Snort 2 policy overridden custom (local) rules."
      },
      {
        "type": "AssignedDevices",
        "status": "INFO",
        "description": "Snort3:0 , Snort2:0"
      },
      {
        "id": "122:6",
        "type": "Threshold",
        "status": "ERROR",
        "description": "PSNG_TCP_FILTERED_DECOY_PORTSCAN"
      },
      {
        "id": "122:15",
        "type": "Threshold",
        "status": "ERROR",
        "description": "PSNG_IP_PORTSWEEP_FILTERED"
      },
      {
        "id": "122:1",
        "type": "Threshold",
        "status": "ERROR",

```

```
"description": "PSNG_TCP_PORTSCAN"
},
```

- Step 7** Click **Close** to close the **Sync Summary** dialog box.
- Step 8** To check the rules with status: ERROR, choose **Policies > Access Control heading > Intrusion** and click the **Snort 2** version of the intrusion policy.
- Step 9** Under **Policy Information**, click **Rules** and filter for the rule. For example, enter **PSNG_TCP_PORTSCAN** in the **Filter** field to find the rule.
- Step 10** Click **Show Details** to view the detailed version of the rule.
- Step 11** Create the rule again in Snort 3 using Snort 3 rule guidelines and save the file as a .txt or .rules file. For more information, see www.snort3.org.
- Step 12** Upload the custom rule that you just created locally to the list of all the Snort 3 rules. See [Add Custom Rules to Rule Groups](#).

What to do next

Deploy configuration changes. See [Deploy Configuration Changes](#).

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.

Procedure

- 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 Firewall 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 Firewall 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 Firewall 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*.