

Upgrade from Snort 2 to Snort 3 via FDM

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Configurations](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to upgrade from snort 2 to Snort 3 version in Firepower Device Manager (FDM).

Prerequisites

Cisco recommends that you have knowledge of these topics:

- Firepower Threat defense (FTD)
- Firepower Device Manager (FDM)
- Snort.

Requirements

Ensure you have the these requirements:

- Access to Firepower Device Manager.
- Administrative privileges on the FDM.
- FTD must be at least version 6.7 in order to use snort 3.

Components Used

The Information in this document is based on these software and hardware versions:

- FTD 7.2.7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

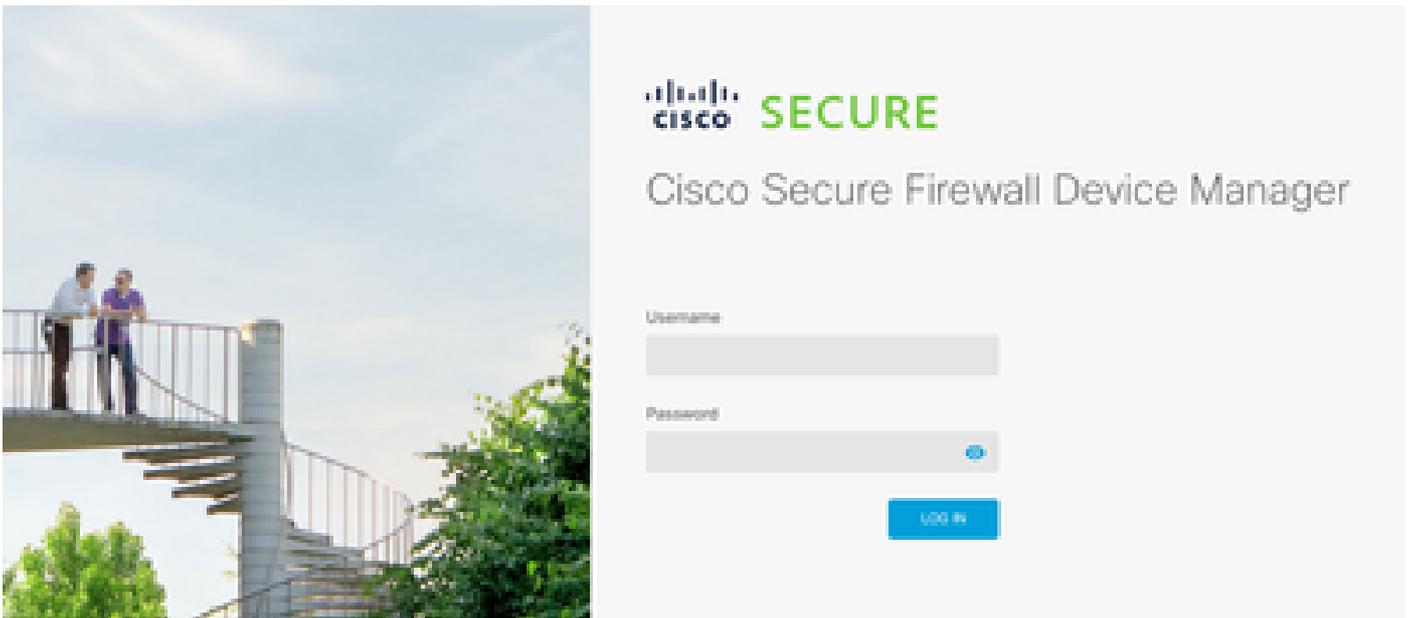
The snort 3 feature was added in the 6.7 release for Firepower Device Manager (FDM). Snort 3.0 was designed to address these challenges:

- Reduce memory and CPU usage.
- Improve HTTP inspection efficacy.
- Faster configuration loading and snort restart.
- Better programmability for faster feature addition.

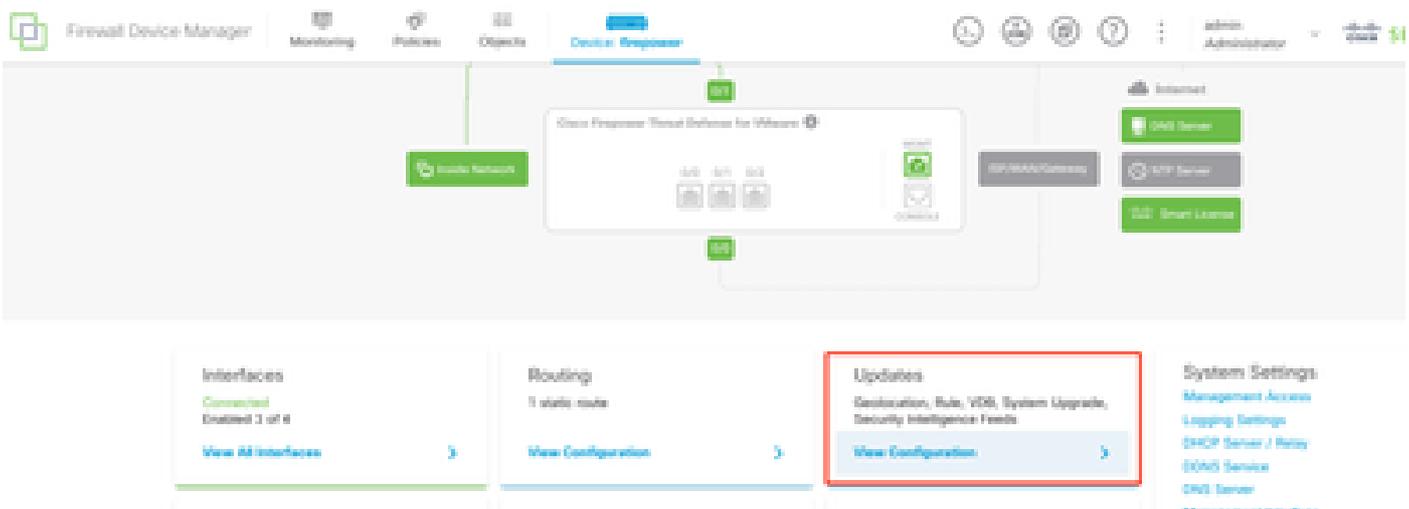
Configure

Configurations

1. Log into Firepower Device Manager.



2. Navigate to **Device > Updates > View configuration**.



3. In the intrusion rules section, click **upgrade to snort 3**.

Intrusion Rule 2022-01-06-001-vrt

Latest Update on 14 Oct 2024

Configure

Set recurring updates

UPDATE FROM CLOUD

Snort

Inspection Engine: 2.9.20-6102 [Upgrade to 3.0](#)

Snort is the main inspection engine in Secure Firewall Threat Defense. It is used for intrusion and file policy analysis, SSL decryption, and layer 7 inspection.

[See more](#)

4. On the warning message to confirm your selection, select the option to **get the latest intrusion rules package**, then click **Yes**.

Enable Snort 3.0



- Switching Snort versions requires an automatic deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be a momentary traffic loss.
- The switch can take up to one hour to complete. During the switch, the device manager might become unresponsive. We recommend that you start the switch at a time you will not need to use the device manager.

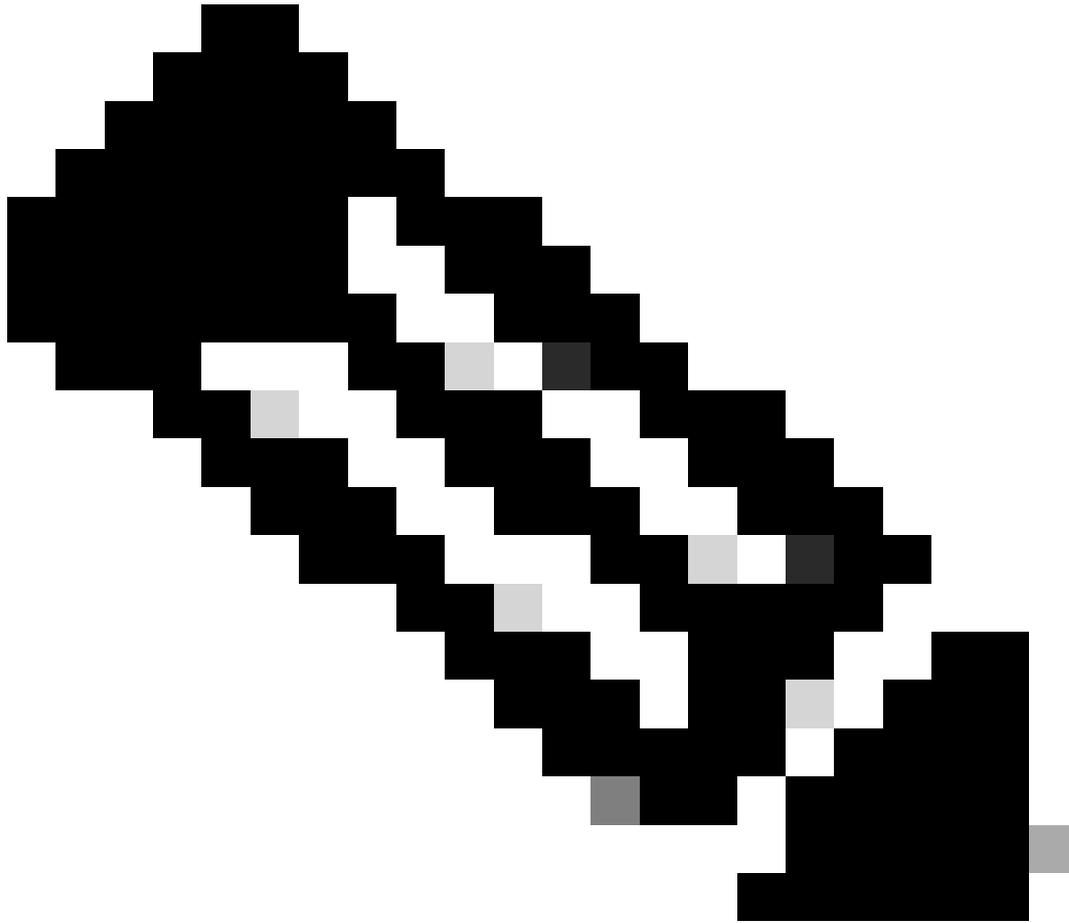
Get latest intrusion rules

Are you sure you want to enable Snort 3.0?

NO

YES

Latest Update on 14 Oct 2024



Note: The system downloads packages for the active Snort version only, so it is unlikely that you have the latest package installed for the Snort version you are switching to. You must wait until the task to switch versions completes before you can edit intrusion policies.



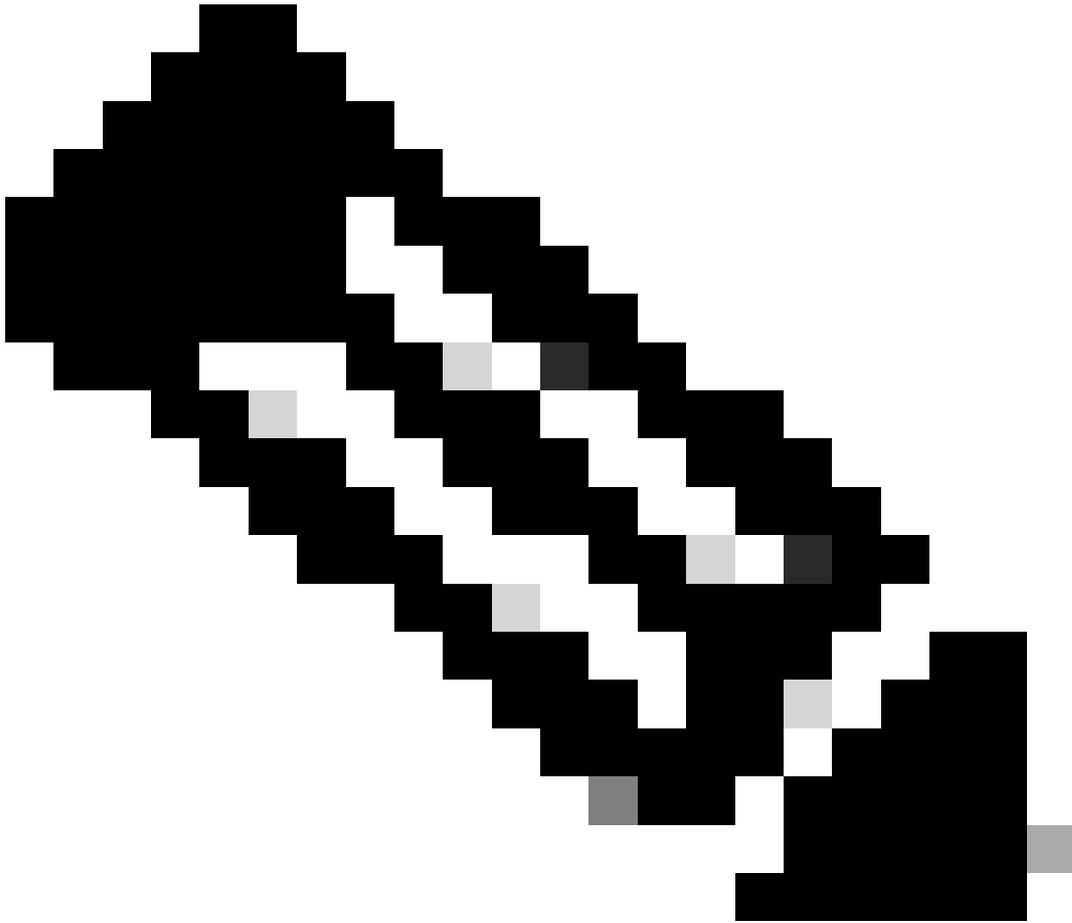
Warning: Switching snort version leads to momentary traffic loss.

5. You must confirm in the task list that the upgrade has started.

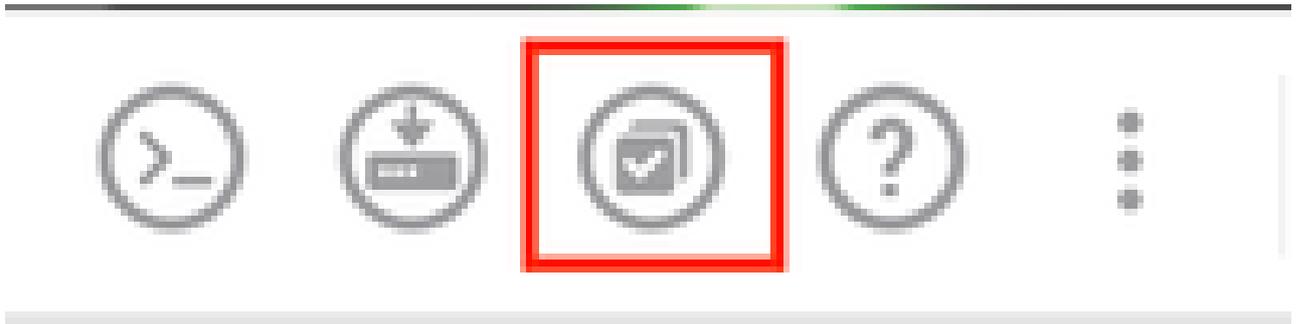
Task List

18 total | 1 running | 13 completed | 4 failures [Delete all finished tasks](#)

Name	Start Time	End Time	Status	Actions
Snort Version Change 2 to 3	14 Oct 2024 12:41 PM		Snort 3 Package Downloading in progress.	



Note: The task list is found in the navigation bar next to the deployments icon.



Verify

The Inspection Engine section shows that the current version of Snort is Snort 3.

Intrusion Rule 20241010-1555

Latest Update on 14 Oct 2024

Configure

Set recurring updates

UPDATE FROM CLOUD

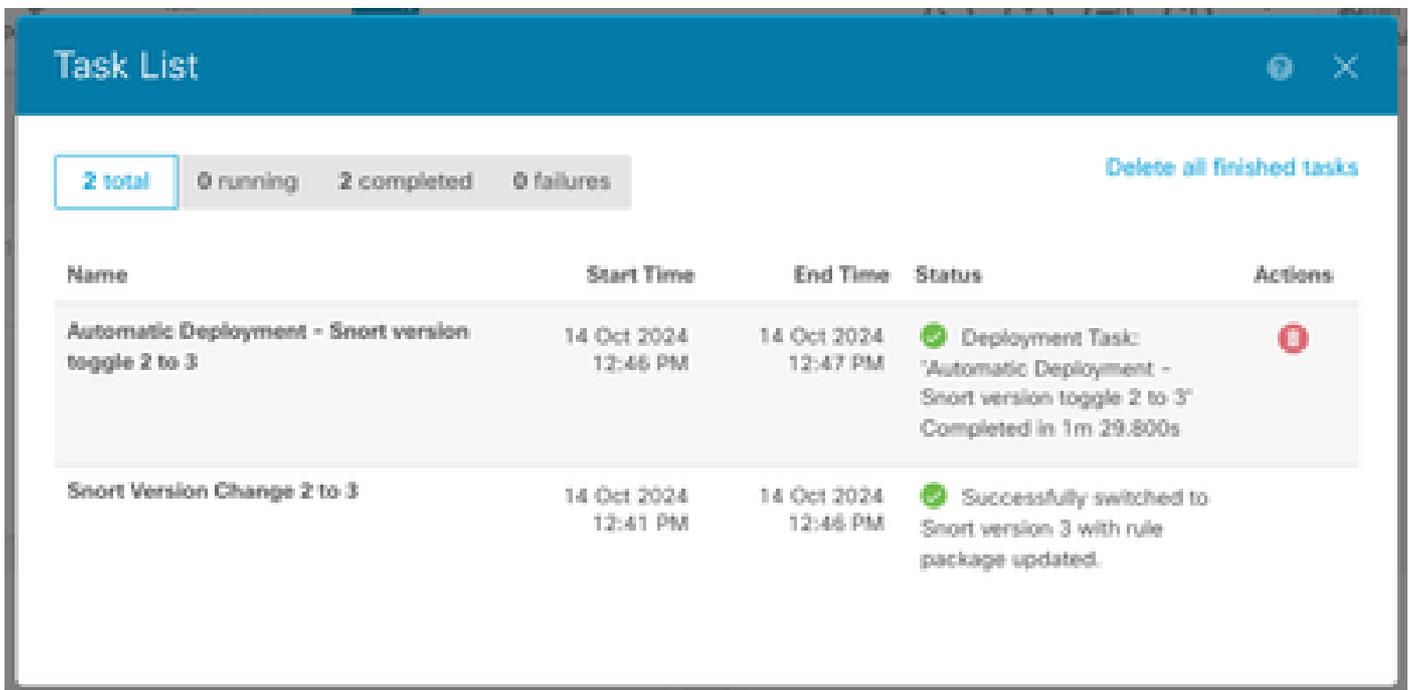
Snort

Inspection Engine: 3.1.21.600-26 [Downgrade to 2.0](#)

Snort is the main inspection engine in Secure Firewall Threat Defense. It is used for intrusion and file policy analysis, SSL decryption, and layer 7 inspection.

[See more](#)

Finally, in the task list, make sure that the change to snort 3 has been successfully completed and deployed.



The screenshot shows a 'Task List' window with a blue header. Below the header, there are summary statistics: 2 total, 0 running, 2 completed, and 0 failures. A 'Delete all finished tasks' link is visible on the right. The main content is a table with columns for Name, Start Time, End Time, Status, and Actions. Two tasks are listed, both with a green checkmark status.

Name	Start Time	End Time	Status	Actions
Automatic Deployment - Snort version toggle 2 to 3	14 Oct 2024 12:46 PM	14 Oct 2024 12:47 PM	✔ Deployment Task: 'Automatic Deployment - Snort version toggle 2 to 3' Completed in 1m 29.800s	🗑️
Snort Version Change 2 to 3	14 Oct 2024 12:41 PM	14 Oct 2024 12:46 PM	✔ Successfully switched to Snort version 3 with rule package updated.	

Troubleshoot

If you encounter issues during the upgrade, consider these steps:

- Ensure that your FTD versions are compatible with Snort 3.

For additional details, check the [Cisco Secure Firewall Threat Defense Compatibility Guide](#)

- Collect the troubleshooting files on the FDM by navigating to the **Device** tab, and then clicking **Request file to be created**. Once collected, open a **case** with TAC and **upload** the file to the case for further assistance.

Troubleshoot

No files created yet

REQUEST FILE TO BE CREATED

Related Information

- [Snort 3 Adoption](#)
- [Snort Documents](#)
- [Cisco Secure Firewall Device Manager Configuration Guide, Version 7.2](#)