Upgrade from Snort 2 to Snort 3 via FDM

Contents

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

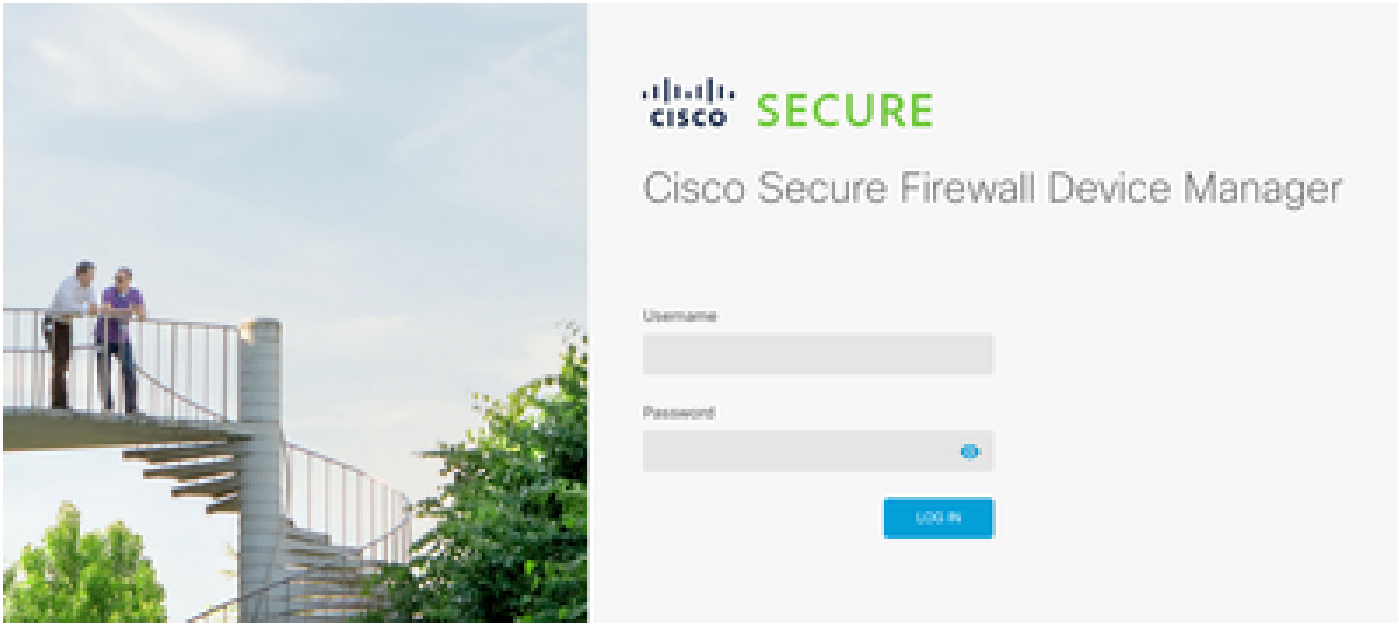
The snort 3 feature was added in the 6.7 release for Firepower Device Manager (FDM). Snort 3.0 was designed to address these challenges:

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

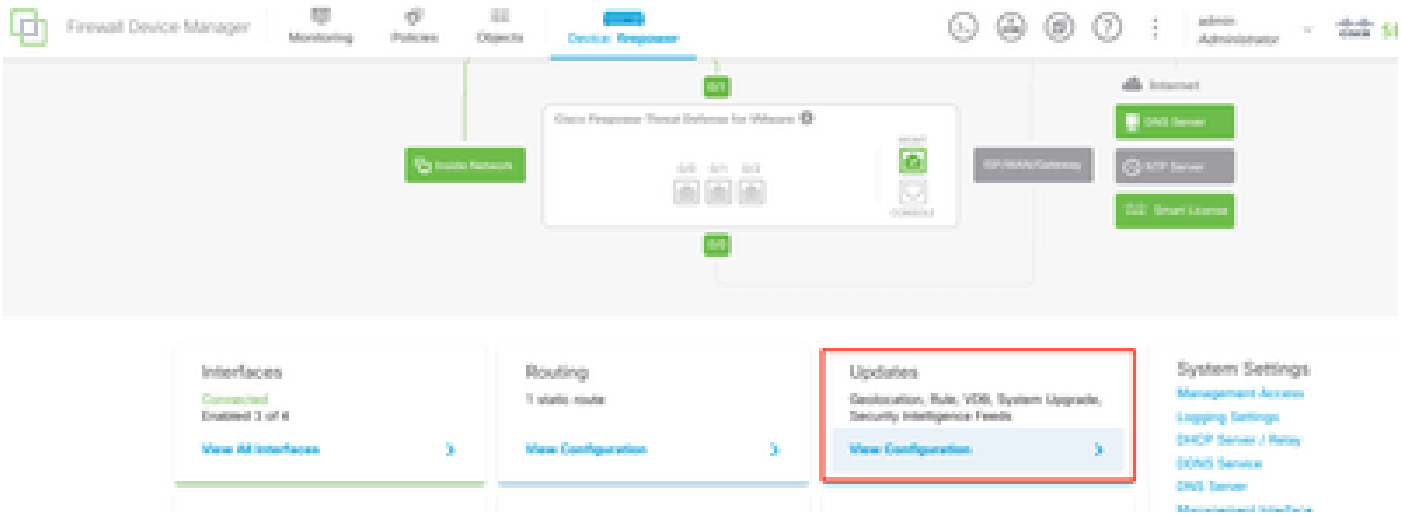
Configure

Configurations

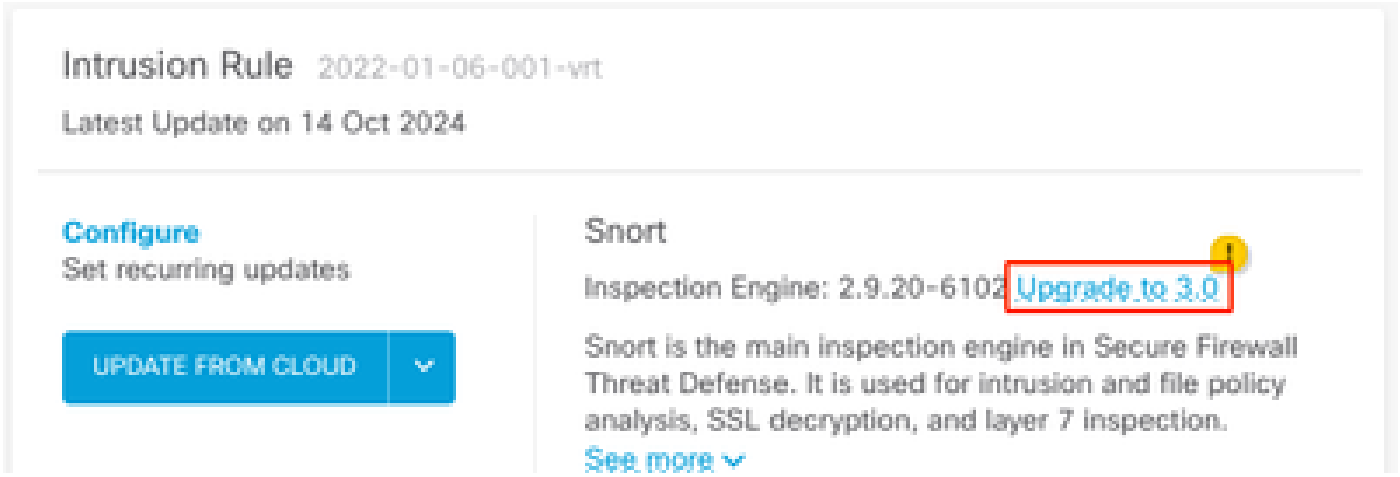
1. Log into Firepower Device Manager.



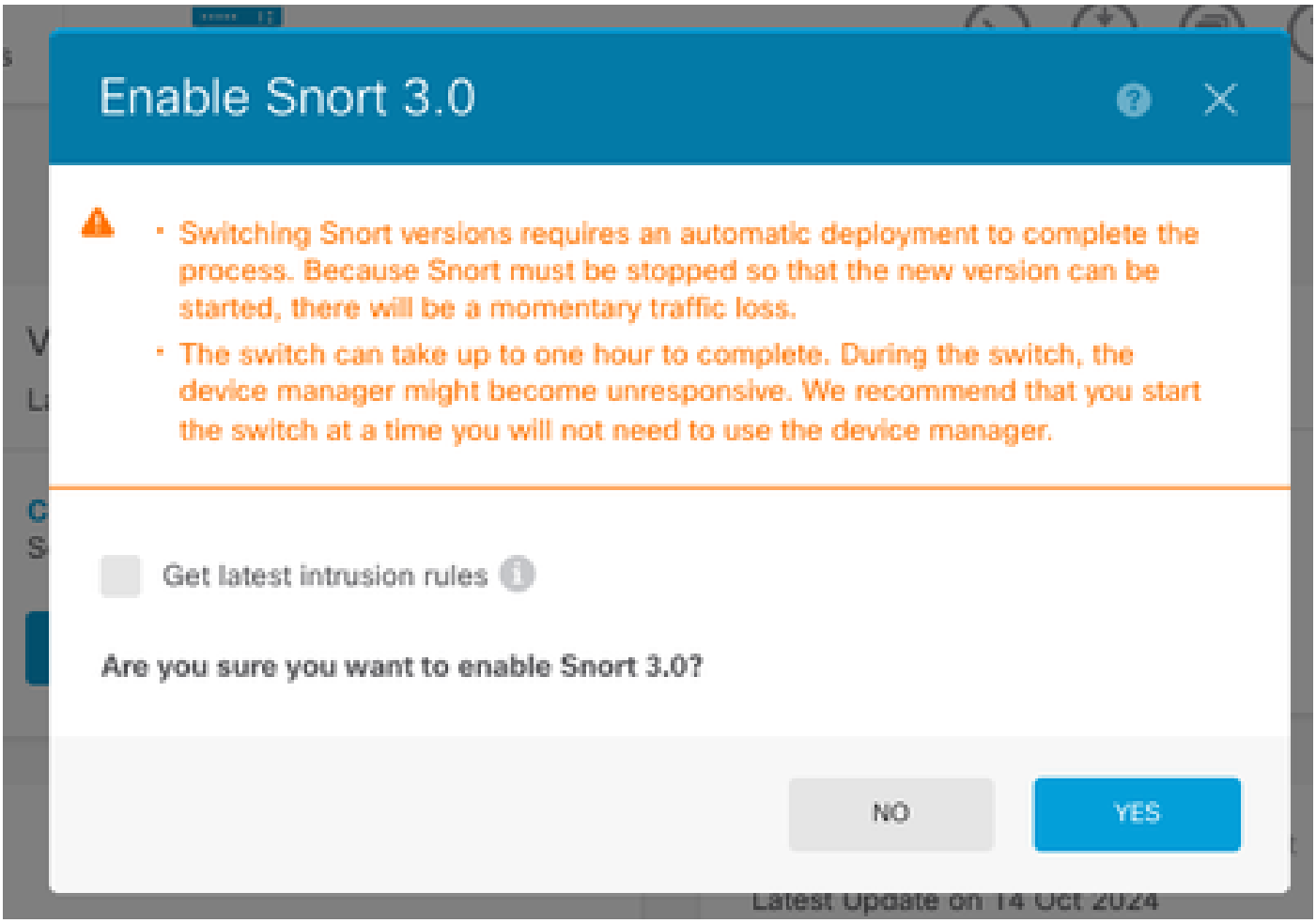
2. Navigate to **Device > Updates > View configuration**.

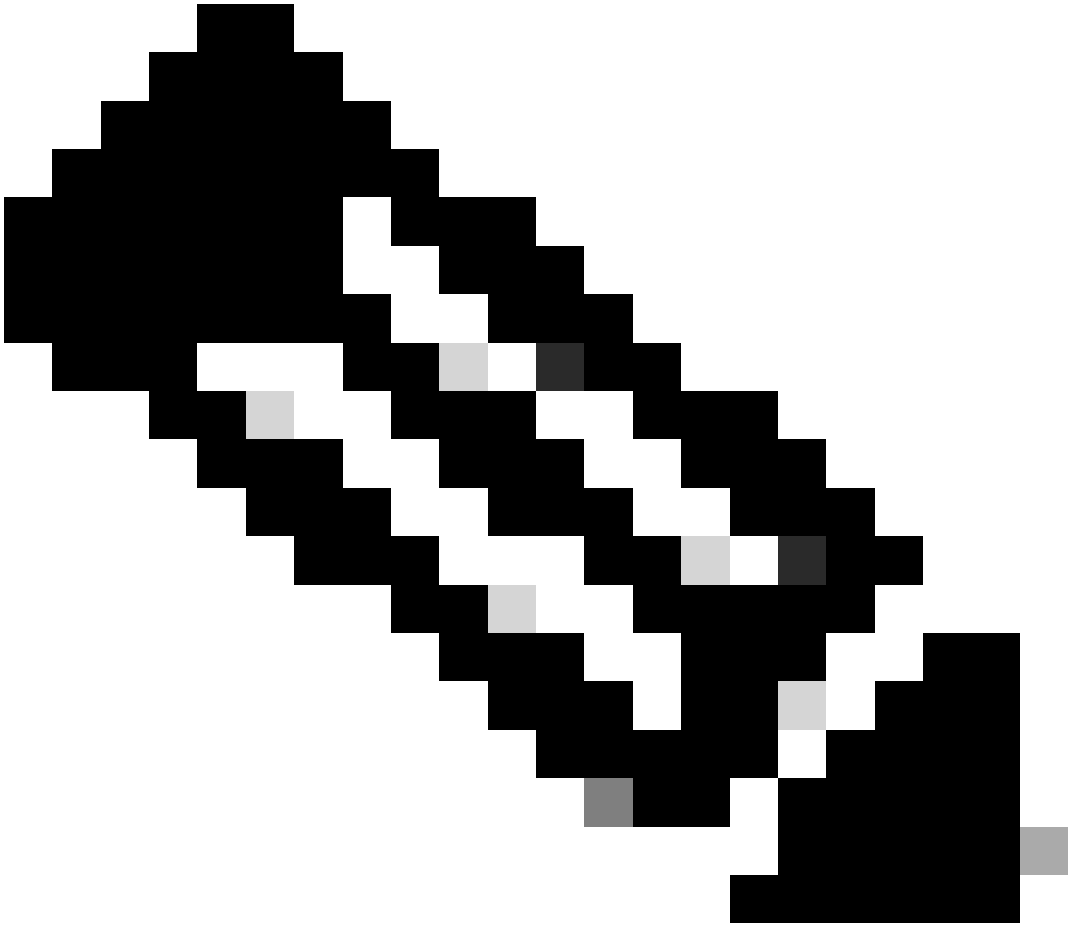


3. In the intrusion rules section, click **upgrade to snort 3**.

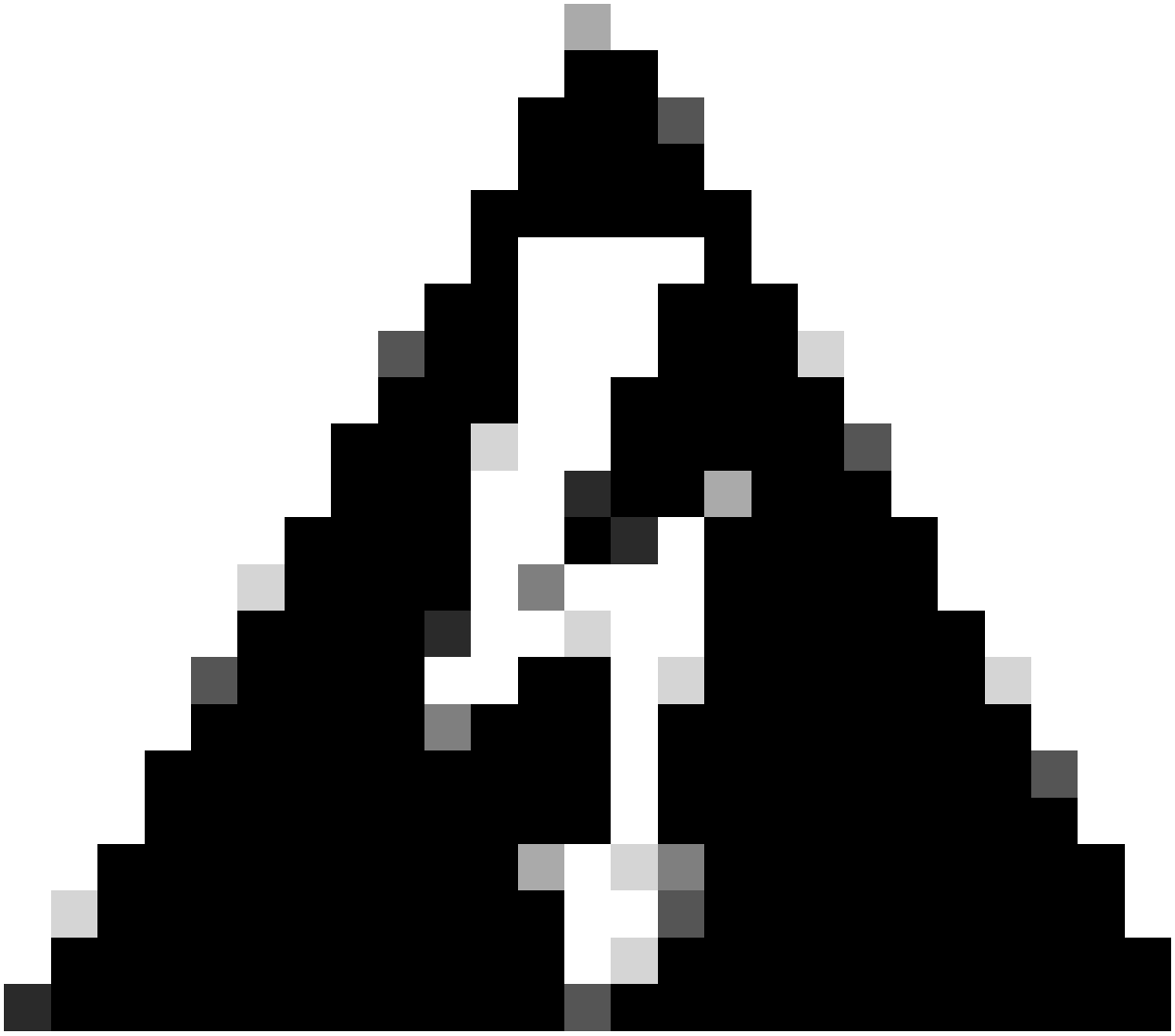


4. On the warning message to confirm your selection, select the option to **get the latest intrusion rules package**, then click **Yes**.



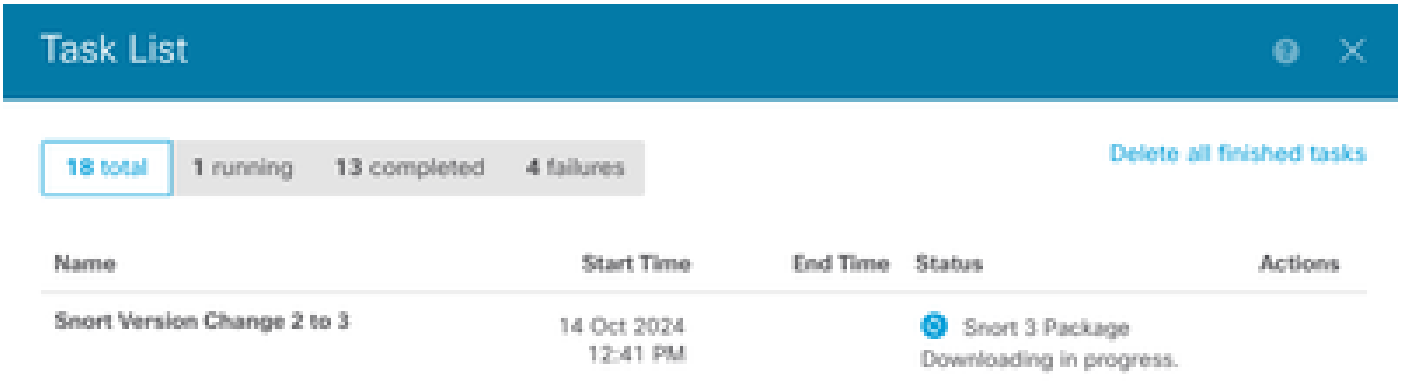


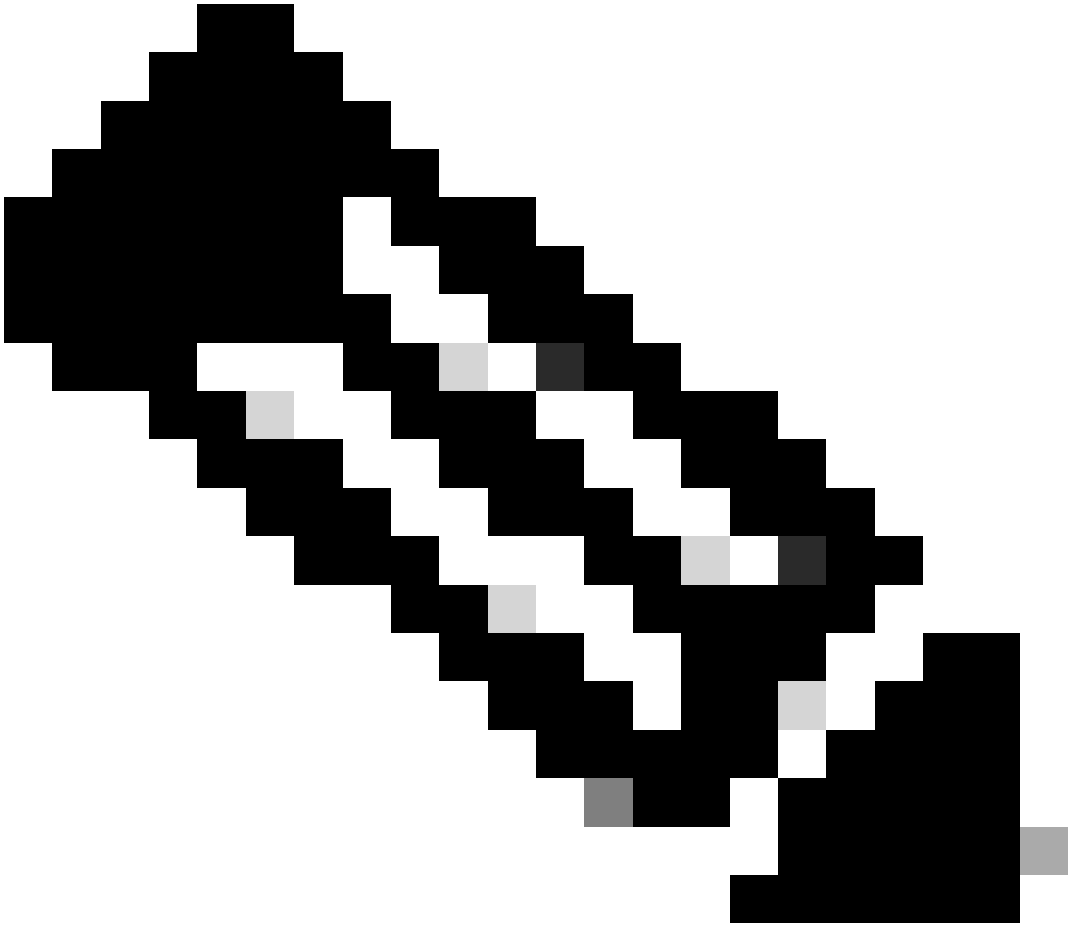
Note: The system downloads packages for the active Snort version only, so it is unlikely that you have the latest package installed for the Snort version you are switching to. You must wait until the task to switch versions completes before you can edit intrusion policies.



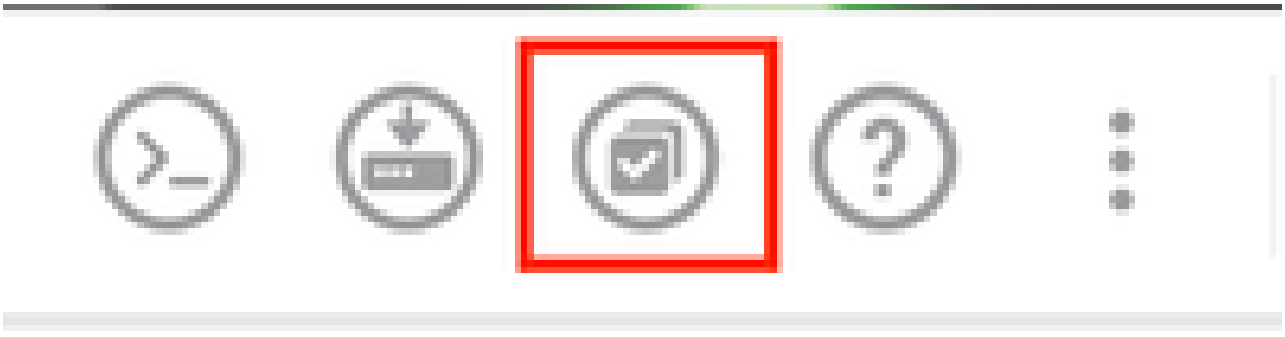
Warning: Switching snort version leads to momentary traffic loss.

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



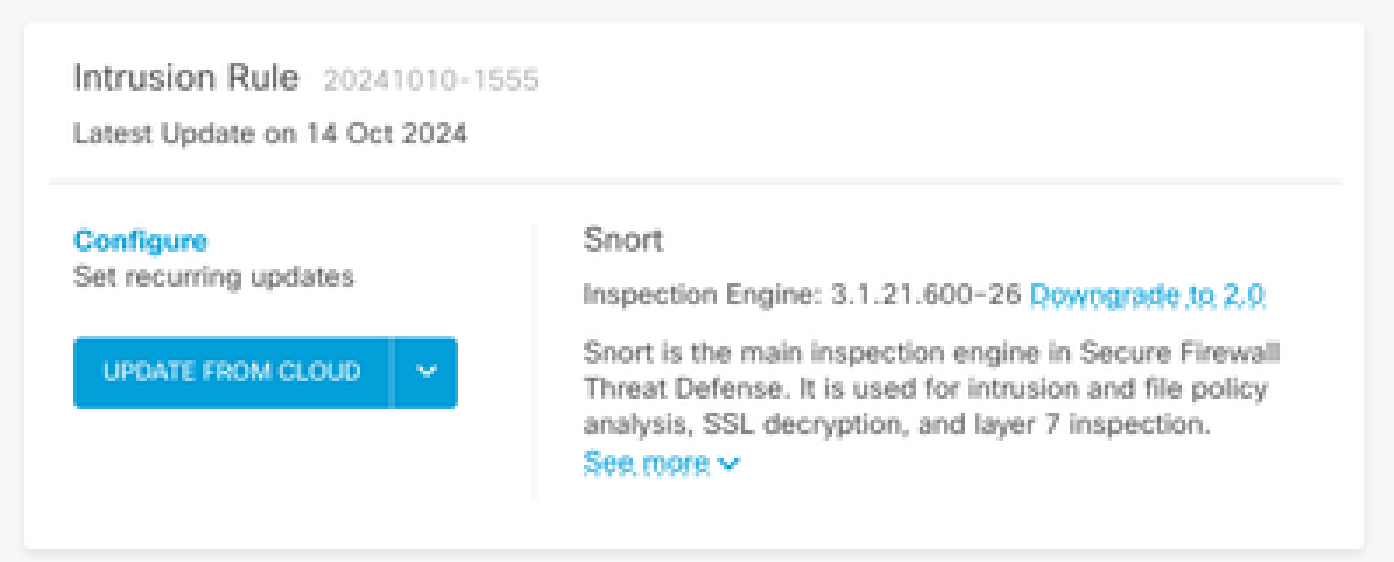


Note: The task list is found in the navigation bar next to the deployments icon.

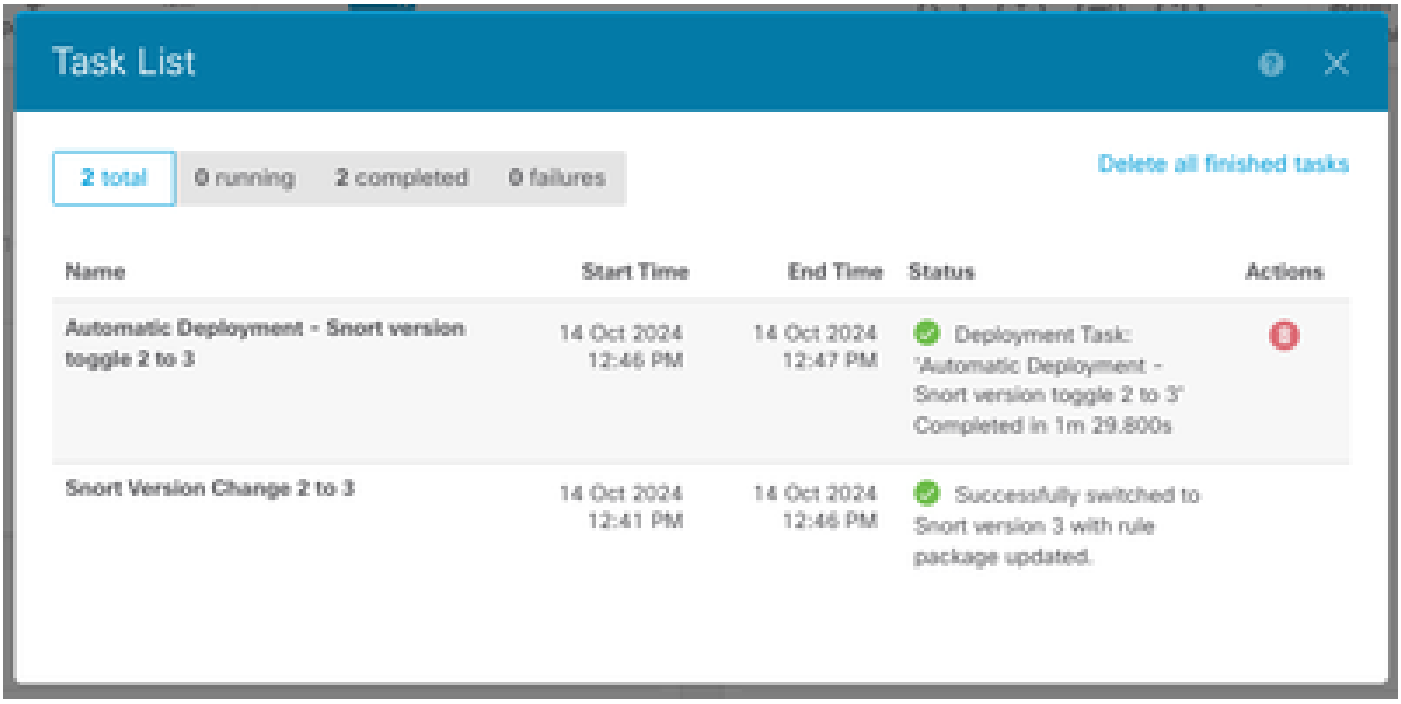


Verify

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



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



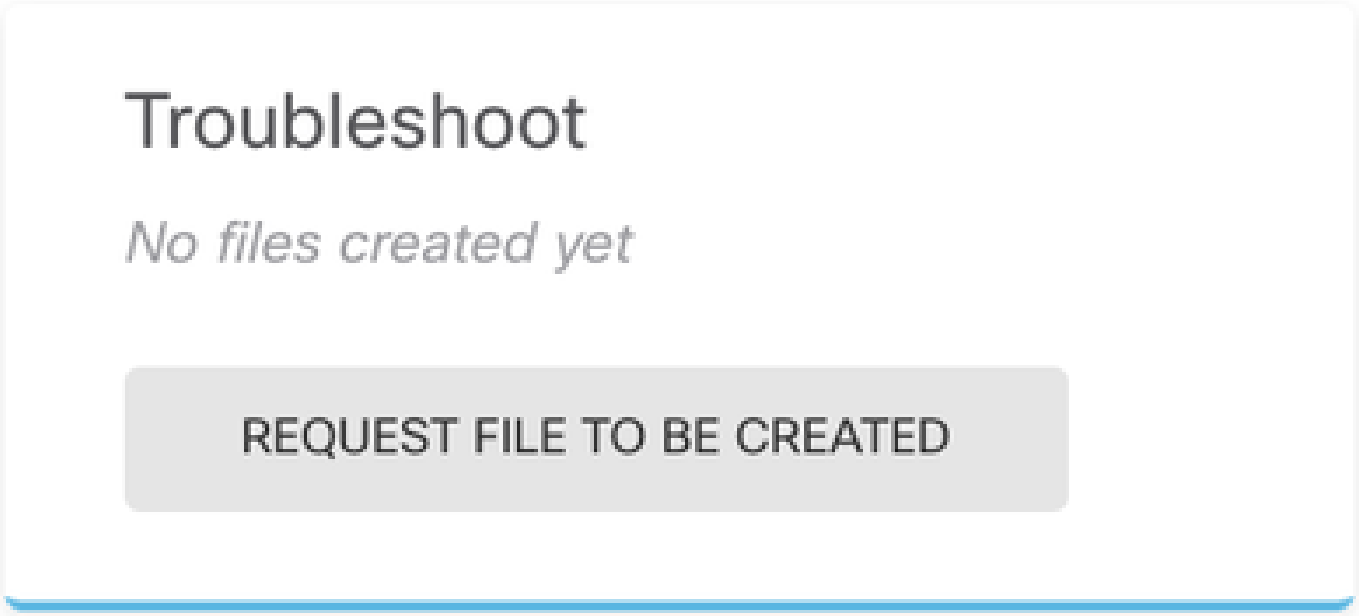
Troubleshoot

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.



Related Information

- Snort 3 Adoption
- Snort Documents
- Cisco Secure Firewall Device Manager Configuration Guide, Version 7.2