Upgrade from Snort 2 to Snort 3 via FMC

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Upgrade the Snort Version
  - Method 1
  - Method 2
- Upgrade of Intrusion Rules

Verify

Troubleshooting

Related Information

Introduction

This document describes how to upgrade from Snort 2 and Snort 3 version in Firepower Manager Center (FMC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Threat Defense (FTD)
- Firepower Management Center
- Snort

Components Used

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

- FMC 7.0
- FTD 7.0

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) and Cisco Defense Orchestrator (CDO); in the 7.0 release for the Firepower Management Center (FMC).

Snort 3.0 was designed to address these challenges:

1. Reduce memory and CPU usage.
2. Improve HTTP inspection efficacy.
3. Faster configuration loading and Snort restart.
4. Better programability for faster feature addition.

Configure

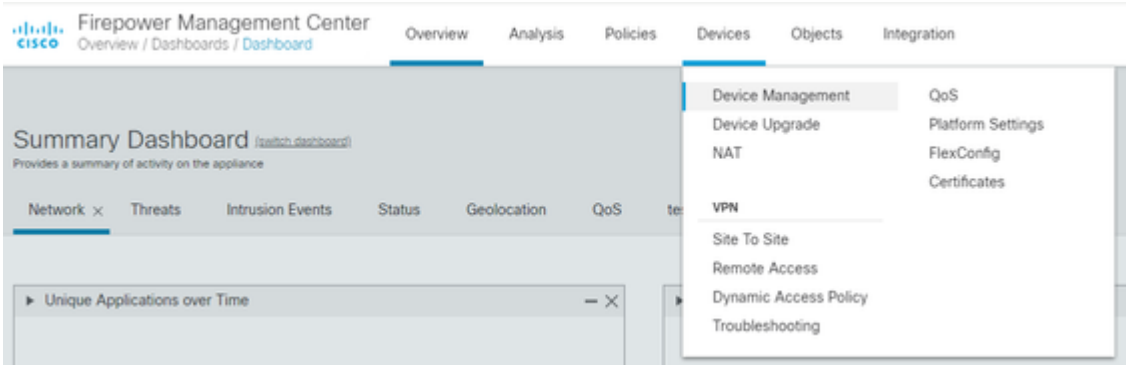
Upgrade the Snort Version

Method 1

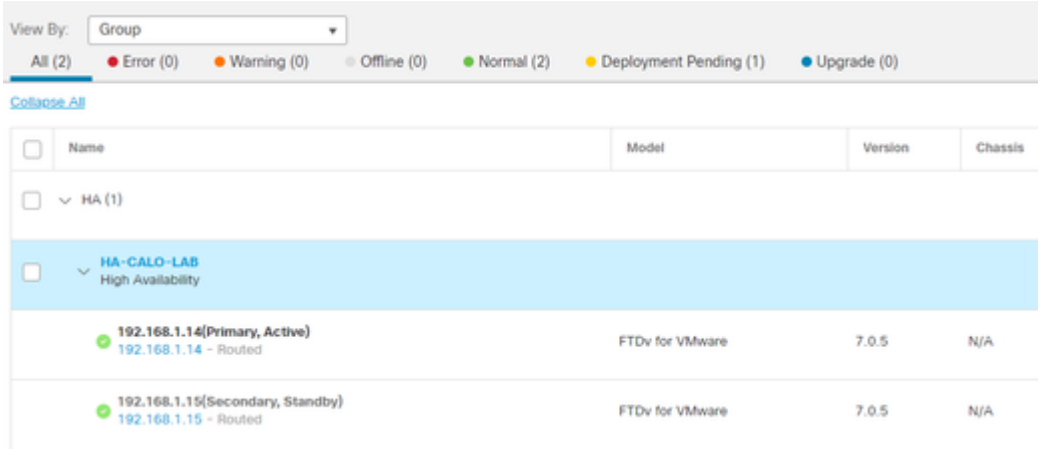
1. Log into **Firepower Management Center**.



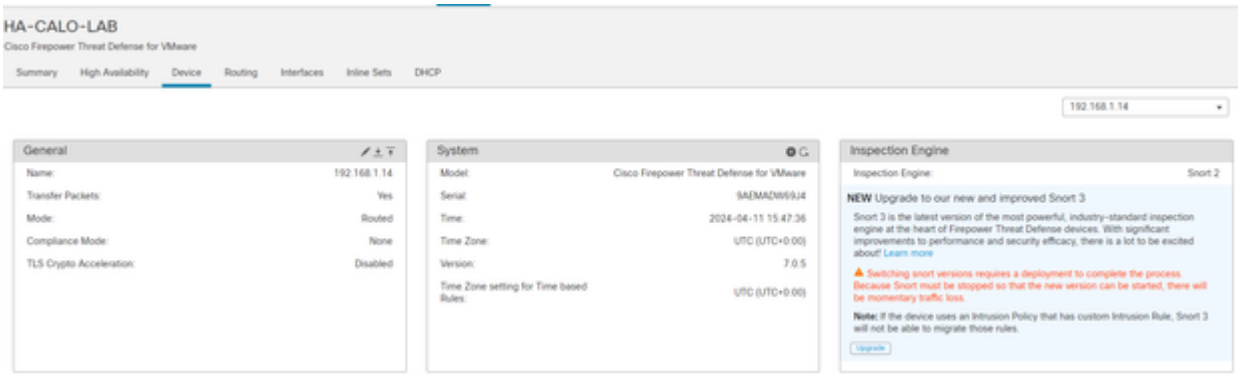
2. On the **Device** tab, navigate to **Devices > Device Manager**.



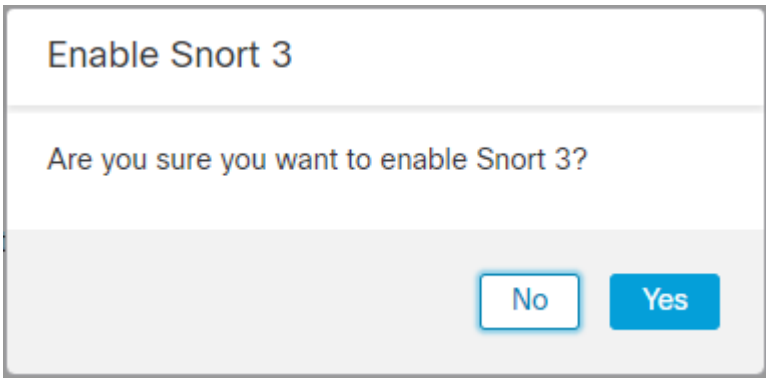
3. Select the **device** that you want to change the Snort version.



4. Click the **Device** tab and click the **Upgrade** button on the Inspection Engine Section.



5. Confirm your **selection**.

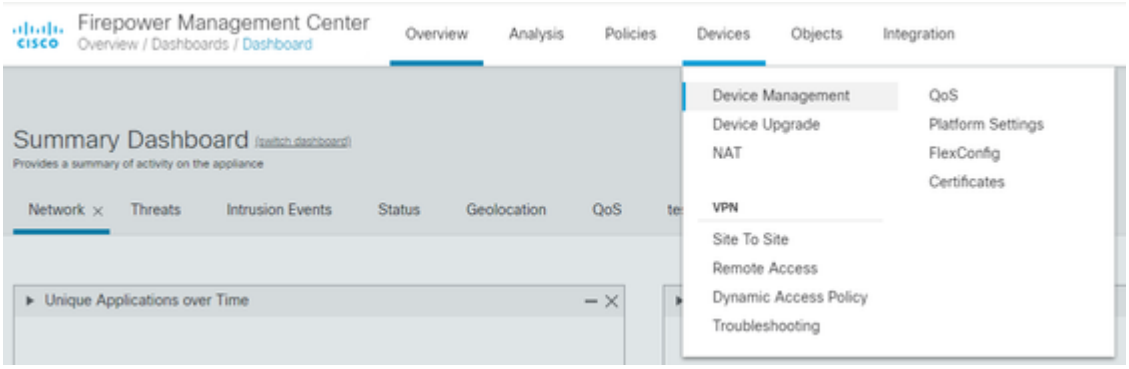


Method 2

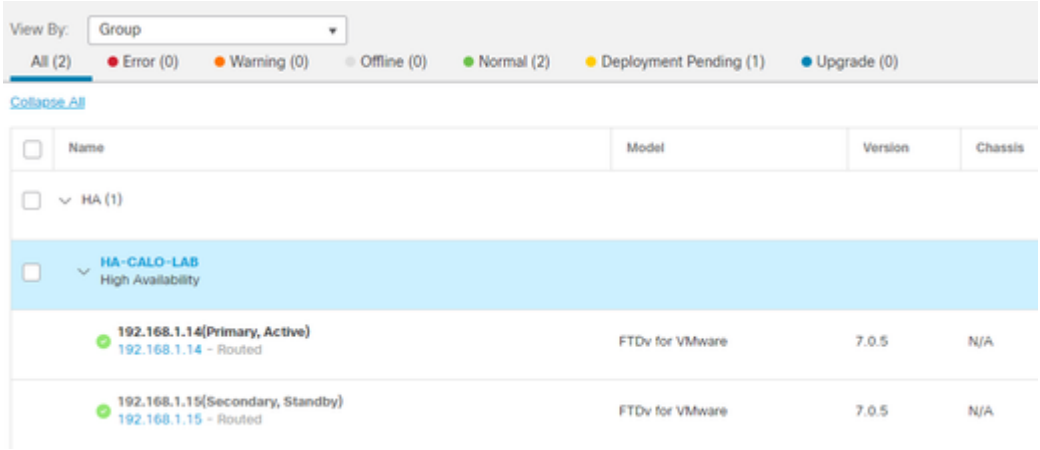
1. Log into **Firepower Management Center**.



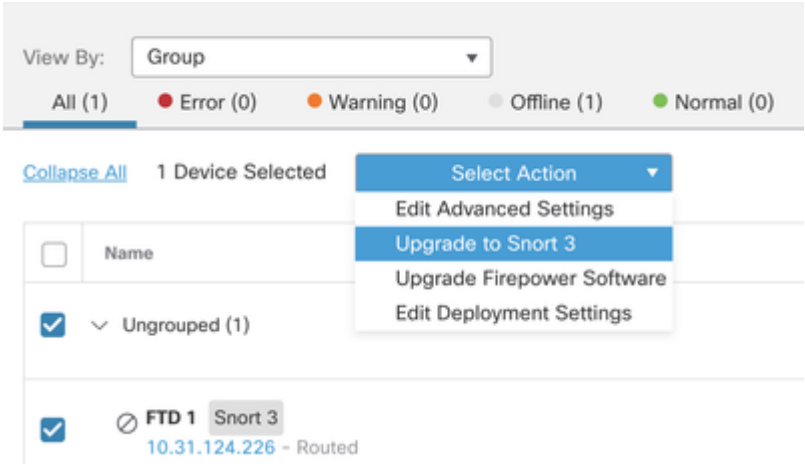
2. On the **Device** tab, navigate to **Devices > Device Manager**.



3. Select the **device** that you want to change the Snort version.



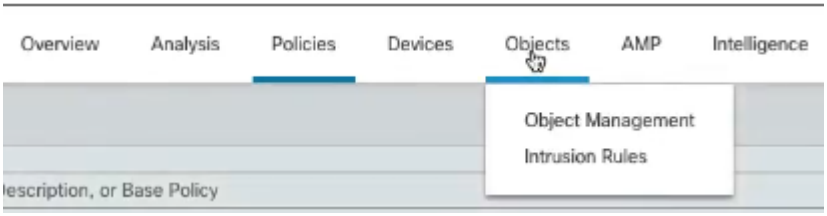
4. Click the **Select Action** button and select **Upgrade to Snort 3**.



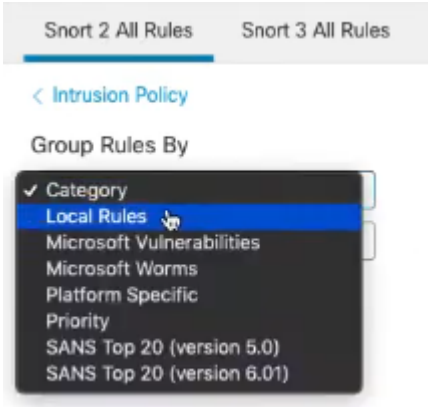
Upgrade of Intrusion Rules

Additionally, you need to convert your Snort 2 rules into Snort 3 rules.

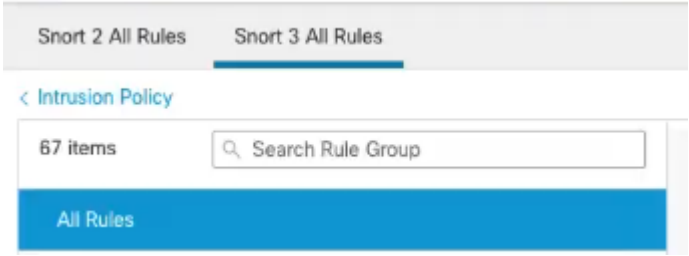
1. Select from the menu **Objects > Intrusion Rules**.



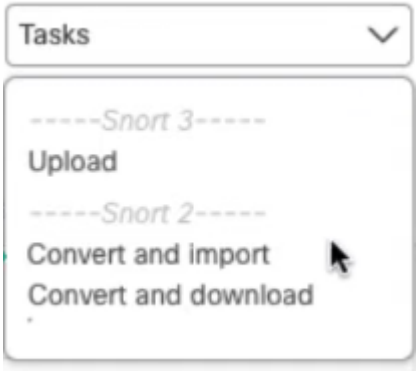
2.Select from the menu **Snort 2 All Rules tab > Group Rules By > Local Rules**.



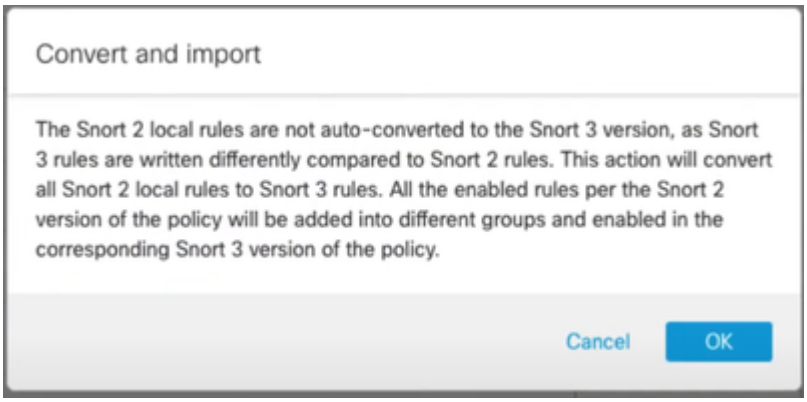
3. Click **Snort 3 All Rules** tab and make sure that **All Rules** is selected.



4.On the **Task** drop down menu, select **Convert and import**.



5. Click **OK** on the warning message.

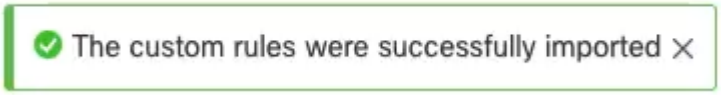


Verify

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



The rule conversion was successful once you see this message:



Finally, you must find on the **Local Rules** group the **All Snort 2 Converted Global** section, which contains all your Snort 2 to Snort 3 converted rules.



Troubleshooting

In case the migration fails or crashes, rollback to Snort 2 and try again.

Related Information

- How to Migrate from Snort 2 to Snort 3
- Cisco Secure - Snort 3 Device Upgrade (External YouTube Video)