Upgrade from Snort 2 to Snort 3 via FMC

Contents

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
- 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:

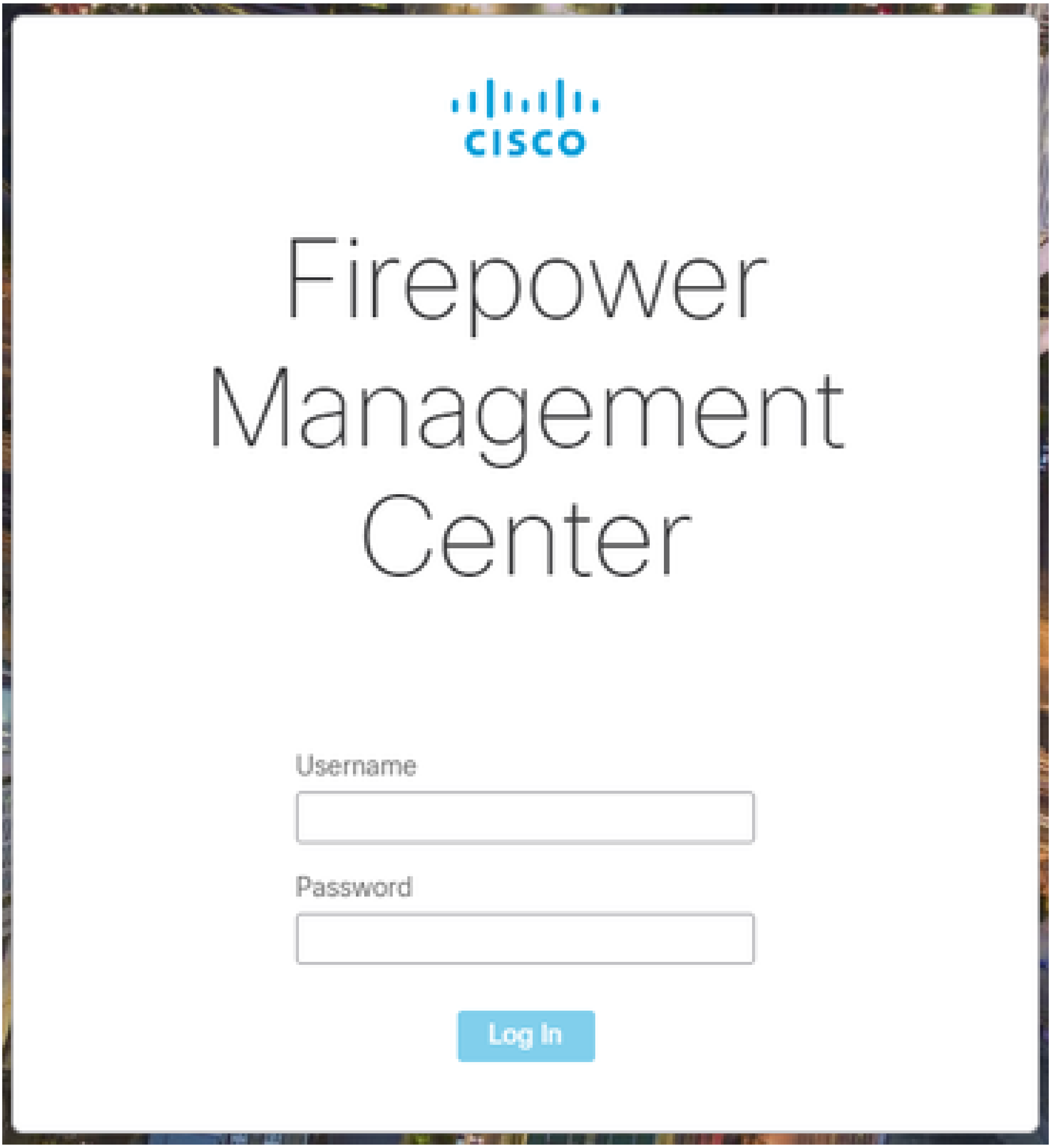
1. Reduce memory and CPU usage.
2. Improve HTTP inspection efficacy.
3. Faster configuration loading and Snort restart.
4. Better programmability for faster feature addition.

Configure

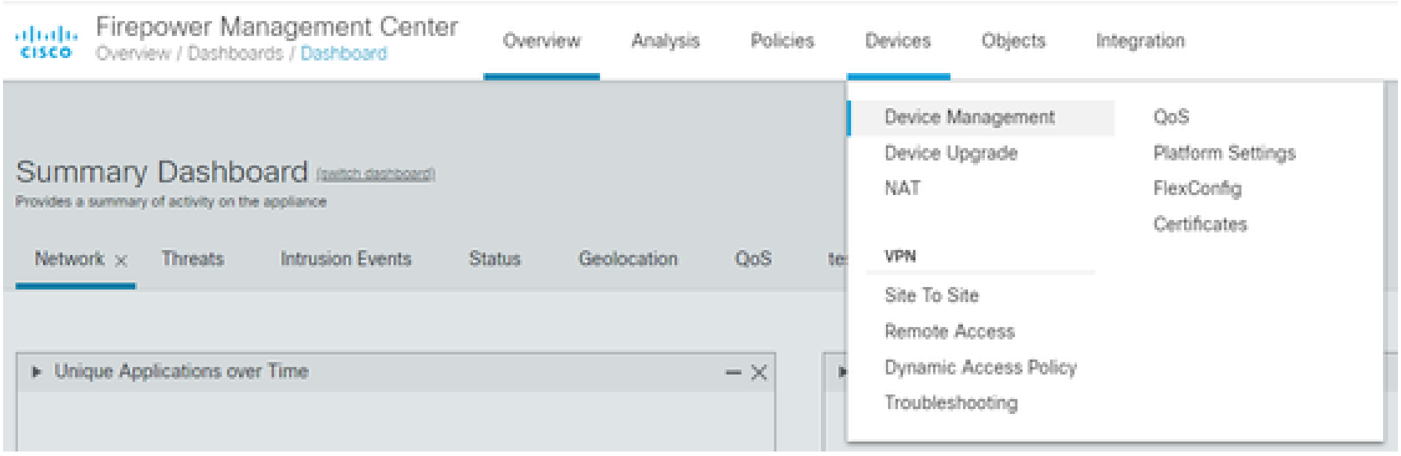
Upgrade the Snort Version

Method 1

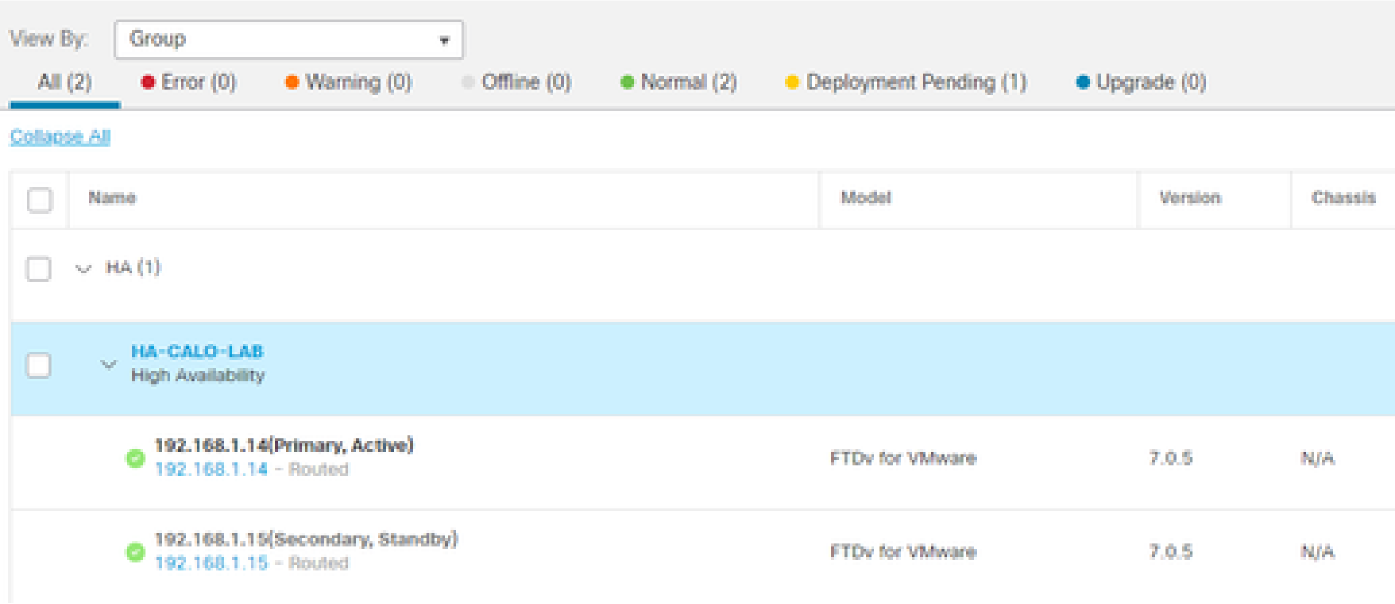
1. Log into Firepower Management Center.



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



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



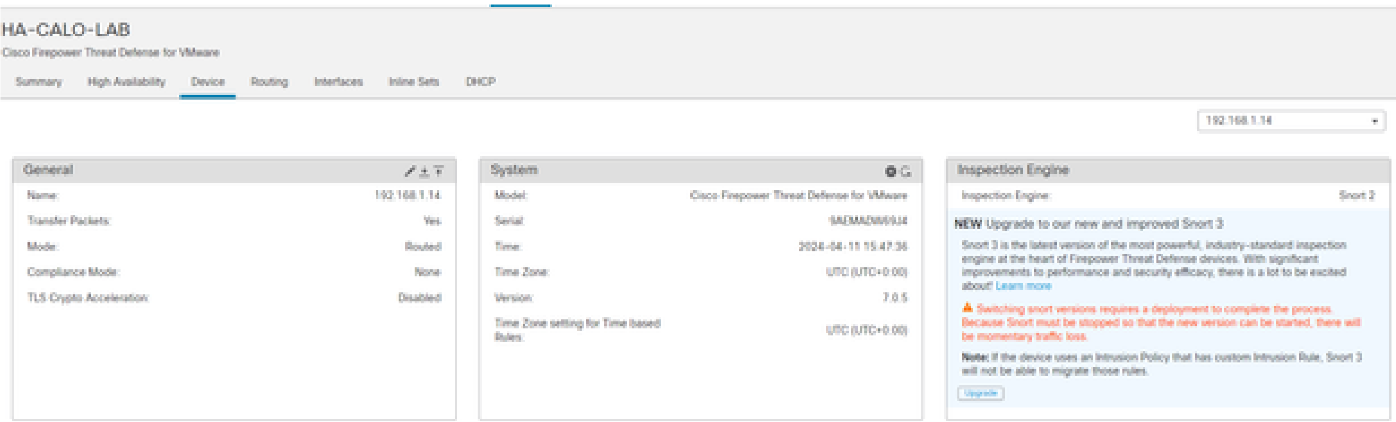
View By: Group

All (2) | ● Error (0) | ● Warning (0) | ● Offline (0) | ● Normal (2) | ● Deployment Pending (1) | ● Upgrade (0)

Collapse All

□	Name	Model	Version	Chassis
□	HA (1)			
□	HA-CALO-LAB High Availability			
	✓ 192.168.1.14(Primary, Active) 192.168.1.14 - Routed	FTDv for VMware	7.0.5	N/A
	✓ 192.168.1.15(Secondary, Standby) 192.168.1.15 - Routed	FTDv for VMware	7.0.5	N/A

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



General

Name:	192.168.1.14
Transfer Packets:	Yes
Mode:	Routed
Compliance Mode:	None
TLS Crypto Acceleration:	Disabled

System

Model:	Cisco Firepower Threat Defense for VMware
Serial:	9AEMADW9JU4
Time:	2024-04-11 15:47:36
Time Zone:	UTC (UTC+0:00)
Version:	7.0.5
Time Zone setting for Time based Rules:	UTC (UTC+0:00)

Inspection Engine

Inspection Engine: Snort 2

NEW Upgrade to our new and improved Snort 3

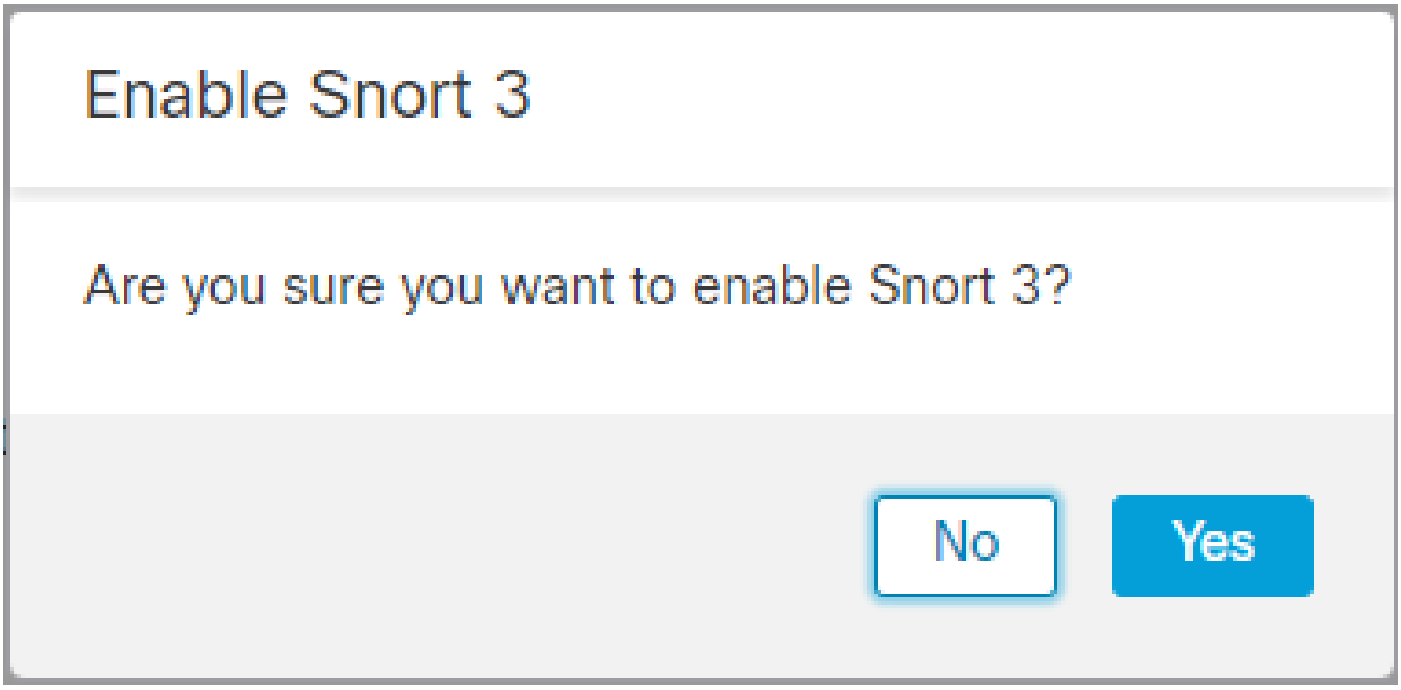
Snort 3 is the latest version of the most powerful, industry-standard inspection engine at the heart of Firepower Threat Defense devices. With significant improvements to performance and security efficacy, there is a lot to be excited about! Learn more

⚠ Switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be momentary traffic loss.

Note: If the device uses an Intrusion Policy that has custom Intrusion Rule, Snort 3 will not be able to migrate those rules.

Upgrade

5. Confirm your selection.

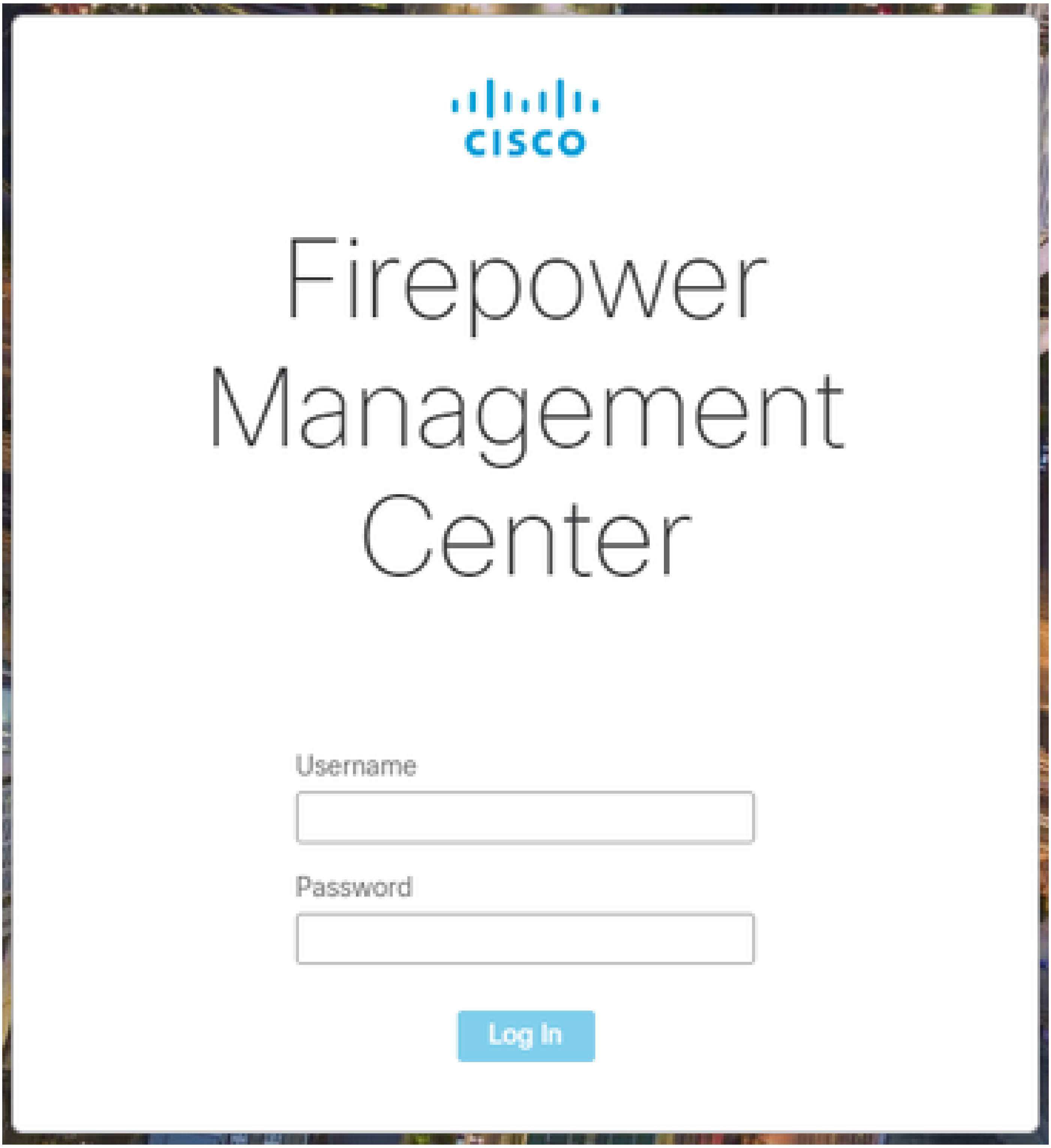


Enable Snort 3

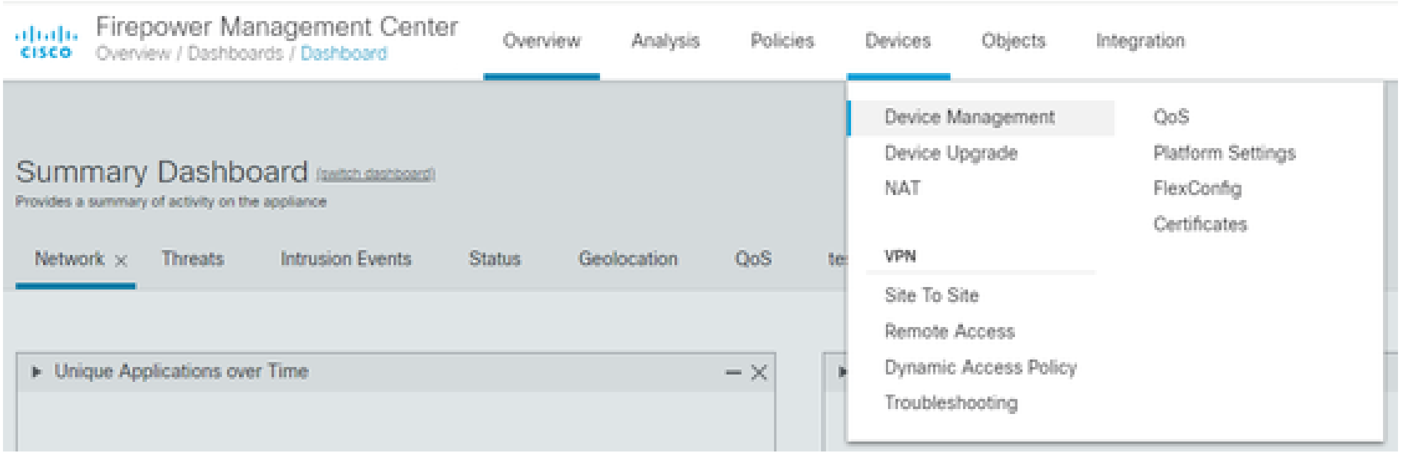
Are you sure you want to enable Snort 3?

Method 2

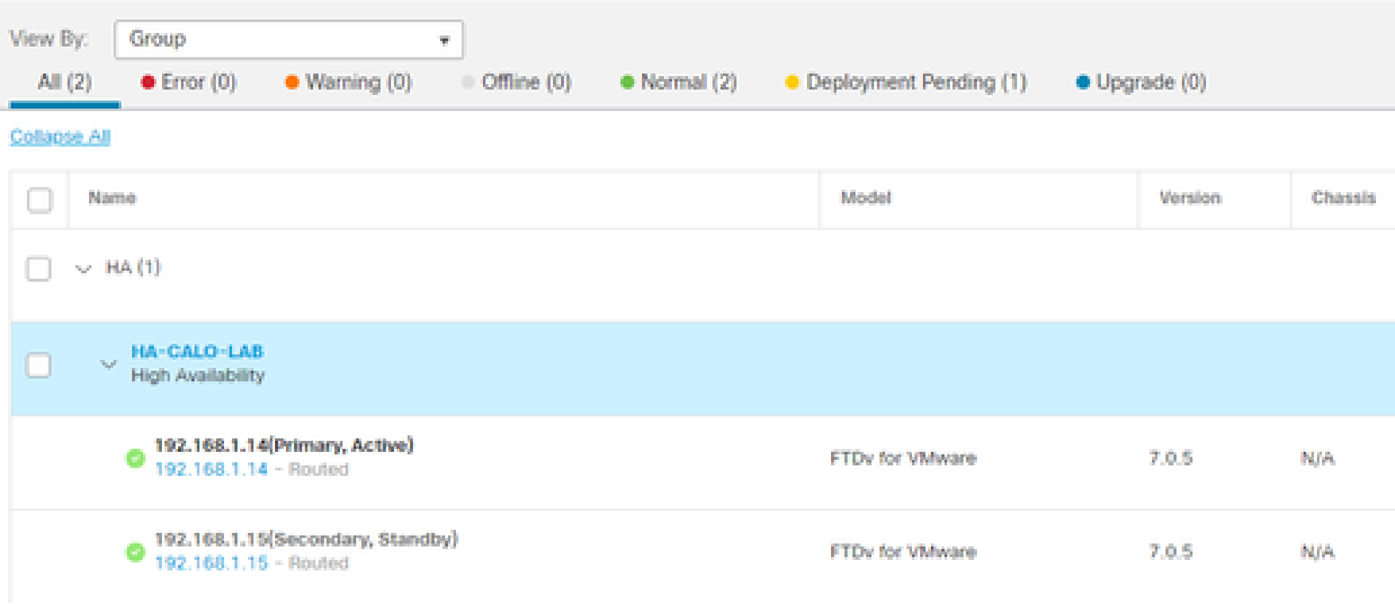
1. Log into Firepower Management Center.



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

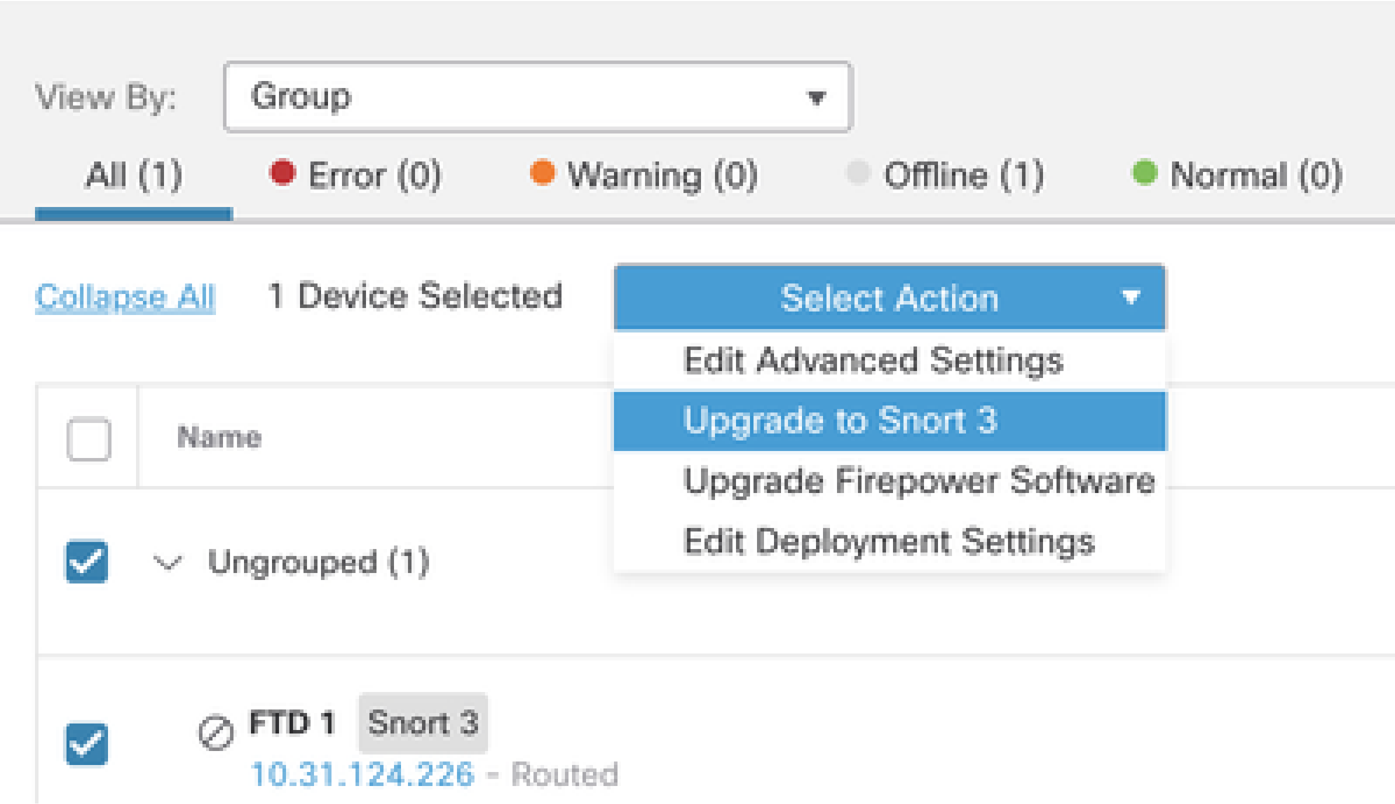


3. Select the device that you want to change the Snort version.



□	Name	Model	Version	Chassis
□	HA (1)			
□	HA-CALO-LAB High Availability			
	192.168.1.14(Primary, Active) 192.168.1.14 - Routed	FTDv for VMware	7.0.5	N/A
	192.168.1.15(Secondary, Standby) 192.168.1.15 - Routed	FTDv for VMware	7.0.5	N/A

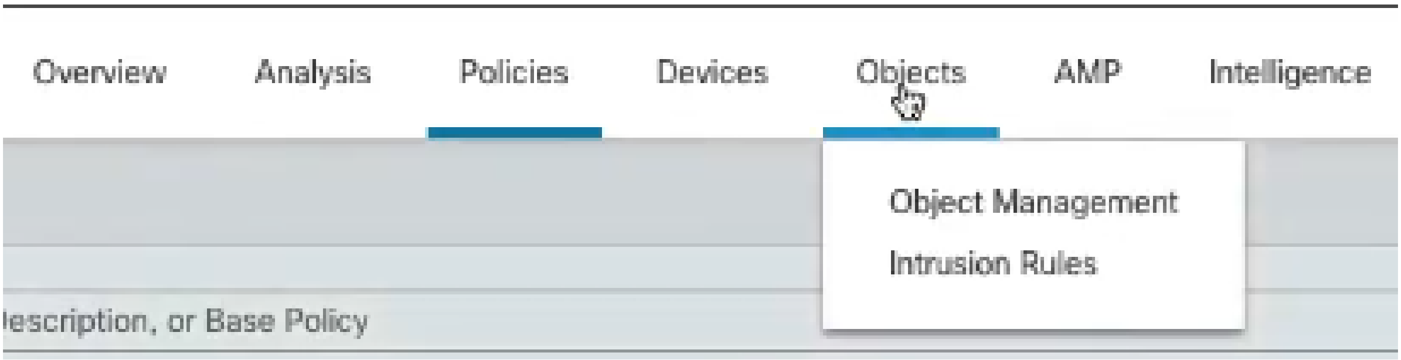
4. Click on the **Select Action** button and select **Upgrade to Snort 3**.



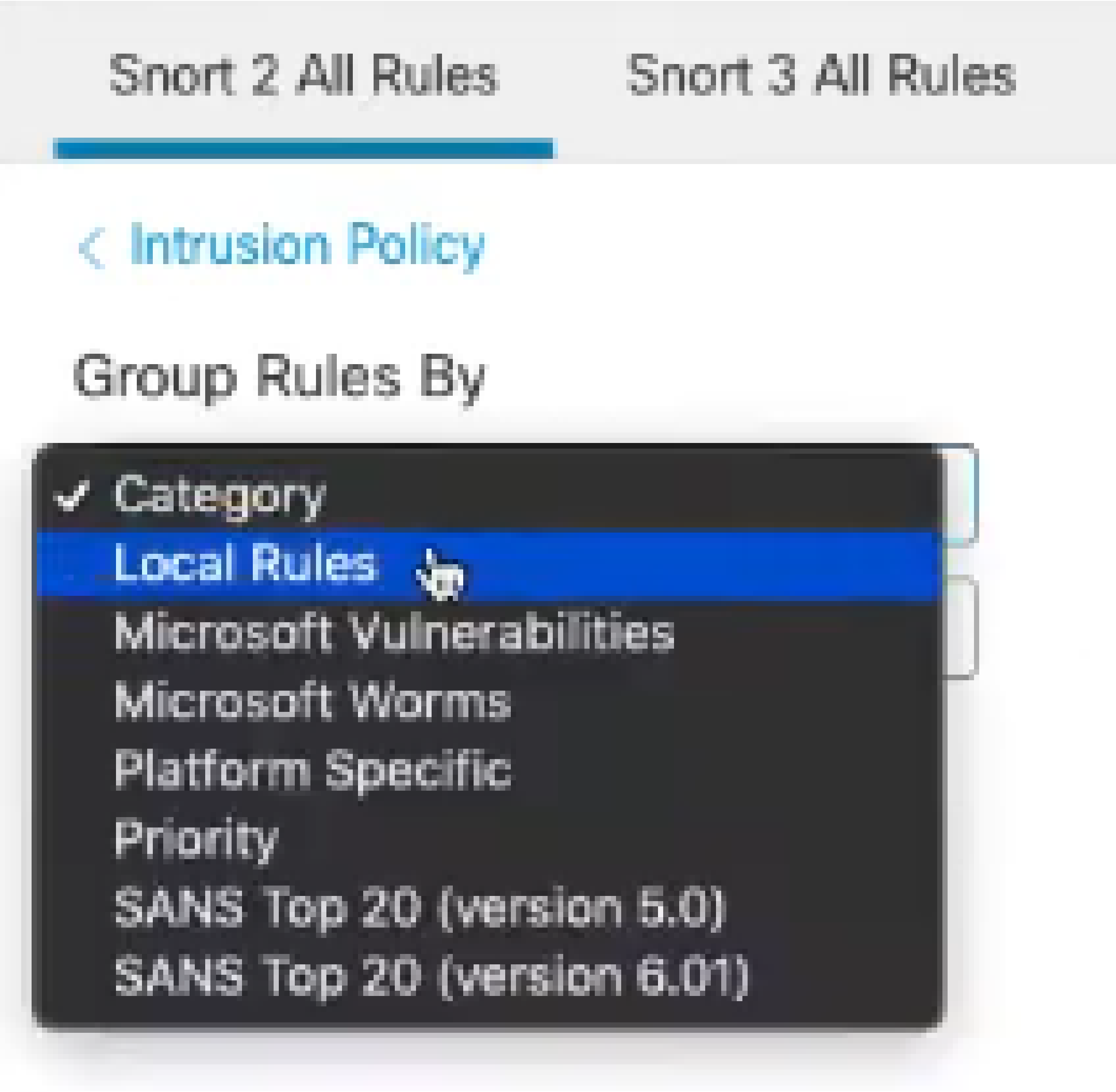
Upgrade of Intrusion Rules

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

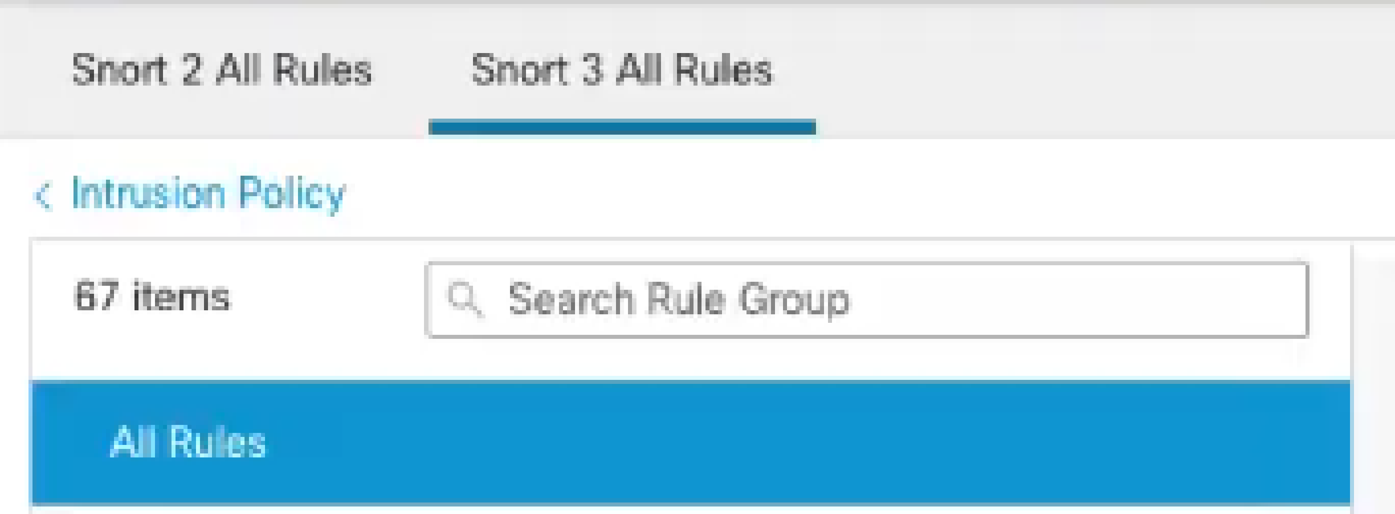
1. Select from the menu **Objects** > **Intrusion Rules**.



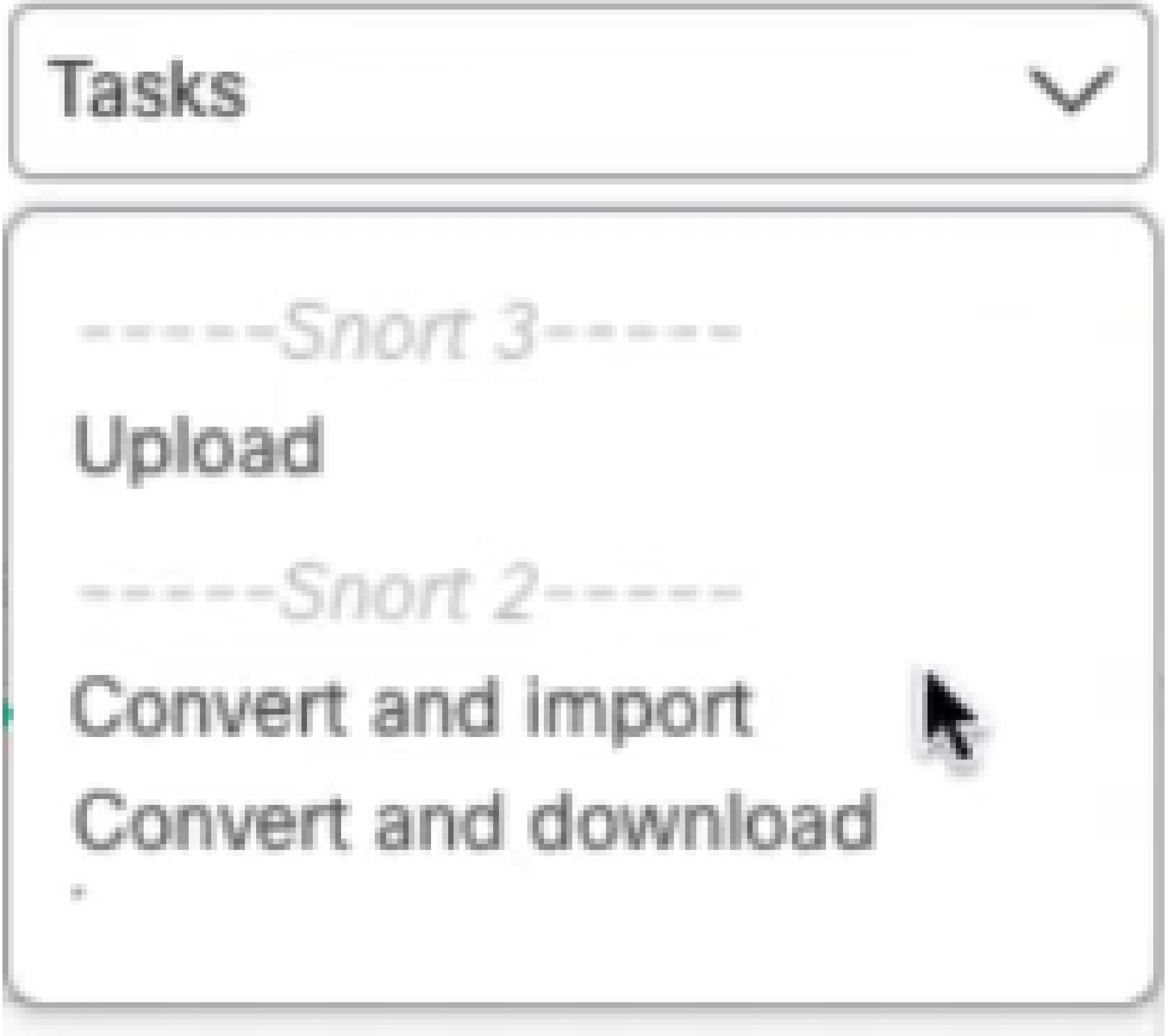
2.Select from the menu **Snort 2 All Rules tab** > **Group Rules By** > **Local Rules**.



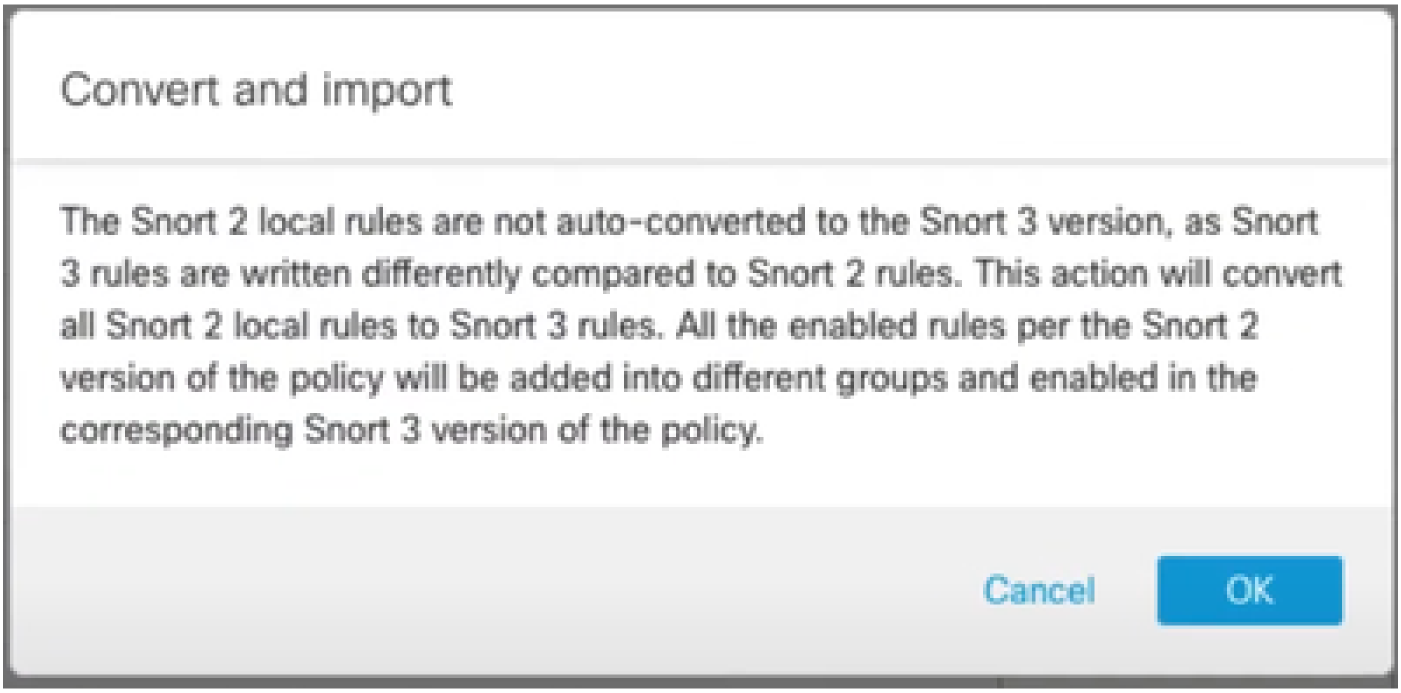
3. Click **Snort 3 All Rules** tab and make sure that **All Rules** is selected.



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



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

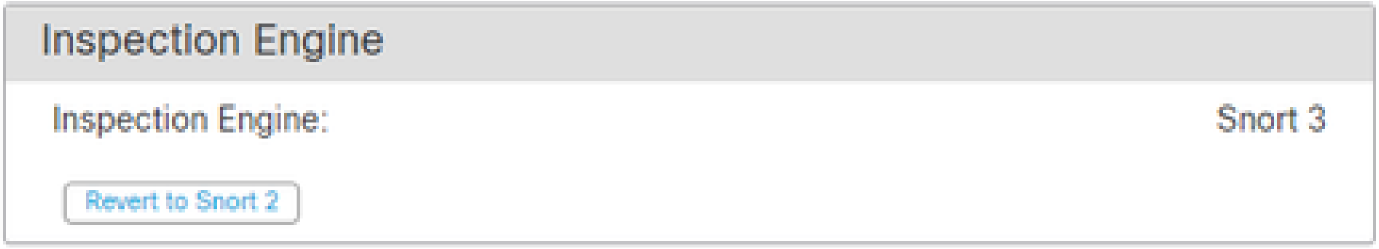


Convert and import

The Snort 2 local rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. This action will convert all Snort 2 local rules to Snort 3 rules. All the enabled rules per the Snort 2 version of the policy will be added into different groups and enabled in the corresponding Snort 3 version of the policy.

Verify

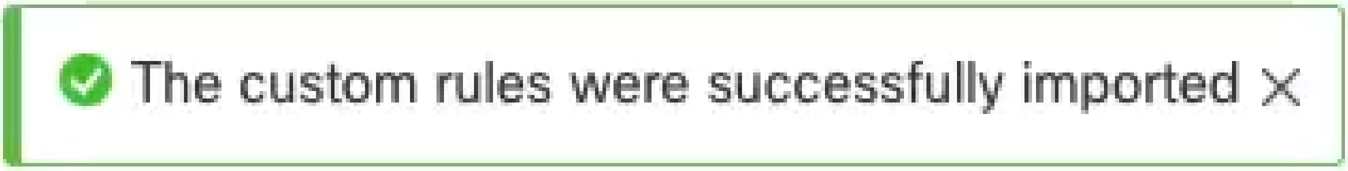
The Inspection Engine section shows that the current version of Snort is Snort 3.



Inspection Engine

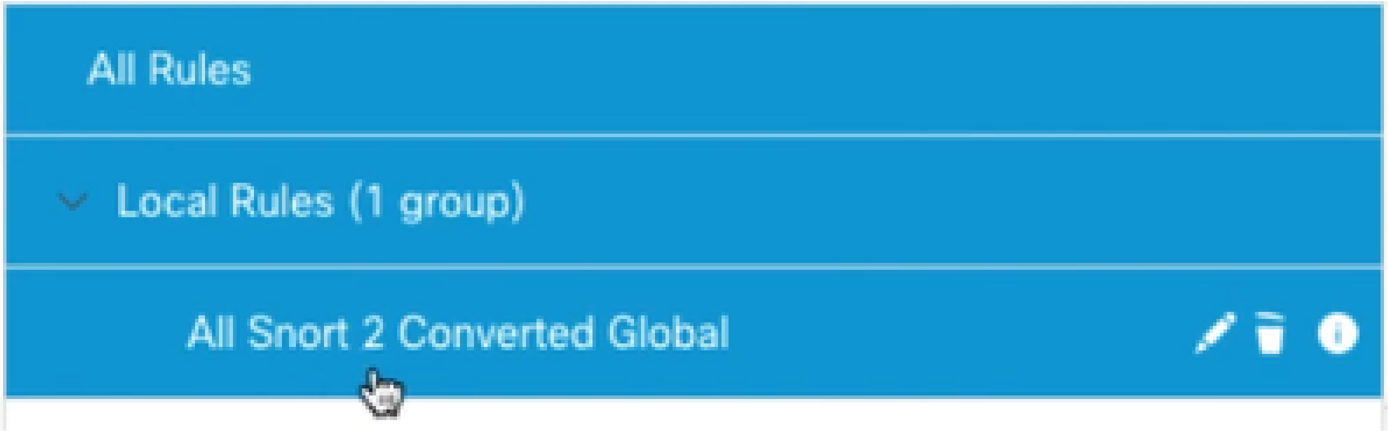
Inspection Engine: Snort 3

The rule conversion was successful once you see this message:



✓ The custom rules were successfully imported

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.



All Rules

Local Rules (1 group)

All Snort 2 Converted Global

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)