Determine the Active Snort Version that Runs on Firepower Threat Defense (FTD)

Contents

Introduction

This document describes steps to confirm the active snort version a Cisco FTD runs when it is managed by the Cisco FDM , the Cisco FMC, or the CDO.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Firepower Management Center (FMC)
- Cisco Firepower Threat Defense (FTD)
- Cisco Firepower Device Manager (FDM)
- Cisco Defense Orchestrator (CDO)

Components Used

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

- Cisco Firepower Threat Defense v6.7.0 and 7.0.0
- Cisco Firepower Management Center v6.7.0 and 7.0.0
- Cisco Defense Orchestrator

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

SNORT® Intrusion Prevention System has officially launched Snort 3, a sweeping upgrade that features improvements and new features that enhance the performance, faster processing, improved scalability for your network, and a range of 200+ plugins so you can create a custom set-up for your network.

Advantages of Snort 3 include, but are not limited to:

- Improved performance
- Improved SMBv2 inspection
- New script detection capabilities
- HTTP/2 inspection
- Custom rule groups
- Syntax that makes custom intrusion rules easier to write.
- Reasons for why it would have dropped inline results in intrusion events.
- No Snort restarts when changes are deployed to the VDB, SSL policies, custom application detectors, captive portal identity sources, and TLS server identity discovery.
- Improved serviceability, due to Snort 3-specific telemetry data sent to Cisco Success Network, and to better troubleshooting logs.

The support for Snort 3.0 was introduced for the 6.7.0 Cisco Firepower Threat Defense (FTD), just when the FTD is managed through the Cisco Firepower Device Manager (FDM).

Note: For new 6.7.0 FTD deployments managed by FDM, Snort 3.0 is the default inspection engine. If you upgrade the FTD to 6.7 from an older release, then Snort 2.0 remains the active inspection engine, but you can switch to Snort 3.0.

Note: For this release, Snort 3.0 does not support virtual routers, time-based access control rules, or the decryption of TLS 1.1 or lower connections. Enable Snort 3.0 only if you do not need these features.

Then, Firepower version 7.0 introduced the Snort 3.0 support for the Firepower Threat Defense devices managed by both; the Cisco FDM and by the Cisco Firepower Management Center (FMC).

Note: For new 7.0 FTD deployments, Snort 3 is now the default inspection engine. Upgraded deployments continue to use Snort 2, but you can switch at any time.

⚠ **Caution**: You can freely switch back and forth between Snort 2.0 and 3.0, so you can revert your change if needed. Traffic is interrupted whenever you switch versions.

⚠ **Caution**: Before you switch to Snort 3, is strongly recommend you read and understand the Firepower Management Center Snort 3 Configuration Guide. Pay special attention to feature limitations and migration instructions. Although the upgrade to Snort 3 is designed for minimal impact, features do not map exactly. The plan and preparation before the upgrade can help you make sure that traffic is handled as expected.

Determine the Active Snort Version that Runs on FTD

FTD Command Line Interface (CLI)

In order to determine the active snort version that runs on an FTD, log in to the FTD CLI and run the **show snort3 status** command:

Example 1: When there is no output displayed, then the FTD runs Snort 2.

```
<#root>

>

show snort3 status


>
```

Example 2: When the output shows, Currently running Snort 2, then the FTD runs Snort 2.

```
<#root>

>

show snort3 status


Currently running Snort 2
```

Example 3: When the output shows, Currently running Snort 3, then the FTD runs Snort 3.

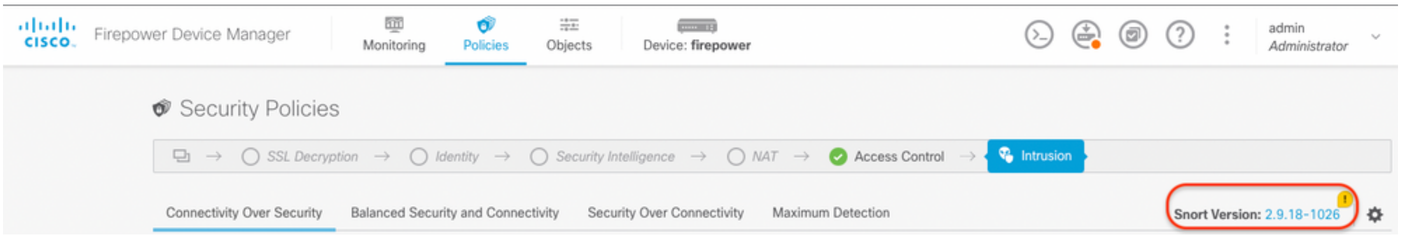
```
<#root>

>

show snort3 status


Currently running Snort 3
```

FTD Managed by the Cisco FDM

In order to determine the active snort version that runs on an FTD that is managed by the Cisco FDM, proceed with the next steps:

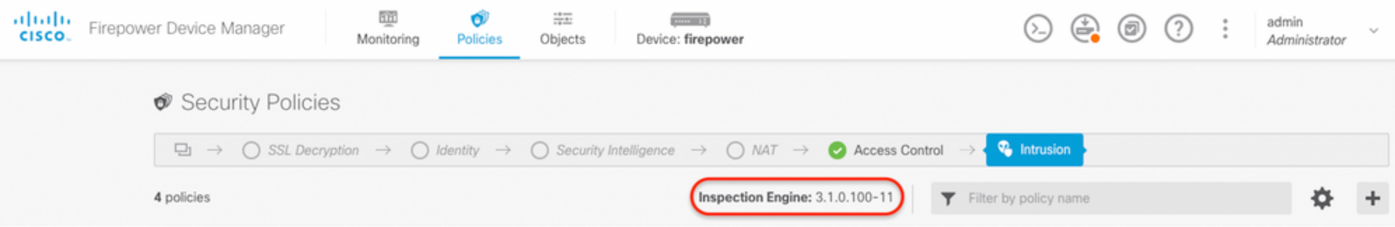
1. Log in to the Cisco FTD through the FDM web interface.
2. From the main menu, select **Policies**.
3. Then, select the **Intrusion** tab.
4. Look for the **Snort Version** or the **Inspection Engine** section to confirm the Snort version that is active in the FTD.

Example 1: The FTD runs snort version 2.



Snort Version: 2.9.18-1026

Example 2: The FTD runs snort version 3.



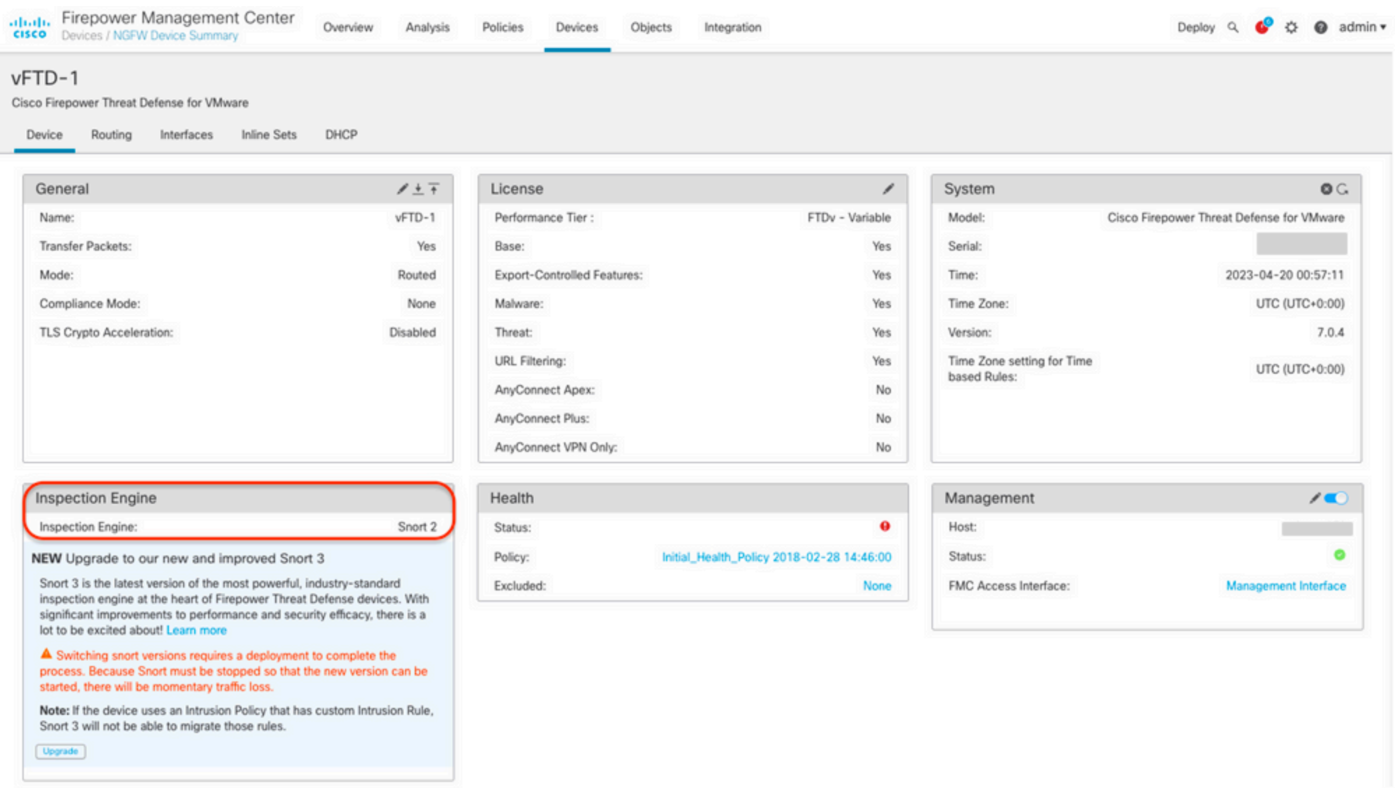
Inspection Engine: 3.1.0.100-11

FTD Managed by the Cisco FMC

In order to determine the active snort version that runs on an FTD that is managed by the Cisco FMC, proceed with the next steps:

1. Log in to the Cisco FMC web interface.
2. From the **Devices** menu, select **Device Management**.
3. Then, select the appropriate FTD device.
4. Click the **Edit** pencil icon.
5. Select the **Device** tab and look for the **Inspection Engine** section to confirm the snort version that is active in the FTD:

Example 1: The FTD runs snort version 2.



vFTD-1
Cisco Firepower Threat Defense for VMware

General
Name: vFTD-1
Transfer Packets: Yes
Mode: Routed
Compliance Mode: None
TLS Crypto Acceleration: Disabled

License
Performance Tier : FTDv - Variable
Base: Yes
Export-Controlled Features: Yes
Malware: Yes
Threat: Yes
URL Filtering: Yes
AnyConnect Apex: No
AnyConnect Plus: No
AnyConnect VPN Only: No

System
Model: Cisco Firepower Threat Defense for VMware
Serial:
Time: 2023-04-20 00:57:11
Time Zone: UTC (UTC+0:00)
Version: 7.0.4
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

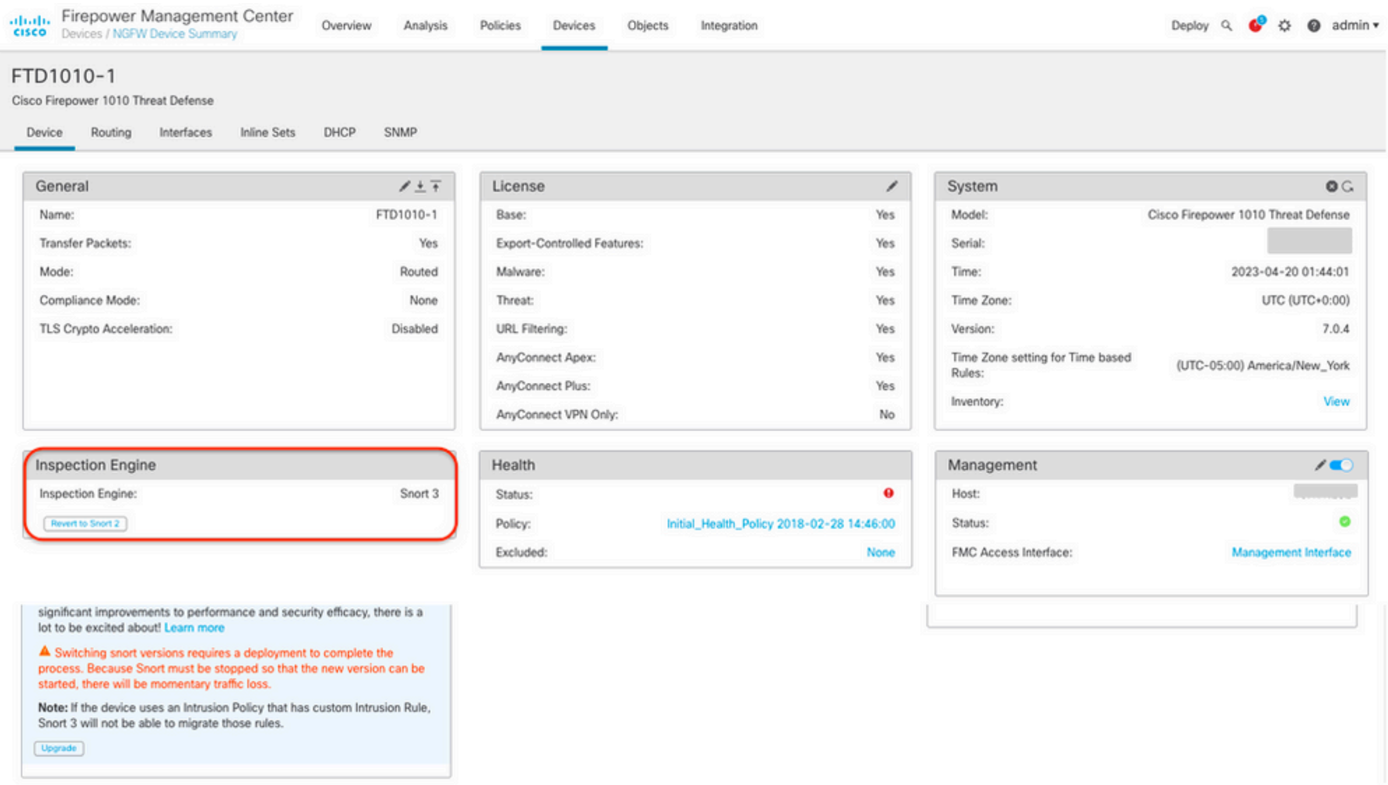
⚠ Switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be momentary traffic loss.

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

Health
Status: ●
Policy: Initial_Health_Policy 2018-02-28 14:46:00
Excluded: None

Management
Host:
Status: ●
FMC Access Interface: Management Interface

Example 2: The FTD runs snort version 3.



Firepower Management Center
Devices / NGFW Device Summary

Overview Analysis Policies Devices Objects Integration Deploy admin

FTD1010-1
Cisco Firepower 1010 Threat Defense

Device Routing Interfaces Inline Sets DHCP SNMP

General

Name:	FTD1010-1
Transfer Packets:	Yes
Mode:	Routed
Compliance Mode:	None
TLS Crypto Acceleration:	Disabled

License

Base:	Yes
Export-Controlled Features:	Yes
Malware:	Yes
Threat:	Yes
URL Filtering:	Yes
AnyConnect Apex:	Yes
AnyConnect Plus:	Yes
AnyConnect VPN Only:	No

System

Model:	Cisco Firepower 1010 Threat Defense
Serial:	[redacted]
Time:	2023-04-20 01:44:01
Time Zone:	UTC (UTC+0:00)
Version:	7.0.4
Time Zone setting for Time based Rules:	(UTC-05:00) America/New_York
Inventory:	View

Inspection Engine

Inspection Engine:	Snort 3

Revert to Snort 2

Health

Status:	●
Policy:	Initial_Health_Policy 2018-02-28 14:46:00
Excluded:	None

Management

Host:	[redacted]
Status:	●
FMC Access Interface:	Management Interface

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.

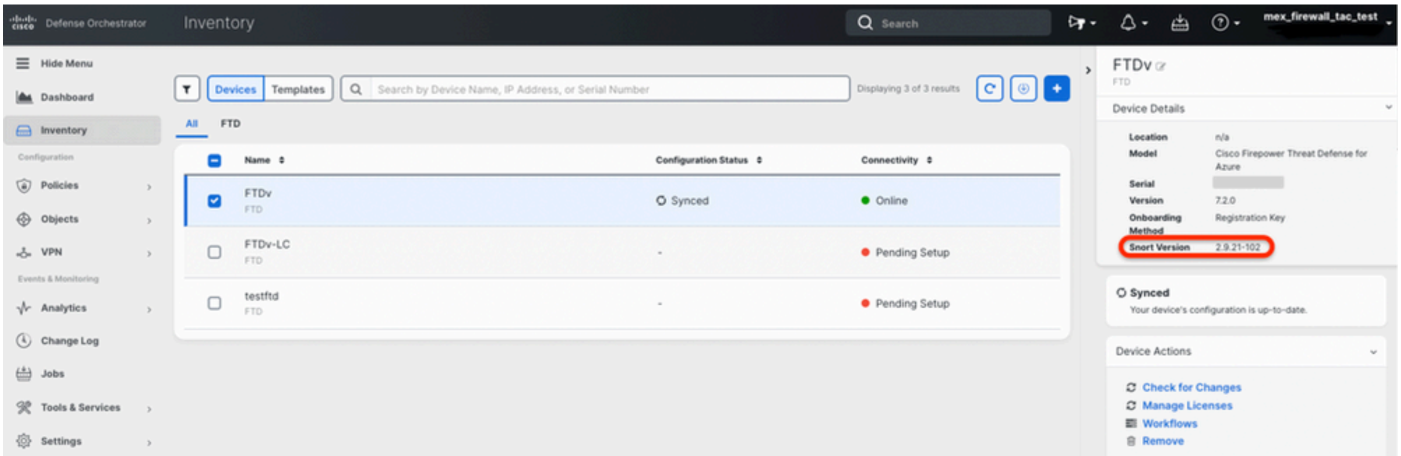
Upgrade

FTD Managed by the Cisco CDO

In order to determine the active snort version that runs on an FTD that is managed by the Cisco Defense Orchestrator, proceed with the next steps:

1. Log in to the Cisco Defense Orchestrator web interface.
2. From the **Inventory** menu, select the appropriate FTD device.
3. In the **Device Details** section, look for **Snort Version**:

Example 1: The FTD runs snort version 2.



Defense Orchestrator Inventory Search mex_firewall_tac_test [redacted]

Hide Menu
Dashboard
Inventory
Configuration
Policies
Objects
VPN
Events & Monitoring
Analytics
Change Log
Jobs
Tools & Services
Settings

Devices Templates Search by Device Name, IP Address, or Serial Number Displaying 3 of 3 results

All FTD

	Name	Configuration Status	Connectivity
☑	FTDv FTD	○ Synced	● Online
□	FTDv-LC FTD	-	● Pending Setup
□	testftd FTD	-	● Pending Setup

FTDv
FTD

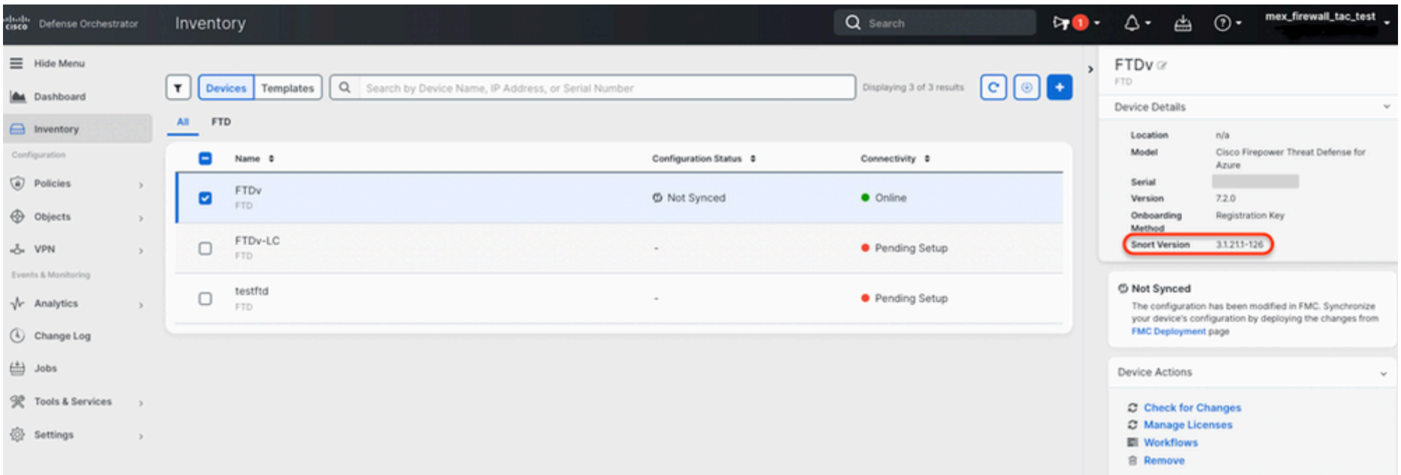
Device Details

Location	n/a
Model	Cisco Firepower Threat Defense for Azure
Serial	[redacted]
Version	7.2.0
Onboarding Method	Registration Key
Snort Version	2.9.21-102

○ Synced
Your device's configuration is up-to-date.

Device Actions
Check for Changes
Manage Licenses
Workflows
Remove

Example 2: The FTD runs snort version 3.



	Name	Configuration Status	Connectivity
☑	FTDv FTD	Not Synced	● Online
□	FTDv-LC FTD	-	● Pending Setup
□	testftd FTD	-	● Pending Setup

FTDv
FTD

Device Details

Location	n/a
Model	Cisco Firepower Threat Defense for Azure
Serial	[redacted]
Version	7.2.0
Onboarding Method	Registration Key
Snort Version	3.1.21.1-126

Not Synced
The configuration has been modified in FMC. Synchronize your device's configuration by deploying the changes from FMC Deployment page

Related Information

- Cisco Firepower Release Notes, Version 6.7.0
- Cisco Firepower Release Notes, Version 7.0
- Snort 3 Website
- Technical Support & Documentation - Cisco Systems