Welcome

This document contains release information for Version 7.0 of Cisco Firepower Threat Defense, Firepower Management Center, Firepower Device Manager, and Firepower Classic devices (NGIPSv, ASA with FirePOWER Services).

For Cisco Defense Orchestrator (CDO) deployments, see the Cisco Cloud-Delivered Firewall Management Center Release Notes or What's New for Cisco Defense Orchestrator.

- Release Highlights, on page 1
- Release Dates, on page 2
- Sharing Data with Cisco, on page 3
- For Assistance, on page 4

Release Highlights

Release Numbering: Why Version 7.0?

Release numbering skips from Version 6.7 to Version 7.0.

This emphasizes the superior value due to the key new features and functionality introduced over the last several releases, in addition to the multiple performance and security enhancements. There are no unexpected incompatibilities with or limitations to upgrading to Version 7.0. Read these release notes for specific details on compatibility, upgrade requirements, deprecated features and functionality, and so on.

Note that Version 7.0 is an *extra long-term release*, as described in the Cisco's Next Generation Firewall Product Line Software Release and Sustaining Bulletin.

Snort 3 for FTD with FMC Deployments

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

Advantages to using 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 'would have dropped' inline results in intrusion events.
- No Snort restarts when deploying changes 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.

A Snort 3 intrusion rule update is called an *LSP* (Lightweight Security Package) rather than an SRU. The system still uses SRUs for Snort 2; downloads from Cisco contain both the latest LSP and SRU. The system automatically uses the appropriate rule set for your configurations.

The FMC can manage a deployment with both Snort 2 and Snort 3 devices, and will apply the correct policies to each device. However, unlike Snort 2, you cannot update Snort 3 on a device by upgrading the FMC only and then deploying. With Snort 3, new features and resolved bugs require you upgrade the software on the FMC *and* its managed devices. For information on the Snort included with each software version, see the *Bundled Components* section of the Cisco Firepower Compatibility Guide.

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

You can also visit the Snort 3 website: https://snort.org/snort3.

Release Dates

Table 1: Version 7.0 Dates

Version	Build	Date	Platforms
7.0.6.3	50	2024-09-10	All
7.0.6.2	65	2024-04-15	All
7.0.6.1	36	2023-11-13	All
7.0.6	236	2023-07-18	All
7.0.5.1	5	2023-04-26	NGIPSv For devices with security certifications compliance enabled (CC/UCAPL mode). Use with a Version 7.0.5 FMC.
7.0.5	72	2022-11-17	All
7.0.4	55	2022-08-10	All

Version	Build	Date	Platforms
7.0.3	37	2022-06-30	All
7.0.2.1	10	2022-06-27	All
7.0.2	88	2022-05-05	All
7.0.1.1	11	2022-02-17	All
7.0.1	84	2021-10-07	All
7.0.0.1	15	2021-07-15	All
7.0.0	94	2021-05-26	All

Sharing Data with Cisco

The following features share data with Cisco.

Cisco Success Network

Cisco Success Network sends usage information and statistics to Cisco, which are essential to provide you with technical support.

During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time.

Cisco Support Diagnostics

Cisco Support Diagnostics (sometimes called *Cisco Proactive Support*) sends configuration and operational health data to Cisco, and processes that data through our automated problem detection system, allowing us to proactively notify you of issues. This feature also allows Cisco TAC to collect essential information from your devices during the course of a TAC case.

During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time. This feature is not supported with FDM.

Web Analytics

Web analytics provides non-personally-identifiable usage data to Cisco, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your FMCs.

You are enrolled by default but you can change your enrollment at any time after you complete initial setup. Note that ad blockers can block web analytics, so if you choose to remain enrolled, please disable ad blocking for the hostnames/IP addresses of your Cisco appliances.

For Assistance

Upgrade Guides

In management center deployments, the management center must run the same or newer version as its managed devices. Upgrade the management center first, then devices. Note that you always want to use the upgrade guide for the version of management center or device manager that you are *currently* running—not your target version.

Table 2: Upgrade Guides

Platform	Upgrade Guide	Link
Management center	Management center version you are *currently* running.	https://www.cisco.com/go/fmc-upgrade
Threat defense with management center	Management center version you are *currently* running.	https://www.cisco.com/go/ftd-fmc-upgrade
Threat defense with device manager	Threat defense version you are *currently* running.	https://www.cisco.com/go/ftd-fdm-upgrade
Threat defense with cloud-delivered Firewall Management Center	Cloud-delivered Firewall Management Center.	https://www.cisco.com/go/ftd-cdfmc-upgrade

Install Guides

If you cannot or do not want to upgrade, you can freshly install major and maintenance releases. This is also called *reimaging*. You cannot reimage to a patch. Install the appropriate major or maintenance release, then apply the patch. If you are reimaging to an earlier threat defense version on an FXOS device, perform a full reimage—even for devices where the operating system and software are bundled.

Table 3: Install Guides

Platform	Install Guide	Link
Management center hardware	Getting started guide for your management center hardware model.	https://www.cisco.com/go/fmc-install
Management center virtual	Getting started guide for the management center virtual.	https://www.cisco.com/go/fmcv-quick
Threat defense hardware	Getting started or reimage guide for your device model.	https://www.cisco.com/go/ftd-quick
Threat defense virtual	Getting started guide for your threat defense virtual version.	https://www.cisco.com/go/ftdv-quick

Platform	Install Guide	Link
FXOS for the Firepower 4100/9300	Configuration guide for your FXOS version, in the *Image Management* chapter.	https://www.cisco.com/go/firepower9300-config
FXOS for the Firepower 1000/2100 and Secure Firewall 3100/4200	Troubleshooting guide, in the *Reimage Procedures* chapter.	Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense

More Online Resources

Cisco provides the following online resources to download documentation, software, and tools; to query bugs; and to open service requests. Use these resources to install and configure Cisco software and to troubleshoot and resolve technical issues.

- Documentation: http://www.cisco.com/go/threatdefense-70-docs
- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.cisco.com/cisco/support/notifications.html

Access to most tools on the Cisco Support & Download site requires a Cisco.com user ID and password.

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts