

System Requirements

This document includes the system requirements for Version 6.7.

- Device Platforms, on page 1
- FMC Platforms, on page 3
- Manager-Device Compatibility, on page 4

Device Platforms

Cisco Firepower devices monitor network traffic and decide whether to allow or block specific traffic based on a defined set of security rules. Some Firepower devices run Firepower Threat Defense (FTD) software; some run NGIPS/ASA FirePOWER software. Some can run either—but not both at the same time.

Note These release notes list the supported devices for *this* release. Even if an older device has reached EOL and you can no longer upgrade, you can still manage that device with a newer FMC, up to a few versions ahead. Similarly, newer versions of ASDM can manage older ASA FirePOWER modules. For supported management methods, including backwards compatibility, see Manager-Device Compatibility, on page 4. For general compatibility information, see the Cisco Secure Firewall Threat Defense Compatibility Guide or the Cisco Firepower Classic Device Compatibility Guide.

Table 1: Firepower Threat Defense in Version 6.7.0/6.7.x

FTD Platform	OS/Hypervisor	Additional Details
Firepower 1010, 1120, 1140, 1150 Firepower 2110, 2120, 2130, 2140	—	—
Firepower 4110, 4120, 4140, 4150 Firepower 4112, 4115, 4125, 4145 Firepower 9300: SM-24, SM-36, SM-44 modules Firepower 9300: SM-40, SM-48, SM-56 modules	FXOS 2.9.1.131 or later build	Upgrade FXOS first. To resolve issues, you may need to upgrade FXOS to the latest build. To help you decide, see the Cisco FXOS Release Notes, 2.9(1).

FTD Platform	OS/Hypervisor	Additional Details
ASA 5508-X, 5516-X ISA 3000	—	Although you do not separately upgrade the operating system on these devices in FTD deployments, you should make sure you have the latest ROMMON image. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.
Firepower Threat Defense Virtual (FTDv)	Any of: • AWS: Amazon Web Services • Azure: Microsoft Azure • GCP: Google Cloud Platform • OCI: Oracle Cloud Infrastructure • KVM: Kernel-based Virtual Machine • VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7	For supported instances, see the appropriate FTDv Getting Started guide.

Table 2: NGIPS/ASA FirePOWER in Version 6.7.0/6.7.x

NGIPS/ASA FirePOWER Platform	OS/Hypervisor	Additional Details
ASA 5508-X, 5516-X ISA 3000	ASA 9.5(2) to 9.16(x)	There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues. See the Cisco ASA Upgrade Guide for order of operations. You should also make sure you have the latest ROMMON image. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.
NGIPSv	VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7	For supported instances, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.

FMC Platforms

The FMC provides a centralized firewall management console. For device compatibility with the FMC, see Device Management. For general compatibility information, see the Cisco Secure Firewall Management Center Compatibility Guide.

FMC Hardware

Version 6.7 supports the following FMC hardware:

- Firepower Management Center 1600, 2600, 4600
- Firepower Management Center 1000, 2500, 4500

You should also keep the BIOS and RAID controller firmware up to date; see the Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes.

FMCv

Version 6.7 supports FMCv deployments in both public and private clouds.

With the FMCv, you can purchase a license to manage 2, 10, or 25 devices. Some platforms support 300 devices. Note that two-device licenses do not support FMC high availability. For full details on supported instances, see the Cisco Secure Firewall Management Center Virtual Getting Started Guide.

Table 3: Version 6.7 FMCv Platforms

Platform	Devices Managed		High Availability
	2, 10, 25	300	
Public Cloud			
Amazon Web Services (AWS)	YES	—	—
Google Cloud Platform (GCP)	YES	—	—
Microsoft Azure	YES	—	—
Oracle Cloud Infrastructure (OCI)	YES	—	—
Private Cloud			
Kernel-based virtual machine (KVM)	YES	—	—
VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7	YES	YES	YES

Cloud-delivered Firewall Management Center

The Cisco cloud-delivered Firewall Management Center is delivered via the Cisco Defense Orchestrator (CDO) platform, which unites management across multiple Cisco security solutions. We take care of feature

updates. Note that a customer-deployed management center is often referred to as *on-prem*, even for virtual platforms.

At the time this document was published, the cloud-delivered Firewall Management Center could manage devices running threat defense . For up-to-date compatibility information, see the Cisco Cloud-Delivered Firewall Management Center Release Notes.

Manager-Device Compatibility

Firepower Management Center

All devices support remote management with the Firepower Management Center, which can manage multiple devices. The FMC must run the *same or newer* version as its managed devices. You *cannot* upgrade a device past the FMC. Even for maintenance (third-digit) releases, you must upgrade the FMC first.

A newer FMC can manage older devices up to a few major versions back, as listed in the following table. However, we recommend you always update your entire deployment. New features and resolved issues often require the latest release on both the FMC and its managed devices.

Table 4: FMC-Device Compatibility

FMC Version	Oldest Device Version You Can Manage
6.7.x	6.3.0
6.6.x	6.2.3
6.5.0	6.2.3
6.4.0	6.1.0
6.3.0	6.1.0
6.2.3	6.1.0

Firepower Device Manager and Cisco Defense Orchestrator

As an alternative to the FMC, many FTD devices support Firepower Device Manager and Cisco Defense Orchestrator management:

- Firepower Device Manager is built into FTD and can manage a single device.

  This lets you configure the basic features of the software that are most commonly used for small or mid-size networks.

- Cisco Defense Orchestrator (CDO) is cloud-based and can manage multiple FTD devices.

  This allows you to establish and maintain consistent security policies across your deployment without using the FMC. Although some configurations still require FDM, CDO allows you to establish and maintain consistent security policies across multiple Firepower Threat Defense devices.

All FTD devices that support local management with the FDM also support CDO concurrently.

Table 5: FDM/CDO Compatibility with FTD

FTD Platform	FDM Compatibility	CDO Compatibility
Firepower 1000 series	6.4.0+	6.4.0+
Firepower 2100 series	6.2.1+	6.4.0+
Firepower 4100/9300	6.5.0+	6.5.0+
ASA 5500-X series	6.1.0 to 7.0.x	6.4.0 to 7.0.x
ISA 3000	6.2.3+	6.4.0+
FTDv for AWS	6.6.0+	6.6.0+
FTDv for Azure	6.5.0+	6.5.0+
FTDv for GCP	—	—
FTDv for KVM	6.2.3+	6.4.0+
FTDv for OCI	—	—
FTDv for VMware	6.2.2+	6.4.0+

Adaptive Security Device Manager

ASA with FirePOWER Services is an ASA firewall that runs Firepower NGIPS software as a separate application, also called the ASA FirePOWER module. You can use Cisco Adaptive Security Device Manager (ASDM) to manage both applications.

In most cases, newer ASDM versions are backwards compatible with all previous ASA versions. However, there are some exceptions. For example, ASDM 7.13(1) can manage an ASA 5516-X on ASA 9.10(1). ASDM 7.13(1) and ASDM 7.14(1) did not support ASA 5512-X, 5515-X, 5585-X, and ASASM; you must upgrade to ASDM 7.13(1.101) or 7.14(1.48) to restore ASDM support. For details, see Cisco ASA Compatibility.

A newer ASA FirePOWER module requires a newer version of ASDM, as listed in the following table.

Table 6: ASDM-ASA FirePOWER Compatibility

ASA FirePOWER Version	Minimum ASDM Version
6.7.x	7.15.1
6.6.x	7.14.1
6.5.0	7.13.1
6.4.0	7.12.1
6.3.0	7.10.1
6.2.3	7.9.2