

System Requirements

This document includes the system requirements for Version 6.4.

- FMC Platforms, on page 1
- Device Platforms, on page 2
- Device Management, on page 5

FMC Platforms

The FMC provides a centralized firewall management console. For device compatibility with the FMC, see Device Management, on page 5. For general compatibility information, see the Cisco Secure Firewall Management Center Compatibility Guide.

FMC Hardware

Version 6.4 supports the following FMC hardware:

- Firepower Management Center 1600, 2600, 4600
- Firepower Management Center 1000, 2500, 4500
- Firepower Management Center 2000, 4000
- Firepower Management Center 750, 1500, 3500 (high availability not supported for FMC 750)

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 6.4 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 versions and platforms support 300 devices. For full details on supported instances, see the Cisco Secure Firewall Management Center Virtual Getting Started Guide.

Table 1: Version 6.4 FMCv Platforms

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

Cloud-delivered Firewall Management Center

The Cisco Cloud-delivered Firewall Management Center is delivered via Firewall in Cisco Security Cloud Control, which unites management across multiple Cisco security solutions. We take care of feature updates. Note that a customer-deployed management center is referred to as *on-prem*, even for public cloud deployments.

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.

Device Platforms

Firepower devices monitor network traffic and decide whether to allow or block specific traffic based on a defined set of security rules. For details on device management methods, see Device Management, on page 5. For general compatibility information, see the Cisco Secure Firewall Threat Defense Compatibility Guide or the Cisco Firepower Classic Device Compatibility Guide.

FTD Hardware

Version 6.4 FTD hardware comes in a range of throughputs, scalability capabilities, and form factors.

Table 2: Version 6.4 FTD Hardware

Platform	FMC Compatibility		FDM Compatibility		Notes
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO	
Firepower 1010, 1120, 1140	YES	—	YES	YES	—
Firepower 2110, 2120, 2130, 2140	YES	—	YES	YES	—

Platform	FMC Compatibility		FDM Compatibility		Notes
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO	
Firepower 4110, 4120, 4140, 4150 Firepower 4115, 4125, 4145 Firepower 9300: SM-24, SM-36, SM-44 modules Firepower 9300: SM-40, SM-48, SM-56 modules	YES	—	—	—	Requires FXOS 2.6.1.157 or later build. We recommend the latest firmware. See the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.
ASA 5515-X ASA 5508-X, 5516-X ASA 5525-X, 5545-X, 5555-X	YES	—	YES	YES	ASA 5508-X and 5516-X devices may require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
ISA 3000	YES	—	YES	YES	May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

FTDv

Version 6.4 supports the following FTDv implementations. For information on supported instances, throughputs, and other hosting requirements, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.

Table 3: Version 6.4 FTDv Platforms

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO
Public Cloud				
Amazon Web Services (AWS)	YES	—	—	—
Microsoft Azure	YES	—	—	—
Private Cloud				
Kernel-based virtual machine (KVM)	YES	—	YES	YES

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO
VMware vSphere/VMware ESXi 6.0 or 6.5	YES	—	YES	YES

Firepower Classic: Firepower 7000/8000, ASA FirePOWER, NGIPSv

Firepower Classic devices run NGIPS software on the following platforms:

- Firepower 7000/8000 series hardware comes in a range of throughputs, scalability capabilities, and form factors.
- ASA devices can run NGIPS software as a separate application (the *ASA FirePOWER module*). Traffic is sent to the module after ASA firewall policies are applied. Although there is wide compatibility between ASA and ASA FirePOWER versions, upgrading allows you to take advantage of new features and resolved issues.
- NGIPSv runs the software in virtualized environments.

Table 4: Version 6.4 NGIPS Platforms

Device Platform	FMC Compatibility	ASDM Compatibility	Notes
Firepower 7010, 7020, 7030, 7050 Firepower 7110, 7115, 7120, 7125 Firepower 8120, 8130, 8140 Firepower 8250, 8260, 8270, 8290 Firepower 8350, 8360, 8370, 8390 AMP 7150, 8050, 8150 AMP 8350, 8360, 8370, 8390	YES	—	—
ASA 5508-X, 5516-X	YES	Requires ASDM 7.12(1).	Requires ASA 9.5(2) to 9.16(x). May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
ASA 5515-X	YES	Requires ASDM 7.12(1).	Requires ASA 9.5(2) to 9.12(x).

Device Platform	FMC Compatibility	ASDM Compatibility	Notes
ASA 5525-X, 5545-X, 5555-X	YES	Requires ASDM 7.12(1).	Requires ASA 9.5(2) to 9.14(x).
ISA 3000	YES	Requires ASDM 7.12(1).	Requires ASA 9.5(2) to 9.16(x). May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
NGIPSv	YES	—	Requires VMware vSphere/VMware ESXi 6.0 or 6.5. For supported instances, throughputs, and other hosting requirements, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.

Device Management

Depending on device model and version, we support the following management methods.

On-Prem FMC

All devices support remote management with a customer-deployed (*on-prem*) FMC.

Versions are major (A.x), maintenance (A.x.y), or patch (A.x.y.z). The management center should run the same or newer version as its devices. New features and resolved issues often require the latest version on both the FMC and its devices, including patches. Upgrade the FMC first—you will still be able to manage older devices, usually a few major versions back

Note You cannot upgrade a device past the FMC to a newer major or maintenance version. Although a patched device (fourth-digit) can be managed with an unpatched FMC, fully patched deployments undergo enhanced testing.

Note that in most cases you can upgrade an older device directly to the FMC's major or maintenance version. However, sometimes you can manage an older device that you cannot directly upgrade, even though the target version is supported on the device. Rarely, there are issues with specific FMC-device combinations. For release-specific requirements, see Upgrade Guidelines.

Table 5: On-Prem FMC-Device Compatibility

FMC Version	Oldest Device Version You Can Manage
7.7	7.2
7.6	7.1

FMC Version	Oldest Device Version You Can Manage
7.4 Last support for NGIPS device management.	7.0
7.3	6.7
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3
6.5	6.2.3
6.4	6.1
6.3	6.1
6.2.3	6.1
6.2.2	6.1
6.2.1	6.1
6.2	6.1
6.1	5.4.0.2/5.4.1.1
6.0.1	5.4.0.2/5.4.1.1
6.0	5.4.0.2/5.4.1.1
5.4.1	5.4.1 for ASA FirePOWER on the ASA-5506-X series, ASA5508-X, and ASA5516-X. 5.3.1 for ASA FirePOWER on the ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, and ASA-5585-X series. 5.3.0 for Firepower 7000/8000 series and legacy devices.

FDM

You can use FDM to locally manage a single FTD device. Most models suppport local management.

Optionally, add Cisco Security Cloud Control to remotely manage multiple FTD devices, as an alternative to the FMC. Although some configurations still require FDM, Security Cloud Control allows you to establish and maintain consistent security policies across your FTD deployment.

ASDM

You can use ASDM to locally manage a single ASA FirePOWER module, which is a separate application on an ASA device. Traffic is sent to the module after ASA firewall policies are applied. Newer versions of ASDM can manage newer ASA FirePOWER modules.