Compatibility

For general compatibility information see:

- Cisco Firepower Compatibility Guide: Detailed compatibility information for all supported versions, including versions and builds of bundled operating systems and other components, as well as links to end-of-sale and end-of-life announcements for deprecated platforms.
- Cisco NGFW Product Line Software Release and Sustaining Bulletin: Support timelines for the Cisco Next Generation Firewall product line, including management platforms and operating systems.

For compatibility information for this version, see:

Firepower Management Center

The Firepower Management Center is a fault-tolerant, purpose-built network appliance that provides a centralized firewall management console. Firepower Management Center Virtual brings full firewall management functionality to virtualized environments.

Firepower Management Center

This release supports the following hardware FMC platforms:

- FMC 1600, 2600, 4600
- FMC 1000, 2500, 4500
- FMC 2000, 4000

We recommend you keep the BIOS and RAID controller firmware up to date. For more information, see the Cisco Firepower Compatibility Guide.

Firepower Management Center Virtual

This release supports the following FMCv public cloud implementations:

- Firepower Management Center Virtual for Amazon Web Services (AWS)
- Firepower Management Center Virtual for Microsoft Azure

This release supports the following FMCv on-prem/private cloud implementations:

- Firepower Management Center Virtual for Kernel-based virtual machine (KVM)
- Firepower Management Center Virtual for VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7

For supported instances, see the Cisco Firepower Management Center Virtual Getting Started Guide.

Firepower Devices

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 3.

Table 1: Firepower Threat Defense in Version 6.5.0

FTD Platform	OS/Hypervisor	Additional Details
Firepower 1010, 1120, 1140, 1150 Firepower 2110, 2120, 2130, 2140	—	—
Firepower 4110, 4120, 4140, 4150 Firepower 4115, 4125, 4145 Firepower 9300 with SM-24, SM-36, SM-44 modules Firepower 9300 with SM-40, SM-48, SM-56 modules	FXOS 2.7.1.92 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, 2.7(1).
ASA 5508-X, 5516-X ASA 5525-X, 5545-X, 5555-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 on the ISA 3000, ASA 5508-X and 5516-X. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.

FTD Platform	OS/Hypervisor	Additional Details
FTDv	Any of: • AWS: Amazon Web Services • Azure: Microsoft Azure • 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 6.5.0

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 on the ISA 3000, ASA 5508-X and 5516-X. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.
ASA 5525-X, 5545-X, 5555-X	ASA 9.5(2) to 9.14(x)	
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.

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 3: 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 FTD devices.

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

Table 4: 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 KVM	6.2.3+	6.4.0+
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 5: 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

Web Browser Compatibility

Browsers

We test with the latest versions of the following popular browsers, running on currently supported versions of macOS and Microsoft Windows:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer 11 (Windows only)

If you encounter issues with any other browser, or are running an operating system that has reached end of life, we ask that you switch or upgrade. If you continue to encounter issues, contact Cisco TAC.

Note We do not perform extensive testing with Apple Safari or Microsoft Edge, nor do we test Microsoft Internet Explorer with FMC walkthroughs. However, Cisco TAC welcomes feedback on issues you encounter.

Browser Settings and Extensions

Regardless of browser, you must make sure JavaScript, cookies, and TLS v1.2 remain enabled.

If you are using Microsoft Internet Explorer 11:

- For the **Check for newer versions of stored pages** browsing history option, choose **Automatically**.
- Disable the **Include local directory path when uploading files to server** custom security setting.
- Enable **Compatibility View** for the appliance IP address/URL.

Note that some browser extensions can prevent you from saving values in fields like the certificate and key in PKI objects. These extensions include, but are not limited to, Grammarly and Whatfix Editor. This happens because these extensions insert characters (such as HTML) in the fields, which causes the system to see them invalid. We recommend you disable these extensions while you're logged into our products.

Securing Communications

When you first log in, the system uses a self-signed digital certificate to secure web communications. Your browser should display an untrusted authority warning, but also should allow you to add the certificate to the trust store. Although this will allow you to continue, we do recommend that you replace the self-signed certificate with a certificate signed by a globally known or internally trusted certificate authority (CA).

To begin replacing the self-signed certificate:

- Firepower Management Center: Select **System** > **Configuration**, then click **HTTPS Certificates**.
- Firepower Device Manager: Click **Device**, then the **System Settings** > **Management Access** link, then the **Management Web Server** tab.

For detailed procedures, see the online help or the configuration guide for your product.

Note If you do not replace the self-signed certificate:

- Google Chrome does not cache static content, such as images, CSS, or JavaScript. Especially in low bandwidth environments, this can extend page load times.
- Mozilla Firefox can stop trusting the self-signed certificate when the browser updates. If this happens, you can refresh Firefox, keeping in mind that you will lose some settings; see Mozilla's Refresh Firefox support page.

Browsing from a Monitored Network

Many browsers use Transport Layer Security (TLS) v1.3 by default. If you are using an SSL policy to handle encrypted traffic, and people in your monitored network use browsers with TLS v1.3 enabled, websites that support TLS v1.3 may fail to load.

For more information, see the software advisory titled: *Failures loading websites using TLS 1.3 with SSL inspection enabled*.

Screen Resolution Requirements

Table 6: Screen Resolution Requirements

Interface	Resolution
Firepower Management Center	1280 x 720
Firepower Device Manager	1024 x 768
ASDM managing an ASA FirePOWER module	1024 x 768
Firepower Chassis Manager for the Firepower 4100/9300	1024 x 768