Compatibility

For detailed compatibility information for all supported Firepower versions, including links to end-of-sale and end-of-life announcements for deprecated platforms, see the Cisco Firepower Compatibility Guide.

For compatibility information for this Firepower version, see:

Firepower Management Centers

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

Firepower Management Center

The following FMC platforms are supported in this release:

- FMC 1000, 2500, 4500
- FMC 2000, 4000
- FMC 750, 1500, 3500

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

The following FMCv implementations are supported in this release:

- FMCv for VMware vSphere/VMware ESXi 5.5, 6.0, or 6.5
- FMCv for Kernel-based virtual machine (KVM)
- FMCv for Amazon Web Services (AWS)

For supported FMCv 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.

The following tables list the device platforms supported in this release, along with any (separately upgradeable) OS/hypervisor requirements. For versions and builds of bundled operating systems, see the *Bundled Components* information in the Cisco Firepower Compatibility Guide.

Note These are 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.

Firepower Threat Defense Devices

These FTD devices are supported in this release.

Table 1: FTD in Version 6.2.3

FTD Platform	OS/Hypervisor	Additional Details
Firepower 2110, 2120, 2130, 2140	—	—
Firepower 4110, 4120, 4140, 4150 Firepower 9300: SM-24, SM-36, SM-44 modules	FXOS 2.3.1.73+. **Note** Firepower 6.2.3.16+ requires FXOS 2.3.1.157+.	Upgrade FXOS first. To resolve issues, you may need to upgrade FXOS to the latest build. To help you decide, see the Cisco Firepower 4100/9300 FXOS Release Notes, 2.3(1).
ASA 5506-X, 5506H-X, 5506W-X ASA 5508-X, 5516-X ASA 5512-X ASA 5515-X ASA 5525-X, 5545-X, 5555-X ISA 3000	—	Although you do not separately upgrade the OS on these devices in FTD deployments, you should make sure you have the latest ROMMON image on the ISA 3000, ASA 5506-X, 5508-X, and 5516-X. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.

FTD Platform	OS/Hypervisor	Additional Details
Firepower Threat Defense Virtual (FTDv)	Any of: • VMware vSphere/VMware ESXi 5.5, 6.0, or 6.5 • KVM • AWS • Microsoft Azure	For supported instances, see the appropriate FTDv Getting Started guide.

NGIPS/ASA FirePOWER Devices

These NGIPS/ASA FirePOWER devices are supported in this release.

Table 2: NGIPS/ASA FirePOWER in Version 6.2.3

NGIPS Platform	OS/Hypervisor	Additional Details
ASA 5506-X, 5506H-X, 5506W-X	ASA 9.6(x) to 9.9(x)	There is wide compatibility between ASA and ASA FirePOWER versions. However, even if an ASA upgrade is not strictly required, resolving issues may require an upgrade to the latest supported version. 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 5506-X, 5508-X, and 5516-X. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.
ASA 5508-X, 5516-X	ASA 9.5(2) to 9.14(x)	
ASA 5512-X	ASA 9.5(2) to 9.9(x)	
ASA 5515-X	ASA 9.5(2) to 9.12(x)	
ASA 5525-X, 5545-X, 5555-X	ASA 9.5(2) to 9.14(x)	
ASA 5585-X-SSP-10, -20, -40, -60	ASA 9.5(2) to 9.12(x)	
NGIPSv	VMware vSphere/VMware ESXi 5.5, 6.0, or 6.5	For supported instances, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.
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	—	—

Manager-Device Compatibility

Firepower Management Center

All Firepower devices support remote management with a Firepower Management Center (FMC), which can manage multiple devices. An newer FMC can manage older devices up to a few major versions back. But, you cannot upgrade a device past the FMC. In other words, the FMC must run the *same or newer* version as its managed devices.

For this release:

- Version 6.2.3 FMC *can manage* Version 6.1.0 through 6.2.3 devices.
- Version 6.2.3 devices *require* a Version 6.2.3 FMC.

Note that technically you can manage a patched device (fourth-digit release) with an unpatched FMC. However, we *strongly* recommend against it. You should always update your entire deployment. New features and resolved issues often require the latest release on *both* the FMC and its managed devices.

Firepower Device Manager

Firepower Device Manager (FDM) can manage a single FTD device. FDM lets you configure the basic features of the software that are most commonly used for small or mid-size networks.

Because FDM is built into FTD, there is no concept of manager-device compatibility in this type of deployment.

For this release, the following FTD devices support FDM:

- Firepower 2100 series
- ASA 5500-X series
- ISA 3000
- FTDv for VMware, KVM

Adaptive Security Device Manager

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

Although there is wide compatibility between ASA, ASDM, and ASA FirePOWER versions, some newer versions of ASDM may not be able to manage ASA FirePOWER modules on some older ASA devices. For details, see Cisco ASA Compatibility.

For this release:

- Version 7.9.2 ASDM *can manage* Version 6.2.3 and earlier ASA FirePOWER modules.
- Version 6.2.3 ASA FirePOWER modules *require* Version 7.9.2 ASDM.

Web Browser Compatibility

Browsers Tested with Firepower Web Interfaces

Firepower web interfaces are tested 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 10 and 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 on this Firepower version with Apple Safari or Microsoft Edge. 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 10 or 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 (Internet Explorer 11 only).
- Enable **Compatibility View** for the Firepower web interface 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 Firepower appliances.

Securing Communications

When you first log in to a Firepower web interface, 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 to the Firepower web interface, 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:

- FMC or 7000/8000 series: Select **System** > **Configuration**, then click **HTTPS Certificates**.
- FDM: 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 Firepower 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 Firepower-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 fail to load. As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation.

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

Screen Resolution Requirements

Table 3: Screen Resolution Requirements for Firepower User Interfaces

Interface	Resolution
Firepower Management Center	1280 x 720
7000/8000 series device (limited local interface)	1280 x 720
Firepower Device Manager	1024 x 768
ASDM managing an ASA FirePOWER module	1024 x 768
Firepower Chassis Manager for Firepower 9300 chassis	1024 x 768

Additional Compatibility Resources

This table provides links to release notes and additional compatibility information. For full documentation roadmaps, see Documentation Roadmaps.

Table 4: Additional Compatibility Resources

Description	Resources
Compatibility guides provide detailed compatibility information for supported hardware models and software versions, including bundled components and integrated products.	Cisco Firepower Compatibility Guide Cisco ASA Compatibility Cisco Firepower 4100/9300 FXOS Compatibility
Release notes provide critical and release-specific information, including upgrade warnings and behavior changes.	Cisco Firepower Release Notes Cisco ASA Release Notes Cisco Firepower 4100/9300 FXOS Release Notes
Sustaining bulletins provide support timelines for the Cisco Next Generation Firewall product line, including management platforms and operating systems.	Cisco NGFW Product Line Software Release and Sustaining Bulletin