System Requirements

This document includes the system requirements for Version 6.2.3.

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 6.2.3 supports the following FMC hardware:

- 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 6.2.3 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 6.2.3 FMCv Platforms

Platform	Devices Managed		High Availability
	2, 10, 25	300	
Public Cloud			
Amazon Web Services (AWS)	YES	—	—
Private Cloud			
Kernel-based virtual machine (KVM)	YES	—	—
VMware vSphere/VMware ESXi 5.5, 6.0, or 6.5	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.

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

Table 2: Version 6.2.3 FTD Hardware

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

Platform	FMC Compatibility		FDM Compatibility		Notes
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO	
Firepower 4110, 4120, 4140, 4150 Firepower 9300: SM-24, SM-36, SM-44 modules	YES	—	—	—	Requires FXOS 2.3.1.73 or later build. **Note** Firepower 6.2.3.16+ requires FXOS 2.3.1.157+. We recommend the latest firmware. See the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.
ASA 5506-X, 5506H-X, 5506W-X ASA 5512-X ASA 5515-X ASA 5508-X, 5516-X ASA 5525-X, 5545-X, 5555-X	YES	—	YES	—	ASA 5506-X, 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	—	May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

FTDv

Version 6.2.3 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 6.2.3 FTDv Platforms

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO
Public Cloud				
Amazon Web Services (AWS)	YES	—	—	—

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO
Microsoft Azure	YES	—	—	—
Private Cloud				
Kernel-based virtual machine (KVM)	YES	—	YES	—
VMware vSphere/VMware ESXi 5.5, 6.0, or 6.5	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 6.2.3 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	—	—

Device Platform	FMC Compatibility	ASDM Compatibility	Notes
ASA 5506-X, 5506H-X, 5506W-X	YES	Requires ASDM 7.9(2).	Requires ASA 9.6(x) to 9.9(x). May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
ASA 5508-X, 5516-X	YES	Requires ASDM 7.9(2).	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 5512-X	YES	Requires ASDM 7.9(2).	Requires ASA 9.5(2) to 9.9(x).
ASA 5515-X	YES	Requires ASDM 7.9(2).	Requires ASA 9.5(2) to 9.12(x).
ASA 5525-X, 5545-X, 5555-X	YES	Requires ASDM 7.9(2).	Requires ASA 9.5(2) to 9.14(x).
NGIPSv	YES	—	Requires VMware vSphere/VMware ESXi 5.5, 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.

FMC

All devices support remote management with FMC, which must run the *same or newer* version as its managed devices. This means:

- You *can* manage older devices with a newer FMC, usually a few major versions back. 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.
- You *cannot* upgrade a device past the FMC. Even for maintenance (third-digit) releases, you must upgrade the FMC first.

Note that in most cases you can upgrade an older device directly to the FMC's major version. However, sometimes you can manage an older device that you cannot directly upgrade, even though the target version is supported on the device. For release-specific requirements, see Minimum Version to Upgrade.

Table 5: FMC-Device Compatibility

FMC Version	Oldest Device Version You Can Manage
7.4	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.

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.

Browser Requirements

Browsers

We test with the latest versions of these 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 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 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.

Screen Resolution

Interface	Minimum Resolution
FMC	1280 x 720
7000/8000 series device (limited local interface)	1280 x 720
FDM	1024 x 768
ASDM managing an ASA FirePOWER module	1024 x 768
Firepower Chassis Manager for the Firepower 4100/9300	1024 x 768

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:

- FMC or 7000/8000 series: Choose **System** (⚙) > **Configuration** > **HTTPS Certificate**.
- 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 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 fail to load. As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation. In Version 6.2.3.7+, a new CLI command allows you to specify when to downgrade; see New Features.

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