Platforms and Environments

The following sections describe the supported platforms and environments in Version 6.2.2, as well as compatibility guidelines:

Supported Platforms and Environments

Specific manager-device compatibility depends on the version of both the manager and device. A Firepower Management Center running Version 6.2.2 can manage the following devices:

- Firepower 2100 series devices—Version 6.2.1, Version 6.2.2
- All other Firepower devices—Version 6.1.0 or later, Version 6.2.0 or later, Version 6.2.2 or later

However, keep in mind that many features depend on the version of the system running on the device. Even if a Firepower Management Center is running Version 6.2.2, your deployment may not support all its features until you also update managed devices to Version 6.2.2.

We *strongly* recommend upgrading the Firepower Management Center to the same maintenance release or later as the version you upgrade the managed device to. As an example, we recommend a Firepower Management Center run at least Version 6.2.2.1 before you upgrade a managed device to Version 6.2.2.1.

For smaller deployments, you can manage devices either locally or with a Firepower Management Center. On specific platforms, you can use Firepower Device Manager to manage Firepower Threat Defense. You can also use ASDM to manage ASA FirePOWER modules. You can use only one management method for a device at a time.

Supported Firepower Management Center

The following table lists supported Firepower Management Center platforms, and their operating system or hosting environment requirements.

Platform	OS/Hosting Environments
Firepower Management Center: MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500	Firepower Threat Defense
Firepower Management Center Virtual (64-bit)	VMware vSphere/VMware ESXi 5.5 VMware vSphere/VMware ESXi 6.0 Amazon Web Services (AWS) VPC/EC2 Kernel-based virtual machine (KVM)

Supported Devices in Version 6.2.2

The following table lists supported device platforms and their supported implementations, management methods, and operating system or hosting environment requirements.

Platform	Implementations	Managers	OS/Hosting Environments
Firepower 2110, 2120, 2130, 2140	Firepower Threat Defense	Firepower Device Manager Firepower Management Center	Firepower Threat Defense
Firepower 4110, 4120, 4140, 4150 Firepower 9300 with SM-24, SM-36, or SM-44 modules	Firepower Threat Defense	Firepower Management Center	FXOS 2.2(2) FXOS 2.2(2.x) **Caution** Do *not* update to FXOS Version 2.3.1.56 if you are running an instance of Firepower Threat Defense that has been updated from Version 6.0.1.x of the Firepower System. Doing so may disable your Firepower Threat Defense application, which could interrupt traffic on your network. As a workaround, use FXOS Version 2.3.1.58 or later. For more information, see CSCvh64138 in the Cisco Bug Search Tool.

Platform	Implementations	Managers	OS/Hosting Environments
ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X ASA5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X	Firepower Threat Defense ASA FirePOWER module	Firepower Device Manager, for Firepower Threat Defense ASDM 7.8(2), for ASA FirePOWER Firepower Management Center, for either	Firepower Threat Defense ASA OS, for ASA FirePOWER: • 9.5(2), 9.5(3) except 5506 models • 9.6(x) • 9.7(x) • 9.8(x) Note that the ASA 5506-X does not support the ASA FirePOWER module when running ASA Version 9.5(x).
ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, ASA5585-X-SSP-60	ASA FirePOWER module	ASDM 7.8(2) Firepower Management Center	ASA OS: • 9.5(2), 9.5(3) • 9.6(x) • 9.7(x) • 9.8(x)
Virtual: VMware	Firepower Threat Defense Virtual NGIPSv	Firepower Device Manager, for Firepower Threat Defense Firepower Management Center, for either	VMware vSphere/VMware ESXi 5.5 VMware vSphere/VMware ESXi 6.0
Virtual: AWS	Firepower Threat Defense Virtual	Firepower Management Center	Amazon Web Services (AWS) EC2/VPC
Virtual: KVM	Firepower Threat Defense Virtual	Firepower Management Center	Kernel-based virtual machine (KVM)
Virtual: Azure	Firepower Threat Defense Virtual	Firepower Management Center	Microsoft Azure Standard D3 Microsoft Azure Standard D3_v2
Firepower 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125 Firepower 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390 AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390	NGIPS	Firepower Management Center	Firepower Management Center

Integrated Product Compatibility

You can integrate a variety of products with Firepower, including:

- Cisco Identity Services Engine (ISE and ISE-PIC)
- Cisco AMP Threat Grid
- Cisco Terminal Services (TS) Agent
- Cisco AnyConnect Secure Mobility Client
- Cisco Firepower System User Agent

See the Firepower System Compatibility Guide for required versions of these integrated products,.

Web Browser Compatibility for Version 6.2.2

The Firepower web interfaces for Version 6.2.2 have been tested on the following browsers:

Table 1: Supported Web Browsers

Browser	Required Settings
Google Chrome 57	JavaScript, cookies **Caution** The Chrome browser does not cache static content, such as images, CSS, or JavaScript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add the self-signed certificate used by the Firepower system to the trust store of the browser/OS or use another web browser..
Mozilla Firefox 52	JavaScript, cookies, Transport Layer Security (TLS) v1.2 The Firepower Management Center uses a self-signed certificate by default; we recommend you replace that certificate with a certificate signed by a trusted certificate authority. For information on replacing server certificates, see the Firepower Management Center Configuration Guide. **Tip** If you use a self-signed certificate on the Firepower Management Center and the Login screen takes a long time to load, enter **about:support** in a Firefox browser search bar and click **Refresh Firefox**. You may lose existing Firefox settings when you refresh. For more information, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings. **Caution** Firefox 56 incorrectly displays HTML instead of the Firepower Management Center UI . We *strongly* recommend using Firefox 55 or earlier or Firefox 57 or later.

Browser	Required Settings
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, Transport Layer Security (TLS) v1.2, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically** **Note** If you use the Microsoft Internet Explorer 11 browser, you must also disable the **Include local directory path when uploading files to server** option in your Internet Explorer settings via **Tools > Internet Options > Security > Custom level**.
Apple Safari	Not supported.
Microsoft Edge	Not supported.

Note Many browsers use Transport Layer Security (TLS) v1.3 by default. If you have an active SSL policy and your browser uses TLSv1.3, websites that support TLSv1.3 fail to load As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation. See this software advisory for more information.

Screen Resolution Compatibility

Firepower user interfaces are not compatible with lower screen resolutions than those recommended in the following table:

Table 2: Recommended Screen Resolutions

User Interface	Minimum Recommended Resolution
Firepower Management Center 7000 and 8000 Series devices (limited local web interface) Firepower 4100 and Firepower 9300 devices	At least 1280 pixels wide
ASDM (managing ASA FirePOWER)	1024 pixels wide by 768 pixels high
Firepower Device Manager (managing Firepower Threat Defense)	1024 pixels wide by 768 pixels high