System Requirements

This document includes the system requirements for Version 7.2.

Management Center Platforms

The management center provides a centralized firewall management console. For device compatibility with the management center, see Threat Defense Management, on page 4. For general compatibility information, see the Cisco Secure Firewall Management Center Compatibility Guide.

Management Center Hardware

Version 7.2 supports the following management center hardware:

- Secure Firewall Management Center 1600
- Secure Firewall Management Center 2600
- Secure Firewall Management Center 4600

You should also keep the BIOS and RAID controller firmware up to date; see the Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes.

Management Center Virtual

Version 7.2 supports management center virtual deployments in both public and private/on-prem clouds.

With the management center virtual, you can purchase licenses that enable you to manage 2, 10, 25, or 300 devices. Note that only some platforms support 300 devices. Also, two-device virtual management centers do not support high availability. For full details on supported instances, see the Cisco Secure Firewall Management Center Virtual Getting Started Guide.

Table 1: Version 7.2 Management Center Virtual Platforms

Platform	Devices Managed		High Availability
	2, 10, 25	300	
Public Cloud			
Alibaba	YES	—	—
Amazon Web Services (AWS)	YES	YES	YES
Google Cloud Platform (GCP)	YES	—	—
Microsoft Azure	YES	—	—
Oracle Cloud Infrastructure (OCI)	YES	YES	YES
On-Prem/Private Cloud			
Cisco HyperFlex	YES	—	YES
Kernel-based virtual machine (KVM)	YES	—	—
Nutanix Enterprise Cloud	YES	—	—
OpenStack	YES	—	—
VMware vSphere/VMware ESXi 6.5, 6.7, or 7.0	YES	YES	YES

Cloud-Delivered 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. The cloud-delivered Firewall Management Center does not have a version, and we take care of feature updates.

Note that the customer-deployed management center is often referred to as the *on-prem* management center, even for virtual platforms.

For upgrade guidelines, see Upgrade Guidelines for Cloud-delivered Firewall Management Center.

Threat Defense Platforms

Threat defense 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 Threat Defense Management, on page 4. For general compatibility information, see the Cisco Secure Firewall Threat Defense Compatibility Guide.

Threat Defense Hardware

Version 7.2 threat defense hardware comes in a range of throughputs, scalability capabilities, and form factors.

Table 2: Version 7.2 Threat Defense Hardware

Platform	Management Center Compatibility		Device Manager Compatibility		Notes
	Customer Deployed	Cloud Delivered	Device Manager Only	Device Manager + CDO	
Firepower 1010E, 1010, 1120, 1140, 1150	YES	YES	YES	YES	Firepower 1010E requires Version 7.2.3+. Do not use a Version 7.2.3 or Version 7.3.0 management center to manage the Firepower 1010E. Instead, use a Version 7.2.3.1+ or Version 7.3.1.1+ management center.
Firepower 2110, 2120, 2130, 2140	YES	YES	YES	YES	—
Secure Firewall3110, 3120, 3130, 3140	YES	YES	YES	YES	—
Firepower 4110, 4120, 4140, 4150 Firepower 4112, 4115, 4125, 4145 Firepower 9300: SM-24, SM-36, SM-44 modules Firepower 9300: SM-40, SM-48, SM-56 modules	YES	YES	YES	YES	Requires FXOS 2.12.0.31 or later build. We recommend the latest firmware. See the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.
ISA 3000	YES	YES	YES	YES	May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

Threat Defense Virtual

Version 7.2 threat defense virtual implementations support performance-tiered Smart Software Licensing, based on throughput requirements and remote access VPN session limits. Options run from FTDv5 (100 Mbps/50 sessions) to FTDv100 (16 Gbps/10,000 sessions). For more information on supported instances, throughputs, and other hosting requirements, see the appropriate *Getting Started Guide*.

Table 3: Version 7.2 Threat Defense Virtual Platforms

Device Platform	Management Center Compatibility		Device Manager Compatibility	
	Customer Deployed	Cloud Delivered	Device Manager Only	Device Manager + CDO
Public Cloud				
Alibaba	YES	YES	—	—
Amazon Web Services (AWS)	YES	YES	YES	YES
Microsoft Azure	YES	YES	YES	YES
Google Cloud Platform (GCP)	YES	YES	YES	YES
Oracle Cloud Infrastructure (OCI)	YES	YES	—	—
On-Prem/Private Cloud				
Cisco Hyperflex	YES	YES	YES	YES
Kernel-based virtual machine (KVM)	YES	YES	YES	YES
Nutanix Enterprise Cloud	YES	YES	YES	YES
OpenStack	YES	YES	—	—
VMware vSphere/VMware ESXi 6.5, 6.7, or 7.0	YES	YES	YES	YES

Threat Defense Management

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

Customer-Deployed Management Center

All devices support remote management with a customer-deployed management center, which must run the *same or newer* version as its managed devices. This means:

- You *can* manage older devices with a newer management center, 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 management center and its managed devices.
- You *cannot* upgrade a device past the management center. Even for maintenance (third-digit) releases, you must upgrade the management center first.

Note that in most cases you can upgrade an older device directly to the management center'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. For release-specific requirements, see Minimum Version to Upgrade. Rarely, there are issues with specfic management center-device combinations, which would be listed in Threat Defense Platforms, on page 2.

Table 4: Customer-Deployed Management Center-Device Compatibility

Management Center 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.

Cloud-delivered Firewall Management Center

The cloud-delivered Firewall Management Center can manage threat defense devices running:

- Version 7.2+

- Version 7.0.3 and later maintenance releases

The cloud-delivered Firewall Management Center cannot manage threat defense devices running Version 7.1, or Classic devices running any version. You cannot upgrade a cloud-managed device from Version 7.0.x to Version 7.1 unless you unregister and disable cloud management. We recommend you upgrade the device directly to Version 7.2+.

You can add a cloud-managed device to a Version 7.2+ customer-deployed management center for event logging and analytics purposes only. Or, you can send security events to the Cisco cloud with Security Analytics and Logging (SaaS).

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 Edge (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, nor do we extensively test Microsoft Edge 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 Edge, do *not* enable IE mode.

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
Management Center	1280 x 720
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, choose **System** (⚙) > **Configuration** > **HTTPS Certificate**.

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

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*.