

System Requirements

This document includes the system requirements for Version 7.2.

- Firewall Management Center Platforms, on page 1
- Firewall Threat Defense Platforms, on page 2
- Firewall Threat Defense Management, on page 4

Firewall Management Center Platforms

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

Firewall Management Center Hardware

Version 7.2 supports the following Firewall Management Center hardware:

- Firepower Management Center 1600
- Firepower Management Center 2600
- Firepower Management Center 4600

You should also keep the BIOS and RAID controller firmware up to date; see the Secure Firewall Threat Defense/Firepower hotfix release notes.

Firewall Management Center Virtual

Version 7.2 supports Firewall Management Center Virtual deployments in both public and private clouds.

With the Firewall Management Center Virtual, you can purchase a license to manage 2, 10, or 25 devices. Some platforms support 300 devices. Note that two-device licenses do not support Firewall Management Center high availability. For full details on supported instances, see the *Cisco Secure Firewall Management Center Virtual Getting Started Guide*.

Table 1: Version 7.2 Firewall 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
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 Firewall Management Center

is delivered via Security Cloud Control, which unites management across multiple Cisco security solutions. We take care of feature updates. Note that a customer-deployed Firewall Management Center is referred to as *on-prem*, even for public cloud deployments.

For up-to-date compatibility information, see the *Cisco Secure Firewall Management Center Compatibility Guide*.

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

Firewall Threat Defense Hardware

Version 7.2 Firewall Threat Defense hardware comes in a range of throughputs, scalability capabilities, and form factors.

Table 2: Version 7.2 Firewall Threat Defense Hardware

Platform	Firewall Management Center Compatibility		Firewall Device Manager Compatibility		Notes
	Customer Deployed	Cloud Delivered	Firewall Device Manager Only	Firewall 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 Firewall Management Center to manage the Firepower 1010E. Instead, use a Version 7.2.3.1+ or Version 7.3.1.1+ Firewall 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 2.12.1.95 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*.

Firewall Threat Defense Virtual

Version 7.2 Firewall 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 Firewall Threat Defense Virtual Platforms

Device Platform	Firewall Management Center Compatibility		Firewall Device Manager Compatibility	
	Customer Deployed	Cloud Delivered	Firewall Device Manager Only	Firewall Device Manager + CDO
Public Cloud				
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	—	—
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

Firewall Threat Defense Management

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

On-Prem Firewall Management Center

All devices support remote management with a customer-deployed (*on-prem*) Firewall Management Center.

Versions are major (A.x), maintenance (A.x.y), or patch (A.x.y.z). The Firewall Management Center should run the same or newer version as its devices. New features and resolved issues often require the latest version on both the Firewall Management Center and its devices. Upgrade the Firewall Management Center first—you will still be able to manage older devices, usually a few major versions back.

Note You cannot upgrade a device past the Firewall Management Center to a newer major or maintenance version. Although a patched device (fourth-digit) can be managed with an unpatched Firewall Management Center, fully patched deployments undergo enhanced testing.

Note that in most cases you can upgrade an older device directly to the Firewall 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. Rarely, there are issues with specific Firewall Management Center-device combinations. For release-specific requirements, see the release notes.

Table 4: On-Prem Firewall Management Center-Device Compatibility

Firewall Management Center Version	Oldest Device Version You Can Manage
10.x	7.3
7.7	7.2
7.6	7.1
7.4 Last support for NGIPS device management.	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
6.4	6.1
6.2.3	6.1

Cloud-Delivered Firewall Management Center

For Firewall Threat Defense compatibility with Cloud-Delivered Firewall Management Center, see the *Cisco Secure Firewall Threat Defense Compatibility Guide*.