

System Requirements

This document includes the system requirements for Version 7.0.

- Firewall Management Center Platforms, on page 1
- Device Platforms, on page 2
- Device Management, on page 5

Firewall Management Center Platforms

The Firewall Management Center provides a centralized firewall management console. For device compatibility with the Firewall Management Center, see Device Management, on page 5. For general compatibility information, see the *Cisco Secure Firewall Management Center Compatibility Guide*.

Firewall Management Center Hardware

Version 7.0 supports the following Firewall Management Center hardware:

- Firepower Management Center 1600, 2600, 4600
- Firepower Management Center 1000, 2500, 4500

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

Firewall Management Center Virtual

Version 7.0 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 7.0 Firewall Management Center Virtual Platforms

Platform	Devices Managed		High Availability
	2, 10, 25	300	
Public Cloud			

Platform	Devices Managed		High Availability
	2, 10, 25	300	
Amazon Web Services (AWS)	YES	—	—
Google Cloud Platform (GCP)	YES	—	—
Microsoft Azure	YES	—	—
Oracle Cloud Infrastructure (OCI)	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*.

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*.

Firewall Threat Defense Hardware

Version 7.0 Firewall Threat Defense hardware comes in a range of throughputs, scalability capabilities, and form factors.

Table 2: Version 7.0 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 1010, 1120, 1140, 1150	YES	YES Requires Version 7.0.3+	YES	YES	—
Firepower 2110, 2120, 2130, 2140	YES	YES Requires Version 7.0.3+	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 Requires Version 7.0.3+	YES	YES	Requires FXOS 2.10.1.331 or later build. We recommend the latest firmware. See the *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*.
ASA 5508-X, 5516-X	YES	YES Requires Version 7.0.3+	YES	YES	ASA 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 Requires Version 7.0.3+	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 7.0 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 7.0 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 Requires Version 7.0.3+	YES	YES
Microsoft Azure	YES	YES Requires Version 7.0.3+	YES	YES
Google Cloud Platform (GCP)	YES	YES Requires Version 7.0.3+	—	—
Oracle Cloud Infrastructure (OCI)	YES	YES Requires Version 7.0.3+	—	—
Private Cloud				
Cisco Hyperflex	YES	YES Requires Version 7.0.3+	YES	YES
Kernel-based virtual machine (KVM)	YES	YES Requires Version 7.0.3+	YES	YES
Nutanix Enterprise Cloud	YES	YES Requires Version 7.0.3+	YES	YES
OpenStack	YES	YES Requires Version 7.0.3+	—	—
VMware vSphere/VMware ESXi 6.5, 6.7, or 7.0	YES	YES Requires Version 7.0.3+	YES	YES

Firepower Classic: ASA FirePOWER, NGIPSv

Firepower Classic devices run NGIPS software on the following platforms:

- 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 7.0 NGIPS Platforms

Device Platform	FMC Compatibility (Customer Deployed)	ASDM Compatibility	Notes
ASA 5508-X, 5516-X	YES	Requires ASDM 7.16(1).	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*.
ISA 3000	YES	Requires ASDM 7.16(1).	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*.
NGIPSv	YES	—	Requires VMware vSphere/VMware ESXi 6.5, 6.7, or 7.0. 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.

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 Upgrade Guidelines.

Table 5: 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*.

Firewall Device Manager

You can use Firewall Device Manager to locally manage a single Firewall Threat Defense device. Most models suppport local management.

Optionally, add Security Cloud Control to remotely manage multiple Firewall Threat Defense devices, as an alternative to the Firewall Management Center. Although some configurations still require Firewall Device

Manager, Security Cloud Control allows you to establish and maintain consistent security policies across your Firewall Threat Defense deployment.

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.