Cisco Secure Firewall Management Center Compatibility Guide

First Published: 2022-05-05

Last Modified: 2025-06-17

Cisco Secure Firewall Management Center Compatibility Guide

This guide provides software and hardware compatibility for the Cisco Secure Firewall Management Center. For related compatibility guides, see the following table.

Note Not all software versions, especially patches, apply to all platforms. A quick way to tell if a version is supported is that its upgrade/installation packages are posted on the Cisco Support & Download site. If the site is "missing" an upgrade or installation package, that version is not supported. You can also check the release notes and End-of-Life Announcements, on page 28. If you feel a version is missing in error, contact Cisco TAC.

Table 1: Additional Resources

Description	Resources
Sustaining bulletins provide support timelines for the Cisco Next Generation Firewall product line, including management platforms and operating systems.	Cisco's Next Generation Firewall Product Line Software Release and Sustaining Bulletin
Compatibility guides provide detailed compatibility information for supported hardware models and software versions, including bundled components and integrated products.	Cisco Secure Firewall Threat Defense Compatibility Guide Cisco Firepower Classic Device Compatibility Guide
Release notes provide critical and release-specific information, including upgrade warnings and behavior changes. Release notes also contain quicklinks to upgrade and installation instructions.	Cisco Secure Firewall Threat Defense Release Notes
New Feature guides provide information on new and deprecated features by release.	Cisco Secure Firewall Management Center New Features by Release
Documentation roadmaps provide links to currently available and legacy documentation. Try the roadmaps if what you are looking for is not listed above.	Navigating the Cisco Secure Firewall Threat Defense Documentation

Suggested Release: Version 7.4.2

To take advantage of new features and resolved issues, we recommend you upgrade all eligible appliances to at least the suggested release, including the latest patch. On the Cisco Support & Download site, the suggested release is marked with a gold star. In Version 7.2.6+/7.4.1+, the management center notifies you when a new suggested release is available, and indicates suggested releases on its product upgrades page.

Suggested Releases for Older Appliances

If an appliance is too old to run the suggested release and you do not plan to refresh the hardware right now, choose a major version then patch as far as possible. Some major versions are designated *long-term* or *extra long-term*, so consider one of those. For an explanation of these terms, see Cisco's Next Generation Firewall Product Line Software Release and Sustaining Bulletin.

If you are interested in a hardware refresh, contact your Cisco representative or partner contact.

Management Center Hardware

The Version 7.0+ management center virtual uses the FXOS operating system. Upgrading the management center virtual software automatically upgrades FXOS. For information on bundled FXOS versions, see Bundled Components, on page 12.

Table 2: Management Center Hardware Compatibility

Management Center	Secure Firewall Management Center	Firepower Management Center				Defense Center
	1700 2700 4700	1600 2600 4600	1000 2500 4500	2000 4000	750 1500 3500	500 1000 3000
7.7	**YES**	**YES**	—	—	—	—
7.6	**YES**	**YES**	—	—	—	—
7.4	**YES**	**YES**	—	—	—	—
7.3	—	**YES**	—	—	—	—
7.2	—	**YES**	—	—	—	—
7.1	—	**YES**	—	—	—	—
7.0	—	**YES**	**YES**	—	—	—
6.7	—	**YES**	**YES**	—	—	—
6.6	—	**YES**	**YES**	**YES**	—	—
6.5	—	**YES**	**YES**	**YES**	—	—
6.4	—	**YES**	**YES**	**YES**	**YES**	—

Management Center	Secure Firewall Management Center	Firepower Management Center				Defense Center
	1700 2700 4700	1600 2600 4600	1000 2500 4500	2000 4000	750 1500 3500	500 1000 3000
6.3	—	YES	YES	YES	YES	—
6.2.3	—	—	YES	YES	YES	—
6.2.2	—	—	YES	YES	YES	—
6.2.1	—	—	YES	YES	YES	—
6.2.0	—	—	YES	YES	YES	—
6.1	—	—	—	YES	YES	—
6.0.1	—	—	—	YES	YES	—
6.0.0	—	—	—	YES	YES	—
5.4 *	—	—	—	YES	YES	YES

* Use 5.4.1.x Defense Centers to manage 5.4.x devices.

BIOS and Firmware for Management Center Hardware

We provide updates for BIOS and RAID controller firmware on management center hardware. If your management center does not meet the requirements, apply the appropriate hotfix. If your management center model and version are not listed and you think you need to update, contact Cisco TAC.

Table 3: BIOS and Firmware Minimum Requirements

Platform	Version	Hotfix	BIOS	RAID Controller Firmware	CIMC Firmware
FMC 1700, 2700, 4700	7.6 7.4	BIOS Update Hotfix FC	C225M6.4.3.4b.0	52.26.0-5016	4.3(4.242038)

Platform	Version	Hotfix	BIOS	RAID Controller Firmware	CIMC Firmware
FMC 1600, 2600, 4600	7.6 7.4 7.3 7.2 7.1 7.0	BIOS Update Hotfix FC	C220M5.4.3.2b.0	51.23.0-5009	4.3(2.240077)
	6.7 6.6 6.4	BIOS Update Hotfix EN	C220M5.4.2.3b.0	51.10.0-3612	4.2(3b)
FMC 1000, 2500, 4500	7.0 6.7 6.6 6.4	BIOS Update Hotfix EN	C220M5.4.2.3b.0	51.10.0-3612	4.2(3b)
	6.2.3	BIOS Update Hotfix EL	C220M4.4.1.2c.0	24.12.1-0456	4.1(2g)
FMC 2000, 4000	6.6 6.4 6.2.3	BIOS Update Hotfix EI	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)
FMC 750, 1500, 3500	6.4 6.2.3	BIOS Update Hotfix EI	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)

Hotfixing is the only way to update the BIOS and RAID controller firmware. Upgrading the software does not accomplish this task, nor does reimaging to a later version. If the management center is already up to date, the hotfix has no effect.

Tip These hotfixes also update the CIMC firmware; for resolved issues see Release Notes for Cisco UCS Rack Server Software. Note that in general, we do not support changing configurations on the management center using CIMC. However, to enable logging of invalid CIMC usernames, apply the latest hotfix, then follow the instructions in the *Viewing Faults and Logs* chapter in the Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Version 4.0 or later.

Use the regular upgrade process to apply hotfixes. For hotfix release notes, which include quicklinks to the Cisco Support & Download site, see the Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes.

Note The management center web interface may display these hotfixes with a version that is different from (usually later than) the current software version. This is expected behavior and the hotfixes are safe to apply.

Determining BIOS and Firmware Versions

To determine the current versions on the management center, run these commands from the Linux shell/expert mode:

- BIOS: **sudo dmidecode -t bios -q**
- RAID controller firmware (FMC 4500): **sudo MegaCLI -AdpAllInfo -aALL | grep "FW Package"**
- RAID controller firmware (all other models): **sudo storcli /c0 show | grep "FW Package"**

Management Center Virtual

With the management center virtual, you can purchase licenses that enable you to manage 2, 10, 25, or 300 devices. For full details on supported instances, see the Cisco Secure Firewall Management Center Virtual Getting Started Guide.

The Version 7.0+ management center virtual uses the FXOS operating system. Upgrading the management center virtual software automatically upgrades FXOS. For information on bundled FXOS versions, see Bundled Components, on page 12.

Management Center Virtual: Public Cloud

Table 4: Management Center Virtual 300 Compatibility: Public Cloud

Management Center 300	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Oracle Cloud Infrastructure (OCI)
7.7	**YES**	**YES**	**YES**
7.6	**YES**	**YES**	**YES**
7.4	**YES**	**YES** Requires 7.4.2+	**YES**
7.3	**YES**	—	**YES**
7.2	**YES**	—	**YES**
7.1	**YES**	—	**YES**

Table 5: Management Center Virtual 2, 10, 25 Compatibility: Public Cloud

Management Center 2, 10, 25	Alibaba Cloud (Alibaba)	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Oracle Cloud Infrastructure (OCI)
7.7	**YES**	**YES**	**YES**	**YES**	**YES**

Management Center 2, 10, 25	Alibaba Cloud (Alibaba)	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Oracle Cloud Infrastructure (OCI)
7.6	**YES**	**YES**	**YES**	**YES**	**YES**
7.4	**YES**	**YES**	**YES**	**YES**	**YES**
7.3	**YES**	**YES**	**YES**	**YES**	**YES**
7.2	**YES**	**YES**	**YES**	**YES**	**YES**
7.1	—	**YES**	**YES**	**YES**	**YES**
7.0	—	**YES**	**YES**	**YES**	**YES**
6.7	—	**YES**	**YES**	**YES**	**YES**
6.6	—	**YES**	**YES**	—	—
6.5	—	**YES**	**YES**	—	—
6.4	—	**YES**	**YES**	—	—
6.3	—	**YES**	—	—	—
6.2.3	—	**YES**	—	—	—
6.2.2	—	**YES**	—	—	—
6.2.1	—	**YES**	—	—	—
6.2.0	—	**YES**	—	—	—
6.1	—	**YES**	—	—	—
6.0.1	—	**YES**	—	—	—

Management Center Virtual: On-Prem/Private Cloud

Table 6: Management Center Virtual 300 Compatibility: On-Prem/Private Cloud

Management Center 300	VMware vSphere/VMware ESXi	Kernel-Based Virtual Machine (KVM)
7.7	**YES** VMware 6.5, 6.7, 7.0, 8.0	**YES**
7.6	**YES** VMware 6.5, 6.7, 7.0, 8.0	**YES**
7.4.2–7.4.x	**YES** VMware 6.5, 6.7, 7.0, 8.0	**YES**

Management Center 300	VMware vSphere/VMware ESXi	Kernel-Based Virtual Machine (KVM)
7.4.0–7.4.1	**YES** VMware 6.5, 6.7, 7.0	**YES**
7.3	**YES** VMware 6.5, 6.7, 7.0	**YES**
7.2.9–7.2.x	**YES** VMware 6.5, 6.7, 7.0, 8.0	—
7.2.0–7.2.8	**YES** VMware 6.5, 6.7, 7.0	—
7.1	**YES** VMware 6.5, 6.7, 7.0	—
7.0	**YES** VMware 6.5, 6.7, 7.0	—
6.6	**YES** VMware 6.0, 6.5, 6.7	—

Table 7: Management Center Virtual 2, 10, 25 Compatibility: On-Prem/Private Cloud

Management Center 2, 10 25	VMware vSphere/VMware ESXi	Cisco HyperFlex (HyperFlex)	Microsoft Hyper-V (Hyper-V)	Kernel-Based Virtual Machine (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack
7.7	**YES** VMware 6.5, 6.7, 7.0, 8.0	**YES**	**YES**	**YES**	**YES**	**YES**
7.6	**YES** VMware 6.5, 6.7, 7.0, 8.0	**YES**	**YES**	**YES**	**YES**	**YES**
7.4.2–7.4.x	**YES** VMware 6.5, 6.7, 7.0, 8.0	**YES**	**YES**	**YES**	**YES**	**YES**
7.4.0–7.4.1	**YES** VMware 6.5, 6.7, 7.0	**YES**	**YES**	**YES**	**YES**	**YES**

Management Center 2, 10 25	VMware vSphere/VMware ESXi	Cisco HyperFlex (HyperFlex)	Microsoft Hyper-V (Hyper-V)	Kernel-Based Virtual Machine (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack
7.3	**YES** VMware 6.5, 6.7, 7.0	**YES**	—	**YES**	**YES**	**YES**
7.2.9–7.2.x	**YES** VMware 6.5, 6.7, 7.0, 8.0	**YES**	—	**YES**	**YES**	**YES**
7.2.0–7.2.8	**YES** VMware 6.5, 6.7, 7.0	**YES**	—	**YES**	**YES**	**YES**
7.1	**YES** VMware 6.5, 6.7, 7.0	**YES**	—	**YES**	**YES**	**YES**
7.0	**YES** VMware 6.5, 6.7, 7.0	**YES**	—	**YES**	**YES**	**YES**
6.6	**YES** VMware 6.0, 6.5, 6.7	—	—	**YES**	—	—
6.4	**YES** VMware 6.0, 6.5	—	—	**YES**	—	—
6.2.3	**YES** VMware 5.5, 6.0, 6.5	—	—	**YES**	—	—

* Use 5.4.1.x Defense Centers to manage 5.4.x devices.

Management Center High Availability

Cloud-Delivered Firewall Management Center

The Cloud-Delivered Firewall Management Center does not support high availability.

Management Center Hardware

All currently supported hardware management centers support high availability.

Management Center Virtual

Table 8: Management Center Virtual: High Availability Support

Platform	High Availability
Public Cloud	
Alibaba	—
Amazon Web Services (AWS)	7.1+
Google Cloud Platform (GCP)	—
Microsoft Azure	7.4.2+
Oracle Cloud Infrastructure (OCI)	7.1+
On-Prem/Private Cloud	
Cisco HyperFlex	7.0+
Kernel-based virtual machine (KVM)	7.3+
Microsoft Hyper-V	7.4+
Nutanix Enterprise Cloud	—
OpenStack	—
VMware vSphere/VMware ESXi	6.7+

Device Management

On-Prem Management Center

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

Versions are major (A.x), maintenance (A.x.y), or patch (A.x.y.z). The 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 management center and its devices. Upgrade the 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 management center to a newer major or maintenance version. Although a patched device (fourth-digit) can be managed with an unpatched management center, fully patched deployments undergo enhanced testing.

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. Rarely, there are issues with specific management center-device combinations. For release-specific requirements, see the release notes.

Table 9: On-Prem Management Center-Device Compatibility

Management Center Version	Oldest Device Version You Can Manage
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

The Cloud-Delivered Firewall Management Center supports a wider range of managed device versions than on-prem management centers. However, to ensure security, reliability, and performance, sometimes we need to end Cloud-delivered Firewall Management Center support for older versions of threat defense. After support ends for older versions, you cannot make or deploy changes to devices running those versions except to upgrade or unregister.

Important After we announce end of support, upgrade affected devices as soon as possible. Do not add any new devices running the deprecated version. If you cannot upgrade due to incompatibility, contact your Cisco representative or partner immediately.

Table 10: Cloud-delivered Firewall Management Center-Threat Defense Compatibility

Threat Defense Version	Support Begins
7.7	March 13, 2025
7.6	August 23, 2024
7.4.1	February 13, 2024
7.4.0	October 19, 2023

Threat Defense Version	Support Begins
7.3	December 13, 2022
7.2	June 9, 2022
7.1	—
7.0.3–7.0.x	June 30, 2022 Support ends October 22, 2025. Also ends support for the ASA-5508-X and ASA-5516-X with Cloud-delivered Firewall Management Center. See: End of Support for Cisco Secure Firewall Threat Defense 7.0.x with Cloud-delivered Firewall Management Center

Co-managing Devices with an Analytics Management Center

You can co-manage a cloud-managed device with a Version 7.2+ on-prem management center for event logging and analytics purposes only. Because the Cloud-Delivered Firewall Management Center supports a wider range of managed device versions than on-prem management centers, you may have issues with devices being "too old" or "too new" to co-manage.

You can be prevented from:

- Registering newer devices to the analytics management center because older devices are blocking the required management center upgrade.
- Upgrading co-managed devices to the latest release, because the analytics management center is "stuck" at an older release.
- Reverting device upgrade, if revert would take the device out of compatibility with the analytics management center.

For example, consider a scenario where you want to add co-managed Version 7.7.0 devices to a deployment that currently includes co-managed Version 7.0.x devices. The Cloud-Delivered Firewall Management Center can manage this full range of devices, but the on-prem analytics management center cannot.

This table explains your options in order of preference.

Table 11:

Result	Action	In this scenario
Get events from all devices.	Upgrade (or replace) the analytics management center and your older devices.	**1.** Upgrade the Version 7.0.x devices to at least Version 7.3.0. **2.** Upgrade the analytics management center to Version 7.7.0. **3.** Add the Version 7.7.0 devices to both management centers.

Result	Action	In this scenario
Forgo events from older devices.	Upgrade (or replace) the analytics management center only.	1. Remove the Version 7.0.x devices from the analytics management center. 2. Upgrade the analytics management center to Version 7.7.0. 3. Add the Version 7.7.0 devices to both management centers.
Forgo events from newer devices.	Leave the analytics management center at an older release.	Leave the analytics management center as it is and do not add your Version 7.7.0 devices.

Bundled Components

These tables list the versions of various components bundled with the management center. Use this information to identify open or resolved bugs in bundled components that may affect your deployment.

Note that sometimes we release updated builds for select releases. If bundled components change from build to build, we list the components in the *latest* build. (In most cases, only the latest build is available for download.) For details on new builds and the issues they resolve, see the release notes for your version.

Operating System

The Version 7.0+ management center uses the FXOS operating system.

Table 12:

Management Center	FXOS
7.7.0	2.17.0.518
7.6.1	2.16.0.3007
7.6.0	2.16.0.128
7.4.2.3	2.14.1.187
7.4.2.2	2.14.1.187
7.4.2.1	2.14.1.176
7.4.2	2.14.1.167
7.4.1.1	2.14.1.131
7.4.1	2.14.1.131
7.4.0	2.14.0.475
7.3.1.1	2.13.0.1022
7.3.1	2.13.0.1022

Management Center	FXOS
7.3.0	2.13.0.198
7.2.10	2.12.1.101
7.2.9	2.12.1.86
7.2.8.1	2.12.1.1703
7.2.8	2.12.1.73
7.2.7	2.12.1.73
7.2.6	2.12.1.73
7.2.5.2	2.12.0.530
7.2.5.1	2.12.0.530
7.2.5	2.12.0.519
7.2.4.1	2.12.0.519
7.2.4	2.12.0.499
7.2.3.1	2.12.0.1030
7.2.3	2.12.0.1030
7.2.2	2.12.0.1104
7.2.1	2.12.0.442
7.2.0.1	2.12.0.31
7.2.0	2.12.0.31
7.1.0.3	2.11.1.191
7.1.0.2	2.11.1.1300
7.1.0.1	2.11.1.154
7.1.0	2.11.1.154
7.0.7	2.10.1.1642
7.0.6.3	2.10.1.1633
7.0.6.2	2.10.1.1625
7.0.6.1	2.10.1.1614
7.0.6	2.10.1.1603
7.0.5.1	—

Management Center	FXOS
7.0.5	2.10.1.1400
7.0.4	2.10.1.208
7.0.3	2.10.1.1200
7.0.2.1	2.10.1.192
7.0.2	2.10.1.192
7.0.1.1	2.10.1.175
7.0.1	2.10.1.175
7.0.0.1	2.10.1.159
7.0.0	2.10.1.159

Snort

Snort is the main inspection engine. Snort 3 is available in threat defense Version 7.0+ with management center. Version 7.6.0 is the last major version that supports Snort 2.

Table 13:

Threat Defense	Snort 2	Snort 3
7.7.0	—	3.3.5.1-77
7.6.1	2.9.23-1019	3.1.79.100-68
7.6.0	2.9.23-227	3.1.79.1-121
7.4.2.3	2.9.22-2000	3.1.53.203-151
7.4.2.2	2.9.22-2000	3.1.53.202-136
7.4.2.1	2.9.22-2000	3.1.53.201-112
7.4.2	2.9.22-2000	3.1.53.200-107
7.4.1.1	2.9.22-1103	3.1.53.100-56
7.4.1	2.9.22-1009	3.1.53.100-56
7.4.0	2.9.22-181	3.1.53.1-40
7.3.1.1	2.9.21-1109	3.1.36.101-2
7.3.1	2.9.21-1000	3.1.36.100-2
7.3.0	2.9.21-105	3.1.36.1-101
7.2.10	2.9.20-10002	3.1.21.1000-54

Threat Defense	Snort 2	Snort 3
7.2.9	2.9.20-9000	3.1.21.900-7
7.2.8.1	2.9.20-8101	3.1.21.800-2
7.2.8	2.9.20-8005	3.1.21.800-2
7.2.7	2.9.20-6102	3.1.21.600-26
7.2.6	2.9.20-6102	3.1.21.600-26
7.2.5.2	2.9.20-5201	3.1.21.501-27
7.2.5.1	2.9.20-5100	3.1.21.501-26
7.2.5	2.9.20-5002	3.1.21.500-21
7.2.4.1	2.9.20-4103	3.1.21.401-6
7.2.4	2.9.20-4004	3.1.21.400-24
7.2.3.1	2.9.20-3100	3.1.21.100-7
7.2.3	2.9.20-3010	3.1.21.100-7
7.2.2	2.9.20-2001	3.1.21.100-7
7.2.1	2.9.20-1000	3.1.21.100-7
7.2.0.1	2.9.20-108	3.1.21.1-126
7.2.0	2.9.20-107	3.1.21.1-126
7.1.0.3	2.9.19-3000	3.1.7.3-210
7.1.0.2	2.9.19-2000	3.1.7.2-200
7.1.0.1	2.9.19-1013	3.1.7.2-200
7.1.0	2.9.19-92	3.1.7.1-108
7.0.7	2.9.18-7019	3.1.0.700-37
7.0.6.3	2.9.18-6306	3.1.0.603-31
7.0.6.2	2.9.18-6201	3.1.0.602-26
7.0.6.1	2.9.18-6008	3.1.0.600-20
7.0.6	2.9.18-6008	3.1.0.600-20
7.0.5.1	2.9.18-5100	—
7.0.5	2.9.18-5002	3.1.0.500-7
7.0.4	2.9.18-4002	3.1.0.400-12

Threat Defense	Snort 2	Snort 3
7.0.3	2.9.18-3005	3.1.0.300-3
7.0.2.1	2.9.18-2101	3.1.0.200-16
7.0.2	2.9.18-2022	3.1.0.200-16
7.0.1.1	2.9.18-1026	3.1.0.100-11
7.0.1	2.9.18-1026	3.1.0.100-11
7.0.0.1	2.9.18-1001	3.1.0.1-174
7.0.0	2.9.18-174	3.1.0.1-174
6.7.0.3	2.9.17-3014	—
6.7.0.2	2.9.17-2003	—
6.7.0.1	2.9.17-1006	—
6.7.0	2.9.17-200	—
6.6.7.2	2.9.16-7101	—
6.6.7.1	2.9.16-7100	—
6.6.7	2.9.16-7017	—
6.6.5.2	2.9.16-5204	—
6.6.5.1	2.9.16-5107	—
6.6.5	2.9.16-5034	—
6.6.4	2.9.16-4022	—
6.6.3	2.9.16-3033	—
6.6.1	2.9.16-1025	—
6.6.0.1	2.9.16-140	—
6.6.0	2.9.16-140	—
6.5.0.5	2.9.15-15510	—
6.5.0.4	2.9.15-15201	—
6.5.0.3	2.9.15-15201	—
6.5.0.2	2.9.15-15101	—
6.5.0.1	2.9.15-15101	—
6.5.0	2.9.15-7	—

Threat Defense	Snort 2	Snort 3
6.4.0.18	2.9.14-28000	—
6.4.0.17	2.9.14-27005	—
6.4.0.16	2.9.14-26002	—
6.4.0.15	2.9.14-25006	—
6.4.0.14	2.9.14-24000	—
6.4.0.13	2.9.14-19008	—
6.4.0.12	2.9.14-18011	—
6.4.0.11	2.9.14-17005	—
6.4.0.10	2.9.14-16023	—
6.4.0.9	2.9.14-15906	—
6.4.0.8	2.9.14-15707	—
6.4.0.7	2.9.14-15605	—
6.4.0.6	2.9.14-15605	—
6.4.0.5	2.9.14-15507	—
6.4.0.4	2.9.12-15301	—
6.4.0.3	2.9.14-15301	—
6.4.0.2	2.9.14-15209	—
6.4.0.1	2.9.14-15100	—
6.4.0	2.9.14-15003	—
6.3.0.5	2.9.13-15503	—
6.3.0.4	2.9.13-15409	—
6.3.0.3	2.9.13-15307	—
6.3.0.2	2.9.13-15211	—
6.3.0.1	2.9.13-15101	—
6.3.0	2.9.13-15013	—
6.2.3.18	2.9.12-1813	—
6.2.3.17	2.9.12-1605	—
6.2.3.16	2.9.12-1605	—

Threat Defense	Snort 2	Snort 3
6.2.3.15	2.9.12-1513	—
6.2.3.14	2.9.12-1401	—
6.2.3.13	2.9.12-1306	—
6.2.3.12	2.9.12-1207	—
6.2.3.11	2.9.12-1102	—
6.2.3.10	2.9.12-902	—
6.2.3.9	2.9.12-806	—
6.2.3.8	2.9.12-804	—
6.2.3.7	2.9.12-704	—
6.2.3.6	2.9.12-607	—
6.2.3.5	2.9.12-506	—
6.2.3.4	2.9.12-383	—
6.2.3.3	2.9.12-325	—
6.2.3.2	2.9.12-270	—
6.2.3.1	2.9.12-204	—
6.2.3	2.9.12-136	—
6.2.2.5	2.9.11-430	—
6.2.2.4	2.9.11-371	—
6.2.2.3	2.9.11-303	—
6.2.2.2	2.9.11-273	—
6.2.2.1	2.9.11-207	—
6.2.2	2.9.11-125	—
6.2.1	2.9.11-101	—
6.2.0.6	2.9.10-301	—
6.2.0.5	2.9.10-255	—
6.2.0.4	2.9.10-205	—
6.2.0.3	2.9.10-160	—
6.2.0.2	2.9.10-126	—

Threat Defense	Snort 2	Snort 3
6.2.0.1	2.9.10-98	—
6.2.0	2.9.10-42	—
6.1.0.7	2.9.9-312	—
6.1.0.6	2.9.9-258	—
6.1.0.5	2.9.9-225	—
6.1.0.4	2.9.9-191	—
6.1.0.3	2.9.9-159	—
6.1.0.2	2.9.9-125	—
6.1.0.1	2.9.9-92	—
6.1.0	2.9.9-330	—
6.0.1.4	2.9.8-490	—
6.0.1.3	2.9.8-461	—
6.0.1.2	2.9.8-426	—
6.0.1.1	2.9.8-383	—
6.0.1	2.9.8-224	—
6.0.0.1	2.9.8-235	—
6.0.0	2.9.8-229	—

System Databases

The vulnerability database (VDB) is a database of known vulnerabilities to which hosts may be susceptible, as well as fingerprints for operating systems, clients, and applications. The system uses the VDB to help determine whether a particular host increases your risk of compromise.

The geolocation database (GeoDB) is a database that you can leverage to view and filter traffic based on geographical location.

Table 14:

Management Center	VDB	GeoDB
7.7.0	4.5.0-400	2024-12-14-066
7.6.0 through 7.6.x	4.5.0-392	2022-07-04-101
7.4.1 through 7.4.x	4.5.0-376	2022-07-04-101
7.4.0	4.5.0-365	2022-07-04-101

Management Center	VDB	GeoDB
7.3.0 through 7.3.x	4.5.0-358	2022-07-04-101
7.2.0 through 7.2.x	4.5.0-353	2022-05-11-103
7.1.0	4.5.0-346	2020-04-28-002
6.7.0 through 7.0.x	4.5.0-338	2020-04-28-002
6.6.1 through 6.6.x	4.5.0-336	2019-06-03-002
6.6.0	4.5.0-328	2019-06-03-002
6.5.0	4.5.0-309	2019-06-03-002
6.4.0	4.5.0-309	2018-07-09-002
6.3.0	4.5.0-299	2018-07-09-002
6.2.3	4.5.0-290	2017-12-12-002
6.0.0 through 6.2.2	4.5.0-271	2015-10-12-001

Integrated Products

The Cisco products listed below may have other compatibility requirements, for example, they may need to run on specific hardware, or on a specific operating system. For that information, see the documentation for the appropriate product.

Note Whenever possible, we recommend you use the latest (newest) compatible version of each integrated product. This ensures that you have the latest features, bug fixes, and security patches.

Identity Services and User Control

Note that with:

- Cisco ISE and ISE-PIC: We list the versions of ISE and ISE-PIC for which we provide enhanced compatibility testing, although other combinations may work.
- Cisco Firepower User Agent: Version 6.6 is the last management center release to support the user agent software as an identity source; this blocks upgrade to Version 6.7+. Instead, use the Passive Identity Agent with Microsoft Active Directory. For more information, see User Control With the Passive Identity Agent.
- Cisco TS Agent: Versions 1.0 and 1.1 are no longer available.

Table 15: Integrated Products: Identity Services/User Control

Management Center/Threat Defense	Cisco Identity Services Engine (ISE)		Cisco Firepower User Agent	Cisco Terminal Services (TS) Agent	Passive Identity Agent
	ISE	ISE-PIC			
Supported with...	Management center Device manager	Management center Device manager	Management center only	Management center only	Management center only
Cloud-delivered Firewall Management Center (no version)	3.3 3.2 3.1 patch 2+ 3.0 patch 6+ 2.7 patch 2+ The pxGrid cloud identity source requires ISE 3.1 patch 3 or later.	3.2 3.1 2.7 patch 2+	—	1.4	1.0, 1.1
7.7	3.4 patch 1+ 3.3 patch 4+ 3.2 patch 5+ 3.1 patch 2+	3.2 3.1	—	1.4	1.0, 1.1
7.6	3.3 patch 2 3.2 patch 5 3.1 patch 2+	3.2 3.1	—	1.4	1.0, 1.1
7.4	3.3 3.2 3.1 patch 2+ 3.0 patch 6+	3.2 3.1	—	1.4	—
7.3	3.2 3.1 3.0 2.7 patch 2+	3.2 3.1 2.7 patch 2+	—	1.4 1.3	—

Management Center/Threat Defense	Cisco Identity Services Engine (ISE)		Cisco Firepower User Agent	Cisco Terminal Services (TS) Agent	Passive Identity Agent
	ISE	ISE-PIC			
7.2.4–7.2.x	3.3 3.2 3.1 3.0 2.7 patch 2+	3.2 3.1 2.7 patch 2+	—	1.4 1.3	—
7.2.0–7.2.3	3.2 3.1 3.0 2.7 patch 2+	3.2 3.1 2.7 patch 2+	—	1.4 1.3	—
7.1	3.2 3.1 3.0 2.7 patch 2+	3.2 3.1 2.7 patch 2+	—	1.4 1.3	—
7.0	3.2 3.1 3.0 2.7 patch 2+ 2.6 patch 6+	3.2 3.1 2.7 patch 2+ 2.6 patch 6+	—	1.4 1.3	—
6.7	3.0 2.7 patch 2+ 2.6 patch 6+	2.7 patch 2+ 2.6 patch 6+	—	1.4 1.3	—
6.6	3.0 2.7, any patch 2.6, any patch 2.4	2.7, any patch 2.6, any patch 2.4	2.5 2.4	1.4 1.3 1.2	—
6.5	2.6 2.4	2.6 2.4	2.5 2.4	1.4 1.3 1.2 1.1	—

Management Center/Threat Defense	Cisco Identity Services Engine (ISE)		Cisco Firepower User Agent	Cisco Terminal Services (TS) Agent	Passive Identity Agent
	ISE	ISE-PIC			
6.4	2.4 2.3 patch 2 2.3	2.4 2.2 patch 1	2.5 2.4 2.3, no ASA FirePOWER	1.4 1.3 1.2 1.1	—
6.3	2.4 2.3 patch 2 2.3	2.4 2.2 patch 1 2.4	2.4 2.3, no ASA FirePOWER	1.2 1.1	—
6.2.3	2.3 patch 2 2.3 2.2 patch 5 2.2 patch 1 2.2	2.2 patch 1	2.4 2.3	1.2 1.1	—
6.2.2	2.3 2.2 patch 1 2.2 2.1	2.2 patch 1	2.3	1.2 1.1 1.0	—
6.2.1	2.1 2.0.1 2.0	2.2 patch 1	2.3	1.1 1.0	—
6.2.0	2.1 2.0.1 2.0 1.3	—	2.3	—	—
6.1	2.1 2.0.1 2.0 1.3	—	2.3	—	—
6.0.1	1.3	—	2.3	—	—
5.x	—	—	2.2	—	

Cisco Secure Dynamic Attributes Connector

The Cisco Secure Dynamic Attributes Connector is a lightweight application that quickly and seamlessly updates firewall policies on the management center based on cloud/virtual workload changes. For more information, see one of:

- On-prem connector: Cisco Secure Dynamic Attributes Connector Configuration Guide
- Cloud-delivered connector: *Managing the Cisco Secure Dynamic Attributes Connector with Cisco Security Cloud Control* chapters in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Security Cloud Control
- Bundled with the Secure Firewall Management Center: Cisco Secure Firewall Management Center Device Configuration Guide

Table 16: Integrated Products: Cisco Secure Dynamic Attributes Connector

Management Center	Cisco Secure Dynamic Attributes Connector	
	On-Prem	**Cloud-delivered (with Security Cloud Control)**
Cloud-delivered management center (no version)	3.1 3.0 2.2 2.0	**YES**
7.1+	3.1 3.0 2.2 2.0 1.1	**YES**
7.0	3.1 3.0 2.2 2.0 1.1	—

The Cisco Secure Dynamic Attributes Connector allows you to use service tags and categories from various cloud service platforms in security rules.

The following table shows supported connectors for the Cisco Secure Dynamic Attributes Connector (CSDAC) provided with the Secure Firewall Management Center. For a list of supported connectors with the on-premises CSDAC, see the Cisco Secure Dynamic Attributes Connector Configuration Guide.

Table 17: List of supported connectors by Cisco Secure Dynamic Attributes Connector version and platform

CSDAC version/platform	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Cisco Multicloud Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	No	Yes	Yes	No	No
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes	Yes	No	No
Version 2.2 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	Yes	No	No
Version 2.3 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Version 3.0 (on-premises)	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cloud-delivered (Cisco Security Cloud Control)	Yes	No	No	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	No	No	No
Secure Firewall Management Center 7.4.1	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Secure Firewall Management Center 7.6	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Secure Firewall Management Center 7.7	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Secure Firewall Management Center 10.0.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Threat Detection

Note that:

- Cisco Security Analytics and Logging (On Premises) requires the Security Analytics and Logging On Prem app for the Stealthwatch Management Console (SMC). For information on Stealthwatch Enterprise (SWE) requirements for the SMC, see Cisco Security Analytics and Logging On Premises: Firepower Event Integration Guide.
- Cisco SecureX integration, which was available with Version 6.4–7.4, has now reached end of support. For a replacement technology, contact your Cisco representative or partner contact.

Table 18: Integrated Products: Threat Detection

Management Center/Threat Defense	Cisco Security Analytics and Logging (SaaS)	Cisco Security Analytics and Logging (On Prem)	Cisco Secure Malware Analytics	Cisco Security Packet Analyzer
Supported with...	Management center Device manager	Management center only	Management center only	Management center only
6.5+	**YES**	**YES**	**YES**	—
6.4	**YES**	**YES**	**YES**	**YES**
6.3	—	—	**YES**	**YES**
6.1–6.2.3	—	—	**YES**	—

Threat Defense Remote Access VPN

Remote access virtual private network (RA VPN) allows individual users to connect to your network from a remote location using a computer or supported mobile device. Keep in mind that newer threat defense features can require newer versions of the client.

For more information, see the Cisco Secure Client/AnyConnect Secure Mobility Client configuration guides.

Table 19: Integrated Products: Threat Defense RA VPN

Threat Defense	Cisco Secure Client/Cisco AnyConnect Secure Mobility Client
6.2.2+	4.0+

Browser Requirements

Browsers

We test with the latest versions of these popular browsers, running on currently supported versions of macOS and Microsoft Windows:

Table 20: Browsers

Browser	Management Center Version
Google Chrome	Any
Mozilla Firefox	Any
Microsoft Edge (Windows only)	Version 6.7+ Not extensively tested with How-Tos.
Apple Safari	Not extensively tested. Feedback welcome.

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 or have feedback, contact Cisco TAC.

Browser Settings and Extensions

Regardless of browser, keep JavaScript and cookies 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

Table 21: 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 on the management center, choose **System** (⚙) > **Configuration** > **HTTPS Certificate**. For detailed procedures, see the online help or the Cisco Secure Firewall Management Center Administration 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.

Note In Version 6.2.3 and earlier, websites that support TLS v1.3 always fail to load. As a workaround, you can configure managed devices to remove extension 43 (TLS 1.3) from ClientHello negotiation; see the software advisory titled: *Failures loading websites using TLS 1.3 with SSL inspection enabled*. In Version 6.2.3.7+, you can specify when to downgrade; see the **system support** commands in the Cisco Secure Firewall Threat Defense Command Reference after consulting with Cisco TAC.

End-of-Life Announcements

The following tables provide end-of-life details. Dates that have passed are in **bold**.

Snort 2

If you are still using the Snort 2 inspection engine with threat defense, switch to Snort 3 now for improved detection and performance. It is available starting in threat defense Version 7.0+ with management center. Snort 2 is deprecated in Version 7.7+, and prevents threat defense upgrade.

In management center deployments, upgrading to threat defense Version 7.2–7.6 also upgrades eligible Snort 2 devices to Snort 3. For devices that are ineligible because they use custom intrusion or network analysis policies, manually upgrade Snort. See *Migrate from Snort 2 to Snort 3* in the Cisco Secure Firewall Management Center Snort 3 Configuration Guide.

Software

These major software versions have reached end of sale and/or end of support. Versions that have reached end of support are removed from the Cisco Support & Download site.

Table 22: Software EOL Announcements

Version	End of Sale	End of Updates	End of Support	Announcement
7.3	2025-11-18	2026-05-18	2027-11-30	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Threat Defense (FTD/FTDv) 7.3(x), Firepower Management Center (FMC/FMCv) 7.3(x) and Firepower eXtensible Operating System (FXOS) 2.13(x)
7.2	2025-11-18	2026-11-18	2027-11-30	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Threat Defense (FTD/FTDv) 7.2(x), Firepower Management Center (FMC/FMCv) 7.2(x) and Firepower eXtensible Operating System (FXOS) 2.12(x)
7.1	**2023-12-22**	**2024-12-21**	2025-12-31	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Threat Defense (FTD) 7.1.(x), Firepower Management Center (FMC) 7.1.(x), Adaptive Security Appliance(ASA) 9.17.(x) and Firepower eXtensible Operating System (FXOS) 2.11.(x)

Version	End of Sale	End of Updates	End of Support	Announcement
7.0	2025-11-18	2026-11-18	2027-11-30	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Threat Defense (FTD/FTDv) 7.0(x), Firepower Management Center (FMC/FMCv) 7.0(x) and Firepower eXtensible Operating System (FXOS) 2.10(x)
6.7	**2021-07-09**	**2022-07-09**	**2024-07-31**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Threat Defense (FTD) 6.7, Firepower Management Center (FMC) 6.7 and Firepower eXtensible Operating System (FXOS) 2.9(x)
6.6	**2022-03-02**	**2023-03-02**	**2025-03-31**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Threat Defense (FTD/FTDv) 6.6(x), Firepower Management Center (FMC/FMCv) 6.6(x) and Firepower eXtensible Operating System (FXOS) 2.8(x)
6.5	**2020-06-22**	**2021-06-22**	**2023-06-30**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Threat Defense (FTD) 6.5(x), Firepower Management Center (FMC) 6.5(x) and Firepower eXtensible Operating System (FXOS) 2.7(x)
6.4	**2023-02-27**	**2024-02-27**	2026-02-28	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Threat Defense (FTD) 6.4(X), Firepower Management Center (FMC) 6.4(X) and Firepower eXtensible Operating System (FXOS) 2.6(x)
6.3	**2020-04-30**	**2021-04-30**	**2023-04-30**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Threat Defense (FTD) 6.2.2, 6.3(x), Firepower eXtensible Operating System (FXOS) 2.4.1 and Firepower Management Center (FMC) 6.2.2 and 6.3(x)
6.2.3	**2022-02-04**	**2023-02-04**	**2025-02-28**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Threat Defense (FTD) 6.2.3, Firepower Management Center (FMC) 6.2.3 and Firepower eXtensible Operating System (FXOS) 2.2(x)
6.2.2	**2020-04-30**	**2021-04-30**	**2023-04-30**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Threat Defense (FTD) 6.2.2, 6.3(x), Firepower eXtensible Operating System (FXOS) 2.4.1 and Firepower Management Center (FMC) 6.2.2 and 6.3(x)
6.2.1	**2019-03-05**	**2020-03-04**	**2022-03-31**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Threat Defense versions 6.2.0 and 6.2.1

Version	End of Sale	End of Updates	End of Support	Announcement
6.2	**2019-03-05**	**2020-03-04**	**2022-03-31**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Threat Defense versions 6.2.0 and 6.2.1
6.1	**2019-11-22**	**2021-05-22**	**2023-05-31**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Threat Defense versions 6.1, NGIPSv and NGFWv versions 6.1, Firepower Management Center 6.1 and Firepower eXtensible Operating System (FXOS) 2.0(x)
6.0.1	**2017-11-10**	**2018-11-10**	**2020-11-30**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Software Releases 5.4, 6.0 and 6.0.1 and Firepower Management Center Software Releases 5.4, 6.0 and 6.0.1
6.0.0	**2017-11-10**	**2018-11-10**	**2020-11-30**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Software Releases 5.4, 6.0 and 6.0.1 and Firepower Management Center Software Releases 5.4, 6.0 and 6.0.1
5.4	**2017-11-10**	**2018-11-10**	**2020-11-30**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Software Releases 5.4, 6.0 and 6.0.1 and Firepower Management Center Software Releases 5.4, 6.0 and 6.0.1
5.3	**2016-01-29**	**2016-07-30**	**2018-07-31**	End-of-Sale and End-of-Life Announcement for the Cisco FirePOWER Software v5.3 and v5.3.1 and FireSIGHT Management Center Software v5.3 and v5.3.1

These software versions on still-supported branches have been removed from the Cisco Support & Download site.

Table 23: Software Removed Versions

Version	Date Removed	Related Bugs and Additional Details
7.2.6	**2024-04-29**	CSCwi63113: FTD Boot Loop with SNMP Enabled after reload/upgrade
6.4.0.6	**2019-12-19**	CSCvr52109: FTD may not match correct Access Control rule following a deploy to multiple devices

These integrated products are deprecated.

Table 24: Deprecated Integrated Products

Product	Details
Cisco Firepower User Agent	Version 6.6 is the last release to support the Cisco Firepower User Agent software as an identity source. You cannot upgrade an FMC with user agent configurations to Version 6.7+. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC). This will also allow you to take advantage of features that are not available with the user agent. To convert your license, contact Sales. For more information, see the End-of-Life and End-of-Support for the Cisco Firepower User Agent announcement and the Firepower User Identity: Migrating from User Agent to Identity Services Engine TechNote.
Cisco Terminal Services (TS) Agent	Cisco TS Agent Versions 1.0 and 1.1 have been removed from the Cisco Support & Download site. If you are using either of these versions, we recommend you upgrade.
Cisco Security Packet Analyzer	Cisco Security Packet Analyzer is compatible with Versions 6.3 and 6.4 only.

Hardware and Virtual Platforms

These platforms have reached end of sale and/or end of support.

Table 25: Management Center Hardware EOL Announcements

Platform	Last Version	End of Sale	End of Support	Announcement
FMC 1600, 2600, 4600	TBD	**2023-11-30**	2028-11-30	End-of-Sale and End-of-Life Announcement for the Cisco Secure Firewall Management Center Platforms - FMC 1600, FMC 2600, FMC 4600
FMC 1000, 2500, 4500	7.0	**2019-07-12**	**2024-07-31**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Management Center Platforms- FMC 1000, FMC 2500, FMC 4500
FMC 4000	6.6	**2017-03-31**	**2022-03-31**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Management Center 4000
FMC 2000	6.6	**2017-03-31**	**2022-03-31**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Management Center 2000
FMC 750	6.4	**2017-03-31**	**2022-03-31**	End-of-Sale and End-of-Life Announcement for the Cisco Firepower Management Center 750

Platform	Last Version	End of Sale	End of Support	Announcement
FMC 1500	6.4	**2015-09-18**	**2020-09-30**	End-of-Sale and End-of-Life Announcement for the Cisco FireSIGHT Management Center 1500 Products
FMC 3500	6.4	**2015-08-31**	**2020-08-31**	End-of-Sale and End-of-Life Announcement for the Cisco FireSIGHT Management Center 3500
FMC 500, 1000, 3000	5.4	**Sales ended**	**Support ended**	—

Table 26: Virtual Platform EOL Announcements

Platform	Last Version	End of Sale	End of Support	Announcement
FMCv with Classic licenses	7.4	**2023-04-19**	**2025-04-30**	End-of-Sale and End-of-Life Announcement for the Cisco Secure Firewall Management Center for Virtual Classic license

Terminology and Branding

Table 27: Product Line

Current Name	Older Names
Secure Firewall Threat Defense	Firepower Firepower System FireSIGHT System Sourcefire 3D System

Table 28: Devices

Current Name		Older Names
Threat Defense	Secure Firewall Threat Defense	Firepower Threat Defense (FTD)
	Secure Firewall Threat Defense Virtual	Firepower Threat Defense Virtual (FTDv)

Current Name		Older Names
Classic NGIPS	ASA FirePOWER ASA FirePOWER module ASA with FirePOWER Services	—
	7000/8000 series	Series 3
	NGIPSv	virtual managed device
Legacy	Series 2	—
	Cisco NGIPS for Blue Coat X-Series	FireSIGHT Software for X-Series Sourcefire Software for X-Series

Table 29: Device Management

Current Name	Older Names
Secure Firewall Management Center	Firepower Management Center (FMC) FireSIGHT Management Center FireSIGHT Defense Center Defense Center
Secure Firewall Management Center Virtual	Firepower Management Center Virtual (FMCv) FireFIGHT Virtual Management Center FireSIGHT Virtual Defense Center Virtual Defense Center
Cloud-delivered Firewall Management Center	—
Secure Firewall device manager	Firepower Device Manager (FDM)
Secure Firewall Adaptive Security Device Manager (ASDM)	Adaptive Security Device Manager (ASDM)
Secure Firewall chassis manager	Firepower Chassis Manager
Security Cloud Control	Cisco Defense Orchestrator (CDO)

Table 30: Operating Systems

Current Name	Older Names
Secure Firewall eXtensible Operating System (FXOS)	Firepower eXtensible Operating System (FXOS)
Secure Firewall Adaptive Security Appliance (ASA) Software	Adaptive Security Appliance (ASA) software