Cisco Secure Firewall Threat Defense Compatibility Guide

First Published: 2022-05-05

Last Modified: 2024-10-04

Cisco Secure Firewall Threat Defense Compatibility Guide

This guide provides software and hardware compatibility for Cisco Secure Firewall Threat Defense. 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 35. 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 NGFW 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 Management Center Compatibility Guide Cisco Firepower 4100/9300 FXOS Compatibility
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 Cisco Firepower 4100/9300 FXOS Release Notes
New Feature guides provide information on new and deprecated features by release.	Cisco Secure Firewall Management Center New Features by Release Cisco Secure Firewall Device Manager New Features by Release

Description	Resources
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 Navigating the Cisco FXOS 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 NGFW Product Line Software Release and Sustaining Bulletin.

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

Threat Defense Platform Summary

These tables summarize the supported devices and on-prem (customer-deployed) management methods for threat defense.

Note The cloud-delivered Firewall Management Center can manage threat defense 7.0.3 to 7.6.0 (except 7.1). For CDO with device manager, you must be running at least threat defense 6.4.

Threat Defense Hardware

Table 2: Secure Firewall Threat Defense Hardware by Manager and Version

Device Platform	Device Versions: With On-Prem Management Center	Device Versions: With Device Manager
Firepower 1010, 1120, 1140	6.4+	6.4+
Firepower 1010E	7.2.3+ No support in 7.3	7.2.3+ No support in 7.3
Firepower 1150	6.5+	6.5+
Firepower 2110, 2120, 2130, 2140	6.2.1 to 7.4	6.2.1 to 7.4
Secure Firewall 3105	7.3.1+	7.3.1+
Secure Firewall 3110, 3120, 3130, 3140	7.1+	7.1+

Device Platform	Device Versions: With On-Prem Management Center	Device Versions: With Device Manager
Firepower 4110, 4120, 4140	6.0.1 to 7.2	6.5 to 7.2
Firepower 4150	6.1 to 7.2	6.5 to 7.2
Firepower 4115, 4125, 4145	6.4+	6.5+
Firepower 4112	6.6+	6.6+
Secure Firewall 4215, 4225, 4245	7.4.0+	—
Firepower 9300: SM-24, SM-36, SM-44	6.0.1 to 7.2	6.5 to 7.2
Firepower 9300: SM-40, SM-48, SM-56	6.4+	6.5+
ISA 3000	6.2.3+	6.2.3+
ASA 5506-X, 5506H-X, 5506W-X	6.0.1 to 6.2.3	6.1 to 6.2.3
ASA 5508-X, 5516-X	6.0.1 to 7.0	6.1 to 7.0
ASA 5512-X	6.0.1 to 6.2.3	6.1 to 6.2.3
ASA 5515-X	6.0.1 to 6.4	6.1 to 6.4
ASA 5525-X, 5545-X, 5555-X	6.0.1 to 6.6	6.1 to 6.6

Threat Defense Virtual

Table 3: Threat Defense Virtual by Manager and Version

Device Platform	Device Versions: With On-Prem Management Center	Device Versions: With Device Manager
Public Cloud		
AWS	6.0.1+	6.6+
Azure	6.2+	6.5+
GCP	6.7+	7.2+
OCI	6.7+	—
Megaport	7.2.8+	7.2.8+
On-Prem/Private Cloud		
HyperFlex	7.0+	7.0+
KVM	6.1+	6.2.3+
Nutanix	7.0+	7.0+

Device Platform	Device Versions: With On-Prem Management Center	Device Versions: With Device Manager
OpenStack	7.0+	—
VMware 8.0	7.6+	7.6+
VMware 7.0	7.0+	7.0+
VMware 6.7	6.5+	6.5+
VMware 6.5	6.2.3+	6.2.3+
VMware 6.0	6.0 to 6.7	6.2.2 to 6.7
VMware 5.5	6.0.1 to 6.2.3	6.2.2 to 6.2.3
VMware 5.1	6.0.1 only	—

Threat Defense Hardware

Firepower 1000/2100 Series

Firepower 1000/2100 series devices use the FXOS operating system. Upgrading threat defense automatically upgrades FXOS. For information on bundled FXOS versions, see Bundled Components, on page 17. These devices can also run ASA instead of threat defense; see Cisco Secure Firewall ASA Compatibility.

Table 4: Firepower 1000/2100 Series Compatibility

Threat Defense	Firepower 1150	Firepower 1010E	Firepower 1010 Firepower 1120 Firepower 1140	Firepower 2110 Firepower 2120 Firepower 2130 Firepower 2140
7.6	**YES**	**YES**	**YES**	—
7.4.1–7.4.x	**YES**	**YES**	**YES**	**YES**
7.4.0	—	—	—	—
7.3	**YES**	—	**YES**	**YES**
7.2	**YES**	**YES** Requires 7.2.3+	**YES**	**YES**
7.1	**YES**	—	**YES**	**YES**
7.0	**YES**	—	**YES**	**YES**
6.7	**YES**	—	**YES**	**YES**
6.6	**YES**	—	**YES**	**YES**

Threat Defense	Firepower 1150	Firepower 1010E	Firepower 1010 Firepower 1120 Firepower 1140	Firepower 2110 Firepower 2120 Firepower 2130 Firepower 2140
6.5	**YES**	—	**YES**	**YES**
6.4	—	—	**YES**	**YES**
6.3	—	—	—	**YES**
6.2.3	—	—	—	**YES**
6.2.2	—	—	—	**YES**
6.2.1	—	—	—	**YES**

Secure Firewall 3100/4200 Series

Secure Firewall 3100/4200 series devices use the FXOS operating system. How FXOS is upgraded depends on whether the device is in application mode or multi-instance mode. These devices can also run ASA instead of threat defense; see Cisco Secure Firewall ASA Compatibility.

Secure Firewall Series 3100/4200 in Application Mode

In application mode, upgrading threat defense automatically upgrades FXOS. For information on bundled FXOS versions, see Bundled Components, on page 17.

Table 5: Secure Firewall 3100/4200 Series Application Mode Compatibility

Threat Defense	Secure Firewall 4215 Secure Firewall 4225 Secure Firewall 4245	Secure Firewall 3105	Secure Firewall 3110 Secure Firewall 3120 Secure Firewall 3130 Secure Firewall 3140
7.6	**YES**	**YES**	**YES**
7.4.1–7.4.x	**YES**	**YES**	**YES**
7.4.0	**YES**	—	—
7.3	—	**YES**	**YES**
7.2	—	—	**YES**
7.1	—	—	**YES**

Secure Firewall 3100/4200 Series in Multi-Instance Mode

In multi-instance mode, you upgrade the chassis (FXOS and firmware) and threat defense separately. However, one package contains both components. It is possible to have a chassis-only upgrade or a threat defense-only upgrade. For information on bundled FXOS versions, see Bundled Components, on page 17.

Although you can run older threat defense instances on a newer FXOS, new features and resolved issues often require a full upgrade.

Table 6: Secure Firewall 3100/4200 Series Multi-Instance Mode Compatibility

Threat Defense	Secure Firewall 4215 Secure Firewall 4225 Secure Firewall 4245	Secure Firewall 3110 Secure Firewall 3120 Secure Firewall 3130 Secure Firewall 3140
7.6	**YES**	**YES**
7.4.1–7.4.x	—	**YES**

Firepower 4100/9300

For the Firepower 4100/9300, major threat defense versions have a specially qualified and recommended companion FXOS version, listed below in **bold**. Use these combinations whenever possible, because we perform enhanced testing for them. Note that the table lists the *minimum* build for each FXOS version, but in most cases we recommend the latest. For more information, see the Cisco Firepower 4100/9300 FXOS Release Notes.

Note Although we document that FXOS 2.14.1.163+ is required for threat defense 7.4.x, this is for reimaging to 7.4.2+. If you are already running an earlier FXOS 2.14.1 build, you can successfully upgrade to 7.4.2+ without upgrading FXOS (CSCwf64429).

These devices can also run ASA instead of threat defense. With ASA 9.12+ and threat defense 6.4.0+, you can run both ASA and threat defense on separate modules in the same Firepower 9300 chassis. For more information, see Cisco Firepower 4100/9300 FXOS Compatibility.

Table 7: Firepower 4100/9300 Compatibility

Threat Defense	FXOS	Firepower 9300		Firepower 4100 Series			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
7.6	**2.16.0.128+**	—	**YES**	—	—	**YES**	**YES**
7.4.1–7.4.x	**2.14.1.163+** 2.16.0.128+	—	**YES**	—	—	**YES**	**YES**

Threat Defense	FXOS	Firepower 9300		Firepower 4100 Series			
		SM-24 **SM-36** **SM-44**	**SM-40** **SM-48** **SM-56**	**4110** **4120** **4140**	**4150**	**4112**	**4115** **4125** **4145**
7.4.0	—	—	—	—	—	—	—
7.3	**2.13.0.198+** 2.14.1.163+ 2.16.0.128+	—	**YES**	—	—	**YES**	**YES**
7.2	**2.12.0.31+** 2.13.0.198+ 2.14.1.163+ 2.16.0.128+	**YES** no 2.13+	**YES**	**YES** no 2.13+	**YES** no 2.13+	**YES**	**YES**
7.1	**2.11.1.154+** 2.12.0.31+ 2.13.0.198+ 2.14.1.163+ 2.16.0.128+	**YES** no 2.13+	**YES**	**YES** no 2.13+	**YES** no 2.13+	**YES**	**YES**
7.0	**2.10.1.159+** 2.11.1.154+ 2.12.0.31+ 2.13.0.198+ 2.14.1.163+	**YES** no 2.13+	**YES**	**YES** no 2.13+	**YES** no 2.13+	**YES**	**YES**
6.7	**2.9.1.131+** 2.10.1.159+ 2.11.1.154+ 2.12.0.31+ 2.13.0.198+ 2.14.1.163+	**YES** no 2.13+	**YES**	**YES** no 2.13+	**YES** no 2.13+	**YES**	**YES**

Threat Defense	FXOS	Firepower 9300		Firepower 4100 Series			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.6	**2.8.1.105+** 2.9.1.131+ 2.10.1.159+ 2.11.1.154+ 2.12.0.31+ 2.13.0.198+ 2.14.1.163+	**YES** no 2.13+	**YES**	**YES** no 2.13+	**YES** no 2.13+	**YES**	**YES**
6.5	**2.7.1.92+** 2.8.1.105+ 2.9.1.131+ 2.10.1.159+ 2.11.1.154+ 2.12.0.31+	**YES**	**YES**	**YES**	**YES**	—	**YES**
6.4	**2.6.1.157+** 2.7.1.92+ 2.8.1.105+ 2.9.1.131+ 2.10.1.159+ 2.11.1.154+ 2.12.0.31+	**YES**	**YES**	**YES**	**YES**	—	**YES**
6.3	**2.4.1.214+** 2.6.1.157+ 2.7.1.92+ 2.8.1.105+ 2.9.1.131+ 2.10.1.159+ 2.11.1.154+ 2.12.0.31+	**YES**	—	**YES**	**YES**	—	—

Threat Defense	FXOS	Firepower 9300		Firepower 4100 Series			
		SM-24 SM-36 SM-44	SM-40 SM-48 SM-56	4110 4120 4140	4150	4112	4115 4125 4145
6.2.3	**2.3.1.73+** 2.4.1.214+ 2.6.1.157+ 2.7.1.92+ 2.8.1.105+ **Note** Firepower 6.2.3.16+ requires FXOS 2.3.1.157+.	**YES**	—	**YES**	**YES**	—	—
6.2.2	**2.2.2.x** 2.3.1.73+ 2.4.1.214+ 2.6.1.157+ 2.7.1.92+	**YES**	—	**YES**	**YES**	—	—
6.2.1	—	—	—	—	—	—	—
6.2.0	**2.1.1.x**, **2.2.1.x**, **2.2.2.x** 2.3.1.73+ 2.4.1.214+ 2.6.1.157+	**YES**	—	**YES**	**YES**	—	—
6.1	**2.0.1.x** 2.1.1.x 2.3.1.73+	**YES**	—	**YES**	**YES**	—	—
6.0.1	**1.1.4.x** 2.0.1.x	**YES**	—	**YES**	—	—	—

ASA 5500-X Series and ISA 3000

ASA 5500-X series and ISA 3000 devices use the ASA operating system. Upgrading threat defense automatically upgrades ASA. For information on the bundled ASA versions, see Bundled Components, on page 17.

Version 7.0 is the last major threat defense release that supports ASA 5500-X series devices.

Table 8: ASA 5500-X Series and ISA 3000 Compatibility

Threat Defense	ISA 3000	ASA 5508-X ASA 5516-X	ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5515-X	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5512-X
7.6	**YES**	—	—	—	—
7.4.1–7.4.x	**YES**	—	—	—	—
7.4.0	—	—	—	—	—
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**	—
6.3	**YES**	**YES**	**YES**	**YES**	—
6.2.3	**YES**	**YES**	**YES**	**YES**	**YES**
6.2.2	—	**YES**	**YES**	**YES**	**YES**
6.2.1	—	—	—	—	—
6.2.0	—	**YES**	**YES**	**YES**	**YES**
6.1	—	**YES**	**YES**	**YES**	**YES**
6.0.1	—	**YES**	**YES**	**YES**	**YES**

Threat Defense Virtual

Table 9: Threat Defense Virtual Compatibility: Public Cloud

Threat Defense Virtual	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Megaport Virtual Edge (Megaport)	Oracle Cloud Infrastructure (OCI)
7.6	**YES**	**YES**	**YES**	**YES**	**YES**
7.4.1–7.4.x	**YES**	**YES**	**YES**	**YES**	**YES**
7.4.0	—	—	—	—	—
7.3	**YES**	**YES**	**YES**	**YES**	**YES**
7.2	**YES**	**YES**	**YES**	**YES** Requires 7.2.8+	**YES**
7.1	**YES**	**YES**	**YES**	—	**YES**
7.0	**YES**	**YES**	**YES**	—	**YES**
6.7	**YES**	**YES**	**YES**	—	**YES**
6.6	**YES**	**YES**	—	—	—
6.6	**YES**	**YES**	—	—	—
6.4	**YES**	**YES**	—	—	—
6.3	**YES**	**YES**	—	—	—
6.2.3	**YES**	**YES**	—	—	—
6.2.2	**YES**	**YES**	—	—	—
6.2.1	—	—	—	—	—
6.2	**YES**	**YES**	—	—	—
6.1	**YES**	—	—	—	—
6.0.1	**YES**	—	—	—	—

Table 10: Threat Defense Virtual Compatibility: On-Prem/Private Cloud

Threat Defense Virtual	VMware vSphere/VMware ESXi	Cisco HyperFlex (HyperFlex)	Kernel-Based Virtual Machine (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack
7.6	**YES** VMware 6.5, 6.7, 7.0, 8.0	**YES**	**YES**	**YES**	**YES**

Threat Defense Virtual	VMware vSphere/VMware ESXi	Cisco HyperFlex (HyperFlex)	Kernel-Based Virtual Machine (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack
7.4.1–7.4.x	**YES** VMware 6.5, 6.7, 7.0	**YES**	**YES**	**YES**	**YES**
7.4.0	—	—	—	—	—
7.3	**YES** VMware 6.5, 6.7, 7.0	**YES**	**YES**	**YES**	**YES**
7.2	**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**
6.7	**YES** VMware 6.0, 6.5, 6.7	—	**YES**	—	—
6.6	**YES** VMware 6.0, 6.5, 6.7	—	**YES**	—	—
6.5	**YES** VMware 6.0, 6.5, 6.7	—	**YES**	—	—
6.4	**YES** VMware 6.0, 6.5	—	**YES**	—	—
6.3	**YES** VMware 6.0, 6.5	—	**YES**	—	—
6.2.3	**YES** VMware 5.5, 6.0, 6.5	—	**YES**	—	—

Threat Defense Virtual	VMware vSphere/VMware ESXi	Cisco HyperFlex (HyperFlex)	Kernel-Based Virtual Machine (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack
6.2.2	**YES** VMware 5.5, 6.0	—	**YES**	—	—
6.2.1	—	—	—	—	—
6.2.0	**YES** VMware 5.5, 6.0	—	**YES**	—	—
6.1	**YES** VMware 5.5, 6.0	—	**YES**	—	—
6.0.1	**YES** VMware 5.1, 5.5	—	—	—	—

Threat Defense High Availability and Clustering

These tables list threat defense support for high availability and clustering. For threat defense hardware, support differs depending on whether you are using standalone devices (also called native instances or application mode) or container instances (also called multi-instance mode). Threat defense virtual does not support container instances.

Standalone Devices

This table lists threat defense hardware support for high availability and clustering with standalone devices. In management center deployments, all threat defense hardware supports high availability. For device manager, high availability support begins in Version 6.3 and clustering is not supported.

Table 11: Hardware Standalone Devices: High Availability and Clustering Support

Platform	High Availability	Clustering
Firepower 1000	**YES**	—
Firepower 2100	**YES**	—
Secure Firewall 3100	**YES**	7.1+ (8 node) 7.6+ (16 node)
Secure Firewall 4200	**YES**	7.4+ (8 node) 7.6+ (16 node)
Firepower 4100	**YES**	7.2+ (16 node) 6.2 to 7.1 (6 node)

Platform	High Availability	Clustering
Firepower 9300	**YES**	7.2+ (16 node) 6.2 to 7.1 (6 node) Intra-chassis clustering (3 node) is also supported in all versions.
ASA 5500-X	**YES**	—
ISA 3000	**YES**	—

This table lists threat defense virtual support for high availability (with management center or device manager) and clustering (management center only).

Table 12: Virtual Standalone Devices: High Availability and Clustering Support

Platform	High Availability	Clustering
Public Cloud		
AWS	—	7.2+ (16 node)
Azure	—	7.3+ (16 node)
GCP	—	7.3+ (16 node)
Megaport	7.2.8+	—
OCI	—	—
On-Prem/Private Cloud		
HyperFlex	—	—
KVM	7.3	7.4.1+ (16 node) 7.2+ (4 node)
Nutanix	—	—
OpenStack	—	—
VMware	6.7	7.4.1+ (16 node) 7.2+ (4 node)

Container Instances

This table lists support for high availability and clustering with container instances, which is available on select threat defense hardware in management center deployments only.

Table 13: Container Instances: High Availability and Clustering Support

Platform	High Availability	Clustering
Secure Firewall 3100 series	7.4.1+	—
Secure Firewall 4200 series	7.6+	—
Firepower 4100 series	6.3+	7.2+ (16 node) 6.6 to 7.1 (6 node)
Firepower 9300	6.3+	7.2+ (16 node) 6.6 to 7.1 (6 node) Intra-chassis clustering (3 node) is also supported in Version 6.6+.

Threat Defense Management

On-Prem Management Center

All devices support remote management with a customer-deployed (*on-prem*) 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. And rarely, there are issues with specific management center-device combinations. For release-specific requirements, see the release notes.

Table 14: On-Prem Management Center-Device Compatibility

Management Center Version	Oldest Device Version You Can Manage
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

Management Center Version	Oldest Device Version You Can Manage
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 7.0.3 to 7.6.0 (except Version 7.1)**.

You can co-manage a cloud-managed device with a Version 7.2+ on-prem 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).

Co-managing Devices with an Analytics Management Center

The cloud-delivered Firewall Management Center supports a wider range of managed device versions than on-prem management centers. This can cause issues if you use an on-prem management center for analytics because devices can be "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 7.6.0 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.

In order of preference, you can:

- Upgrade the Version 7.0.x devices to at least Version 7.2.0, upgrade the analytics management center to Version 7.6.0, then add the Version 7.6.0 devices to both management centers.
- Remove the Version 7.0.x devices from the analytics management center, upgrade the analytics management center to Version 7.6.0, then add the Version 7.6.0 devices to both management centers.
- Leave the analytics management center as it is and do not add your Version 7.6.0 devices.

That is, your choices are:

- To get events from all devices, upgrade (or replace) the analytics management center and your older devices.
- To forgo events from older devices, upgrade (or replace) the analytics management center only.
- To forgo events from newer devices, leave the analytics management center at an older release.

Device Manager

You can use device manager to locally manage a single threat defense device. Most models suppport local management.

Optionally, add Cisco Defense Orchestrator to remotely manage multiple threat defense devices, as an alternative to the management center. Although some configurations still require device manager, CDO allows you to establish and maintain consistent security policies across your threat defense deployment.

Bundled Components

These tables list the versions of various components bundled with threat defense. 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 Systems

ASA 5500-X series and ISA 3000 devices use the ASA operating system. Firepower 1000/2100 and Secure Firewall 3100/4200 series devices use the FXOS operating system. For the Firepower 4100/9300, see Firepower 4100/9300, on page 6.

Table 15:

Threat Defense	ASA	FXOS
7.6.0	9.22(1.1)	2.16.0.128
7.4.2	9.20(2.32)	2.14.1.167
7.4.1.1	9.20(2.201)	2.14.1.131
7.4.1	9.20(2.2)	2.14.1.131
7.4.0	9.20(1.84)	2.14.0.475
7.3.1.1	9.19(1.202)	2.13.0.1022
7.3.1	9.19(1.200)	2.13.0.1022
7.3.0	9.19(1)	2.13.0.198
7.2.8.1	9.18(4.212)	2.12.1.1703
7.2.8	9.18(4.210)	2.12.1.73
7.2.7	9.18(4.201)	2.12.1.73
7.2.6	9.18(4.22)	2.12.1.73
7.2.5.2	9.18(3.61)	2.12.0.530
7.2.5.1	9.18(3.60)	2.12.0.530
7.2.5	9.18(3.53)	2.12.0.519
7.2.4.1	9.18(3.53)	2.12.0.519
7.2.4	9.18(3.39)	2.12.0.499
7.2.3.1	—	—
7.2.3	9.18(2.219)	2.12.0.1030
7.2.2	9.18(2.200)	2.12.0.1104
7.2.1	9.18(2.4)	2.12.0.442
7.2.0.1	9.18(1.200)	2.12.0.31
7.2.0	9.18(1)	2.12.0.31
7.1.0.3	9.17(1.24)	2.11.1.191
7.1.0.2	9.17(1.201)	2.11.1.1300
7.1.0.1	9.17(1.150)	2.11.1.154
7.1.0	9.17(1.0)	2.11.1.154

Threat Defense	ASA	FXOS
7.0.6.3	9.16(4.70)	2.10.1.1633
7.0.6.2	9.16(4.57)	2.10.1.1625
7.0.6.1	9.16(4.45)	2.10.1.1614
7.0.6	9.16(4.35)	2.10.1.1603
7.0.5.1	—	—
7.0.5	9.16(4.200)	2.10.1.1400
7.0.4	9.16(3.18)	2.10.1.208
7.0.3	9.16(3.201)	2.10.1.1200
7.0.2.1	9.16(3.200)	2.10.1.192
7.0.2	9.16(3.11)	2.10.1.192
7.0.1.1	9.16(2.5)	2.10.1.175
7.0.1	9.16(2.5)	2.10.1.175
7.0.0.1	9.16(1.25)	2.10.1.159
7.0.0	9.16(1)	2.10.1.159
6.7.0.3	9.15(1.19)	2.9.1.138
6.7.0.2	9.15(1.15)	2.9.1.138
6.7.0.1	9.15(1.8)	2.9.1.135
6.7.0	9.15(1)	2.9.1.131
6.6.7.2	9.14(4.201)	2.8.1.192
6.6.7.1	9.14(4.21)	2.8.1.192
6.6.7	9.14(4.13)	2.8.1.186
6.6.5.2	9.14(3.22)	2.8.1.172
6.6.5.1	9.14(3.15)	2.8.1.172
6.6.5	9.14(3.6)	2.8.1.165
6.6.4	9.14(2.155)	2.8.1.1148
6.6.3	9.14(2.151)	2.8.1.1146
6.6.1	9.14(1.150)	2.8.1.129
6.6.0.1	9.14(1.216)	2.8.1.105

Threat Defense	ASA	FXOS
6.6.0	9.14(1.1)	2.8.1.105
6.5.0.5	9.13(1.18)	2.7.1.129
6.5.0.4	9.13(1.5)	2.7.1.117
6.5.0.3	9.13(1.4)	2.7.1.117
6.5.0.2	9.13(1.151)	2.7.1.115
6.5.0.1	9.13(1.2)	2.7.1.115
6.5.0	9.13(1)	2.7.1.107
6.4.0.18	9.12(4.68)	2.6.1.272
6.4.0.17	9.12(4.62)	2.6.1.265
6.4.0.16	9.12(4.54)	2.6.1.260
6.4.0.15	9.12(4.41)	2.6.1.254
6.4.0.14	9.12(4.37)	2.6.1.239
6.4.0.13	9.12(4.37)	2.6.1.239
6.4.0.12	9.12(4.152)	2.6.1.230
6.4.0.11	9.12(2.40)	2.6.1.214
6.4.0.10	9.12(2.38)	2.6.1.214
6.4.0.9	9.12(2.33)	2.6.1.201
6.4.0.8	9.12(2.18)	2.6.1.166
6.4.0.7	9.12(2.151)	2.6.1.156
6.4.0.6	9.12(2.12)	2.6.1.156
6.4.0.5	9.12(2.4)	2.6.1.144
6.4.0.4	9.12(2.4)	2.6.1.144
6.4.0.3	9.12(1.12)	2.6.1.133
6.4.0.2	9.12(1.10)	2.6.1.133
6.4.0.1	9.12(1.7)	2.6.1.133
6.4.0	9.12(1.6)	2.6.1.133
6.3.0.5	9.10(1.31)	2.4.1.255
6.3.0.4	9.10(1.28)	2.4.1.248

Threat Defense	ASA	FXOS
6.3.0.3	9.10(1.18)	2.4.1.237
6.3.0.2	9.10(1.12)	2.4.1.237
6.3.0.1	9.10(1.8)	2.4.1.222
6.3.0	9.10(1.3)	2.4.1.216
6.2.3.18	9.9(2.91)	2.3.1.219
6.2.3.17	9.9(2.88)	2.3.1.217
6.2.3.16	9.9(2.74)	2.3.1.180
6.2.3.15	9.9(2.60)	2.3.1.167
6.2.3.14	9.9(2.55)	2.3.1.151
6.2.3.13	9.9(2.51)	2.3.1.144
6.2.3.12	9.9(2.48)	2.3.1.144
6.2.3.11	9.9(2.43)	2.3.1.132
6.2.3.10	9.9(2.41)	2.3.1.131
6.2.3.9	9.9(2.37)	2.3.1.122
6.2.3.8	9.9(2.37)	2.3.1.122
6.2.3.7	9.9(2.32)	2.3.1.118
6.2.3.6	9.9(2.26)	2.3.1.115
6.2.3.5	9.9(2.245)	2.3.1.108
6.2.3.4	9.9(2.15)	2.3.1.108
6.2.3.3	9.9(2.13)	2.3.1.104
6.2.3.2	9.9(2.8)	2.3.1.85
6.2.3.1	9.9(2.4)	2.3.1.84
6.2.3	9.9(2)	2.3.1.84
6.2.2.5	9.8(2.44)	2.2.2.107
6.2.2.4	9.8(2.36)	2.2.2.86
6.2.2.3	9.8(2.30)	2.2.2.79
6.2.2.2	9.8(2.22)	2.2.2.75
6.2.2.1	9.8(2.10)	2.2.2.63

Threat Defense	ASA	FXOS
6.2.2	9.8(2.3)	2.2.2.52
6.2.1	9.8(1)	2.2.1.49
6.2.0.6	9.7(1.25)	—
6.2.0.5	9.7(1.23)	—
6.2.0.4	9.7(1.19)	—
6.2.0.3	9.7(1.15)	—
6.2.0.2	9.7(1.10)	—
6.2.0.1	9.7(1.7)	—
6.2.0	9.7(1.4)	—
6.1.0.7	9.6(4.12)	—
6.1.0.6	9.6(3.23)	—
6.1.0.5	9.6(2.21)	—
6.1.0.4	9.6(2.16)	—
6.1.0.3	9.6(2.16)	—
6.1.0.2	9.6(2.4)	—
6.1.0.1	9.6(2.4)	—
6.1.0	9.6(2)	—
6.0.1.4	9.6(1.19)	—
6.0.1.3	9.6(1.12)	—
6.0.1.2	9.6(1.11)	—
6.0.1.1	9.6(1)	—
6.0.1	9.6(1)	—
6.0.0.1	9.6(1)	—
6.0.0	9.6(1)	—

Snort

Snort is the main inspection engine. Snort 3 is available in Version 6.7+ with device manager, and Version 7.0+ with management center.

Table 16:

Threat Defense	Snort 2	Snort 3
7.6.0	2.9.23-227	3.1.79.1-121
7.4.2	2.9.22-2000	3.1.53.220-107
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
7.2.8.1	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

Threat Defense	Snort 2	Snort 3
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
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	3.0.1.4-129
6.7.0.2	2.9.17-2003	3.0.1.4-129
6.7.0.1	2.9.17-1006	3.0.1.4-129
6.7.0	2.9.17-200	3.0.1.4-129
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	—

Threat Defense	Snort 2	Snort 3
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	—
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	—

Threat Defense	Snort 2	Snort 3
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	—
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	—

Threat Defense	Snort 2	Snort 3
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	—
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	—

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 17:

Threat Defense	VDB	GeoDB
7.6.0	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
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
6.0.1 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+.
- Cisco TS Agent: Versions 1.0 and 1.1 are no longer available.

Table 18: 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
7.6	3.3 patch 2 3.2 patch 5 3.1 patch 2+	3.2 3.1	—	1.4	1.0
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	—
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	—

Management Center/Threat Defense	Cisco Identity Services Engine (ISE)		Cisco Firepower User Agent	Cisco Terminal Services (TS) Agent	Passive Identity Agent
	ISE	ISE-PIC			
7.2.0–7.2.3	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	—
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	—

Management Center/Threat Defense	Cisco Identity Services Engine (ISE)		Cisco Firepower User Agent	Cisco Terminal Services (TS) Agent	Passive Identity Agent
	ISE	ISE-PIC			
6.3	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	—	—

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 Defense Orchestrator* chapters in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator
- Bundled with the Secure Firewall Management Center: Cisco Secure Firewall Management Center Device Configuration Guide

Table 19: Integrated Products: Cisco Secure Dynamic Attributes Connector

Management Center	Cisco Secure Dynamic Attributes Connector	
	On-Prem	Cloud-delivered (with CDO)
Cloud-delivered management center (no version)	3.0 2.2 2.0	**YES**
7.1+	3.0 2.2 2.0 1.1	**YES**
7.0	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 20: 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 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	Yes	Yes	No	No
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	No
Version 2.2 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	No
Version 2.3 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Version 3.0 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

CSDAC version/platform	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco Cyber Vision	Cisco Multicloud Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	vCenter	Webex	Zoom
Cloud-delivered (Cisco Defense Orchestrator)	Yes	No	No	Yes	Yes	No	Yes	No	Yes	Yes	Yes	No	No	No
Secure Firewall Management Center 7.4.1	Yes	No	No	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Secure Firewall Management Center 7.6	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 21: 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** Requires management center with threat defense 6.4.	**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 22: 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 23: Browsers

Browser	Device Manager Version
Google Chrome	Any
Mozilla Firefox	Any
Microsoft Edge (Windows only)	Version 6.7+
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 24: Screen Resolution

Interface	Minimum Resolution
Device manager	1024 x 768
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 device manager, click **Device**, then the **System Settings** > **Management Access** link, then the **Management Web Server** tab. For detailed procedures, see the online help or the Cisco Secure Firewall Device Manager 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.

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

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 6.7+ (with device manager) and Version 7.0+ (with management center). Snort 2 will be deprecated in a future release. You will eventually be unable to upgrade Snort 2 devices.

In management center deployments, upgrading to threat defense Version 7.2+ 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.

In device manager deployments, manually upgrade Snort. See *Intrusion Policies* in the Cisco Secure Firewall Device Manager 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 25: Software EOL Announcements

Version	End of Sale	End of Updates	End of Support	Announcement
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)
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)

Version	End of Sale	End of Updates	End of Support	Announcement
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
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

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

Note In Version 6.2.3+, uninstalling a patch (fourth-digit release) results in an appliance running the version you upgraded from. This means that you can end up running a deprecated version simply by uninstalling a later patch. Unless otherwise stated, do *not* remain at a deprecated version. Instead, we recommend you upgrade. If upgrade is impossible, uninstall the deprecated patch.

Table 26: 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

Version	Date Removed	Related Bugs and Additional Details
6.2.3.8	**2019-01-07**	CSCvn82378: Traffic through ASA/FTD might stop passing upon upgrading FMC to 6.2.3.8-51

Hardware and Virtual Platforms

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

Table 27: Threat Defense Hardware EOL Announcements

Platform	Last Device Version	Last Mgmt. Center to Manage	End of Sale	End of Support	Announcement
Firepower 2110, 2120, 2130, 2140	7.4	TBD	TBD	TBD	—
Firepower 4110	7.2	TBD	**2024-07-31**	2027-01-31	End-of-Sale and End-of-Life Announcement for the Cisco Firepower 4110 Series Security Appliances 3 YR Subscriptions
			2022-01-31	2027-01-31	End-of-Sale and End-of-Life Announcement for the Cisco Firepower 4110 Series Security Appliances & 5 YR Subscriptions
ASA 5508-X, 5516-X	7.0	7.4	**2021-08-02**	2026-08-31	End-of-Sale and End-of-Life Announcement for the Cisco ASA5508 and ASA5516 Series Security Appliance and 5 YR Subscriptions
ASA 5525-X, 5545-X, 5555-X	6.6	7.2	**2020-09-04**	2025-09-30	End-of-Sale and End-of-Life Announcement for the Cisco ASA5525, ASA5545 & ASA5555 Series Security Appliance & 5 YR Subscriptions
Firepower 4120, 4140, 4150	7.2	TBD	**2020-08-31**	2025-08-31	End-of-Sale and End-of-Life Announcement for the Cisco Firepower 4120/40/50 and FPR 9300 SM24/36/44 Series Security Appliances/Modules & 5 YR Subscription
Firepower 9300: SM-24, SM-36, SM-44 modules	7.2	TBD	**2020-08-31**	2025-08-31	End-of-Sale and End-of-Life Announcement for the Cisco Firepower 4120/40/50 and FPR 9300 SM24/36/44 Series Security Appliances/Modules & 5 YR Subscription

Platform	Last Device Version	Last Mgmt. Center to Manage	End of Sale	End of Support	Announcement
ASA 5515-X	6.4	7.0	**2017-08-25**	**2022-08-31**	End-of-Sale and End-of-Life Announcement for the Cisco ASA 5512-X and ASA 5515-X
ASA 5506-X, 5506H-X, 5506W-X	6.2.3	6.6	**2021-08-02**	2026-08-31	End-of-Sale and End-of-Life Announcement for the Cisco ASA5506 Series Security Appliance with ASA software
			2021-07-31	**2022-07-31**	End-of-Sale and End-of-Life Announcement for the Cisco ASA5506 Series Security Appliance 1 YR Subscriptions
			2020-05-05	**2022-07-31**	End-of-Sale and End-of-Life Announcement for the Cisco ASA5506 Series Security Appliance 3 YR Subscriptions
			2018-09-30	**2022-07-31**	End-of-Sale and End-of-Life Announcement for the Cisco ASA5506 Series Security Appliance 5 YR Subscriptions
ASA 5512-X	6.2.3	6.6	**2017-08-25**	**2022-08-31**	End-of-Sale and End-of-Life Announcement for the Cisco ASA 5512-X and ASA 5515-X

Terminology and Branding

Table 28: Product Line

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

Table 29: 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)
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 30: 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
Cisco Defense Orchestrator (CDO)	—

Table 31: 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