Cisco Secure Firewall Threat Defense Compatibility Guide

First Published: 2022-05-05

Last Modified: 2026-09-22

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 33. 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 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.	Release Notes for Secure Firewall Threat Defense 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 7.6.6

The current suggested release is Version 7.6.6.

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 Firewall 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 upgrade or 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.

Firewall Threat Defense compatibility per model

Firewall Threat Defense on Secure Firewall hardware

This section provides Secure Firewall hardware compatibility with Firewall Threat Defense. These devices can also run ASA instead of Firewall Threat Defense; see *Cisco Secure Firewall ASA Compatibility*.

For information on bundled FXOS versions, see Bundled components, on page 17.

Secure Firewall hardware compatibility with Firewall Threat Defense and Firewall Management Center

This table lists Secure Firewall hardware compatibility with Firewall Threat Defense and Firewall Management Center.

Table 2: Secure Firewall hardware compatibility with Firewall Threat Defense and Firewall Management Center

Threat Defense	Management Center		Secure Firewall model with Firewall Management Center						
	On-Prem	Cloud-Delivered	220	1210 1220	1230 1240 1250	3105	3110 3120 3130 3140	4215 4225 4245	6160 6170
10.x	10+	YES	YES	YES	YES	YES	YES	YES	YES
7.7	7.7+	YES	—	YES	YES	YES	YES	YES	—

Threat Defense	Management Center		Secure Firewall model with Firewall Management Center						
	On-Prem	Cloud-Delivered	220	1210 1220	1230 1240 1250	3105	3110 3120 3130 3140	4215 4225 4245	6160 6170
7.6	7.6+	YES	—	YES	—	YES	YES	YES	—
7.4.1–7.4.x	7.4.1+	YES	—	—	—	YES	YES	YES	—
7.4.0	7.4.0+	YES	—	—	—	—	—	YES	—
7.3	7.3+	YES	—	—	—	YES	YES	—	—
7.2	7.2–7.7	YES	—	—	—	—	YES	—	—
7.1	7.1–7.6	—	—	—	—	—	YES	—	—

Secure Firewall hardware compatibility with Firewall Threat Defense and Firewall Device Manager

This table lists Secure Firewall hardware compatibility with Firewall Threat Defense and Firewall Device Manager.

Table 3: Secure Firewall hardware compatibility with Firewall Threat Defense and Firewall Device Manager

Threat Defense	Secure Firewall model with Firewall Device Manager				
	220	1210 1220	1230 1240 1250	3105	3110 3120 3130 3140
10.x	YES	YES	YES	YES	YES
7.7	—	YES	YES	YES	YES
7.6	—	YES	—	YES	YES
7.4.1–7.4.x	—	—	—	YES	YES
7.4.0	—	—	—	—	—
7.3	—	—	—	YES	YES
7.2	—	—	—	—	YES
7.1	—	—	—	—	YES

Firewall Threat Defense on Firepower hardware

This section provides Firepower hardware compatibility with Firewall Threat Defense. These devices can also run ASA instead of Firewall Threat Defense; see *Cisco Secure Firewall ASA Compatibility*.

For information on FXOS for the Firepower 1000/2100, see Bundled components, on page 17. For information on FXOS for the Firepower 4100/9300, see Firepower 4100/9300 compatibility with FXOS, on page 11.

Firepower hardware compatibility with Firewall Threat Defense and Firewall Management Center

This table lists Firepower hardware compatibility with Firewall Threat Defense and Firewall Management Center.

Table 4: Firepower hardware compatibility with Firewall Threat Defense and Firewall Management Center

Threat Defense	Management Center		Firepower model with Firewall Management Center									
	On-Prem	Cloud-delivered	1010E	1010 1120 1140	1150	2110 2120 2130 2140	4110 4120 4140	4112	4115 4125 4145	4150	9300 SM-24 9300 SM-36 9300 SM-44	9300 SM-40 9300 SM-48 9300 SM-56
10.x	10.x+	YES	YES	YES	YES	—	—	YES	YES	—	—	YES
7.7	7.7+	YES	YES	YES	YES	—	—	YES	YES	—	—	YES
7.6	7.6+	YES	YES	YES	YES	—	—	YES	YES	—	—	YES
7.4.1–7.4.x	7.4.1+	YES	YES	YES	YES	YES	—	YES	YES	—	—	YES
7.4.0	—	—	—	—	—	—	—	—	—	—	—	—
7.3	7.3+	YES	—	YES	YES	YES	—	YES	YES	—	—	YES
7.2	7.2–7.7	YES	YES Requires 7.2.3+	YES	YES	YES	YES	YES	YES	YES	YES	YES
7.1	7.1–7.6	—	—	YES	YES	YES	YES	YES	YES	YES	YES	YES
7.0	7.0–7.4	—	—	YES	YES	YES	YES	YES	YES	YES	YES	YES
6.7	6.7–7.3	—	—	YES	YES	YES	YES	YES	YES	YES	YES	YES
6.6	6.6–7.2	—	—	YES	YES	YES	YES	YES	YES	YES	YES	YES
6.4	6.4–7.0	—	—	YES	—	YES	YES	—	YES	YES	YES	YES

Firepower hardware compatibility with Firewall Threat Defense and Firewall Device Manager

This table lists Firepower hardware compatibility with Firewall Threat Defense and Firewall Device Manager.

Table 5: Firepower hardware compatibility with Firewall Threat Defense and Firewall Device Manager

Threat Defense	Firepower model with Firewall Device Manager									
	1010E	1010 1120 1140	1150	2110 2120 2130 2140	4110 4120 4140	4112	4115 4125 4145	4150	9300 SM-24 9300 SM-36 9300 SM-44	9300 SM-40 9300 SM-48 9300 SM-56
10.x	YES	YES	YES	—	—	YES	YES	—	—	YES
7.7	YES	YES	YES	—	—	YES	YES	—	—	YES
7.6	YES	YES	YES	—	—	YES	YES	—	—	YES
7.4.1–7.4.x	YES	YES	YES	YES	—	YES	YES	—	—	YES
7.4.0	—	—	—	—	—	—	—	—	—	—
7.3	—	YES	YES	YES	—	YES	YES	—	—	YES
7.2	YES Requires 7.2.3+	YES	YES	YES	YES	YES	YES	YES	YES	YES
7.1	—	YES	YES	YES	YES	YES	YES	YES	YES	YES
7.0	—	YES	YES	YES	YES	YES	YES	YES	YES	YES
6.7	—	YES	YES	YES	YES	YES	YES	YES	YES	YES
6.6	—	YES	YES	YES	YES	YES	YES	YES	YES	YES
6.4	—	YES	—	YES	YES	—	—	—	—	—

Firewall Threat Defense on ASA 5500-X series and ISA 3000 hardware

This section lists ASA 5500-X series and ISA 3000 hardware compatibility with Firewall Threat Defense. These devices use the ASA operating system. Upgrading Firewall Threat Defense automatically upgrades ASA. For information on the bundled ASA versions, see Bundled components, on page 17.

These devices can also run ASA instead of Firewall Threat Defense; see *Cisco Secure Firewall ASA Compatibility*.

Version 7.0 is the last major Firewall Threat Defense release that supports the ASA 5500-X series.

ASA 5500-X series and ISA 3000 hardware compatibility with Firewall Threat Defense and Firewall Management Center

This table lists ASA 5500-X series and ISA 3000 hardware compatibility with Firewall Threat Defense and Firewall Management Center.

Table 6: ASA 5500-X series and ISA 3000 hardware compatibility with Firewall Threat Defense and Firewall Management Center

Threat Defense	Management Center		Device model with Firewall Management Center			
	On-Prem	Cloud-Delivered	ISA 3000	ASA 5508-X ASA 5516-X	ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5515-X
10.x	10.x+	**YES**	**YES**	—	—	—
7.7	7.7+	**YES**	**YES**	—	—	—
7.6	7.6+	**YES**	**YES**	—	—	—
7.4.1–7.4.x	7.4.1+	**YES**	**YES**	—	—	—
7.4.0	—	—	—	—	—	—
7.3	7.3+	**YES**	**YES**	—	—	—
7.2	7.2–7.7	**YES**	**YES**	—	—	—
7.1	7.1–7.6	—	**YES**	—	—	—
7.0	7.0–7.4	—	**YES**	**YES**	—	—
6.7	6.7–7.3	—	**YES**	**YES**	—	—
6.6	6.6–7.2	—	**YES**	**YES**	**YES**	—
6.4	6.4–7.0	—	**YES**	**YES**	**YES**	**YES**

ASA 5500-X series and ISA 3000 hardware compatibility with Firewall Threat Defense and Firewall Device Manager

This table lists ASA 5500-X series and ISA 3000 hardware compatibility with Firewall Threat Defense and Firewall Device Manager.

Table 7: ASA 5500-X series and ISA 3000 hardware compatibility with Firewall Threat Defense and Firewall Device Manager

Threat Defense	Device model with Firewall Device Manager			
	ISA 3000	ASA 5508-X ASA 5516-X	ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5515-X
10.x	**YES**	—	—	—

Threat Defense	Device model with Firewall Device Manager			
	ISA 3000	ASA 5508-X ASA 5516-X	ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5515-X
7.7	YES	—	—	—
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	—
6.4	YES	YES	YES	YES

Firewall Threat Defense Virtual in a public cloud

This section lists public cloud compatibility with Firewall Threat Defense Virtual. For full details on supported instances, see the Secure Firewall Threat Defense Virtual getting started guides for your version.

Public cloud compatibility with Firewall Threat Defense Virtual and Firewall Management Center

This table lists public cloud compatibility with Firewall Threat Defense Virtual and Firewall Management Center.

Table 8: Public cloud compatibility with Firewall Threat Defense Virtual and Firewall Management Center

Threat Defense Virtual	Management Center		Public cloud with Firewall Management Center					
	On-Prem	Cloud-Delivered	Alibaba Cloud (Alibaba)	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Megaport Virtual Edge (Megaport)	Oracle Cloud Infrastructure (OCI)
10.x	10.0+	YES	YES	YES	YES	YES	YES	YES
7.7	7.7+	YES	YES	YES	YES	YES	YES	YES
7.6	7.6+	YES	YES	YES	YES	YES	YES	YES
7.4.1–7.4.x	7.4.1+	YES	YES	YES	YES	YES	YES	YES

Threat Defense Virtual	Management Center		Public cloud with Firewall Management Center					
	On-Prem	Cloud-Delivered	Alibaba Cloud (Alibaba)	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Megaport Virtual Edge (Megaport)	Oracle Cloud Infrastructure (OCI)
7.4.0	—	—	—	—	—	—	—	—
7.3	7.3+	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
7.2	7.2–7.7	**YES**	**YES**	**YES**	**YES**	**YES**	**YES** Requires 7.2.8+	**YES**
7.1	7.1–7.6	—	—	**YES**	**YES**	**YES**	—	**YES**
7.0	7.0–7.4	—	—	**YES**	**YES**	**YES**	—	**YES**
6.7	6.7–7.3	—	—	**YES**	**YES**	**YES**	—	**YES**
6.6	6.6–7.2	—	—	**YES**	**YES**	—	—	—
6.4	6.4–7.0	—	—	**YES**	**YES**	—	—	—

Public cloud compatibility with Firewall Threat Defense Virtual and Firewall Device Manager

This table lists public cloud compatibility with Firewall Threat Defense Virtual and Firewall Device Manager.

Table 9: Public cloud compatibility with Firewall Threat Defense Virtual and Firewall Device Manager

Threat Defense Virtual	Public cloud with Firewall Device Manager			
	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Megaport Virtual Edge (Megaport)
10.x	**YES**	**YES**	**YES**	**YES**
7.7	**YES**	**YES**	**YES**	**YES**
7.6	**YES**	**YES**	**YES**	**YES**
7.4.1–7.4.x	**YES**	**YES**	**YES**	**YES**
7.4.0	—	—	—	—
7.3	**YES**	**YES**	**YES**	**YES**
7.2	**YES**	**YES**	**YES**	**YES** Requires 7.2.8+
7.1	**YES**	**YES**	**YES**	—
7.0	**YES**	**YES**	**YES**	—

Threat Defense Virtual	Public cloud with Firewall Device Manager			
	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Megaport Virtual Edge (Megaport)
6.7	**YES**	**YES**	**YES**	—
6.6	**YES**	**YES**	—	—
6.4	**YES**	**YES**	—	—

Hypervisors and instances for Firewall Threat Defense Virtual in a public cloud

For full details on supported hypervisors and instances, see the chapter for your hypervisor in the Secure Firewall Threat Defense Virtual getting started guides for your version. This table indicates where you can find the information you need.

Table 10: Hypervisors and instances for Firewall Threat Defense Virtual in a public cloud

Hypervisor	*Getting Started Guide* section
Alibaba Cloud	Alibaba Cloud Supported Instance Types Threat Defense Virtual Versions
AWS	AWS Supported Instance Types Threat Defense Virtual Versions
Azure	Azure Supported VM Sizes Threat Defense Virtual Versions
GCP	GCP Machine Types Threat Defense Virtual Versions
Megaport	Guidelines and Limitations to Deploy the Threat Defense Virtual as a Megaport Virtual Edge
OCI	OCI Compute Shapes

Firewall Threat Defense Virtual in an on-prem/private cloud

This section lists on-prem/private cloud compatibility with Firewall Threat Defense Virtual.

On-prem/private cloud compatibility with Firewall Threat Defense Virtual and Firewall Management Center

This table lists on-prem/private cloud compatibility with Firewall Threat Defense Virtual and Firewall Management Center.

Table 11: On-prem/private cloud compatibility with Firewall Threat Defense Virtual and Firewall Management Center

Threat Defense Virtual	Management Center		On-prem/private cloud with Firewall Management Center					
	On-Prem	Cloud-Delivered	VMware vSphere/VMware ESXi	Cisco HyperFlex (HyperFlex)	Microsoft Hyper-V (Hyper-V)	Kernel-Based Virtual Machine (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack
10.x	10.x+	YES	YES	YES	YES	YES	YES	YES
7.7	7.7+	YES	YES	YES	—	YES	YES	YES
7.6	7.6+	YES	YES	YES	—	YES	YES	YES
7.4.1–7.4.x	7.4.1+	YES	YES	YES	—	YES	YES	YES
7.4.0	—	—	—	—	—	—	—	—
7.3	7.3+	YES	YES	YES	—	YES	YES	YES
7.2	7.2–7.7	YES	YES	YES	—	YES	YES	YES
7.1	7.1–7.6	—	YES	YES	—	YES	YES	YES
7.0	7.0–7.4	—	YES	YES	—	YES	YES	YES
6.7	6.7–7.3	—	YES	—	—	YES	—	—
6.6	6.6–7.2	—	YES	—	—	YES	—	—
6.4	6.4–7.0	—	YES	—	—	YES	—	—

On-prem/private cloud compatibility with Firewall Threat Defense Virtual and Firewall Device Manager

This table lists on-prem/private cloud compatibility with Firewall Threat Defense Virtual and Firewall Device Manager.

Table 12: On-prem/private cloud compatibility with Firewall Threat Defense Virtual and Firewall Device Manager

Threat Defense Virtual	On-prem/private cloud with Firewall Device Manager				
	VMware vSphere/VMware ESXi	Cisco HyperFlex (HyperFlex)	Kernel-Based Virtual Machine (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack
10.x	YES	YES	YES	YES	—
7.7	YES	YES	YES	YES	—
7.6.4–7.6.x	YES	YES	YES	YES	YES
7.6.0–7.6.3	YES	YES	YES	YES	—
7.4.1–7.4.x	YES	YES	YES	YES	—

Threat Defense Virtual	On-prem/private cloud with Firewall Device Manager				
	VMware vSphere/VMware ESXi	Cisco HyperFlex (HyperFlex)	Kernel-Based Virtual Machine (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack
7.4.0	—	—	—	—	—
7.3	**YES**	**YES**	**YES**	**YES**	—
7.2	**YES**	**YES**	**YES**	**YES**	—
7.1	**YES**	**YES**	**YES**	**YES**	—
7.0	**YES**	**YES**	**YES**	**YES**	—
6.7	**YES**	—	**YES**	—	—
6.6	**YES**	—	**YES**	—	—
6.4	**YES**	—	**YES**	—	—

Hypervisors and instances for Firewall Threat Defense Virtual in an on-prem/private cloud

For full details on supported hypervisors and instances, see the chapter for your hypervisor in the Secure Firewall Threat Defense Virtual getting started guides for your version. This table indicates where you can find the information you need.

Table 13: Hypervisors and instances for Firewall Threat Defense Virtual in an on-prem/private cloud

Hypervisor	*Getting Started Guide* section
HyperFlex	HyperFlex Components and Versions
Hyper-V	Guidelines and Limitations
KVM	System Requirements
Nutanix	Nutanix Components and Versions
OpenStack	System Requirements
VMware	System Requirements

Firepower 4100/9300 compatibility with FXOS

This table lists Firepower 4100/9300 compatibility with Firewall Threat Defense and FXOS. Major Firewall Threat Defense versions have a specially qualified and recommended companion FXOS version. These versions appear in **bold**. Use these combinations whenever possible, because we perform enhanced testing for them. The table lists the minimum build for each FXOS version, but in most cases we recommend the latest. For more information, see the Firepower 4100/9300 FXOS release notes.

For Firepower 4100/9300 compatibility with Firewall Threat Defense by model, see Firewall Threat Defense on Firepower hardware, on page 4.

Table 14: Firepower 4100/9300 compatibility with Firewall Threat Defense and FXOS

Threat Defense	Minimum FXOS	Notes
10.1	**2.18.10.288+**	—
10.0	**2.18.0.520+** 2.18.10.288+	—
7.7	**2.17.0.518+** 2.18.0.520+ 2.18.10.288+	—
7.6	**2.16.0.136+** 2.17.0.518+ 2.18.0.520+ 2.18.10.288+	2.16.0.136+ required with Version 7.6.1+ to use the recommended **RADIUS Server-Enabled Message Authenticator** option. 2.16.0.128+ required to run Version 7.6.x.
7.4.1–7.4.x	**2.14.2.137+** 2.16.0.136+ 2.17.0.518+ 2.18.0.520+ 2.18.10.288+	2.14.2.137+ required with Version 7.4.3+ to use the recommended **RADIUS Server-Enabled Message Authenticator** option. 2.14.1.163+ required to reimage to 7.4.2+ (CSCwf64429). 2.14.1.131+ required to run Version 7.4.1+.
7.4.0	—	—
7.3	**2.13.0.198+** 2.14.2.137+ 2.16.0.136+ 2.17.0.518 2.18.0.520+ 2.18.10.288+	—
7.2	**2.12.1.95+** 2.13.0.198+ 2.14.2.137+ 2.16.0.136+ 2.17.0.518+	2.12.1.95+ required with Version 7.2.10+ to use the recommended **RADIUS Server-Enabled Message Authenticator** option. 2.12.0.31+ required to run Version 7.2.x. Version 7.2 is the last support for the Firepower 4110, 4120, 4140, 4150 and Firepower 9300 SM-24, SM-36, SM-44. These devices do not run FXOS 2.13+.

Threat Defense	Minimum FXOS	Notes
7.1	**2.11.1.154+** 2.12.1.95+ 2.13.0.198+ 2.14.2.137+ 2.16.0.136+	—
7.0	**2.10.1.331+** 2.11.1.154+ 2.12.1.95+ 2.13.0.198+ 2.14.2.137+	2.10.1.331+ required with Version 7.0.7+ to use the recommended **RADIUS Server-Enabled Message Authenticator** option. 2.10.1.179+ required to run Version 7.0.2+. 2.10.1.159+ required to run Version 7.0.0 or 7.0.1.
6.7	**2.9.1.131+** 2.10.1.331+ 2.11.1.154+ 2.12.1.95+ 2.13.0.198+ 2.14.2.137+	—
6.6	**2.8.1.105+** 2.9.1.131+ 2.10.1.331+ 2.11.1.154+ 2.12.1.95+ 2.13.0.198+ 2.14.2.137+	—
6.4	**2.6.1.157+** 2.7.1.92+ 2.8.1.105+ 2.9.1.131+ 2.10.1.331+ 2.11.1.154+ 2.12.1.95+	—

Firewall Threat Defense high availability and scalability

Firewall Threat Defense high availability and clustering

These tables list Firewall Threat Defense support for high availability and clustering.

Native instances on hardware platforms

This table lists Firewall Threat Defense hardware support for high availability and clustering with standalone devices, also called native instances or application mode.

Table 15: High availability and clustering for native instances on hardware platforms

Platform	High availability	Clustering (with Management Center only)
Secure Firewall hardware		
Secure Firewall 200	**YES**	—
Secure Firewall 1200	**YES**	—
Secure Firewall 3100	**YES**	7.6+ (16 node) 7.1+ (8 node) Clustering is not supported with the Secure Firewall 3105.
Secure Firewall 4200	**YES**	7.6+ (16 node) 7.4+ (8 node)
Secure Firewall 6100	**YES**	10.0.0 (4 node)
Firepower hardware		
Firepower 1000	**YES**	—
Firepower 2100	**YES**	—
Firepower 4100	**YES**	7.2+ (16 node) 6.2+ (6 node)
Firepower 9300	**YES**	7.2+ (16 node) 6.2+ (6 node) Intra-chassis clustering (3 node) is also supported in all versions.
ASA-based hardware		
ASA 5500-X	**YES**	—
ISA 3000	**YES**	—

Native instances on virtual platforms

This table lists Firewall Threat Defense Virtual support for high availability and clustering with standalone devices.

Table 16: High availability and clustering for native instances on virtual platforms

Platform	High availability	Clustering (with Management Center only)
Public cloud		
Alibaba	—	—
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	—	—
Hyper-V	10.0+	—
KVM	7.3+	7.4.1+ (16 node) 7.2+ (4 node)
Nutanix	7.2+	—
OpenStack	—	—
VMware	6.7+	7.4.1+ (16 node) 7.2+ (4 node)

Container instances on hardware platforms

This table lists Firewall Threat Defense support for high availability and clustering with container instances, also called multi-instance mode. Multi-instance mode is available only on select hardware in Firewall Management Center deployments; see Firewall Threat Defense multi-instance mode, on page 16.

Table 17: High availability and clustering for container instances on hardware platforms

Platform	High availability	Clustering
Secure Firewall hardware		
Secure Firewall 3100	7.4.1+	—
Secure Firewall 4200	7.6+	—

Platform	High availability	Clustering
Firepower hardware		
Firepower 4100	6.3+	7.2+ (16 node) 6.6+ (6 node)
Firepower 9300	6.3+	7.2+ (16 node) 6.6+ (6 node) Intra-chassis clustering (3 node) is also supported in Version 6.6+.

Firewall Threat Defense multi-instance mode

This table lists Firewall Threat Defense support for container instances, also called multi-instance mode. This is in contrast to native instances, also called application mode. For container instance support with high availability and clustering, see Firewall Threat Defense high availability and clustering, on page 14.

In multi-instance mode, you upgrade the chassis (FXOS and firmware) and Firewall Threat Defense separately. Although you can run older Firewall Threat Defense instances on a newer FXOS, new features and resolved issues often require a full upgrade.

Table 18: Firewall Threat Defense multi-instance mode support

Threat Defense	Secure Firewall 3110 Secure Firewall 3120 Secure Firewall 3130 Secure Firewall 3140	Secure Firewall 4215 Secure Firewall 4225 Secure Firewall 4245	Firepower 4100/9300
10.x	**YES**	**YES**	**YES**
7.7	**YES**	**YES**	**YES**
7.6	**YES**	**YES**	**YES**
7.4.1–7.4.x	**YES**	—	**YES**
7.4.0	—	—	—
7.2	—	—	**YES**
7.1	—	—	**YES**
7.0	—	—	**YES**
6.7	—	—	**YES**
6.6	—	—	**YES**
6.4	—	—	**YES**

Bundled components

These tables list the versions of various components bundled with Firewall 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

Most devices use the FXOS operating system. ASA 5500-X and ISA 3000 devices use ASA. Note that for the Firepower 4100/9300, FXOS is not bundled.

Table 19: Operating systems

Threat Defense	ASA	FXOS
10.1.0	9.24(10.0)	2.18.10.228
10.0.2	89.24(1.218)	2.18.0.6008
10.0.1	—	—
10.0.0	9.24(1.0)	2.18.0.516
7.7.13	99.23(37.153)	82.17.26.4004
7.7.12	99.23(37.134)	82.17.26.1001
7.7.11	99.23(37.133)	82.17.26.1001
7.7.10.1	99.23(37.127)	82.17.26.14
7.7.10	99.23(37.126)	82.17.26.14
7.7.0	9.23(1)	2.17.0.518
7.6.6	89.22(3.226)	2.16.1.6012
7.6.5	—	—
7.6.4	9.22(2.29)	2.16.1.147
7.6.3	9.22(1.129)	2.16.0.4006
7.6.2.1	9.22(1.128)	2.16.0.4006
7.6.2	9.22(1.127)	2.16.0.4006
7.6.1	9.22(1.21)	2.16.0.3007
7.6.0	9.22(1.1)	2.16.0.128
7.4.8	89.20(4.217)	2.14.3.2005
7.4.7	9.20(4.30)	2.14.3.124

Threat Defense	ASA	FXOS
7.4.6	—	—
7.4.5	—	—
7.4.4	9.20(3.58)	2.14.2.2004
7.4.3	9.20(3.50)	2.14.2.137
7.4.2.4	9.20(2.121)	2.14.1.187
7.4.2.3	9.20(2.43)	2.14.1.187
7.4.2.2	9.20(2.42)	2.14.1.187
7.4.2.1	9.20(2.36)	2.14.1.176
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
7.2.12	89.18(4.212)	2.12.1.3001
7.2.11	9.18(4.77)	2.12.1.112
7.2.10.2	9.18(4.205)	2.12.1.101
7.2.10.1	—	—
7.2.10	9.18(4.60)	2.12.1.101
7.2.9	9.18(4.47)	2.12.1.86
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

Threat Defense	ASA	FXOS
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
7.0.10	9.16(4.103)	2.10.1.5005
7.0.9	9.16(4.90)	2.10.1.5001
7.0.8.1	9.16(4.127)	2.10.1.4006
7.0.8	9.16(4.125)	2.10.1.4003
7.0.7	9.16(4.80)	2.10.1.1642
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

Threat Defense	ASA	FXOS
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
6.6.0	9.14(1.1)	2.8.1.105
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

Threat Defense	ASA	FXOS
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

Snort

Snort is the main inspection engine. Snort 3 is available in Firewall Threat Defense Version 6.7+ with Firewall Device Manager, and Version 7.0+ with Firewall Management Center. Version 7.6.0 is the last major version that supports Snort 2.

Table 20: Snort

Threat Defense	Snort 2	Snort 3
10.1.0	2.9.25-20096	3.9.31.1-150
10.0.2	2.9.25-2007	3.9.3.200-17
10.0.1	—	—
10.0.0	—	3.9.3.1-61
7.7.13	2.9.24-13000	3.3.5.1300-58
7.7.12	—	3.3.5.1000-66
7.7.11	—	3.3.5.1000-66
7.7.10.1	—	3.3.5.1000-57
7.7.10	—	3.3.5.1000-57
7.7.0	—	3.3.5.1-77
7.6.6	2.9.23-6003	3.1.79.600-71
7.6.5	—	—
7.6.4	2.9.23-4000	3.1.79.400-43

Threat Defense	Snort 2	Snort 3
7.6.3	2.9.23-1019	3.1.79.300-10
7.6.2.1	2.9.23-1019	3.1.79.200-7
7.6.2	2.9.23-1019	3.1.79.200-7
7.6.1	2.9.23-1019	3.1.79.100-68
7.6.0	2.9.23-227	3.1.79.1-121
7.4.8	2.9.22-8001	3.1.53.800-11
7.4.7	2.9.22-6000	3.1.53.700-12
7.4.6	—	—
7.4.5	—	—
7.4.4	2.9.22-4019	3.1.53.400-105
7.4.3	2.9.22-3010	3.1.53.300-90
7.4.2.4	2.9.22-2000	3.1.53.203-175
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
7.2.12	2.9.20-12006	3.1.21.1200-20
7.2.11	2.9.20-11007	3.1.21.1100-38
7.2.10.2	2.9.20-10002	3.1.21.1000-54
7.2.10.1	2.9.20-10002	3.1.21.1000-54
7.2.10	2.9.20-10002	3.1.21.1000-54
7.2.9	2.9.20-9000	3.1.21.900-7

Threat Defense	Snort 2	Snort 3
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
7.0.10	2.9.18-10005	3.1.0.1000-18
7.0.9	2.9.18-9002	3.1.0.900-19
7.0.8.1	2.9.18-7019	3.1.0.800-9
7.0.8	2.9.18-7019	3.1.0.800-9
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

Threat Defense	Snort 2	Snort 3
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	—
6.6.0	2.9.16-140	—
6.4.0.18	2.9.14-28000	—
6.4.0.17	2.9.14-27005	—
6.4.0.16	2.9.14-26002	—

Threat Defense	Snort 2	Snort 3
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	—

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 21: System databases

Threat Defense	VDB	GeoDB
10.1.0+	4.5.0-433	2025-09-25-018
10.0.2 through 10.0.x	4.5.0-428	2025-09-25-018
10.0.0 through 10.0.1	4.5.0-416	2025-09-25-018
7.7.13 through 7.7.x	4.5.0-428	2024-12-14-066
7.7.0 through 7.7.12	4.5.0-400	2024-12-14-066

Threat Defense	VDB	GeoDB
7.6.6 through 7.6.x	4.5.0-428	2022-07-04-101
7.6.0 through 7.6.5	4.5.0-392	2022-07-04-101
7.4.8 through 7.4.x	4.5.0-428	2022-07-04-101
7.4.1 through 7.4.7	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
6.4.0	4.5.0-309	2018-07-09-002

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 Firewall 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 22: Integrated products: identity services and 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)	3.5 3.4 3.3 The pxGrid Cloud identity source requires ISE 3.3 or any later version or patch.	3.2 3.1 2.7 patch 2+	—	1.4	1.0 1.1
10.0.0 10.1.0	3.5 3.4 3.3 The pxGrid Cloud identity source requires ISE 3.3 or any later version or patch.	3.4 patch 5 3.3 patch 10 3.2 3.1 2.7 patch 2+	—	1.4	1.0 1.1
7.7	3.5 3.4 3.3	3.2 3.1	—	1.4	1.0 1.1
7.6	3.5 3.4 3.3 3.2	3.4 patch 5 3.3 ptach 10 3.2 3.1	—	1.4	1.0 1.1
7.4	3.5 3.4 3.3 3.2 3.1	3.2 3.1	—	1.4	—

Management Center/Threat Defense	Cisco Identity Services Engine (ISE)		Cisco Firepower User Agent	Cisco Terminal Services (TS) Agent	Passive Identity Agent
	ISE	ISE-PIC			
7.3	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	—
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	—

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	—

Dynamic Attributes Connector

The Dynamic Attributes Connector is a lightweight application that quickly and seamlessly updates firewall policies on the Firewall 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 Security Cloud Control* chapters in *Cisco Security Cloud Control: Cloud-Delivered Firewall Management Center for Firewall Threat Defense*
- Bundled with the Secure Firewall Management Center: *Cisco Secure Firewall Management Center Device Configuration Guide*

Table 23: Integrated Products: Dynamic Attributes Connector

Management Center	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**

Management Center	Dynamic Attributes Connector	
	On-Prem	Cloud-delivered (with Security Cloud Control)
7.0	3.1 3.0 2.2 2.0 1.1	—

The 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 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 24: List of supported connectors by dynamic attributes connector version and platform

CSDAC version	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	No	Yes	No	Yes	No	No
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes	No	Yes	No	No
Version 2.2 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	No	No
Version 2.3 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes
Version 3.0 (on-premises)	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Version 3.1 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cloud-delivered (Security Cloud Control)	Yes	No	No	Yes	Yes	No	No	Yes	No	Yes	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	No	Yes	Yes	Yes
Secure Firewall Management Center 7.6	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Secure Firewall Management Center 7.7	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

CSDAC version	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
Secure Firewall Management Center 10.0.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Secure Firewall Management Center 10.1.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	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 25: 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**	—

Firewall 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 26: Integrated products: Firewall Threat Defense RA VPN

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

Browser requirements

Browsers

We support the latest three released versions of Google Chrome, Mozilla Firefox, and Microsoft Edge, running on currently supported versions of macOS and Microsoft Windows (with Edge on Windows only). Apple Safari is not extensively tested, but feedback is welcome. If you encounter issues with any other browser, an older browser version, 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

This table lists minimum screen reolutions for various interfaces.

Table 27: Screen resolution

Interface	Minimum resolution
Firewall Device Manager	1024 x 768
Firewall 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 Firewall 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 a decryption 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.

End-of-life announcements

This section provides end-of-life details. Dates that have passed are in **bold**.

Snort 2

If you are still using the Snort 2 inspection engine with Firewall Threat Defense, switch to Snort 3 now for improved detection and performance. It is available starting in Firewall Threat Defense Version 6.7+ with Firewall Device Manager and Version 7.0+ with Firewall Management Center. Snort 2 is deprecated in Version 7.7+, and prevents Firewall Threat Defense upgrade.

In Firewall Management Center deployments, upgrading to Firewall 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 *Custom Snort 3 Intrusion Policies for Access Control*.

In Firewall 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 28: Software EOL announcements

Version	End of sale	End of updates	End of support	Announcement
7.7	2026-09-29	2027-09-29	2028-09-30	End-of-Sale and End-of-Life Announcement for the Cisco Secure Firewall Threat Defense (FTD/FTDv) 7.7(x), Secure Firewall Management Center (FMC/FMCv) 7.7(x) and Secure Firewall eXtensible Operating System (FXOS) 2.17(x)

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)
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)

Version	End of sale	End of updates	End of support	Announcement
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.

Table 29: Software removed versions

Version	Date removed	Related bugs and additional details
7.4.4	**2025-10-13**	CSCws69719: Not able to post dynamic objects or TSAgents logins with 7.4.4
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

Hardware

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

Table 30: Firewall 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	**2025-05-27**	2030-05-31	End-of-Sale and End-of-Life Announcement for the Cisco Firepower 2100 Series Security Appliances & 5 YR Subscriptions

Platform	Last device version	Last Mgmt. Center to manage	End of sale	End of support	Announcement
Firepower 4110	7.2	7.7	**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	7.7	**2024-08-31**	**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 1 YR Subscriptions
			2022-08-31	**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 3 YR Subscriptions
			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	7.7	**2024-08-31**	**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 1 YR Subscriptions
			2022-08-31	**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 3 YR Subscriptions
			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
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

Platform	Last device version	Last Mgmt. Center to manage	End of sale	End of support	Announcement
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 31: Product line

Current name	Older names
Secure Firewall Threat Defense	Firepower Firepower System FireSIGHT System Sourcefire 3D System

Table 32: Devices

Current name		Older names
Firewall 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 33: 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 34: 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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022–2026 Cisco Systems, Inc. All rights reserved.