# Cisco Secure Firewall Threat Defense Compatibility Guide

**First Published:** 2022-05-05

**Last Modified:** 2022-06-06

## 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 Additional Resources, on page 1.

**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 22. If you feel a version is missing in error, contact Cisco TAC.

## Additional Resources

*Table 1:*

| 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<br><br>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<br><br>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<br><br>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 Firepower Documentation <br><br> Navigating the Cisco FXOS Documentation |

# Threat Defense Management

These tables list the supported devices and management methods for threat defense, by version.

### Management Methods

Use the management center to remotely manage multiple devices. The management center is available as a hardware, virtual, or cloud platform. A hardware management center or management center virtual must run the same or newer version as its managed devices.

Use device manager to locally manage a single threat defense device.

Use Cisco Defense Orchestrator (CDO) with device manager 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.

### Threat Defense Hardware

*Table 2: Threat Defense Hardware by Manager and Version*

| Device Platform | Device Versions: With Management Center | | Device Versions: With Device Manager | |
|---|---|---|---|---|
| | Hardware or Virtual Management Center | Cloud-Delivered Management Center | Device Manager Only | Device Manager + CDO |
| Firepower 1010, 1120, 1140 | 6.4+ | 7.2+ | 6.4+ | 6.4+ |
| Firepower 1150 | 6.5+ | 7.2+ | 6.5+ | 6.5+ |
| Firepower 2110, 2120, 2130, 2140 | 6.2.1+ | 7.2+ | 6.2.1+ | 6.4+ |
| Secure Firewall 3110, 3120, 3130, 3140 | 7.1+ | 7.2+ | 7.1+ | 7.1+ |
| Firepower 4110, 4120, 4140 | 6.0.1+ | 7.2+ | 6.5+ | 6.5+ |
| Firepower 4150 | 6.1+ | 7.2+ | 6.5+ | 6.5+ |
| Firepower 4115, 4125, 4145 | 6.4+ | 7.2+ | 6.5+ | 6.5+ |
| Firepower 4112 | 6.6+ | 7.2+ | 6.6+ | 6.6+ |

| Device Platform | Device Versions: With Management Center | | Device Versions: With Device Manager | |
|---|---|---|---|---|
| | Hardware or Virtual Management Center | Cloud-Delivered Management Center | Device Manager Only | Device Manager + CDO |
| Firepower 9300: SM-24, SM-36, SM-44 | 6.0.1+ | 7.2+ | 6.5+ | 6.5+ |
| Firepower 9300: SM-40, SM-48, SM-56 | 6.4+ | 7.2+ | 6.5+ | 6.5+ |
| ISA 3000 | 6.2.3+ | 7.2+ | 6.2.3+ | 6.4+ |
| 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 | 6.4 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 | 6.4 |
| ASA 5525-X, 5545-X, 5555-X | 6.0.1 to 6.6 | — | 6.1 to 6.6 | 6.4 to 6.6 |

## Threat Defense Virtual

*Table 3: Threat Defense Virtual by Manager and Version*

| Device Platform | Device Versions: With Management Center | | Device Versions: With Device Manager | |
|---|---|---|---|---|
| | Hardware/Virtual Management Center | Cloud-Delivered Management Center | Device Manager Only | Device Manager + CDO |
| Alibaba | 7.2+ | 7.2+ | — | — |
| AWS | 6.0.1+ | 7.2+ | 6.6+ | 6.6+ |
| Azure | 6.2+ | 7.2+ | 6.5+ | 6.5+ |
| GCP | 6.7+ | 7.2+ | 7.2+ | 7.2+ |
| HyperFlex | 7.0+ | 7.2+ | 7.0+ | 7.0+ |
| KVM | 6.1+ | 7.2+ | 6.2.3+ | 6.4+ |
| Nutanix | 7.0+ | 7.2+ | 7.0+ | 7.0+ |
| OCI | 6.7+ | 7.2+ | — | — |

| Device Platform | Device Versions: With Management Center | | Device Versions: With Device Manager | |
|---|---|---|---|---|
| | Hardware/Virtual Management Center | Cloud-Delivered Management Center | Device Manager Only | Device Manager + CDO |
| OpenStack | 7.0+ | 7.2+ | — | — |
| VMware | 6.0.1+ | 7.2+ | 6.2.2+ | 6.4+ |

# Threat Defense Hardware

## Firepower 1000/2100 and Secure Firewall 3100 Series

Firepower 1000/2100 and Secure Firewall 3100 series devices use the FXOS operating system. Upgrading threat defense automatically upgrades FXOS. For information on bundled FXOS versions, see Bundled Components, on page 10.

These devices can also run ASA; see Cisco Secure Firewall ASA Compatibility.

*Table 4: Firepower 1000/2100 and Secure Firewall 3100 Series Compatibility*

| Threat Defense | Secure Firewall 3110 Secure Firewall 3120 Secure Firewall 3130 Secure Firewall 3140 | Firepower 1150 | Firepower 1010 Firepower 1120 Firepower 1140 | Firepower 2110 Firepower 2120 Firepower 2130 Firepower 2140 |
|---|---|---|---|---|
| 7.2 | **YES** | **YES** | **YES** | **YES** |
| 7.1 | **YES** | **YES** | **YES** | **YES** |
| 7.0 | | **YES** | **YES** | **YES** |
| 6.7 | | **YES** | **YES** | **YES** |
| 6.6 | | **YES** | **YES** | **YES** |
| 6.5 | | **YES** | **YES** | **YES** |
| 6.4 | | — | **YES** | **YES** |
| 6.3 | | — | — | **YES** |
| 6.2.3 | | — | — | **YES** |
| 6.2.2 | | — | — | **YES** |

| Threat Defense | Secure Firewall 3110

Secure Firewall 3120

Secure Firewall 3130

Secure Firewall 3140 | Firepower 1150 | Firepower 1010

Firepower 1120

Firepower 1140 | Firepower 2110

Firepower 2120

Firepower 2130

Firepower 2140 |
|---|---|---|---|---|
| 6.2.1 | | — | — | **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.

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 .

To resolve issues, you may need to upgrade FXOS to the latest build. To help you decide, see the Cisco Firepower 4100/9300 FXOS Release Notes.

✎ **Note** To perform flow offload in the following major version sequences, you must be running a specific combination of threat defense and FXOS:

- Version 6.2.2.x: Version 6.2.2.2+ on FXOS 2.3.1.130+

- Version 6.2.0.x: Version 6.2.0.3+ on either FXOS 2.2.1.x *or* FXOS 2.2.2, builds 17-86

*Table 5: Firepower 4100/9300 Compatibility*

| Threat Defense | FXOS | Firepower 9300 | | Firepower 4100 Series | | | |
|---|---|---|---|---|---|---|---|
| | | SM-26

SM-36

SM-44 | SM-40

SM-48

SM-56 | 4110

4120

4140 | 4150 | 4112 | 4115

4125

4145 |
| 7.2 | **2.12.0.31+** | YES | YES | YES | YES | YES | YES |
| 7.1 | **2.11.1.154+**

2.12.0.31+ | YES | YES | YES | YES | YES | YES |
| 7.0 | **2.10.1.159+**

2.11.1.154+

2.12.0.31+ | YES | YES | YES | YES | YES | YES |

| Threat Defense | FXOS | Firepower 9300 | | Firepower 4100 Series | | | |
|---|---|---|---|---|---|---|---|
| | | SM-26 SM-36 SM-44 | SM-40 SM-48 SM-56 | 4110 4120 4140 | 4150 | 4112 | 4115 4125 4145 |
| 6.7 | **2.9.1.131**+ 2.10.1.159+ 2.11.1.154+ 2.12.0.31+ | YES | YES | YES | YES | YES | YES |
| 6.6 | **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 | YES |
| 6.5 | **2.7.1.92**+ 2.8.1.105+ 2.9.1.131+ 2.10.1.159+ 2.11.1.154+ | 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+ | 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+ | YES | — | YES | YES | — | — |

| Threat Defense | FXOS | Firepower 9300 | | Firepower 4100 Series | | | |
|---|---|---|---|---|---|---|---|
| | | SM-26 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 .

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

*Table 6: 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 |
|---|---|---|---|---|---|
| 7.2 | 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

In Version 7.0 and later, threat defense virtual supports performance-tiered Smart Software Licensing, based on throughput requirements and remote access VPN session limits. For more information on supported instances, throughputs, and other hosting requirements deployments, see the appropriate *Getting Started Guide*.

*Table 7: Threat Defense Virtual Compatibility: VMware*

| Threat Defense Virtual | VMware vSphere/VMware ESXi | | | | | |
|---|---|---|---|---|---|---|
| | 7.0 | 6.7 | 6.5 | 6.0 | 5.5 | 5.1 |
| 7.2 | YES | YES | YES | — | — | — |
| 7.1 | YES | YES | YES | — | — | — |

| Threat Defense Virtual | VMware vSphere/VMware ESXi | | | | | |
|---|---|---|---|---|---|---|
| | 7.0 | 6.7 | 6.5 | 6.0 | 5.5 | 5.1 |
| 7.0 | YES | YES | YES | — | — | — |
| 6.7 | — | YES | YES | YES | — | — |
| 6.6 | — | YES | YES | YES | — | — |
| 6.5 | — | YES | YES | YES | — | — |
| 6.4 | — | — | YES | YES | — | — |
| 6.3 | — | — | YES | YES | — | — |
| 6.2.3 | — | — | YES | YES | YES | — |
| 6.2.2 | — | — | — | YES | YES | — |
| 6.2.1 | — | — | — | — | — | — |
| 6.2.0 | — | — | — | YES | YES | — |
| 6.1 | — | — | — | YES | YES | — |
| 6.0.1 | — | — | — | — | YES | YES |

*Table 8: Threat Defense Virtual Compatibility: Other Hypervisors*

| Threat Defense Virtual | Alibaba | Amazon Web Services (AWS) | Microsoft Azure (Azure) | Google Cloud Platform (GCP) | Cisco HyperFlex (HyperFlex) | Kernel-Based Virtual Machine (KVM) | Nutanix Enterprise Cloud (Nutanix) | OpenStack | Oracle Cloud Infrastructure (OCI) |
|---|---|---|---|---|---|---|---|---|---|
| 7.2 | YES | YES | YES | YES | YES | YES | YES | YES | YES |
| 7.1 | — | YES | YES | YES | YES | YES | YES | YES | YES |
| 7.0 | — | YES | YES | YES | YES | YES | YES | YES | YES |
| 6.7 | — | YES | YES | YES | — | YES | — | — | YES |
| 6.6 | — | YES | YES | — | — | YES | — | — | — |
| 6.5 | — | YES | YES | — | — | YES | — | — | — |
| 6.4 | — | YES | YES | — | — | YES | — | — | — |
| 6.3 | — | YES | YES | — | — | YES | — | — | — |
| 6.2.3 | — | YES | YES | — | — | YES | — | — | — |
| 6.2.2 | — | YES | YES | — | — | YES | — | — | — |

| Threat Defense Virtual | Alibaba | Amazon Web Services (AWS) | Microsoft Azure (Azure) | Google Cloud Platform (GCP) | Cisco HyperFlex (HyperFlex) | Kernel-Based Virtual Machine (KVM) | Nutanix Enterprise Cloud (Nutanix) | OpenStack | Oracle Cloud Infrastructure (OCI) |
|---|---|---|---|---|---|---|---|---|---|
| 6.2.1 | — | — | — | — | — | — | — | — | — |
| 6.2.0 | — | **YES** | **YES** | — | — | **YES** | — | — | — |
| 6.1 | — | **YES** | — | — | — | **YES** | — | — | — |
| 6.0.1 | — | **YES** | — | — | — | — | — | — | — |

# 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 series devices use the FXOS operating system. Upgrading threat defense on these devices automatically upgrades the operating system.

*Table 9:*

| Threat Defense | ASA | FXOS |
|---|---|---|
| 7.2.0 | 9.18(1) | 2.12.0.31 |
| 7.1.0.1 | 9.17(1.150) | 2.11.1.154 |
| 7.1.0 | 9.17(1.0) | 2.11.1.154 |
| 7.0.1.1 | 9.16(2.5) | 2.10.1.175 |
| 7.0.2 | 9.16(3.11) | 2.10.1.192 |
| 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 |

| Threat Defense | ASA | FXOS |
|---|---|---|
| 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 |
| 6.5.0.5 | 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 |
| 6.4.0.15 | 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 |

| Threat Defense | ASA | FXOS |
|---|---|---|
| 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 |
| 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 |

| Threat Defense | ASA | FXOS |
|---|---|---|
| 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 |
| 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 10:*

| Threat Defense | Snort 2 | Snort 3 |
|---|---|---|
| 7.2.0 | 2.9.20-107 | 3.1.21.1-126 |
| 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 |
| 7.0.2 | 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 |
| 6.6.5.2 | 2.9.16-5204 | — |
| 6.6.5.1 | 2.9.16-5107 | — |
| 6.6.5 | 2.9.16-5034 | — |
| 6.6.4 | 2.9.16-4022 | — |
| 6.6.3 | 2.9.16-3033 | — |
| 6.6.1 | 2.9.16-1025 | — |
| 6.6.0.1 | 2.9.16-140 | — |
| 6.6.0 | 2.9.16-140 | — |
| 6.5.0.5 | 2.9.15-15510 | — |
| 6.5.0.4 | 2.9.15-15201 | — |
| 6.5.0.3 | 2.9.15-15201 | — |
| 6.5.0.2 | 2.9.15-15101 | — |

| Threat Defense | Snort 2 | Snort 3 |
|---|---|---|
| 6.5.0.1 | 2.9.15-15101 | — |
| 6.5.0 | 2.9.15-7 | — |
| 6.4.0.14 | 2.9.14-24000 | — |
| 6.4.0.13 | 2.9.14-19008 | — |
| 6.4.0.12 | 2.9.14-18011 | — |
| 6.4.0.11 | 2.9.14-17005 | — |
| 6.4.0.10 | 2.9.14-16023 | — |
| 6.4.0.9 | 2.9.14-15906 | — |
| 6.4.0.8 | 2.9.14-15707 | — |
| 6.4.0.7 | 2.9.14-15605 | — |
| 6.4.0.6 | 2.9.14-15605 | — |
| 6.4.0.5 | 2.9.14-15507 | — |
| 6.4.0.4 | 2.9.12-15301 | — |
| 6.4.0.3 | 2.9.14-15301 | — |
| 6.4.0.2 | 2.9.14-15209 | — |
| 6.4.0.1 | 2.9.14-15100 | — |
| 6.4.0 | 2.9.14-15003 | — |
| 6.3.0.5 | 2.9.13-15503 | — |
| 6.3.0.4 | 2.9.13-15409 | — |
| 6.3.0.3 | 2.9.13-15307 | — |
| 6.3.0.2 | 2.9.13-15211 | — |
| 6.3.0.1 | 2.9.13-15101 | — |
| 6.3.0 | 2.9.13-15013 | — |
| 6.2.3.18 | 2.9.12-1813 | — |
| 6.2.3.17 | 2.9.12-1605 | — |
| 6.2.3.16 | 2.9.12-1605 | — |
| 6.2.3.15 | 2.9.12-1513 | — |
| 6.2.3.14 | 2.9.12-1401 | — |

| Threat Defense | Snort 2 | Snort 3 |
|---|---|---|
| 6.2.3.13 | 2.9.12-1306 | — |
| 6.2.3.12 | 2.9.12-1207 | — |
| 6.2.3.11 | 2.9.12-1102 | — |
| 6.2.3.10 | 2.9.12-902 | — |
| 6.2.3.9 | 2.9.12-806 | — |
| 6.2.3.8 | 2.9.12-804 | — |
| 6.2.3.7 | 2.9.12-704 | — |
| 6.2.3.6 | 2.9.12-607 | — |
| 6.2.3.5 | 2.9.12-506 | — |
| 6.2.3.4 | 2.9.12-383 | — |
| 6.2.3.3 | 2.9.12-325 | — |
| 6.2.3.2 | 2.9.12-270 | — |
| 6.2.3.1 | 2.9.12-204 | — |
| 6.2.3 | 2.9.12-136 | — |
| 6.2.2.5 | 2.9.11-430 | — |
| 6.2.2.4 | 2.9.11-371 | — |
| 6.2.2.3 | 2.9.11-303 | — |
| 6.2.2.2 | 2.9.11-273 | — |
| 6.2.2.1 | 2.9.11-207 | — |
| 6.2.2 | 2.9.11-125 | — |
| 6.2.1 | 2.9.11-101 | — |
| 6.2.0.6 | 2.9.10-301 | — |
| 6.2.0.5 | 2.9.10-255 | — |
| 6.2.0.4 | 2.9.10-205 | — |
| 6.2.0.3 | 2.9.10-160 | — |
| 6.2.0.2 | 2.9.10-126 | — |
| 6.2.0.1 | 2.9.10-98 | — |
| 6.2.0 | 2.9.10-42 | — |

| Threat Defense | Snort 2 | Snort 3 |
|---|---|---|
| 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 11:**

| Threat Defense | VDB | GeoDB |
|---|---|---|
| 7.2.0 | 4.5.0-353 | 2022-05-11-103 |
| 7.1.0 | 4.5.0-346 | 2020-04-28-002 |
| 7.0.2 | 4.5.0-338 | 2020-04-28-002 |
| 7.0.1 | 4.5.0-338 | 2020-04-28-002 |
| 7.0.0 | 4.5.0-338 | 2020-04-28-002 |
| 6.7.0 | 4.5.0-338 | 2020-04-28-002 |
| 6.6.5 | 4.5.0-336 | 2019-06-03-002 |
| 6.6.4 | 4.5.0-336 | 2019-06-03-002 |

| Threat Defense | VDB | GeoDB |
|---|---|---|
| 6.6.3 | 4.5.0-336 | 2019-06-03-002 |
| 6.6.1 | 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 |
| 6.2.2 | 4.5.0-271 | 2017-01-17-002 |
| 6.2.1 | 4.5.0-271 | 2017-01-17-002 |
| 6.2.0 | 4.5.0-271 | 2015-10-12-001 |
| 6.0.1 | 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 12: Integrated Products: Identity Services/User Control*

| Management Center/Threat Defense | Cisco Identity Services Engine (ISE) | | Cisco Firepower User Agent | Cisco Terminal Services (TS) Agent |
| --- | --- | --- | --- | --- |
| | ISE | ISE-PIC | | |
| Supported with... | Management center Device manager | Management center Device manager | Management center only | Management center only |
| 7.2 | 3.1 3.0 2.7 patch 2+ | 3.1 2.7 patch 2+ | — | 1.4 1.3 |
| 7.1 | 3.1 3.0 2.7 patch 2+ | 3.1 2.7 patch 2+ | — | 1.4 1.3 |
| 7.0 | 3.1 3.0 2.7 patch 2+ 2.6 patch 6+ | 3.1 2.7 patch 2+ 2.6 patch 6+ | — | 1.4 1.3 |
| 6.7.x | 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 2.6, any patch 2.4 | 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 |
| 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 |

| Management Center/Threat Defense | Cisco Identity Services Engine (ISE) | | Cisco Firepower User Agent | Cisco Terminal Services (TS) Agent |
|---|---|---|---|---|
| | ISE | ISE-PIC | | |
| 6.2.3 | 2.3 patch 2<br>2.3<br>2.2 patch 5<br>2.2 patch 1<br>2.2 | 2.2 patch 1 | 2.4<br>2.3 | 1.2<br>1.1 |
| 6.2.2 | 2.3<br>2.2 patch 1<br>2.2<br>2.1 | 2.2 patch 1 | 2.3 | 1.2<br>1.1<br>1.0 |
| 6.2.1 | 2.1<br>2.0.1<br>2.0 | 2.2 patch 1 | 2.3 | 1.1<br>1.0 |
| 6.2.0 | 2.1<br>2.0.1<br>2.0<br>1.3 | — | 2.3 | — |
| 6.1 | 2.1<br>2.0.1<br>2.0<br>1.3 | — | 2.3 | — |
| 6.0.1 | 1.3 | — | 2.3 | — |

## Threat Detection

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.

*Table 13: Integrated Products: Threat Detection*

| Management Center/Threat Defense | Cisco SecureX | 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<br><br>Device manager | Management center<br><br>Device manager | Management center only | Management center only | Management center only |
| 7.2 | **YES** | **YES** | **YES** | **YES** | — |
| 7.1 | **YES** | **YES** | **YES** | **YES** | — |
| 7.0 | **YES** | **YES** | **YES** | **YES** | — |
| 6.7 | **YES** | **YES** | **YES** | **YES** | — |
| 6.6 | **YES** | **YES** | **YES** | **YES** | — |
| 6.5 | **YES** | **YES** | **YES** | **YES** | — |
| 6.4 | **YES** | **YES**<br><br>Requires FMC with FTD 6.4. | **YES** | **YES** | **YES** |
| 6.3 | — | — | — | **YES** | **YES** |
| 6.2.3 | — | — | — | **YES** | — |
| 6.2.2 | — | — | — | **YES** | — |
| 6.2.1 | — | — | — | **YES** | — |
| 6.2.0 | — | — | — | **YES** | — |
| 6.1 | — | — | — | **YES** | — |

## 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 Cisco Secure Dynamic Attributes Connector Configuration Guide.

*Table 14: Integrated Products: Cisco Secure Dynamic Attributes Connector*

| Management Center | Cisco Secure Dynamic Attributes Connector |
|---|---|
| 7.0+ | 1.0+ |

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

*Table 15: Integrated Products: Threat Defense RA VPN*

| Threat Defense | Cisco AnyConnect Secure Mobility Client |
|---|---|
| 6.2.2+ | 4.0+ |

# End-of-Life Announcements

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

### Software

These major software versions have reached end of sale and/or end of support.

*Table 16: Software EOL Announcements*

| Version | End of Sale | End of Support | Announcement |
|---|---|---|---|
| 6.7 | **2021-07-09** | 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) |
| 6.5 | **2020-06-22** | 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) |
| 6.3 | **2020-04-30** | 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** | 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** | 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 Support | Announcement |
|---------|-------------|----------------|--------------|
| 6.2.1 | **2019-03-05** | **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** | **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** | 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** | **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 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 17: Software Removed Versions*

| Version | Date Removed | Related Bugs and Additional Details |
|---------|-------------|-------------------------------------|
| 6.5.0.3 | **2020-03-02**: devices<br>**2020-02-04**: FMC | CSCvs86257: FMC Upgrade is failing at 800_post/1025_vrf_policy_upgrade.pl<br>This is an upgrade bug. If you are already running this version it is safe to continue. |
| 6.5.0.1 | **2019-12-19** | CSCvr52109: FTD may not match correct Access Control rule following a deploy to multiple devices |
| 6.4.0.6 | **2019-12-19** | CSCvr52109: FTD may not match correct Access Control rule following a deploy to multiple devices |
| 6.2.3.8 | **2019-01-07** | CSCvn82378: Traffic through ASA/FTD might stop passing upon upgrading FMC to 6.2.3.8-51 |
| 6.2.1 | **2017-11-17** | This version is replaced by Version 6.2.2, which offers the same functionality and supports the full set of platforms. |

## Hardware

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

*Table 18: Threat Defense Hardware EOL Announcements*

| Platform | Last Version | End of Sale | End of Support | Announcement |
|---|---|---|---|---|
| Firepower 4110 | — | **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 | **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 | **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<br><br>Firepower 9300: SM-24, SM-36, SM-44 modules | — | **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 | **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 | **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 | **2017-08-25** | 2022-08-31 | End-of-Sale and End-of-Life Announcement for the Cisco ASA 5512-X and ASA 5515-X |