Navigating the Cisco Secure Firewall Threat Defense Documentation

First Published: 2019-10-26

Navigating the Cisco Secure Firewall Threat Defense Documentation

About Cisco Secure Firewall Threat Defense Documentation

This roadmap provides links to currently available documentation for Cisco Secure Firewall Threat Defense (including Secure Firewall Management Center and Secure Firewall device manager).

To view all available documentation for a specific release, see the following documentation landing pages:

- Secure Firewall Threat Defense 7.6 Documentation—https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/landing-page/threat-defense/threatdefense-76-docs.html
- Cisco Secure Firewall Threat Defense 7.4 Documentation—https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/landing-page/threat-defense/threatdefense-74-docs.html
- Cisco Secure Firewall Threat Defense 7.3 Documentation—https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/landing-page/threat-defense/threatdefense-73-docs.html
- Cisco Secure Firewall Threat Defense 7.2 Documentation—https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/landing-page/threat-defense/threatdefense-72-docs.html
- Cisco Firepower Threat Defense 7.1 Documentation—https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/landing-page/threat-defense/threatdefense-71-docs.html
- Cisco Firepower Threat Defense 7.0 Documentation—https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/landing-page/threat-defense/threatdefense-70-docs.html
- Cisco Firepower Threat Defense 6.7 Documentation—https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/landing-page/threat-defense/threatdefense-67-docs.html
- Cisco Firepower Threat Defense 6.6 Documentation—https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/landing-page/threat-defense/threatdefense-66-docs.html
- Cisco Firepower Threat Defense 6.5 Documentation—https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/landing-page/threat-defense/threatdefense-65-docs.html
- Cisco Firepower Threat Defense 6.4 Documentation—https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/landing-page/threat-defense/threatdefense-64-docs.html
- Secure Firewall Threat Defense Use Cases—https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/landing-page/threat-defense/threatdefense-usecases.html

Related Roadmaps

- ASA documentation roadmap—http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html.
- FXOS documentation roadmap—http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html.

License Documentation

- Feature license information:
  - Cisco Secure Firewall Management Center Feature Licenses
  - Frequently Asked Questions (FAQ) about Licensing
  - The Licensing chapter in the Cisco Secure Firewall Management Center Administration Guide for your version.
- Open source license information:
  - Open source license information for all Cisco products is available at https://www.cisco.com/go/opensource.
  - Each product has its own open source licensing document, available from the Licensing Information link on the top-level documentation listing page for the product. See Top-Level Documentation Listing Pages for Management Center Deployments, on page 2.

Top-Level Documentation Listing Pages for Management Center Deployments

The following documents may be helpful when configuring Secure Firewall Management Center deployments, Version 6.0+.

Note Some of the linked documents are not applicable to Secure Firewall Management Center deployments. For example, some links on Secure Firewall Threat Defense pages are specific to deployments managed by Secure Firewall device manager, and some links on hardware pages are unrelated to management center. To avoid confusion, pay careful attention to document titles. Also, some documents cover multiple products and therefore may appear on multiple product pages.

Secure Firewall Management Center

- Secure Firewall Management Center hardware appliances:

  http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html
- Secure Firewall Management Center Virtual appliances:
  - http://www.cisco.com/c/en/us/support/security/defense-center-virtual-appliance/tsd-products-support-series-home.html
  - http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

Secure Firewall Threat Defense, also called NGFW (Next Generation Firewall) devices

- Secure Firewall Threat Defense software:

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw/tsd-products-support-series-home.html

- Secure Firewall Threat Defense Virtual:

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/tsd-products-support-series-home.html

- Firepower 1000 series:

  https://www.cisco.com/c/en/us/support/security/firepower-1000-series/tsd-products-support-series-home.html

- Secure Firewall 3100:

  https://www.cisco.com/c/en/us/support/security/secure-firewall-3100-series/series.html

- Firepower 4100 series:

  https://www.cisco.com/c/en/us/support/security/firepower-4100-series/tsd-products-support-series-home.html

- Secure Firewall 4200:

  https://www.cisco.com/c/en/us/support/security/secure-firewall-4200-series/series.html

- Firepower 9300:

  https://www.cisco.com/c/en/us/support/security/firepower-9000-series/tsd-products-support-series-home.html

- ISA 3000:

  https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/tsd-products-support-series-home.html

Compatibility Guide

The Cisco Secure Firewall Threat Defense Compatibility Guide lists the system software and hardware compatibility and requirements.

Release Notes

Release notes provide critical and release-specific information.

Note For ASA release notes, see the ASA documentation roadmap.

For FXOS release notes, see the FXOS documentation roadmap.

For Firepower hotfix release notes, see the Firepower Hotfix Release Notes.

Release	Guide
Version 7.6.0	Cisco Secure Firewall Threat Defense Release Notes, Version 7.6.0

Release	Guide
Version 7.4.1	Cisco Secure Firewall Threat Defense Release Notes, Version 7.4.x
Version 7.4.0	Cisco Secure Firewall Threat Defense Release Notes, Version 7.4.x
Version 7.3.0	Cisco Secure Firewall Threat Defense Release Notes, Version 7.3.x
Version 7.2.0	Cisco Secure Firewall Threat Defense Release Notes, Version 7.2.x
Version 7.1.0	Cisco Firepower Release Notes, Version 7.1
Version 7.0.0	Cisco Firepower Release Notes, Version 7.0
Version 6.7.0	• Cisco Firepower Release Notes, Version 6.7.0 • Cisco Firepower Release Notes, Version 6.7.0.1
Version 6.6.0	• Cisco Firepower Release Notes, Version 6.6.0 • Cisco Firepower Release Notes, Version 6.6.0.1
Version 6.5.0	• Cisco Firepower Release Notes, Version 6.5.0 • Cisco Firepower Release Notes, Version 6.5.0.2 and 6.5.0.4
Version 6.4.0.x	• Cisco Firepower Release Notes, Version 6.4.0 • Cisco Firepower Release Notes, Version 6.4.0.1, 6.4.0.2, 6.4.0.3, 6.4.04, 6.4.0.5, 6.4.0.7, and 6.4.0.8
Version 6.3.0.x	• Cisco Firepower Release Notes, Version 6.3.0 • Cisco Firepower Release Notes, Version 6.3.0.1, 6.3.0.2, 6.3.0.3, 6.3.0.4, and 6.3.0.5
Version 6.2.3.x	• Cisco Firepower Release Notes, Version 6.2.3 • Cisco Firepower Release Notes, Version 6.2.3.1, 6.2.3.2, 6.2.3.3, 6.2.3.4, 6.2.3.5, 6.2.3.6, 6.2.3.7, 6.2.3.9, 6.2.3.10, 6.2.3.11, 6.2.3.12, 6.2.3.13, 6.2.3.14, and 6.2.3.15
Version 6.2.2.x	• Firepower Release Notes, Version 6.2.2 • Firepower Release Notes, Version 6.2.2.1, 6.2.2.2, 6.2.2.3, 6.2.2.4, and 6.2.2.5
Version 6.2.1	Cisco Firepower Version 6.2.1 has been replaced by Cisco Firepower Version 6.2.2, which offers the same functionality and supports the full set of Firepower platforms; we strongly recommend updating to Version 6.2.2 in place of Version 6.2.1.
Version 6.2.0.x	• Firepower System Release Notes, Version 6.2.0 • Firepower Release Notes, Version 6.2.0.1, 6.2.0.2, 6.2.0.3, 6.2.0.4, 6.2.0.5, and 6.2.0.6

Release	Guide
Version 6.1.x	• Firepower System Release Notes Pre Installation Package, Version 6.1.0 • Firepower System Release Notes, Version 6.1.0 • Firepower System Release Notes for Hotfix AF • Firepower System Release Notes for Hotfix AI • Firepower System Release Notes for Hotfix AJ • Firepower System Release Notes for Hotfix AZ • Firepower System Release Notes for Hotfix CF • Firepower System Release Notes, Version 6.1.0.1 • Firepower System Release Notes, Version 6.1.0.2 • Firepower System Release Notes, Version 6.1.0.3 • Firepower System Release Notes, Version 6.1.0.4 • Firepower System Release Notes, Version 6.1.0.5 • Firepower System Release Notes for Hotfix DQ • Firepower System Release Notes, Version 6.1.0.6 • Firepower System Release Notes, Version 6.1.0.7
Version 6.0.1.x	• Firepower System Release Notes, Version 6.0.1 Pre-Install • Firepower System Release Notes, Version 6.0.1 • Firepower System Release Notes, Version 6.0.1.1 • Firepower System Verizon 6.0.1.1 Hotfix AU • Firepower System Release Notes, Version 6.0.1.2 • Firepower System Release Notes, Version 6.0.1.3 • Firepower System Release Notes, Version 6.0.1.4
Version 6.0.0.x	• Firepower System Release Notes, Version 6.0.0 Pre-Installation • Firepower System Release Notes, Version 6.0 • Firepower System Release Notes, Version 6.0.0.1

Migration Guides

Secure Firewall migration tool

You can use the Secure Firewall migration tool to migrate supported configurations to supported Secure Firewall Threat Defense confgurations for releases 6.2.3 and later.

- Migrating ASA Firewall to Threat Defense with the Firewall Migration Tool
- Migrating ASA to Firepower Threat Defense Using Cisco Defense Orchestrator
- Migrating Check Point Firewall to Threat Defense with the Firewall Migration Tool
- Migrating Palo Alto Networks Firewall to Firepower Threat Defense with the Firepower Migration Tool
- Migrating Fortinet Firewall to Threat Defense with the Firewall Migration Tool

For other related ASA to Threat Defense documents, see:

https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-guides-list.html

ASA-to-Firepower Threat Defense Migration Tool Image

The *Cisco ASA to Firepower Threat Defense Migration Guide* describes how to use Cisco's migration tool to convert ASA configurations to Firepower Threat Defense configurations.

Note This migration tool is deprecated and cannot migrate your ASA images to the latest Firepower Threat Defense releases.

- Cisco ASA to Firepower Threat Defense Migration Guide, Version 6.2.2
- Cisco ASA to Firepower Threat Defense Migration Guide, Version 6.2.1
- Cisco ASA to Firepower Threat Defense Migration Guide, Version 6.2

Upgrade Guides

- Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.6
- Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager, Version 7.4.x–7.6.x
- Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.4.1
- Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.3—Upgrade Threat Defense with Management Center to Version 7.3.0.
- Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager, Version 7.3—Upgrade Threat Defense with device manager to Version 7.3.0.
- Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.2—Upgrade Threat Defense with Management Center to Version 7.2.0.
- Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager, Version 7.2—Upgrade Threat Defense with device manager to Version 7.2.0.
- Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1.0—Upgrade Firepower Threat Defense with Firepower Management Center to Version 7.1.0.
- Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0—Upgrade a Firepower Management Center deployment to Version 7.0.0 or earlier.

- Cisco ASA Upgrade Guide—Upgrade an ASA device with an ASA FirePOWER module managed by ASDM.

Configuration Guides

This section lists configuration guides by management device:

Note For ASA configuration guides, see the ASA documentation roadmap.

For FXOS configuration guides, see the FXOS documentation roadmap.

Management Center

The management center configuration guides include detailed information on configuration using the management center web interface.

Release	Guide
All Versions	Threat Defense on 4100 or 9300 hardware, managed by Management Center: Deploy a Cluster for Threat Defense on the Firepower 4100/9300.
Version 7.4/7.4.1	• Cisco Secure Firewall Management Center Administration Guide, 7.6 • Cisco Secure Firewall Management Center Device Configuration Guide, 7.6 • Cisco Secure Firewall Management Center Snort 3 Configuration Guide, Version 7.6
Version 7.4/7.4.1	• Cisco Secure Firewall Management Center Administration Guide, 7.4 • Cisco Secure Firewall Management Center Device Configuration Guide, 7.4 • Cisco Secure Firewall Management Center Snort 3 Configuration Guide, Version 7.4
Version 7.3	• Cisco Secure Firewall Management Center Administration Guide, 7.3 • Cisco Secure Firewall Management Center Device Configuration Guide, 7.3 • Cisco Secure Firewall Management Center Snort 3 Configuration Guide, Version 7.3
Version 7.2	• Cisco Secure Firewall Management Center Administration Guide, 7.2 • Cisco Secure Firewall Management Center Device Configuration Guide, 7.2 • Cisco Secure Firewall Management Center Snort 3 Configuration Guide, Version 7.2

Release	Guide
Version 7.1	• Firepower Management Center Administration Guide, 7.1 • Firepower Management Center Device Configuration Guide, 7.1 • Firepower Management Center Snort 3 Configuration Guide, Version 7.1
Version 7.0	• Firepower Management Center Configuration Guide, Version 7.0 • Firepower Management Center Snort 3 Configuration Guide, Version 7.0
Version 6.7.0	• Firepower Management Center Configuration Guide, Version 6.7
Version 6.6.0	• Firepower Management Center Configuration Guide, Version 6.6
Version 6.5.0	• Firepower Management Center Configuration Guide, Version 6.5
Version 6.4.0	• Firepower Management Center Configuration Guide, Version 6.4
Version 6.3.0	• Firepower Management Center Configuration Guide, Version 6.3
Version 6.2.3	• Firepower Management Center Configuration Guide, Version 6.2.3
Version 6.2.2	• Firepower Management Center Configuration Guide, Version 6.2.2
Version 6.2.1	• Firepower Management Center Configuration Guide, Version 6.2.1
Version 6.2.0.x	• Firepower Management Center Configuration Guide, Version 6.2
Version 6.1.x	• Firepower Management Center Configuration Guide, Version 6.1
Version 6.0.1.x	• Firepower Management Center Configuration Guide, Version 6.0.1
Version 6.0.0.x	• Firepower Management Center Configuration Guide, Version 6.0

ASA with FirePOWER Services Local Management via ASDM

On an ASA device running version 6.0+ of the ASA FirePOWER module, you can configure ASA FirePOWER module functionality via ASDM. The *ASA with FirePOWER Services Local Management Configuration Guide* provides information on configuring the module.

Release	Guide
Version 7.0	ASA with FirePOWER Services Local Management Configuration Guide, Version 7.0
Version 6.7.0	ASA with FirePOWER Services Local Management Configuration Guide, Version 6.7

Release	Guide
Version 6.6.0	ASA with FirePOWER Services Local Management Configuration Guide, Version 6.6
Version 6.5.0	ASA with FirePOWER Services Local Management Configuration Guide, Version 6.5
Version 6.4.0	ASA with FirePOWER Services Local Management Configuration Guide, Version 6.4
Version 6.3.0	ASA with FirePOWER Services Local Management Configuration Guide, Version 6.3
Version 6.2.3	ASA with FirePOWER Services Local Management Configuration Guide, Version 6.2.3
Version 6.2.2	ASA with FirePOWER Services Local Management Configuration Guide, Version 6.2.2
Version 6.2.0.x	ASA with FirePOWER Services Local Management Configuration Guide, Version 6.2
Version 6.1.x	ASA with FirePOWER Services Local Management Configuration Guide, Version 6.1
Version 6.0.1.x	No updates were made to the *ASA FirePOWER Services Local Management Configuration Guide* for Version 6.0.1; see Version 6.0 documentation set for applicable information.
Version 6.0.0.x	ASA with FirePOWER Services Local Management Configuration Guide, Version 6.0

Device Manager

Release	Guide
Version 7.6	Cisco Secure Firewall Device Manager Configuration Guide, Version 7.6
Version 7.4	Cisco Secure Firewall Device Manager Configuration Guide, Version 7.4
Version 7.3	Cisco Secure Firewall Device Manager Configuration Guide, Version 7.4
Version 7.3	Cisco Secure Firewall Device Manager Configuration Guide, Version 7.3
Version 7.2	Cisco Secure Firewall Device Manager Configuration Guide, Version 7.2
Version 7.1	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 7.1
Version 7.0	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 7.0
Version 6.7.0	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.7.0

Release	Guide
Version 6.6.0	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.6.0
Version 6.5.0	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.5.0
Version 6.4.0	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.4.0
Version 6.3.0	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.3.0
Version 6.2.3	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.2.3
Version 6.2.2	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.2.2
Version 6.2.1	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.2.1
Version 6.2.0.x	Firepower Device Manager Configuration Guide, Version 6.2
Version 6.1.x	Firepower Device Manager Configuration Guide, Version 6.1

Configuration Examples and Tech Notes

Configuration examples are "how to" guides that provide an end-to-end example of the procedures required to complete a specific configuration. If the example requires configuration in more than one management application, such as Secure Firewall chassis manager and Secure Firewall Management Center the configuraton example includes the procedures for both management applications.

- How to Manage a Device with the Firepower Management Center

Command Reference Guide

The Cisco Secure Firewall Threat Defense Command Reference explains how to use the command line interface (CLI) for Threat Defense devices.

Snort 3 Inspector Reference

The Snort 3 Inspector Reference explains the options, rules, and best practices for configuring the Snort 3 inspectors.

Application Detector References for VDB Releases

Beginning with VDB Release 343, all application detector information is available through Secure Firewall Application Detectors. This site includes a searchable database of application detectors. The Release Notes provide an update on the newest VDB release.

Note The Cisco Vulnerability Database Library for Firepower System provides links to the Cisco Firepower Application Detector Reference for VDB release 297-343.

Hardware Guides

This section contains the following topics:

Hardware Installation

These guides provide information about Firepower hardware, including deployment information, physical installation procedures, field-replaceable components, specifications, and safety and regulatory information.

Note For virtual installation guides, see Quick Start and Getting Started Guides, on page 12.

Firepower Hardware Installation Guides

- Cisco Secure Firewall Management Center 1700, 2700, and 4700 Hardware Installation Guide
- Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide
- Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide
- Cisco Firepower Management Center 750, 1500, 2000, 3500, and 4000 Hardware Installation Guide
- Cisco Firepower 1010 Hardware Installation Guide
- Cisco Firepower 1100 Series Hardware Installation Guide
- Cisco Firepower 2100 Series Hardware Installation Guide
- Cisco Secure Firewall 3110, 3120, 3130, and 3140 Hardware Installation Guide
- Cisco Firepower 4110, 4120, 4140, and 4150 Hardware Installation Guide
- Cisco Firepower 4112, 4115, 4125, and 4145 Hardware Installation Guide
- Cisco Secure Firewall 4200 Series Hardware Installation Guide
- Cisco Firepower 9300 Hardware Installation Guide
- Firepower 7000 Series Installation Guide
- Firepower 8000 Series Installation Guide

ASA 5500-X Series Hardware Installation Guides

- Cisco ASA 5506-X, 5506W-X, 5506H-X Hardware Installation Guide

- Cisco ASA 5508-X and 5516-X Hardware Installation Guide
- Cisco ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Hardware Installation Guide
- Cisco ASA 5585-X Hardware Installation Guide

ISA 3000 Hardware Installation Guide

- Cisco ISA 3000 Industrial Security Appliance Hardware Installation Guide

Regulatory Compliance and Safety Information

Regulatory compliance and safety information guides provides general safety guidelines and regulatory information for Firepower devices. The books related to regulatory compliance and safety information are:

Firepower Regulatory Compliance and Safety Information

- Regulatory Compliance and Safety Information—Cisco Firepower Management Center 1600, 2600, 4600
- Regulatory Compliance and Safety Information—Cisco Firepower Management Center 1000, 2500, and 4500
- Regulatory Compliance and Safety Information—Cisco Firepower 1010
- Regulatory Compliance and Safety Information—Cisco Firepower 1100 Series
- Regulatory Compliance and Safety Information—Cisco Firepower 2100 Series
- Regulatory Compliance and Safety Information—Cisco Secure Firewall 3100 Series
- Regulatory Compliance and Safety Information—Cisco Firepower 4100 Series
- Regulatory Compliance and Safety Information—Cisco Secure Firewall 4215, 4225, 4245
- Regulatory Compliance and Safety Information-Cisco Firepower 9300

ASA Regulatory Compliance and Safety Information

- Regulatory Compliance and Safety Information for the Cisco ASA 5506-X, ASA 5508-X, ASA 5516-X Series Adaptive Security Appliance
- Regulatory Compliance and Safety Information for the Cisco ASA 5500-X Series Adaptive Security Appliance

Quick Start and Getting Started Guides

Quick start and getting started guides provide information on deploying the appliance, procedures for installing your appliance on your network, initial setup and configuration, and reimaging an appliance. Virtual quick start guides include deployment, installation, and initial setup information for virtual environments.

Module	Guide

Management Center quick start guides	• Cisco Secure Firewall Management Center 1700, 2700, and 4700 Getting Started Guide
	• Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
	• Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
	• Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide
	• Cisco Secure Firewall Management Center Virtual Getting Started Guide
	  • Deploy the Management Center Virtual Using VMware
	  • Deploy the Management Center Virtual Using KVM
	  • Deploy the Management Center Virtual On the AWS Cloud
	  • Deploy the Management Center Virtual On the Microsoft Azure Cloud
	  • Deploy the Management Center Virtual On the Google Cloud Platform
	  • Deploy the Management Center Virtual On the Oracle Cloud Infrastructure
	  • Deploy the Management Center Virtual Using OpenStack
	  • Deploy the Management Center Virtual Using Cisco Hyperflex
	  • Deploy the Management Center Virtual Using Nutanix
	  • Deploy the Management Center Virtual On the Alibaba Cloud

Module	Guide
Threat Defense quick start guides for hardware (Management Center)	• Cisco Firepower 1010 Getting Started Guide • Cisco Firepower 1100 Getting Started Guide • Cisco Firepower 2100 Getting Started Guide • Cisco Secure Firewall 3100 Getting Started Guide • Cisco Firepower 4100 Getting Started Guide • Cisco Secure Firewall 4200 Getting Started Guide • Cisco Firepower 9300 Getting Started Guide • Cisco Firepower Threat Defense for the ASA 5506-X Series Using Firepower Management Center Quick Start Guide • Cisco Firepower Threat Defense for the ASA 5508-X and 5516-X Series Using Firepower Management Center Quick Start Guide • Cisco Firepower Threat Defense for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Using Firepower Management Center Quick Start Guide • Cisco ISA 3000 Getting Started Guide
Threat Defense quick start guides for hardware (Device Manager)	• Cisco Firepower 1010 Getting Started Guide • Cisco Firepower 1100 Getting Started Guide • Cisco Firepower 2100 Getting Started Guide • Cisco Secure Firewall 3100 Getting Started Guide • Cisco Firepower 4100 Getting Started Guide • Cisco Firepower 9300 Getting Started Guide • Cisco Firepower Threat Defense for the ASA 5506-X Series Using Firepower Device Manager Quick Start Guide • Cisco Firepower Threat Defense for the ASA 5508-X and 5516-X Series Using Firepower Device Manager Quick Start Guide • Cisco Firepower Threat Defense for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Using Firepower Device Manager Quick Start Guide • Cisco ISA 3000 Getting Started Guide

Module	Guide

Threat Defense quick start guides for virtual appliances	• Cisco Secure Firewall Threat Defense Virtual Getting Started Guide, Version 7.3
	  • Deploy the Threat Defense Virtual on VMware
	  • Deploy the Threat Defense Virtual on KVM
	  • Deploy the Threat Defense Virtual on AWS
	  • Deploy the Threat Defense Virtual on Azure
	  • Deploy the Threat Defense Virtual on Oracle Cloud Infrastructure
	  • Deploy the Threat Defense Virtual on Google Cloud Platform
	  • Deploy the Threat Defense Virtual on Cisco HyperFlex
	  • Deploy the Threat Defense Virtual on Nutanix
	  • Deploy the Threat Defense Virtual on OpenStack
	  • Deploy the Threat Defense Virtual on the Alibaba Cloud
	• Cisco Secure Firewall Threat Defense Virtual Getting Started Guide, Version 7.2 and Earlier
	  • Deploy the Threat Defense Virtual on VMware
	  • Deploy the Threat Defense Virtual on KVM
	  • Deploy the Threat Defense Virtual on AWS
	  • Deploy the Threat Defense Virtual on Azure
	  • Deploy the Threat Defense Virtual on Oracle Cloud Infrastructure
	  • Deploy the Threat Defense Virtual on Google Cloud Platform
	  • Deploy the Threat Defense Virtual on Cisco HyperFlex
	  • Deploy the Threat Defense Virtual on Nutanix
	  • Deploy the Threat Defense Virtual on OpenStack
	  • Deploy the Threat Defense Virtual on the Alibaba Cloud

Module	Guide
ASA FirePOWER module quick start guide	The ASA FirePOWER module runs a separate application from the ASA. Refer to the Cisco ASA FirePOWER Module Quick Start Guide for instructions on setting up the module on supported ASA devices. For additional information on installation of supported ASA devices for use with Firepower, see the ASA documentation roadmap.
Firepower classic device quick start guides	• Cisco Firepower 7000 Series Getting Started Guide • Cisco Firepower 8000 Series Getting Started Guide • Cisco Firepower NGIPSv Quick Start Guide for VMware

Hardening Guides

Hardening guides provide information on hardening your Firepower deployment and reducing its vulnerability to cyber attack. Each hardening guide focuses on a specific area of a Firepower deployment.

Release	Guide
Version 7.2	• Cisco Secure Firewall Threat Defense Hardening Guide, Version 7.2 • Cisco Secure Firewall Management Center Hardening Guide, Version 7.2 • Cisco Firepower 4100/9300 FXOS Hardening Guide
Version 7.0	• Cisco Firepower Threat Defense Hardening Guide, Version 7.0 • Cisco Firepower Management Center Hardening Guide, Version 7.0 • Cisco Firepower 4100/9300 FXOS Hardening Guide
Version 6.4.0	• Cisco Firepower Threat Defense Hardening Guide, Version 6.4 • Cisco Firepower Management Center Hardening Guide, Version 6.4 • Cisco Firepower 4100/9300 FXOS Hardening Guide

Troubleshooting Guides and Articles

Links to troubleshooting Tech Notes and other troubleshooting resources are available under the "Troubleshooting and Alerts" heading on the top-level document listing page for each product on Cisco.com. See the links for your products in Top-Level Documentation Listing Pages for Management Center Deployments, on page 2.

Troubleshooting guides are listed below:

- Cisco Secure Firewall Threat Defense Syslog Messages
- Cisco Firepower 2100 Series Faults and Error Messages
- Cisco FXOS Troubleshooting Guide for the Firepower 2100 Series

Integration and API Documentation

Integration guides provide information on extending Firepower capabilities through custom application development using exposed APIs.

Release	Guide
Version 7.4	• Secure Firewall Management Center REST API Quick Start Guide, Version 7.4.0 • Cisco Success Network Telemetry Data Collected from the Management Center Devices

Release	Guide
Version 7.3	• Secure Firewall Management Center REST API Quick Start Guide, Version 7.3.0 • Cisco Secure Firewall Threat Defense REST API Guide • Cisco Secure Firewall Management Center (Version 7.2 and later) and SecureX Integration Guide • Cisco Secure Firewall Threat Defense and SecureX Integration Guide • Cisco Secure Firewall Threat Defense and Cisco SecureX Threat Response Integration Guide • Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide • User Guide for Cisco Secure Firewall (f.k.a. Firepower) App for Splunk • Integration Guide for the Cisco Secure Firewall Management Center App for IBM Qradar • Cisco Secure Firewall Threat Defense Syslog Messages • Secure Firewall Management Center Database Access Guide v7.3 No updates were made to the following guides for Version 7.3. You can follow the guides listed below: • Secure Firewall Management Center Event Streamer Integration Guide, Version 7.2.0 • Firepower System Host Input API Guide, Version 6.5 • Firepower System Remediation API Guide, Version 6.0.0

Release	Guide
Version 7.2	• Secure Firewall Management Center REST API Quick Start Guide, Version 7.2.0 • Cisco Secure Firewall Threat Defense REST API Guide • Cisco Secure Firewall Management Center (Version 7.2 and later) and SecureX Integration Guide • Cisco Firepower Threat Defense (FTD) and SecureX Integration Guide • Firepower and Cisco SecureX threat response Integration Guide • Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide • User Guide for Cisco Secure Firewall (f.k.a. Firepower) App for Splunk • Integration Guide for the Cisco Secure Firewall Management Center App for IBM Qradar • Cisco Secure Firewall Threat Defense Syslog Messages • Secure Firewall Management Center Event Streamer Integration Guide, Version 7.2.0 • Secure Firewall Management Center Database Access Guide v7.2 No updates were made to the following guides for Version 7.2. You can follow the guides listed below: • Firepower System Host Input API Guide, Version 6.5 • Firepower System Remediation API Guide, Version 6.0.0

Release	Guide
Version 7.1	• Cisco Firepower Management Center REST API Quick Start Guide, Version 7.1 • Cisco Firepower Threat Defense REST API Guide • Cisco Firepower Management Center and SecureX Integration Guide • Cisco Firepower and SecureX Integration Guide • Firepower and Cisco SecureX threat response Integration Guide • Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide • User Guide for Cisco Secure Firewall (f.k.a. Firepower) App for Splunk • Integration Guide for the Cisco Firepower App for IBM QRadar • Cisco Firepower Threat Defense Syslog Messages • Firepower System Event Streamer Integration Guide, Version 7.1.0 No updates were made to the following guides for Version 7.1. You can follow the guides listed below: • Firepower System Database Access Guide v6.7 - 7.1 • Firepower System Host Input API Guide, Version 6.5 • Firepower System Remediation API Guide, Version 6.0.0

Release	Guide
Version 7.0	• Cisco Firepower Management Center REST API Quick Start Guide, Version 7.0 • Cisco Firepower Threat Defense REST API Guide • Cisco Firepower Management Center and SecureX Integration Guide • Cisco Firepower and SecureX Integration Guide • Firepower and Cisco SecureX threat response Integration Guide • Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide • Cisco Firepower App for Splunk User Guide • Integration Guide for the Cisco Firepower App for IBM QRadar • Cisco Firepower Threat Defense Syslog Messages • Firepower System Event Streamer Integration Guide, Version 7.0 No updates were made to the following guides for Version 7.0. You can follow the guides listed below: • Firepower System Database Access Guide v6.7 - 7.1 • Firepower System Host Input API Guide, Version 6.5 • Firepower System Remediation API Guide, Version 6.0.0

Release	Guide
Version 6.7.0	• Cisco Firepower Management Center REST API Quick Start Guide, Version 6.7.0 • Cisco Firepower Threat Defense REST API Guide • Cisco Firepower System Database Access Guide, Version 6.7 • Cisco Firepower and SecureX Integration Guide • Firepower and Cisco SecureX threat response Integration Guide • Cisco Firepower App for Splunk User Guide • Integration Guide for the Cisco Firepower App for IBM QRadar • Cisco Firepower Threat Defense Syslog Messages • Firepower System Event Streamer Integration Guide, Version 6.7.0 No updates were made to the following guides for Version 6.7. You can follow the guides listed below: • Firepower System Host Input API Guide, Version 6.5 • Firepower System Remediation API Guide, Version 6.0.0
Version 6.6.0	• Cisco Firepower Management Center REST API Quick Start Guide, Version 6.6.0 • Cisco Firepower Threat Defense REST API Guide • Firepower System Event Streamer Integration Guide, Version 6.6.0 • Firepower and Cisco SecureX threat response Integration Guide • Cisco Firepower App for Splunk User Guide • Integration Guide for the Cisco Firepower App for IBM QRadar • Cisco Firepower Threat Defense Syslog Messages No updates were made to the following guides for Version 6.6. You can follow the guides listed below: • Firepower System Host Input API Guide, Version 6.5 • Cisco Firepower System Database Access Guide, Version 6.3 • Firepower System Remediation API Guide, Version 6.0.0

Release	Guide
Version 6.5.0	• Cisco Firepower Management Center REST API Quick Start Guide, Version 6.5.0 • Cisco Firepower Threat Defense REST API Guide • Firepower System Host Input API Guide, Version 6.5 • Firepower System Event Streamer Integration Guide, Version 6.5.0 • Firepower and Cisco SecureX threat response Integration Guide • Cisco Firepower App for Splunk User Guide • Cisco Firepower Threat Defense Syslog Messages No updates were made to the following guides for Version 6.5. You can follow the guides listed below: • Cisco Firepower System Database Access Guide, Version 6.3 • Firepower System Remediation API Guide, Version 6.0.0
Version 6.4.0	• Cisco Firepower Management Center REST API Quick Start Guide, Version 6.4.0 • Cisco Firepower Threat Defense REST API Guide No updates were made to the following guides for Version 6.4. You can follow the guides listed below: • Cisco Firepower System Database Access Guide, Version 6.3 • Cisco Firepower System Event Streamer Integration Guide, Version 6.3.0 • Firepower System Host Input API Guide, Version 6.0.0 • Firepower System Remediation API Guide, Version 6.0.0

Release	Guide
Version 6.3.0	• Cisco Firepower System Event Streamer Integration Guide, Version 6.3.0 • Cisco Firepower Management Center REST API Quick Start Guide, Version 6.3.0 • Cisco Firepower System Database Access Guide, Version 6.3 • Cisco Firepower Threat Defense REST API Guide No updates were made to the following guides for Version 6.3. You can follow the guides listed below: • Firepower System Host Input API Guide, Version 6.0.0 • Firepower System Remediation API Guide, Version 6.0.0
Version 6.2.3	• Cisco Firepower System Event Streamer Integration Guide, Version 6.2.3 • Cisco Firepower Management Center REST API Quick Start Guide, Version 6.2.3 • Cisco Firepower Threat Defense REST API Guide No updates were made to the following guides for Version 6.2.3. You can follow the guides listed below: • Firepower System Database Access Guide, Version 6.1 • Firepower System Host Input API Guide, Version 6.0.0 • Firepower System Remediation API Guide, Version 6.0.0
Version 6.2.2	• Cisco Firepower System Event Streamer Integration Guide • Cisco Firepower REST API Quick Start Guide No updates were made to the following guides for Version 6.2.2. You can follow the guides listed below: • Firepower System Database Access Guide, Version 6.1 • Firepower System Host Input API Guide, Version 6.0.0 • Firepower System Remediation API Guide, Version 6.0.0

Release	Guide
Version 6.2.1	• Cisco Firepower System Event Streamer Integration Guide • Cisco Firepower REST API Quick Start Guide No updates were made to the following guides for Version 6.2.1. You can follow the guides listed below: • Firepower System Database Access Guide, Version 6.1 • Firepower System Host Input API Guide, Version 6.0.0 • Firepower System Remediation API Guide, Version 6.0.0
Version 6.2.0.x	• Cisco Firepower System Event Streamer Integration Guide • Cisco Firepower REST API Quick Start Guide No updates were made to the following guides for Version 6.2. You can follow the guides listed below: • Firepower System Database Access Guide, Version 6.1 • Firepower System Host Input API Guide, Version 6.0.0 • Firepower System Remediation API Guide, Version 6.0.0
Version 6.1.x	• Firepower System Database Access Guide, Version 6.1 • Firepower System Event Streamer Integration Guide, Version 6.1 • Firepower REST API Quick Start Guide No updates were made to the Host Input or Remediation API guides for Version 6.1. You can follow the guides listed below: • Firepower System Host Input API Guide, Version 6.0.0 • Firepower System Remediation API Guide, Version 6.0.0
Version 6.0.1.x	No updates were made to the API documentation for Version 6.0.1; see Version 6.0 documentation.
Version 6.0.0.x	• Firepower System Database Access Guide, Version 6.0.0 • Firepower System Event Streamer Integration Guide, Version 6.0.0 • Firepower System Host Input API Guide, Version 6.0.0 • Firepower System Remediation API Guide, Version 6.0.0

Terminal Services (TS) Agent Documentation

The Firepower System TS Agent is a utility that assigns unique port ranges to users reported by Windows Terminal Servers to uniquely identify the users on the Firepower Management Center, to support user awareness and user control.

Release	Guide
Version 1.4	Cisco Terminal Services (TS) Agent Guide, Version 1.4
Version 1.3	Cisco Terminal Services (TS) Agent Guide, Version 1.3
Version 1.2	Cisco Terminal Services (TS) Agent Guide, Version 1.2

User Agent Documentation

Caution The user agent is reaching its end of support period. Firepower Management Center version 6.6 is the last version with which you can enable the user agent. The user agent cannot be enabled in Firepower Management Center 6.7 and upgrades to 6.7 will warn you to disable the user agent before upgrading.

Release	Guide
Version 2.5	Cisco Firepower User Agent Configuration Guide, version 2.5
Version 2.4	Cisco Firepower User Agent Configuration Guide, version 2.4
Version 2.3	Firepower User Agent Configuration Guide, Version 2.3
Version 2.2.x	FireSIGHT System User Agent Configuration Guide, Version 2.2 FireSIGHT System User Agent Version 2.2 Release Notes

Additional Resources

The Firewalls Community is an exhaustive repository of reference material that complements our extensive documentation. This includes links to 3D models of our hardware, hardware configuration selector, product collateral, configuration examples, troubleshooting tech notes, training videos, lab and Cisco Live sessions, social media channels, Cisco Blogs and all the documentation published by the Technical Publications team.

Some of the individuals posting to community sites or video sharing sites, including the moderators, work for Cisco Systems. Opinions expressed on those sites and in any corresponding comments are the personal opinions of the original authors, not of Cisco. The content is provided for informational purposes only and is not meant to be an endorsement or representation by Cisco or any other party.

Note Some of the videos, technical notes, and reference material in the Firewalls Community points to older versions of the management center. Your version of the management center and the version referenced in the videos or technical notes might have differences in the user interface that cause the procedures not to be identical.