

System Requirements

This document includes the system requirements for Version 7.2.

- Firewall Threat Defense Platforms, on page 1
- Firewall Threat Defense Management, on page 3

Firewall Threat Defense Platforms

Threat defense devices monitor network traffic and decide whether to allow or block specific traffic based on a defined set of security rules. For details on device management methods, see Firewall Threat Defense Management, on page 3. For general compatibility information, see the *Cisco Secure Firewall Threat Defense Compatibility Guide*.

Firewall Threat Defense Hardware

Version 7.2 Firewall Threat Defense hardware comes in a range of throughputs, scalability capabilities, and form factors.

Table 1: Version 7.2 Firewall Threat Defense Hardware

Platform	Firewall Management Center Compatibility		Firewall Device Manager Compatibility		Notes
	Customer Deployed	Cloud Delivered	Firewall Device Manager Only	Firewall Device Manager + CDO	
Firepower 1010E, 1010, 1120, 1140, 1150	YES	YES	YES	YES	Firepower 1010E requires Version 7.2.3+.
Firepower 2110, 2120, 2130, 2140	YES	YES	YES	YES	—
Secure Firewall3110, 3120, 3130, 3140	YES	YES	YES	YES	—

Platform	Firewall Management Center Compatibility		Firewall Device Manager Compatibility		Notes
	Customer Deployed	Cloud Delivered	Firewall Device Manager Only	Firewall Device Manager + CDO	
Firepower 4110, 4120, 4140, 4150 Firepower 4112, 4115, 4125, 4145 Firepower 9300: SM-24, SM-36, SM-44 modules Firepower 9300: SM-40, SM-48, SM-56 modules	YES	YES	YES	YES	Requires FXOS 2.12.1.95 or later build. We recommend the latest firmware. See the *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*.
ISA 3000	YES	YES	YES	YES	May require a ROMMON update. See the *Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide*.

Firewall Threat Defense Virtual

Version 7.2 Firewall Threat Defense Virtual implementations support performance-tiered Smart Software Licensing, based on throughput requirements and remote access VPN session limits. Options run from FTDv5 (100 Mbps/50 sessions) to FTDv100 (16 Gbps/10,000 sessions). For more information on supported instances, throughputs, and other hosting requirements, see the appropriate *Getting Started Guide*.

Table 2: Version 7.2 Firewall Threat Defense Virtual Platforms

Device Platform	Firewall Management Center Compatibility		Firewall Device Manager Compatibility	
	Customer Deployed	Cloud Delivered	Firewall Device Manager Only	Firewall Device Manager + CDO
Public Cloud				
Amazon Web Services (AWS)	YES	YES	YES	YES
Microsoft Azure	YES	YES	YES	YES
Google Cloud Platform (GCP)	YES	YES	YES	YES
Oracle Cloud Infrastructure (OCI)	YES	YES	—	—
Private Cloud				

Device Platform	Firewall Management Center Compatibility		Firewall Device Manager Compatibility	
	Customer Deployed	Cloud Delivered	Firewall Device Manager Only	Firewall Device Manager + CDO
Cisco Hyperflex	YES	YES	YES	YES
Kernel-based virtual machine (KVM)	YES	YES	YES	YES
Nutanix Enterprise Cloud	YES	YES	YES	YES
OpenStack	YES	YES	—	—
VMware vSphere/VMware ESXi 6.5, 6.7, or 7.0	YES	YES	YES	YES

Firewall Threat Defense Management

You can use Firewall Device Manager to locally manage a single Firewall Threat Defense device. Most models suppport local management.

Optionally, add Security Cloud Control to remotely manage multiple Firewall Threat Defense devices, as an alternative to the Firewall Management Center. Although some configurations still require Firewall Device Manager, Security Cloud Control allows you to establish and maintain consistent security policies across your Firewall Threat Defense deployment.