



System Requirements

This document includes the system requirements for Version 7.3.

- [Threat Defense Platforms, on page 1](#)
- [Threat Defense Management, on page 3](#)
- [Browser Requirements, on page 3](#)

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 [Threat Defense Management, on page 3](#). For general compatibility information, see the [Cisco Secure Firewall Threat Defense Compatibility Guide](#).

Threat Defense Hardware

Version 7.3 threat defense hardware comes in a range of throughputs, scalability capabilities, and form factors.

Table 1: Version 7.3 Threat Defense Hardware

| Platform | Management Center Compatibility | | Device Manager Compatibility | | Notes |
|--|---------------------------------|-----------------|------------------------------|----------------------|--|
| | Customer Deployed | Cloud Delivered | Device Manager Only | Device Manager + CDO | |
| Firepower 1010, 1120, 1140, 1150 | YES | YES | YES | YES | The Firepower 1010E cannot run threat defense 7.3. Support will return in a later release. |
| Firepower 2110, 2120, 2130, 2140 | YES | YES | YES | YES | — |
| Secure Firewall 3105, 3110, 3120, 3130, 3140 | YES | YES | YES | YES | Secure Firewall 3105 requires Version 7.3.1+. |

| Platform | Management Center Compatibility | | Device Manager Compatibility | | Notes |
|---|---------------------------------|-----------------|------------------------------|----------------------|---|
| | Customer Deployed | Cloud Delivered | Device Manager Only | Device Manager + CDO | |
| Firepower 4112, 4115, 4125, 4145 Firepower 9300: SM-40, SM-48, SM-56 modules | YES | YES | YES | YES | Requires FXOS 2.13.0.198 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 . |

Threat Defense Virtual

Version 7.3 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 7.3 Threat Defense Virtual Platforms

| Device Platform | Management Center Compatibility | | Device Manager Compatibility | |
|-----------------------------------|---------------------------------|-----------------|------------------------------|----------------------|
| | Customer Deployed | Cloud Delivered | Device Manager Only | Device Manager + CDO |
| Public Cloud | | | | |
| Alibaba | YES | YES | — | — |
| 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 | — | — |
| On-Prem/Private Cloud | | | | |
| Cisco Hyperflex | YES | YES | YES | YES |

| Device Platform | Management Center Compatibility | | Device Manager Compatibility | |
|---|---------------------------------|-----------------|------------------------------|----------------------|
| | Customer Deployed | Cloud Delivered | Device Manager Only | Device Manager + CDO |
| 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 |

Threat Defense Management

Depending on device model and version, we support the following management methods.

You can use device manager to locally manage a single threat defense device.

Optionally, add Cisco Defense Orchestrator (CDO) 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.

Browser Requirements

Browsers

We test with the latest versions of these popular browsers, running on currently supported versions of macOS and Microsoft Windows:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge (Windows only)

If you encounter issues with any other browser, or are running an operating system that has reached end of life, we ask that you switch or upgrade. If you continue to encounter issues, contact Cisco TAC.



Note We do not perform extensive testing with Apple Safari, nor do we extensively test Microsoft Edge with FMC walkthroughs. However, Cisco TAC welcomes feedback on issues you encounter.

Browser Settings and Extensions

Regardless of browser, you must make sure JavaScript, cookies, and TLS v1.2 remain 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

| Interface | Minimum Resolution |
|---|--------------------|
| Device Manager | 1024 x 768 |
| Chassis Manager for the Firepower 4100/9300 | 1024 x 768 |

Securing Communications

When you first log in, the system uses a self-signed digital certificate to secure web communications. Your browser should display an untrusted authority warning, but also should allow you to add the certificate to the trust store. Although this will allow you to continue, we do recommend that you replace the self-signed certificate with a certificate signed by a globally known or internally trusted certificate authority (CA).

To begin replacing the self-signed certificate, click **Device**, then the **System Settings > Management Access** link, then the **Management Web Server** tab.

For detailed procedures, see the online help or the configuration guide.



Note If you do not replace the self-signed certificate:

- Google Chrome does not cache static content, such as images, CSS, or JavaScript. Especially in low bandwidth environments, this can extend page load times.
- Mozilla Firefox can stop trusting the self-signed certificate when the browser updates. If this happens, you can refresh Firefox, keeping in mind that you will lose some settings; see Mozilla's [Refresh Firefox](#) support page.

Browsing from a Monitored Network

Many browsers use Transport Layer Security (TLS) v1.3 by default. If you are using an SSL policy to handle encrypted traffic, and people in your monitored network use browsers with TLS v1.3 enabled, websites that support TLS v1.3 may fail to load. For more information, see the software advisory titled: [Failures loading websites using TLS 1.3 with SSL inspection enabled](#).