Welcome

This document contains release information for Version 7.3 of Cisco Secure Firewall Threat Defense, Secure Firewall Management Center, and Secure Firewall device manager.

For Cisco Defense Orchestrator (CDO) deployments, see the Cisco Cloud-Delivered Firewall Management Center Release Notes or What's New for Cisco Defense Orchestrator.

- Release Dates, on page 1
- Suggested Release, on page 1
- Sharing Data with Cisco, on page 2
- For Assistance, on page 2

Release Dates

Table 1: Version 7.3 Dates

Version	Build	Date	Platforms
7.3.1.1	83	2023-08-24	All
7.3.1	19	2023-03-14	All
7.3.0	69	2022-11-29	All

Suggested Release

To take advantage of new features and resolved issues, we recommend you upgrade all eligible appliances to at least the suggested release, including any patches. On the Cisco Support & Download site, the suggested release is marked with a gold star.

We also list the suggested release in the new feature guides:

- Cisco Secure Firewall Management Center New Features by Release
- Cisco Secure Firewall Device Manager New Features by Release

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 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 NGFW Product Line Software Release and Sustaining Bulletin.

If you are interested in a hardware refresh, contact your Cisco representative or partner contact.

Sharing Data with Cisco

The following features share data with Cisco.

Cisco Success Network

Cisco Success Network sends usage information and statistics to Cisco, which are essential to provide you with technical support.

During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time.

Cisco Support Diagnostics

Cisco Support Diagnostics (sometimes called *Cisco Proactive Support*) sends configuration and operational health data to Cisco, and processes that data through our automated problem detection system, allowing us to proactively notify you of issues. This feature also allows Cisco TAC to collect essential information from your devices during the course of a TAC case.

During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time. This feature is not supported with device manager.

Web Analytics

Web analytics provides non-personally-identifiable usage data to Cisco, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your management centers.

You are enrolled by default but you can change your enrollment at any time after you complete initial setup. Note that ad blockers can block web analytics, so if you choose to remain enrolled, please disable ad blocking for the hostnames/IP addresses of your Cisco appliances.

For Assistance

Online Resources

Cisco provides the following online resources to download documentation, software, and tools; to query bugs; and to open service requests. Use these resources to install and configure Cisco software and to troubleshoot and resolve technical issues.

- Documentation: http://www.cisco.com/go/threatdefense-73-docs
- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html

- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.cisco.com/cisco/support/notifications.html

Access to most tools on the Cisco Support & Download site requires a Cisco.com user ID and password.

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts