

Getting Started

- Is this Guide for You?, on page 1
- Planning Your Upgrade, on page 3
- Upgrade Feature History, on page 4
- For Assistance, on page 4

Is this Guide for You?

This guide explains how to prepare for and complete a successful upgrade of **Secure Firewall Threat Defense** with **Secure Firewall Device Manager** currently running **Version 7.2**.

Upgrades can be major (A.x), maintenance (A.x.y), or patch (A.x.y.z) releases. We also may provide hotfixes, which are minor updates that address particular, urgent issues.

Additional Resources

If you are upgrading a different platform/component, upgrading to/from a different version, or are using a cloud-based manager, see one of these resources.

Table 1: Upgrade Guides for Firewall Management Center

Current Firewall Management Center Version	Guide
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1
7.0 or earlier	*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*

Table 2: Upgrade Guides for Firewall Threat Defense with Firewall Management Center

Current Firewall Management Center Version	Guide
Cloud-Delivered Firewall Management Center	Secure Firewall Threat Defense upgrade guides for Cloud-Delivered Firewall Management Center
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1
7.0 or earlier	*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*

Table 3: Upgrade Guides for Firewall Threat Defense with Firewall Device Manager

Current Firewall Threat Defense Version	Guide
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager for your version
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Device Manager, Version 7.1
7.0 or earlier	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for your version: *System Management* For the Firepower 4100/9300, also see the FXOS upgrade instructions in *Cisco Firepower 4100/9300 Upgrade Guide, FTD 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1*.
Version 6.4+, with Security Cloud Control	*Cisco Security Cloud Control: FDM-Managed Firewall Threat Defense*

Table 4: Upgrade Other Components

Version	Component	Guide
Any	ASA logical devices on the Firepower 4100/9300	*Cisco Secure Firewall ASA Upgrade Guide*
Latest	BIOS and firmware for Firewall Management Center	Release Notes for Cisco Secure Firewall Threat Defense and Firepower Hotfixes
Latest	Firmware for the Firepower 4100/9300	*Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*
Latest	ROMMON image for the ISA 3000	*Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide*

Planning Your Upgrade

Careful planning and preparation can help you avoid missteps. This table summarizes the upgrade planning process. For detailed checklists and procedures, see the upgrade chapters.

Table 5: Upgrade Planning Phases

Planning Phase	Includes
Planning and Feasibility	Assess your deployment. Plan your upgrade path. Read *all* upgrade guidelines and plan configuration changes. Check appliance access. Check bandwidth. Schedule maintenance windows.
Backups	Back up the software. Back up FXOS on the Firepower 4100/9300.
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.
Associated Upgrades	Upgrade virtual hosting in virtual deployments. Upgrade firmware on the Firepower 4100/9300. Upgrade FXOS on the Firepower 4100/9300.
Final Checks	Check configurations. Check NTP synchronization. Deploy configurations. Run readiness checks. Check disk space. Check running tasks. Check deployment health and communications.

Upgrade Feature History

Table 6: Device Upgrade Feature History

Feature	Minimum Threat Defense	Details
Pre-upgrade readiness check.	7.0.0	You can run a readiness check before upgrade. The readiness check verifies that the upgrade is valid for the system, and that the system meets other requirements needed to install the package. Running an upgrade readiness check helps you avoid failed installations. A link to run the upgrade readiness check was added to the **System Upgrade** section of the **Device** > **Updates** page.
Cancel and revert a failed upgrade.	6.7.0	If a major software upgrade fails or is otherwise not functioning correctly, you can revert to the state of the device as it was when you installed the upgrade. We added the ability to revert the upgrade to the System Upgrade panel in FDM. During an upgrade, the FDM login screen shows the upgrade status and gives you the option to cancel or revert in case of upgrade failure. In the Firewall Threat Defense API, we added the CancelUpgrade, RevertUpgrade, RetryUpgrade, and UpgradeRevertInfo resources. In the Firewall Threat Defense CLI, we added the following commands: **show last-upgrade status**, **show upgrade status**, **show upgrade revert-info**, **upgrade cancel**, **upgrade revert**, **upgrade cleanup-revert**, **upgrade retry**.
Upgrade with Firewall Device Manager.	6.2.0	You can install software upgrades through Firewall Device Manager. Select **Device** > **Updates**.

For Assistance

Upgrade Guides

In Firewall Management Center deployments, the Firewall Management Center must run the same or newer maintenance (third-digit) release as its managed devices. Upgrade the Firewall Management Center first, then devices. Use the upgrade guide for the version you are *currently* running—not your target version.

Table 7: Upgrade Guides

Platform	Upgrade Guide	Link
Firewall Management Center	Firewall Management Center version you are *currently* running.	https://cisco.com/go/fmc-upgrade

Platform	Upgrade Guide	Link
Firewall Threat Defense with Firewall Management Center	Firewall Management Center version you are *currently* running.	https://cisco.com/go/ftd-fmc-upgrade
Firewall Threat Defense with device manager	Firewall Threat Defense version you are *currently* running.	https://cisco.com/go/ftd-fdm-upgrade
Firewall Threat Defense with Cloud-Delivered Firewall Management Center	Cloud-Delivered Firewall Management Center.	https://cisco.com/go/ftd-cdfmc-upgrade

Install Guides

If you cannot or do not want to upgrade, you can freshly install major and maintenance releases. This is also called *reimaging*. You cannot reimage to a patch. Install the appropriate major or maintenance release, then apply the patch. If you are reimaging to an earlier Firewall Threat Defense version on an FXOS device, perform a full reimage—even for devices where the operating system and software are bundled.

Table 8: Install Guides

Platform	Install Guide	Link
Firewall Management Center hardware	Getting started guide for your Firewall Management Center hardware model.	https://cisco.com/go/fmc-install
Firewall Management Center Virtual	Getting started guide for the Firewall Management Center Virtual.	https://cisco.com/go/fmcv-quick
Firewall Threat Defense hardware	Getting started or reimage guide for your device model.	https://cisco.com/go/ftd-quick
Firewall Threat Defense Virtual	Getting started guide for your Firewall Threat Defense Virtual version.	https://cisco.com/go/ftdv-quick
FXOS for the Firepower 4100/9300	Configuration guide for your FXOS version, in the *Image Management* chapter.	https://cisco.com/go/firepower9300-config
FXOS for the Firepower 1000/2100 and Secure Firewall 3100	Troubleshooting guide, in the *Reimage Procedures* chapter.	*Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense*

More 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: https://cisco.com/go/threatdefense-72-docs

- Cisco Support & Download site: https://cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://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