

Getting Started

- Is This Guide for You?, on page 1
- Upgrade Feature History, on page 4

Is This Guide for You?

This guide explains how to prepare for and complete a successful upgrade to Firepower **Version 7.0.x or earlier**, for:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD) devices with FMC, including FXOS for the Firepower 4100/9300
- 7000/8000 series devices with FMC
- NGIPSv devices with FMC
- ASA FirePOWER devices with FMC, including ASA OS

Additional Resources

If you are upgrading a different platform/component, or to a different version, see one of these resources.

Table 1: Upgrade Guides for FMC

Current FMC 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 FTD with FMC

Current FMC Version	Guide
Cloud-Delivered Firewall Management Center	Cisco Secure Firewall Threat Defense Upgrade Guide 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 FTD with FDM

Current FTD 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	Managing FDM Devices with Firewall in Security Cloud Control

Table 4: Upgrade Guides for NGIPS

Platform	Current Manager Version	Guide
Firepower 7000/8000 series with FMC	6.0.0–7.0.x	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
NGIPSv with FMC	6.0.0–7.1.x 7.2.0–7.2.5 7.3.x 7.4.0	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
	7.2.6–7.2.x 7.4.1–7.4.x	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version

Platform	Current Manager Version	Guide
ASA FirePOWER with FMC	6.0.0–7.1.x 7.2.0–7.2.5 7.3.x 7.4.0	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
	7.2.6–7.2.x 7.4.1–7.4.x	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version
ASA FirePOWER with ASDM	Any	Cisco Secure Firewall ASA Upgrade Guide

Table 5: 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 FMC	Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes
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

Upgrade Feature History

Table 6: History for FMC Upgrades

Feature	Minimum Management Center	Minimum Threat Defense	Details
Upgrades postpone scheduled tasks.	6.4.0	Any	The FMC upgrade process now postpones scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. **Note** Before you begin any upgrade, you must still make sure running tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Note that this feature is supported for all upgrades *from* a supported version. This includes Version 6.4.0.10 and later patches, Version 6.6.3 and later maintenance releases, and Version 6.7.0+. This feature is not supported for upgrades *to* a supported version from an unsupported version.

Table 7: History for Device Upgrades

Feature	Minimum Management Center	Minimum Threat Defense	Details
Improved FTD upgrade performance and status reporting.	7.0.0	7.0.0	FTD upgrades are now easier faster, more reliable, and take up less disk space. A new **Upgrades** tab in the Message Center provides further enhancements to upgrade status and error reporting.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Easy-to-follow upgrade workflow for FTD devices.	7.0.0	Any	A new device upgrade page (**Devices** > **Device Upgrade**) on the FMC provides an easy-to-follow wizard for upgrading Version 6.4+ FTD devices. It walks you through important pre-upgrade stages, including selecting devices to upgrade, copying the upgrade package to the devices, and compatibility and readiness checks. To begin, use the new **Upgrade Firepower Software** action on the Device Management page **Devices** > **Device Management** > **Selection**. As you proceed, the system displays basic information about your selected devices, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a device does not "pass" a stage in the wizard, it does not appear in the next stage. If you navigate away from wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the wizard. **Note** You must still use **System** > **Updates** to upload or specify the location of FTD upgrade packages. You must also use the System Updates page to upgrade the FMC itself, as well as all non-FTD managed devices. **Note** In Version 7.0, the wizard does not correctly display devices in clusters or high availability pairs. Even though you must select and upgrade these devices as a unit, the wizard displays them as standalone devices. Device status and upgrade readiness are evaluated and reported on an individual basis. This means it is possible for one unit to appear to "pass" to the next stage while the other unit or units do not. However, these devices are still grouped. Running a readiness check on one, runs it on all. Starting the upgrade on one, starts it on all. To avoid possible time-consuming upgrade failures, *manually* ensure all group members are ready to move on to the next step of the wizard before you click **Next**.
Upgrade more FTD devices at once.	7.0.0	Any (source) 6.7.0 (target)	The number of devices you can upgrade at once is now limited by your management network bandwidth—not the system's ability to manage simultaneous upgrades. Previously, we recommended against upgrading more than five devices at a time. **Important** Only upgrades to FTD Version 6.7+ using the FTD upgrade wizard see this improvement. If you are upgrading devices to an older FTD release—even if you are using the new upgrade wizard—we still recommend you limit to five devices at a time.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Upgrade different device models together.	7.0.0	Any	You can now use the FTD upgrade wizard to queue and invoke upgrades for all FTD models at the same time, as long as the system has access to the appropriate upgrade packages. Previously, you would choose an upgrade package, then choose the devices to upgrade using that package. That meant that you could upgrade multiple devices at the same time *only* if they shared an upgrade package. For example, you could upgrade two Firepower 2100 series devices at the same time, but not a Firepower 2100 series and a Firepower 1000 series.
Upgrades remove PCAP files to save disk space.	6.7.0	6.7.0	Upgrades now remove locally stored PCAP files. To upgrade, you must have enough free disk space or the upgrade fails.
Improved FTD upgrade status reporting and cancel/retry options.	6.7.0	6.7.0	You can now view the status of FTD device upgrades and readiness checks in progress on the Device Management page, as well as a 7-day history of upgrade success/failures. The Message Center also provides enhanced status and error messages. A new Upgrade Status pop-up, accessible from both Device Management and the Message Center with a single click, shows detailed upgrade information, including percentage/time remaining, specific upgrade stage, success/failure data, upgrade logs, and so on. Also on this pop-up, you can manually cancel failed or in-progress upgrades (**Cancel Upgrade**), or retry failed upgrades (**Retry Upgrade**). Canceling an upgrade reverts the device to its pre-upgrade state. **Note** To be able to manually cancel or retry a failed upgrade, you must disable the new auto-cancel option, which appears when you use the FMC to upgrade an FTD device: **Automatically cancel on upgrade failure and roll back to the previous version**. With the option enabled, the device automatically reverts to its pre-upgrade state upon upgrade failure. Auto-cancel is not supported for patches. In an HA or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. New/modified screens: • **System** > **Updates** > **Product Updates** > **Available Updates** > **Install** icon for the FTD upgrade package • **Devices** > **Device Management** > **Upgrade** • **Message Center** > **Tasks** New/modified CLI commands: **show upgrade status detail**, **show upgrade status continuous**, **show upgrade status**, **upgrade cancel**, **upgrade retry**

Feature	Minimum Management Center	Minimum Threat Defense	Details
Get FTD upgrade packages from an internal web server.	6.6.0	6.6.0	FTD devices can now get upgrade packages from your own internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC. **Note** This feature is supported only for FTD devices running Version 6.6+. It is not supported for upgrades *to* Version 6.6, nor is it supported for the FMC or Classic devices. New/modified screens: We added a **Specify software update source** option to the page where you upload upgrade packages.
Copy upgrade packages to managed devices before the upgrade.	6.2.3	Any	You can now copy (or push) an upgrade package from the FMC to a managed device before you run the actual upgrade. This is useful because you can push during times of low bandwidth use, outside of the upgrade maintenance window. When you push to high availability, clustered, or stacked devices, the system sends the upgrade package to the active/control/primary first, then to the standby/data/secondary. New/modified screens: **System** > **Updates**