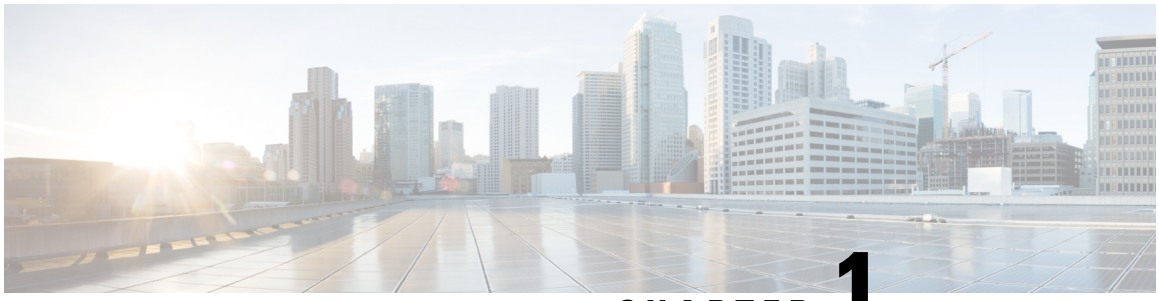
Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0

First Published: 2018-03-29

Last Modified: 2022-12-19

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Getting Started

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: Upgrading FMC

Current FMC Version	Guide
Cloud-delivered management center (no version)	None. We take care of updates.
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: Upgrading FTD with FMC

Current FMC Version	Guide
Cloud-delivered management center (no version)	The latest released version of the Cisco Secure Firewall Threat Defense Upgrade Guide for 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: Upgrading 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	*System Management* in the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for your version. For the Firepower 4100/9300, also see the FXOS upgrade instructions in the 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 CDO	*Onboard Devices and Services* in Managing FDM Devices with Cisco Defense Orchestrator.

Table 4: Upgrading NGIPS Devices

Current Manager Version	Platform	Guide
Any	Firepower 7000/8000 series	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.
Any	ASA FirePOWER with FMC	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.
Any	ASA FirePOWER with ASDM	Cisco Secure Firewall ASA Upgrade Guide.

Table 5: Upgrading 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.

Feature History

Table 6: Version 7.0.0 Features

Feature	Description
Improved FTD upgrade performance and status reporting.	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	Description
Easy-to-follow upgrade workflow for FTD devices.	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 > Select Action**). 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**.

Feature	Description
Upgrade more FTD devices at once.	The FTD upgrade wizard lifts the following restrictions: • Simultaneous device upgrades. 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+ 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. • Grouping upgrades by device model. You can now 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.

Table 7: Version 6.7.0 Features

Feature	Description
Improved FTD upgrade status reporting and cancel/retry options.	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 upgrade: **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 a high availability/scalability 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** > **Update** > **Product Updates** > **Available Updates** > **Install** icon for the FTD upgrade package • **Devices** > **Device Management** > **Upgrade** • **Message Center > Tasks** New FTD CLI commands: • **show upgrade status detail** • **show upgrade status continuous** • **show upgrade status** • **upgrade cancel** • **upgrade retry**
Upgrades remove PCAP files to save disk space.	Upgrades now remove locally stored PCAP files. To upgrade, you must have enough free disk space or the upgrade fails.

Table 8: Version 6.6.0 Features

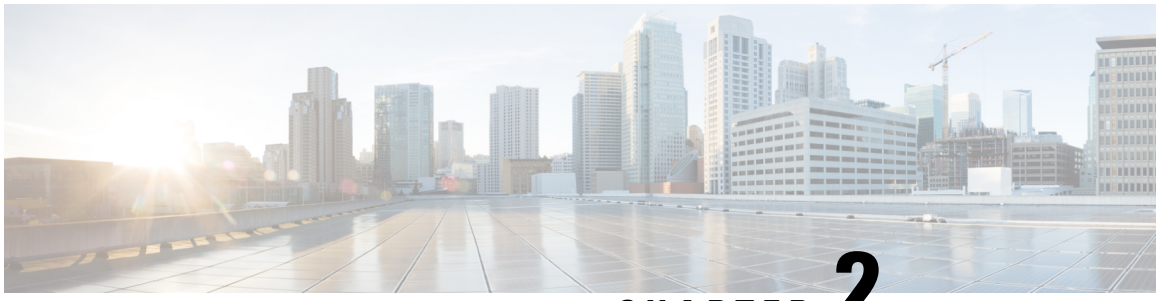
Feature	Description
Get device upgrade packages from an internal web server.	Devices can now get upgrade packages from your own internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC. New/modified screens: **System > Updates > Upload Update** button > **Specify software update source** option
Upgrades postpone scheduled tasks.	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 9: Version 6.4.0 Features

Feature	Description
Upgrades postpone scheduled tasks.	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 10: Version 6.2.3 Features

Feature	Description
Copy upgrade packages to managed devices before the upgrade.	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**



CHAPTER 2

Planning Your Upgrade

Upgrade Planning Phases

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 11: 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. Back up ASA for ASA FirePOWER.
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.

Planning Phase	Includes
Associated Upgrades	Upgrade virtual hosting in virtual deployments. Upgrade FXOS on the Firepower 4100/9300. Upgrade ASA for ASA FirePOWER.
Final Checks	Check configurations. Check NTP synchronization. Check disk space. Deploy configurations. Run readiness checks. Check running tasks. Check deployment health and communications.

Current Version and Model Information

Use these commands to find current version and model information for your deployment,

Table 12:

Component	Information
Firepower Management Center	On the FMC, choose **Help** > **About**.
Firepower managed devices	On the FMC, choose **Devices** > **Device Management**.
FXOS for Firepower 4100/9300	Firepower Chassis Manager: Choose **Overview**. FXOS CLI: For the version, use the **show version** command. For the model, enter **scope chassis 1**, and then **show inventory**.
ASA OS for ASA with FirePOWER Services	On the ASA CLI, use the **show version** command.
Virtual hosting environment	See the documentation for your virtual hosting environment.

Upgrade Paths

Your upgrade path is a detailed plan for what you will upgrade and when, including virtual hosting environments and appliance operating systems. At all times, you must maintain hardware, software, operating system, and hosting compatibility.

Tip This guide covers Firepower 7.0.x and earlier. See Is This Guide for You?, on page 1

What Do I Have?

Before you upgrade any Firepower appliance, determine the current state of your deployment. In addition to current version and model information, determine if your devices are configured for high availability/scalability, and if they are deployed passively, as an IPS, as a firewall, and so on.

See Current Version and Model Information, on page 10.

Where Am I Going?

Now that you know what you have, make sure you can get to where you want to go:

- Can your deployment run the target Firepower version?
- Do your appliances require a separate operating system upgrade before they can run the target Firepower version? Can your appliances run the target OS?
- Do your virtual appliances require a hosting environment upgrade before they can run the target Firepower version?

For answers to all these questions, see one of:.

- Cisco Secure Firewall Management Center Compatibility Guide
- Cisco Secure Firewall Threat Defense Compatibility Guide
- Cisco Firepower Classic Device Compatibility Guide

How Do I Get There?

After you determine that your appliances can run the target version, make sure direct upgrade is possible:

- Is direct Firepower software upgrade possible?
- Is direct FXOS upgrade possible, for the Firepower 4100/9300?
- Is direct ASA upgrade possible, for ASA with FirePOWER Services?

For answers to all these questions, see the upgrade paths provided in this guide.

Tip Upgrade paths that require intermediate versions can be time consuming. Especially in larger Firepower deployments where you must alternate FMC and device upgrades, consider reimaging older devices instead of upgrading. First, remove the devices from the FMC. Then, upgrade the FMC, reimage the devices, and re-add them to the FMC.

Can I Maintain Deployment Compatibility?

At all times, you must maintain hardware, software, and operating system compatibility:

- Can I maintain Firepower version compatibility between the FMC and its managed devices: Cisco Secure Firewall Management Center Compatibility Guide.
- Can I maintain FXOS compatibility with logical devices, for the Firepower 4100/9300: Cisco Firepower 4100/9300 FXOS Compatibility .

- Can I maintain ASA compatibility with ASA FirePOWER modules, for ASA with FirePOWER services: Cisco Secure Firewall ASA Compatibility.

Upgrade Path: Firepower Management Centers

This table provides upgrade paths for the FMC, including FMCv.

Find your current version in the left column. You can upgrade directly to any of the versions listed in the right column.

Note If your current version was released on a date after your target version, you may not be able to upgrade as expected. In those cases, the upgrade quickly fails and displays an error explaining that there are data store incompatibilities between the two versions. The release notes for both your current and target version list any specific restrictions.

Table 13: FMC Direct Upgrades

Current Version	Target Version
7.0.0 7.0.x Last support for FMC 1000, 2500, and 4500	→ Any later 7.0.x maintenance release
6.7.0 6.7.x	Any of: → 7.0.0 or any 7.0.x maintenance release → Any later 6.7.x maintenance release
6.6.0 6.6.x Last support for FMC 2000 and 4000.	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → Any later 6.6.x maintenance release **Note:** Due to data store incompatibilities, you cannot upgrade from Version 6.6.5+ to Version 6.7.0. We recommend you upgrade directly to Version 7.0.0+.
6.5.0	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release

Current Version	Target Version
6.4.0 Last support for FMC 750, 1500, and 3500.	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release → 6.5.0
6.3.0	Any of: → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release → 6.5.0 → 6.4.0
6.2.3	Any of: → 6.6.0 or any 6.6.x maintenance release → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	Any of: → 6.4.0 → 6.3.0 → 6.2.3
6.2.1	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.2.0	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2

Current Version	Target Version
6.1.0	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	Any of: → 6.1.0
6.0.0	Any of: → 6.0.1 Requires a preinstallation package: Firepower System Release Notes Version 6.0.1 Preinstallation.
5.4.1.1	Any of: → 6.0.0 Requires a preinstallation package: FireSIGHT System Release Notes Version 6.0.0 Preinstallation.

Upgrade Path: Firepower 4100/9300 with FTD Logical Devices

This table provides upgrade paths for the Firepower 4100/9300 with FTD logical devices, managed by a Firepower Management Center.

Note If you are upgrading a Firepower 9300 chassis with FTD *and* ASA logical devices running on separate modules, see the Cisco Firepower 4100/9300 Upgrade Guide, Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1.

Find your current version combination in the left column. You can upgrade to any of the version combinations listed in the right column. This is a multi-step process: first upgrade FXOS, then upgrade the logical devices.

Note that this table lists only Cisco's specially qualified version combinations. Because you must upgrade FXOS first, you will *briefly* run a supported—but not recommended—combination, where FXOS is "ahead" of the logical devices. For minimum builds and other detailed compatibility information, see Cisco Firepower 4100/9300 FXOS Compatibility .

Note For early versions of FXOS, you must upgrade to all intermediate versions between the current version and the target version. Once you reach FXOS 2.2.2, your upgrade options are wider.

Table 14: Upgrade Paths: Firepower 4100/9300 with FTD Logical Devices

Current Versions	Target Versions
FXOS 2.9.1 with FTD 6.7.0/6.7.x	→ FXOS 2.10.1 with FTD 7.0.0/7.0.x
FXOS 2.8.1 with FTD 6.6.0/6.6.x	Any of: → FXOS 2.10.1 with FTD 7.0.0/7.0.x → FXOS 2.9.1 with FTD 6.7.x
FXOS 2.7.1 with FTD 6.5.0	Any of: → FXOS 2.10.1 with FTD 7.0.0/7.0.x → FXOS 2.9.1 with FTD 6.7.0/6.7.x → FXOS 2.8.1 with FTD 6.6.0/6.6.x
FXOS 2.6.1 with FTD 6.4.0	Any of: → FXOS 2.10.1 with FTD 7.0.0/7.0.x → FXOS 2.9.1 with FTD 6.7.0/6.7.x → FXOS 2.8.1 with FTD 6.6.0/6.6.x → FXOS 2.7.1 with FTD 6.5.0
FXOS 2.4.1 with FTD 6.3.0	Any of: → FXOS 2.9.1 with FTD 6.7.0/6.7.x → FXOS 2.8.1 with FTD 6.6.0/6.6.x → FXOS 2.7.1 with FTD 6.5.0 → FXOS 2.6.1 with FTD 6.4.0
FXOS 2.3.1 with FTD 6.2.3	Any of: → FXOS 2.8.1 with FTD 6.6.0/6.6.x → FXOS 2.7.1 with FTD 6.5.0 → FXOS 2.6.1 with FTD 6.4.0 → FXOS 2.4.1 with FTD 6.3.0
FXOS 2.2.2 with FTD 6.2.2	Any of: → FXOS 2.6.1 with FTD 6.4.0 → FXOS 2.4.1 with FTD 6.3.0 → FXOS 2.3.1 with FTD 6.2.3

Current Versions	Target Versions
FXOS 2.2.2 with FTD 6.2.0	Any of: → FXOS 2.6.1 with FTD 6.4.0 → FXOS 2.4.1 with FTD 6.3.0 → FXOS 2.3.1 with FTD 6.2.3 → FXOS 2.2.2 with FTD 6.2.2
FXOS 2.2.1 with FTD 6.2.0	→ FXOS 2.2.2 with FTD 6.2.0 (upgrade *only* FXOS) Another option is to upgrade to FXOS 2.2.2 with FTD 6.2.2, which is a recommended combination. However, if you plan to further upgrade your deployment, don't bother. Now that you are running FXOS 2.2.2, you can upgrade all the way to FXOS 2.6.1 with FTD 6.4.0.
FXOS 2.1.1 with FTD 6.2.0	→ FXOS 2.2.1 with FTD 6.2.0 (upgrade *only* FXOS)
FXOS 2.0.1 with FTD 6.1.0	→ FXOS 2.1.1 with FTD 6.2.0
FXOS 1.1.4 with FTD 6.0.1	→ FXOS 2.0.1 with FTD 6.1.0

Upgrading FXOS with FTD Logical Devices in Clusters or HA Pairs

In Firepower Management Center deployments, you upgrade clustered and high availability FTD logical devices as a unit. However, you upgrade FXOS on each chassis independently.

Table 15: FXOS + FTD Upgrade Order

Deployment	Upgrade Order
Standalone device Cluster, units on the same chassis (Firepower 9300 only)	**1.** Upgrade FXOS. **2.** Upgrade FTD.
High availability	To minimize disruption, always upgrade the standby. **1.** Upgrade FXOS on the standby. **2.** Switch roles. **3.** Upgrade FXOS on the new standby. **4.** Upgrade FTD.

Deployment	Upgrade Order
Cluster, units on different chassis (6.2+)	To minimize disruption, always upgrade an all-data unit chassis. For example, for a two-chassis cluster: **1.** Upgrade FXOS on the all-data unit chassis. **2.** Switch the control module to the chassis you just upgraded. **3.** Upgrade FXOS on the new all-data unit chassis. **4.** Upgrade FTD.

With older versions, hitless upgrades have some additional requirements.

Table 16: Hitless Upgrades in Older Versions

Scenario	Details
Upgrading high availability or clustered devices and you are currently running any of: • FXOS 1.1.4.x through 2.2.1.x • FXOS 2.2.2.17 through FXOS 2.2.2.68 • FXOS 2.3.1.73 through FXOS 2.3.1.111 With: • FTD 6.0.1 through 6.2.2.x	Due to bug fixes in the flow offload feature, some combinations of FXOS and FTD do not support flow offload; see the Cisco Firepower Compatibility Guide. Performing a hitless upgrade requires that you always run a compatible combination. If your upgrade path includes upgrading FXOS to 2.2.2.91, 2.3.1.130, or later (including FXOS 2.4.1.x, 2.6.1.x, and so on) use this path: 1. Upgrade FTD to 6.2.2.2 or later. 2. Upgrade FXOS to 2.2.2.91, 2.3.1.130, or later. 3. Upgrade FTD to your final version. For example, if you are running FXOS 2.2.2.17 with FTD 6.2.2.0, and you want to upgrade to FXOS 2.6.1 with FTD 6.4.0, then you can: 1. Upgrade FTD to 6.2.2.5. 2. Upgrade FXOS to 2.6.1. 3. Upgrade FTD to 6.4.0.
Upgrading high availability devices to FTD Version 6.1.0	Requires a preinstallation package. For more information, see Firepower System Release Notes Version 6.1.0 Preinstallation Package.

Note on Downgrades

Downgrade of FXOS images is not officially supported. The only Cisco-supported method of downgrading an image version of FXOS is to perform a complete re-image of the device.

Upgrade Path: Other FTD Devices

This table provides upgrade paths for FTD devices managed by an FMC, where you do not have to update the operating system: Firepower 1000/2100 series, ASA 5500-X series, ISA 3000, and Firepower Threat Defense Virtual.

Find your current version in the left column. You can upgrade directly to any of the versions listed in the right column.

Table 17: Upgrade Paths: Firepower 1000/2100 series, ASA 5500-X series, ISA 3000, and Firepower Threat Defense Virtual with FMC

Current Version	Target Version
7.0.0 7.0.x Last FTD support for ASA 5508-X and 5516-X.	→ Any later 7.0.x maintenance release
6.7.0 6.7.x	Any of: → 7.0.0 or any 7.0.x maintenance release → Any later 6.7.x maintenance release
6.6.0 6.6.x Last FTD support for ASA 5525-X, 5545-X, and 5555-X.	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → Any later 6.6.x maintenance release
6.5.0	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release
6.4.0 Last FTD support for ASA 5515-X.	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release → 6.5.0
6.3.0	Any of: → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release → 6.5.0 → 6.4.0

Current Version	Target Version
6.2.3 Last FTD support for ASA 5506-X series.	Any of: → 6.6.0 or any 6.6.x maintenance release → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	Any of: → 6.4.0 → 6.3.0 → 6.2.3
6.2.1 Firepower 2100 series only.	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.2.0	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	→ 6.1.0

Upgrade Path: Firepower 7000/8000 Series

This table provides upgrade paths for Firepower 7000/8000 series devices, managed by an FMC.

Find your current version in the left column. You can upgrade directly to any of the versions listed in the right column.

Table 18: Upgrade Paths: Firepower 7000/8000 Series with FMC

Current Version	Target Version
6.4.0	None. Version 6.4.0 is the last major release for Firepower 7000/8000 series devices.
6.3.0	Any of: → 6.4.0
6.2.3	Any of: → 6.4.0 → 6.3.0
6.2.2	Any of: → 6.4.0 → 6.3.0 → 6.2.3
6.2.1 Not supported on this platform.	—
6.2.0	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	Any of: → 6.1.0
6.0.0	Any of: → 6.0.1

Current Version	Target Version
5.4.0.2	Any of: → 6.0.0 Requires a preinstallation package: FireSIGHT System Release Notes Version 6.0.0 Preinstallation.

Upgrade Path: ASA FirePOWER

This table provides upgrade paths for ASA FirePOWER modules, managed by an FMC.

Find your current version in the left column. You can upgrade directly to any of the versions listed in the right column.

If desired, you can also upgrade ASA. There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues. For ASA upgrade paths, see Upgrade Path: ASA for ASA FirePOWER, on page 25.

Table 19: Upgrade Paths: ASA FirePOWER with FMC

Current Version	Target Version
7.0.0 7.0.x Last ASA FirePOWER support on any platform.	→ Any later 7.0.x maintenance release
6.7.0 6.7.x	Any of: → 7.0.0 or any 7.0.x maintenance release → Any later 6.7.x maintenance release
6.6.0 6.6.x Last ASA FirePOWER support for ASA 5525-X, 5545-X, and 5555-X.	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → Any later 6.6.x maintenance release
6.5.0	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release

Current Version	Target Version
6.4.0 Last ASA FirePOWER support for ASA 5585-X series and ASA 5515-X.	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release → 6.5.0
6.3.0	Any of: → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release → 6.5.0 → 6.4.0
6.2.3 Last ASA FirePOWER support for ASA 5506-X series and ASA 5512-X.	Any of: → 6.6.0 or any 6.6.x maintenance release → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	Any of: → 6.4.0 → 6.3.0 → 6.2.3
6.2.1 Not supported on this platform.	—
6.2.0	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2

Current Version	Target Version
6.1.0	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	Any of: → 6.1.0
6.0.0	Any of: → 6.0.1
5.4.0.2 or 5.4.1.1	Any of: → 6.0.0 Requires a preinstallation package: FireSIGHT System Release Notes Version 6.0.0 Preinstallation.

Upgrading ASA

There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues. For detailed compatibility information, see Cisco Secure Firewall ASA Compatibility.

You upgrade ASA on each device independently, even if you have ASA clustering or failover pairs configured. Exactly when you upgrade the ASA FirePOWER module (before or after ASA reload) depends on your deployment. This table outlines ASA upgrade order for standalone and HA/scalability deployments. For detailed instructions, see Upgrade the ASA, on page 89.

Table 20: ASA + ASA FirePOWER Upgrade Order

ASA Deployment	Upgrade Order
Standalone device	1. Upgrade ASA, including reload. 2. Upgrade ASA FirePOWER.

ASA Deployment	Upgrade Order
ASA failover: active/standby	Always upgrade the standby. **1.** Upgrade ASA on the standby, but do not reload. **2.** Upgrade ASA FirePOWER on the standby. **3.** Reload ASA on the standby. **4.** Fail over. **5.** Upgrade ASA on the new standby. **6.** Upgrade ASA FirePOWER on the new standby. **7.** Reload ASA on the new standby.
ASA failover: active/active	Make both failover groups active on the unit you are not upgrading. **1.** Make both failover groups active on the primary. **2.** Upgrade ASA on the secondary, but do not reload. **3.** Upgrade ASA FirePOWER on the secondary. **4.** Reload ASA on the secondary. **5.** Make both failover groups active on the secondary. **6.** Upgrade ASA on the primary, but do not reload. **7.** Upgrade ASA FirePOWER on the primary. **8.** Reload ASA on the primary.
ASA cluster	Disable clustering on each unit before you upgrade. Upgrade one unit at a time, leaving the control unit for last. **1.** On a data unit, disable clustering. **2.** Upgrade ASA on that data unit, but do not reload. **3.** Upgrade ASA FirePOWER on the unit. **4.** Reload ASA. **5.** Reenable clustering. Wait for the unit to rejoin the cluster. **6.** Repeat for each data unit. **7.** On the control unit, disable clustering. Wait for a new control to take over. **8.** Upgrade ASA on the former control unit, but do not reload. **9.** Upgrade ASA FirePOWER on the former control unit. **10.** Reenable clustering.

Upgrade Path: ASA for ASA FirePOWER

This table provides upgrade paths for ASA on ASA with FirePOWER Services. There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues.

Find your current ASA version in the left column. You can upgrade directly to the target versions listed. Recommended versions are in **bold**.

Table 21: Upgrade Paths: ASA for ASA FirePOWER

Current Version	Target Version
9.15(x) Last ASA FirePOWER support on any platform, with Firepower Version 7.0.x.	→ **9.16(x)**
9.14(x) Last ASA FirePOWER support for ASA 5525-X, ASA 5545-X, and ASA 5555-X, with Firepower Version 6.6.x.	Any of: → **9.16(x)** → **9.15(x)**
9.13(x)	Any of: → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)**
9.12(x) Last ASA FirePOWER support for ASA 5515-X and ASA 5585-X, with Firepower Version 6.4.0.	Any of: → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)**
9.10(x)	Any of: → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x)

Current Version	Target Version
9.9(x) Last ASA FirePOWER Firepower support for ASA 5506-X series and ASA 5512-X, with Firepower Version 6.2.3.	Any of: → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x)
9.8(x)	Any of: → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**
9.7(x)	Any of: → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**

Current Version	Target Version
9.6(x)	Any of: → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.5(x)	Any of: → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.4(x)	Any of: → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)

Current Version	Target Version
9.3(x)	Any of: → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.2(x)	Any of: → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)

Upgrade Path: NGIPSv

This table provides upgrade paths for NGIPSv, managed by an FMC.

Find your current version in the left column. You can upgrade directly to any of the versions listed in the right column.

Table 22: Upgrade Paths: NGIPSv with FMC

Current Version	Target Version
7.0.0 7.0.x Last NGIPSv support.	→ Any later 7.0.x maintenance release

Current Version	Target Version
6.7.0 6.7.x	Any of: → 7.0.0 or any 7.0.x maintenance release → Any later 6.7.x maintenance release
6.6.0 6.6.x	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → Any later 6.6.x maintenance release
6.5.0	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release
6.4.0	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release → 6.5.0
6.3.0	Any of: → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release → 6.5.0 → 6.4.0
6.2.3	Any of: → 6.6.0 or any 6.6.x maintenance release → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	Any of: → 6.4.0 → 6.3.0

Current Version	Target Version
6.2.1 Not supported on this platform.	—
6.2.0	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	Any of: → 6.1.0
6.0.0	Any of: → 6.0.1
5.4.1.1	Any of: → 6.0.0 Requires a preinstallation package: FireSIGHT System Release Notes Version 6.0.0 Preinstallation.

Unresponsive Upgrades

Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down during upgrade. You could place the system in an unusable state and require a reimage.

Unresponsive FMC or Classic Device Upgrade

Do not restart an upgrade in progress. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Unresponsive FTD Upgrade

For major and maintenance upgrades, you can manually cancel failed or in-progress upgrades, and retry failed upgrades. On the FMC, use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page, and from the Message Center. You can also use the FTD CLI.

Note By default, FTD automatically reverts to its pre-upgrade state upon upgrade failure ("auto-cancel"). To be able to manually cancel or retry a failed upgrade, disable the auto-cancel option when you initiate the upgrade. Auto-cancel is not supported for patches. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

This feature is not supported for patches or for upgrades from Version 6.6 and earlier.

Time and Disk Space Tests

For reference purposes, we provide reports of in-house time and disk space tests for FMC and device software upgrades. For the actual reports, see the release notes for your target version.

Time Tests

We report the *slowest* tested time of all software upgrades tested on a particular platform/series. Your upgrade will likely take longer than the provided times for multiple reasons, as explained in the following table. We recommend you track and record your own upgrade times so you can use them as future benchmarks.

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive Upgrades, on page 30.

Table 23: Time Test Conditions for Software Upgrades

Condition	Details
Deployment	Times for device upgrades are from tests in a FMC deployments. Raw upgrade times for remotely and locally managed devices are similar, given similar conditions.
Versions	For major and maintenance releases, we test upgrades from all eligible previous major versions. For patches, we test upgrades from the base version. Upgrade time usually increases if your upgrade skips versions.
Models	In most cases, we test on the lowest-end models in each series, and sometimes on multiple models in a series.
Virtual appliances	We test with the default settings for memory and resources. However, note that upgrade time in virtual deployments is highly hardware dependent.

Condition	Details
High availability/scalability	Unless otherwise noted, we test on standalone devices. In a high availability or clustered configuration, devices upgrade one at a time to preserve continuity of operations, with each device operating in maintenance mode while it upgrades. Upgrading a device pair or entire cluster, therefore, takes longer than upgrading a standalone device.
Configurations	We test on appliances with minimal configurations and traffic load. Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how those things are affected by the upgrade. For example, if you use a lot of access control rules and the upgrade needs to make a backend change to how those rules are stored, the upgrade can take longer.
Components	We report times for the software upgrade itself and the subsequent reboot *only*. This does not include time for operating system upgrades, transferring upgrade packages, readiness checks, VDB and intrusion rule (SRU/LSP) updates, or deploying configurations.

Disk Space Tests

We report the *most* disk space used of all software upgrades tested on a particular platform/series. This includes the space needed to copy the upgrade package to the device.

We also report the space needed on the FMC (in either /Volume or /var) for the device upgrade package. If you have an internal server for FTD upgrade packages, or if you are using FDM, ignore those values.

When we report disk space estimates for a particular location (for example, /var or /ngfw), we are reporting the disk space estimate for the partition mounted in that location. On some platforms, these locations may be on the same partition.

Without enough free disk space, the upgrade fails.

Table 24: Checking Disk Space

Platform	Command
FMC	Choose **System** > **Monitoring** > **Statistics** and select the FMC. Under Disk Usage, expand the By Partition details.
FTD with FMC	Choose **System** > **Monitoring** > **Statistics** and select the device you want to check. Under Disk Usage, expand the By Partition details.

Download Upgrade Packages

Download upgrade packages from the Cisco Support & Download site before you start your upgrade. Depending on the specific upgrade, you should put the packages on either your local computer or a server that the appliance can access. The individual checklists and procedures in this guide explain your choices.

Note Downloads require a Cisco.com login and service contract.

Firepower Software Packages

Upgrade packages are available on the Cisco Support & Download site.

- Firepower Management Center, including Firepower Management Center Virtual: https://www.cisco.com/go/firepower-software
- Firepower Threat Defense (ISA 3000): https://www.cisco.com/go/isa3000-software
- Firepower Threat Defense (all other models, including Firepower Threat Defense Virtual): https://www.cisco.com/go/ftd-software
- Firepower 7000 series: https://www.cisco.com/go/7000series-software
- Firepower 8000 series: https://www.cisco.com/go/8000series-software
- ASA with FirePOWER Services (ASA 5500-X series): https://www.cisco.com/go/asa-firepower-sw
- ASA with FirePOWER Services (ISA 3000): https://www.cisco.com/go/isa3000-software
- NGIPSv: https://www.cisco.com/go/ngipsv-software

To find an upgrade package, select or search for your appliance model, then browse to the software download page for your current version. Available upgrade packages are listed along with installation packages, hotfixes, and other applicable downloads.

Tip A Firepower Management Center with internet access can download select releases directly from Cisco, some time after the release is available for manual download. The length of the delay depends on release type, release adoption, and other factors.

You use the same upgrade package for all models in a family or series. Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), and software version. Maintenance releases use the upgrade package type.

For example:

- Package: `Cisco_Firepower_Mgmt_Center_Upgrade--999.sh.REL.tar`
- Platform: Firepower Management Center
- Package type: Upgrade
- Version and build: -999
- File extension: sh.REL.tar

So that the system can verify that you are using the correct files, upgrade packages from Version 6.2.1+ are *signed* tar archives (.tar). Do not untar signed (.tar) packages. And, do not transfer upgrade packages by email.

Note After you upload a signed upgrade package, the Firepower Management Center GUI can take several minutes to load as the system verifies the package. To speed up the display, remove these packages after you no longer need them.

Firepower Software Upgrade Packages

Table 25:

Platform	Versions	Package
FMC/FMCv	6.3.0+	Cisco_Firepower_Mgmt_Center
	5.4.0 to 6.2.3	Sourcefire_3D_Defense_Center_S3
Firepower 1000 series	Any	Cisco_FTD_SSP-FP1K
Firepower 2100 series	Any	Cisco_FTD_SSP-FP2K
Firepower 4100/9300	Any	Cisco_FTD_SSP
ASA 5500-X series with FTD ISA 3000 with FTD FTDv	Any	Cisco_FTD
Firepower 7000/8000 series AMP models	6.3.0 to 6.4.0	Cisco_Firepower_NGIPS_Appliance
	5.4.0 to 6.2.3	Sourcefire_3D_Device_S3
ASA FirePOWER	Any	Cisco_Network_Sensor
NGIPSv	6.3.0+	Cisco_Firepower_NGIPS_Virtual
	6.2.2 to 6.2.3	Sourcefire_3D_Device_VMware
	5.4.0 to 6.2.0	Sourcefire_3D_Device_Virtual64_VMware

FXOS Packages

FXOS packages for the Firepower 4100/9300 are available on the Cisco Support & Download site.

- Firepower 4100 series: http://www.cisco.com/go/firepower4100-software
- Firepower 9300: http://www.cisco.com/go/firepower9300-software

To find FXOS packages, select or search for your Firepower appliance model, then browse to the Firepower Extensible Operating System download page for the target version.

Note If you plan to use the CLI to upgrade FXOS, copy the upgrade package to a server that the Firepower 4100/9300 can access using SCP, SFTP, TFTP, or FTP.

Table 26: FXOS Packages for the Firepower 4100/9300

Package Type	Package
FXOS image	fxos-k9.*version*.**SPA**
Recovery (kickstart)	fxos-k9-**kickstart**.*version*.**SPA**
Recovery (manager)	fxos-k9-**manager**.*version*.**SPA**
Recovery (system)	fxos-k9-**system**.*version*.**SPA**
MIBs	fxos-**mibs**-fp9k-fp4k.*version*.**zip**
Firmware: Firepower 4100 series	fxos-k9-fpr4k-**firmware**.*version*.**SPA**
Firmware: Firepower 9300	fxos-k9-fpr9k-**firmware**.*version*.**SPA**

ASA Packages

ASA software is available on the Cisco Support & Download site.

- ASA with FirePOWER Services (ASA 5500-X series): https://www.cisco.com/go/asa-firepower-sw
- ASA with FirePOWER Services (ISA 3000): https://www.cisco.com/go/isa3000-software

To find ASA software, select or search for your Firepower appliance model, browse to the appropriate download page, and select a version.

Note If you are using the ASDM upgrade wizard, you do not have to pre-download. Otherwise, download to your local computer. For CLI upgrades, you should then copy the software to a server that the device can access via any protocol supported by the ASA **copy** command, including HTTP, FTP, and SCP.

Table 27: ASA Software

Download Page	Software Type	Package
Adaptive Security Appliance (ASA) Software	ASA and ASDM upgrade	asa*version*-**lfbff-k8.SPA** for the ASA 5506-X, ASA 5508-X, ASA 5516-X, and ISA 3000
		asa*version*-**smp-k8.bin** for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, and ASA 5585-X
Adaptive Security Appliance (ASA) Device Manager	ASDM upgrade only	asdm-*version***.bin**
Adaptive Security Appliance REST API Plugin	ASA REST API	asa-restapi-*version*-**lfbff-k8.SPA**

Upload Firepower Software Upgrade Packages

To upgrade Firepower software, the software upgrade package must be on the appliance.

Upload to the Firepower Management Center

Use this procedure to manually upload Firepower software upgrade packages to the Firepower Management Center, for itself and the devices it manages.

Before you begin

If you are upgrading the standby Firepower Management Center in a high availability pair, pause synchronization.

In FMC high availability deployments, you must upload the FMC upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to HA synchronization, you can transfer the package to the active peer during the preparation stage of the upgrade, and to the standby peer as part of the actual upgrade process, after you pause synchronization.

Step 1 On the Firepower Management Center web interface, choose **System** > **Updates**.

Step 2 Click **Upload Update**.

Tip Select upgrade packages become available for direct download by the Firepower Management Center some time after the release is available for manual download. The length of the delay depends on release type, release adoption, and other factors. If your Firepower Management Center has internet access, you can instead click **Download Updates** to download *all* eligible packages for your deployment, as well as the latest VDB if needed.

Step 3 (Version 6.6.0+) For the **Action**, click the **Upload local software update package** radio button.

Step 4 Click **Choose File**.

Step 5 Browse to the package and click **Upload**.

Upload to an Internal Server (Version 6.6.0+ FTD with FMC)

Starting with Version 6.6.0, Firepower Threat Defense devices can get upgrade packages from an 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 6.6.0+. It is not supported for upgrades *to* Version 6.6.0, nor is it supported for the FMC or Classic devices.

To configure this feature, you save a pointer (URL) to an upgrade package's location on the web server. The upgrade process will then get the upgrade package from the web server instead of the FMC. Or, you can use the FMC to copy the package before you upgrade.

Repeat this procedure for each FTD upgrade package. You can configure only one location per upgrade package.

Before you begin

- Download the appropriate upgrade packages from the Cisco Support & Download site and copy them to an internal web server that your FTD devices can access.
- For secure web servers (HTTPS), obtain the server's digital certificate (PEM format). You should be able to obtain the certificate from the server's administrator. You may also be able to use your browser, or a tool like OpenSSL, to view the server's certifcate details and export or copy the certificate.

Step 1 On the FMC web interface, choose **System** > **Updates**.

Step 2 Click **Upload Update**.

Choose this option even though you will not upload anything. The next page will prompt you for a URL.

Step 3 For the **Action**, click the **Specify software update source** radio button.

Step 4 Enter a **Source URL** for the upgrade package.

Provide the protocol (HTTP/HTTPS) and full path, for example:

`https://internal_web_server/upgrade_package.sh.REL.tar`

Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), and the Firepower version you are upgrading to. Make sure you enter the correct file name.

Step 5 For HTTPS servers, provide a **CA Certificate**.

This is the server's digital certificate you obtained earlier. Copy and paste the entire block of text, including the BEGIN CERTIFICATE and END CERTIFICATE lines.

Step 6 Click **Save**.

You are returned to the Product Updates page. Uploaded upgrade packages and upgrade package URLs are listed togther, but are labeled distinctly.

Copy to Managed Devices

To upgrade Firepower software, the upgrade package must be on the device. When supported, we recommend you use this procedure to copy (*push*) packages to managed devices before you initiate the device upgrade.

Note For the Firepower 4100/9300, we recommend (and sometimes require) you copy the Firepower Threat Defense upgrade package before you begin the required companion FXOS upgrade.

Support varies by Firepower version:

- Version 6.2.2 and earlier do not support pre-upgrade copy.

  When you start a device upgrade, the system copies the upgrade package from the Firepower Management Center to the device as the first task.

- Version 6.2.3 adds the ability to manually copy upgrade packages to the device from the Firepower Management Center.

  This reduces the length of your upgrade maintenance window.

- Version 6.6.0 adds the ability to manually copy upgrade packages from an internal web server to Firepower Threat Defense devices.

  This is useful if you have limited bandwidth between the Firepower Management Center and its Firepower Threat Defense devices. It also saves space on the Firepower Management Center.

- Version 7.0.0 introduces a new Firepower Threat Defense upgrade workflow that prompts you to copy the upgrade package to Firepower Threat Defense devices.

  If your Firepower Management Center is running Version 7.0.0+, we recommend you use the Device Upgrade page to copy the upgrade package to FTD devices; see Upgrade Firepower Threat Defense with FMC (Version 7.0.0), on page 74. You must still use this procedure to copy upgrade packages in older deployments, and to Classic devices (Firepower 7000/8000 series, ASA FirePOWER, NGIPSv).

Note that when you copy manually, each device gets the upgrade package from the source—the system does not copy upgrade packages between cluster, stack, or HA member units.

Before you begin

Make sure your management network has the bandwidth to perform large data transfers. See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).

Step 1 On the Firepower Management Center web interface, choose **System** > **Updates**.

Step 2 Put the upgrade package where the device can get it.

- Firepower Management Center: Manually upload or directly retrieve the package to the FMC.

- Internal web server (Firepower Threat Defense Version 6.6.0+): Upload to an internal web server and configure Firepower Threat Defense devices to get the package from that server.

Step 3 Click the **Push** (Version 6.5.0 and earlier) or **Push or Stage update** (Version 6.6.0+) icon next to the upgrade package you want to push, then choose destination devices.

If the devices where you want to push the upgrade package are not listed, you chose the wrong upgrade package.

Step 4 Push the package

- Firepower Management Center: Click **Push**.
- Internal web server: Click **Download Update to Device from Source**.

Firepower Software Readiness Checks

Readiness checks assess a Firepower appliance's preparedness for a software upgrade. If the appliance fails the readiness check, correct the issues and run the readiness check again. If the readiness check exposes issues that you cannot resolve, we recommend you do not begin the upgrade.

The time required to run a readiness check varies depending on appliance model and database size. Later releases also have faster readiness checks.

Run Readiness Checks with FMC (Version 7.0.0+ FTD)

If your FMC is running Version 7.0.0+, we recommend you use the Device Upgrage page to run readiness checks on FTD devices; see Upgrade Firepower Threat Defense with FMC (Version 7.0.0), on page 74.

See the next topics if you are:

- Running readiness checks on the FMC itself.
- Running readiness checks on managed devices, and your FMC is running Version 6.7.x.
- Running readiness checks on managed devices, and your FMC is running Version 6.6.x or earlier.

Run Readiness Checks with FMC (Version 6.7.0+)

This procedure is valid for FMCs *currently* running Version 6.7.0+, and their managed devices, including devices running older versions (6.3.0–6.6.x), and FTD devices in high availability and scalability deployments.

Important If your FMC is running Version 7.0.0+, we recommend you use the Device Upgrade page to run readiness checks on FTD devices; see Upgrade Firepower Threat Defense with FMC (Version 7.0.0), on page 74. You must still use this procedure to run readiness checks on the FMC and on any Classic devices.

Before you begin

- Upgrade the FMC to at least Version 6.7.0. If your FMC is currently running an older version, see Run Readiness Checks with FMC (Version 6.0.1–6.6.x), on page 40.
- Upload the upgrade package to the FMC, for the appliance you want to check. If you want to check Version 6.6.0+ FTD devices, you can also specify the upgrade package location on an internal web server. This is required because readiness checks are included in upgrade packages.
- (Optional) If you are upgrading a Classic device to any version, or an FTD device to Version 6.3.0.1–6.6.x, copy the upgrade package to the device. This can reduce the time required to run the readiness check. If you are upgrading an FTD device to Version 6.7.0+, you can skip this step. Although we still recommend you push the upgrade package to the device before you begin the upgrade itself, you no longer have to do so before you run the readiness check.

Step 1 On the FMC web interface, choose **System** > **Updates**.

Step 2 Under Available Updates, click the **Install** icon next to the appropriate upgrade package.

The system displays a list of eligible appliances, along with their pre-upgrade compatibility check results. Starting with Version 6.7.0, FTD devices must pass certain basic checks before you can run the more complex readiness check. This pre-check catches issues that *will* cause your upgrade to fail—but we now catch them earlier and block you from proceeding.

Step 3 Select the appliances you want to check and click **Check Readiness**.

If you cannot select an otherwise eligible appliance, make sure it passed its compatibility checks. You may need to upgrade an operating system, or deploy configuration changes.

Step 4 Monitor the progress of the readiness check in the Message Center.

If the check fails, the Message Center provides failure logs.

What to do next

On the **System** > **Updates** page, click **Readiness Checks** to view readiness check status for your FTD deployment, including checks in progress and failed checks. You can also use this page to easily re-run checks after a failure.

Run Readiness Checks with FMC (Version 6.0.1–6.6.x)

This procedure is valid for FMCs *currently* running Version 6.0.1–6.6.x, and their standalone managed devices.

Note For clustered devices, stacked devices, and devices in high availability pairs, you can run the readiness check from the Linux shell, also called *expert mode*. To run the check, you must first push or copy the upgrade package to the correct location on each device, then use this command: `sudo install_update.pl --detach --readiness-check /var/sf/updates/upgrade_package_name`. For detailed instructions, contact Cisco TAC.

Before you begin

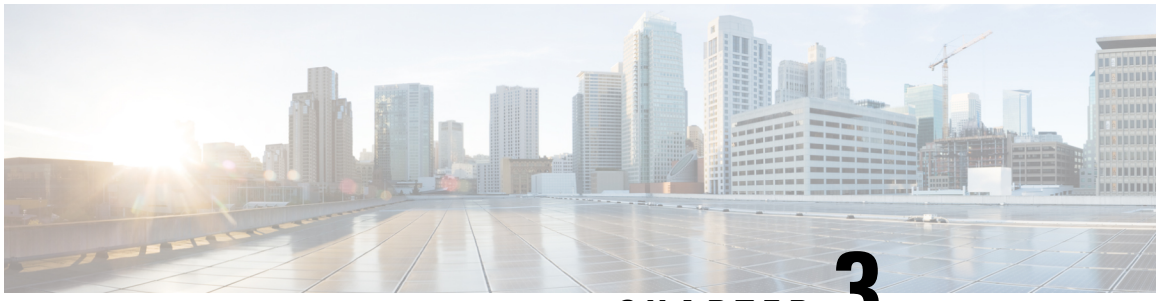
- (Version 6.0.1) If you want to run readiness checks on a Version 6.0.1 → 6.1.0 upgrade, first install the Version 6.1 preinstallation package. You must do this for the FMC and managed devices. See the Firepower System Release Notes Version 6.1.0 Pre-Installation Package.
- Upload the upgrade package to the FMC, for the appliance you want to check. If you want to check Version 6.6.x FTD devices, you can also specify the upgrade package location on an internal web server. This is required because readiness checks are included in upgrade packages.
- (Optional, Version 6.2.3+) Push the upgrade package to the managed device. This can reduce the time required to run the check.
- Deploy configurations to managed devices whose configurations are out of date. Otherwise, the readiness check may fail.

Step 1 On the FMC web interface, choose **System** > **Updates**.

Step 2 Click the **Install** icon next to the appropriate upgrade package.

Step 3 Select the appliances you want to check and click **Launch Readiness Check**.

Step 4 Monitor the progress of the readiness check in the Message Center.



CHAPTER 3

Upgrade Firepower Management Centers

Upgrade Checklist: Firepower Management Center

Complete this checklist before you upgrade an FMC, including FMCv. If you are upgrading a high availability pair, complete the checklist for each peer.

Note At all times during the process, make sure you maintain deployment communication and health. Do *not* restart an FMC upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 28:

✓	Action/Check
	Plan your upgrade path. This is especially important for multi-appliance deployments, multi-hop upgrades, or situations where you need to upgrade operating systems or hosting environments, all while maintaining deployment compatibility. Always know which upgrade you just performed and which you are performing next. **Note** In FMC deployments, you usually upgrade the FMC, then its managed devices. However, in some cases you may need to upgrade devices first. See Upgrade Paths, on page 10.

✓	Action/Check
	Read *all* upgrade guidelines and plan configuration changes. Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. Start with the release notes, which contain critical and release-specific information, including upgrade warnings, behavior changes, new and deprecated features, and known issues.
	Check bandwidth. Make sure your management network has the bandwidth to perform large data transfers. In FMC deployments, if you transfer an upgrade package to a managed device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. Whenever possible, copy upgrade packages to managed devices before you initiate the device upgrade. See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).
	Schedule maintenance windows. Schedule maintenance windows when they will have the least impact, considering any effect on traffic flow and inspection and the time the upgrade is likely to take. Also consider the tasks you *must* perform in the window, and those you can perform ahead of time. For example, do not wait until the maintenance window to copy upgrade packages to appliances, run readiness checks, perform backups, and so on.

Upgrade Packages

Upgrade packages are available on the Cisco Support & Download site.

Table 29:

✓	Action/Check
	Upload the upgrade package. In FMC high availability deployments, you must upload the FMC upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to HA synchronization, you can transfer the package to the active peer during the preparation stage of the upgrade, and to the standby peer as part of the actual upgrade process, after you pause synchronization. See Upload to the Firepower Management Center, on page 36.

Backups

The ability to recover from a disaster is an essential part of any system maintenance plan.

Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your deployment.

Caution We *strongly* recommend you back up to a secure remote location and verify transfer success, both before and after upgrade.

Table 30:

✓	Action/Check
	Back up. Back up before and after upgrade: • Before upgrade: If an upgrade fails catastrophically, you may have to reimage and restore. Reimaging returns most settings to factory defaults, including the system password. If you have a recent backup, you can return to normal operations more quickly. • After upgrade: This creates a snapshot of your freshly upgraded deployment. In FMC deployments, we recommend you back up the FMC after you upgrade its managed devices, so your new FMC backup file 'knows' that its devices have been upgraded.

Associated Upgrades

Because operating system and hosting environment upgrades can affect traffic flow and inspection, perform them in a maintenance window.

Table 31:

✓	Action/Check
	Upgrade virtual hosting. If needed, upgrade the hosting environment. If this is required, it is usually because you are running an older version of VMware and are performing a major FMC upgrade.

Final Checks

A set of final checks ensures you are ready to upgrade.

Table 32:

✓	Action/Check
	Check configurations. Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes.

✓	Action/Check
	Check NTP synchronization. Make sure all appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In FMC deployments, the health monitor does alert if clocks are out of sync by more than 10 seconds, but you should still check manually. To check time: • FMC: Choose **System > Configuration > Time**. • Devices: Use the **show time** CLI command.
	Check disk space. Run a disk space check for the software upgrade. Without enough free disk space, the upgrade fails. See the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.
	Deploy configurations. Deploying configurations before you upgrade reduces the chance of failure. In some deployments, you may be blocked from upgrade if you have out-of-date configurations. In FMC high availability deployments, you only need to deploy from the active peer. When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device handles traffic, may interrupt traffic until the restart completes. See the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.
	Run readiness checks. If your FMC is running Version 6.1.0+, we recommend compatibility and readiness checks. These checks assess your preparedness for a software upgrade. See Firepower Software Readiness Checks, on page 39.
	Check running tasks. Make sure essential tasks are complete before you upgrade, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. We also recommend you check for tasks that are scheduled to run during the upgrade, and cancel or postpone them. **Note** In some deployments, upgrades automatically postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. This feature is currently supported for FMCs running Version 6.4.0.10 and later patches, Version 6.6.3 and later maintenance releases, and Version 6.7.0+. Note that this feature is supported for all upgrades *from* a supported version. This feature is not supported for upgrades *to* a supported version from an unsupported version.

Upgrade a Standalone Firepower Management Center

Use this procedure to upgrade a standalone Firepower Management Center, including Firepower Management Center Virtual.

Caution Do *not* make or deploy configuration changes, manually reboot, or shut down while you are upgrading the FMC. Do *not* restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Before you begin

Complete the pre-upgrade checklist. Make sure the appliances in your deployment are healthy and successfully communicating.

Step 1 Choose **System** > **Updates**.

Step 2 Click the Install icon next to the upgrade package you want to use, then choose the FMC.

Step 3 Click **Install** to begin the upgrade.

Confirm that you want to upgrade and reboot.

Step 4 Monitor precheck progress until you are logged out. Do not make configuration changes during this time.

Step 5 Log back in when you can.

- Minor upgrades (patches and hotfixes): You can log in after the upgrade and reboot are completed.
- Major and maintenance upgrades: You can log in before the upgrade is completed. The system displays a page you can use to monitor the upgrade's progress and view the upgrade log and any error messages. You are logged out again when the upgrade is completed and the system reboots. After the reboot, log back in again.

Step 6 If prompted, review and accept the End User License Agreement (EULA).

Step 7 Verify upgrade success.

If the system does not notify you of the upgrade's success when you log in, choose **Help** > **About** to display current software version information.

Step 8 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 9 Complete any post-upgrade configuration changes described in the release notes.

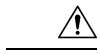
Step 10 Redeploy configurations.

Redeploy to *all* managed devices. If you do not deploy to a device, its eventual upgrade may fail and you may have to reimage it.

Upgrade High Availability Firepower Management Centers

Use this procedure to upgrade the Firepower software on FMCs in a high availability pair.

You upgrade peers one at a time. With synchronization paused, first upgrade the standby, then the active. When the standby starts prechecks, its status switches from standby to active, so that both peers are active. This temporary state is called *split-brain* and is *not* supported except during upgrade. Do *not* make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you restart synchronization.



Caution Do *not* make or deploy configuration changes, manually reboot, or shut down while you are upgrading the FMC. Do *not* restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Before you begin

Complete the pre-upgrade checklist for both peers. Make sure the appliances in your deployment are healthy and successfully communicating.

Step 1 Pause synchronization.

a) Choose **System** > **Integration**.
b) On the **High Availability** tab, click **Pause Synchronization**.

Step 2 Upload the upgrade package to the standby.

In FMC high availability deployments, you must upload the FMC upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to HA synchronization, you can transfer the package to the active peer during the preparation stage of the upgrade, and to the standby peer as part of the actual upgrade process, after you pause synchronization.

Step 3 Upgrade peers one at a time — first the standby, then the active.

Follow the instructions in Upgrade a Standalone Firepower Management Center, on page 47, stopping after you verify update success on each peer. In summary, for each peer:

a) On the **System** > **Updates** page, install the upgrade.
b) Monitor progress until you are logged out, then log back in when you can (this happens twice for major upgrades).
c) Verify upgrade success.

Do *not* make or deploy configuration changes while the pair is split-brain.

Step 4 Restart synchronization.

a) Log into the FMC that you want to make the active peer.
b) Choose **System** > **Integration**.
c) On the **High Availability** tab, click **Make-Me-Active**.
d) Wait until synchronization restarts and the other FMC switches to standby mode.

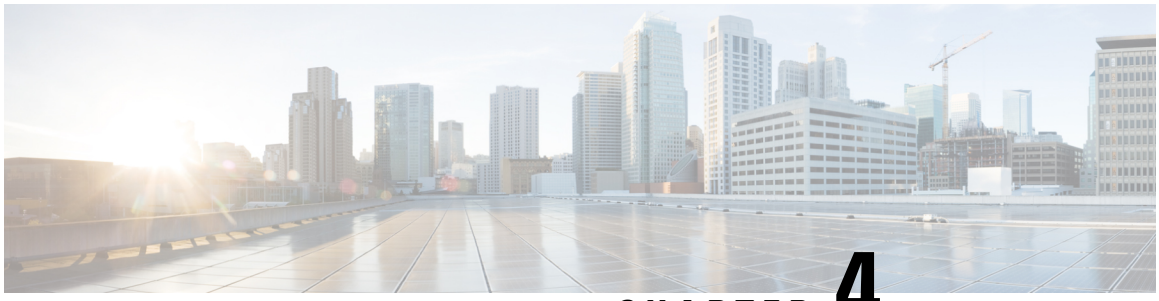
Step 5 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 6 Complete any post-upgrade configuration changes described in the release notes.

Step 7 Redeploy configurations.

Redeploy to *all* managed devices. If you do not deploy to a device, its eventual upgrade may fail and you may have to reimage it.



CHAPTER 4

Upgrade Firepower Threat Defense

Upgrade Checklist: Firepower Threat Defense with FMC

Complete this checklist before you upgrade Firepower Threat Defense.

Note At all times during the process, make sure you maintain deployment communication and health.

In most cases, do *not* restart an upgrade in progress. However, starting with major and maintenance FTD upgrades *from* Version 6.7.0, you can manually cancel failed or in-progress upgrades, and retry failed upgrades; use the Upgrade Status pop-up, accessible from the Device Management page and the Message Center, or use the FTD CLI. Note that by default, FTD automatically reverts to its pre-upgrade state upon upgrade failure ("auto-cancel"). To be able to *manually* cancel or retry a failed upgrade, disable the auto-cancel option when you initiate the upgrade. Note that auto-cancel is not supported for patches. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. If you have exhausted all options, or if your deployment does not support cancel/retry, contact Cisco TAC.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 33:

✓	Action/Check
	Plan your upgrade path. This is especially important for multi-appliance deployments, multi-hop upgrades, or situations where you need to upgrade operating systems or hosting environments, all while maintaining deployment compatibility. Always know which upgrade you just performed and which you are performing next. **Note** In FMC deployments, you usually upgrade the FMC, then its managed devices. However, in some cases you may need to upgrade devices first. See Upgrade Paths, on page 10.
	Read *all* upgrade guidelines and plan configuration changes. Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. Start with the release notes, which contain critical and release-specific information, including upgrade warnings, behavior changes, new and deprecated features, and known issues.
	Check appliance access. Devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also able to access the FMC management interface without traversing the device.
	Check bandwidth. Make sure your management network has the bandwidth to perform large data transfers. In FMC deployments, if you transfer an upgrade package to a managed device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. Whenever possible, copy upgrade packages to managed devices before you initiate the device upgrade. See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).
	Schedule maintenance windows. Schedule maintenance windows when they will have the least impact, considering any effect on traffic flow and inspection and the time the upgrade is likely to take. Also consider the tasks you *must* perform in the window, and those you can perform ahead of time. For example, do not wait until the maintenance window to copy upgrade packages to appliances, run readiness checks, perform backups, and so on.

Upgrade Packages

Upgrade packages are available on the Cisco Support & Download site.

Table 34:

✓	Action/Check
	Upload the upgrade package to the FMC or internal web server. In Version 6.6.0+ you can configure an internal web server instead of the FMC as the source for FTD upgrade packages. This is useful if you have limited bandwidth between the FMC and its devices, and saves space on the FMC. See Upload to an Internal Server (Version 6.6.0+ FTD with FMC), on page 37.
	Copy the upgrade package to the device. When supported, we recommend you copy (*push*) packages to managed devices before you initiate the device upgrade: • Version 6.2.2 and earlier do not support pre-upgrade copy. • Version 6.2.3 allows you to manually copy upgrade packages from the FMC. • Version 6.6.0 adds the ability to manually copy upgrade packages from an internal web server. • Version 7.0.0 adds a FTD upgrade workflow that prompts you to copy upgrade packages. **Note** For the Firepower 4100/9300, we recommend (and sometimes require) you copy the upgrade package before you begin the required companion FXOS upgrade. See Copy to Managed Devices, on page 38.

Backups

The ability to recover from a disaster is an essential part of any system maintenance plan.

Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your deployment.

Caution We *strongly* recommend you back up to a secure remote location and verify transfer success, both before and after upgrade.

Table 35:

✓	Action/Check
	Back up FTD. Use the FMC to back up devices. Not all FTD platforms and configurations support backup. Requires Version 6.3.0+. Back up before and after upgrade: • Before upgrade: If an upgrade fails catastrophically, you may have to reimage and restore. Reimaging returns most settings to factory defaults, including the system password. If you have a recent backup, you can return to normal operations more quickly. • After upgrade: This creates a snapshot of your freshly upgraded deployment. In FMC deployments, we recommend you back up the FMC after you upgrade its managed devices, so your new FMC backup file 'knows' that its devices have been upgraded.
	Back up FXOS on the Firepower 4100/9300. Use the Firepower Chassis Manager or the FXOS CLI to export chassis configurations before and after upgrade, including logical device and platform configuration settings.

Associated Upgrades

Because operating system and hosting environment upgrades can affect traffic flow and inspection, perform them in a maintenance window.

Table 36:

✓	Action/Check
	Upgrade virtual hosting. If needed, upgrade the hosting environment for any virtual appliances. If this is required, it is usually because you are running an older version of VMware and are performing a major device upgrade.
	Upgrade FXOS on the Firepower 4100/9300. If needed, upgrade FXOS before you upgrade FTD. This is usually a requirement for major upgrades, but very rarely for maintenance releases and patches. To avoid interruptions in traffic flow and inspection, upgrade FXOS in FTD high availability pairs and inter-chassis clusters *one chassis at a time*. **Note** Before you upgrade FXOS, make sure you read all upgrade guidelines and plan configuration changes. Start with the FXOS release notes: Cisco Firepower 4100/9300 FXOS Release Notes.

Final Checks

A set of final checks ensures you are ready to upgrade.

Table 37:

✓	Action/Check
	Check configurations. Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes.
	Check NTP synchronization. Make sure all appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In FMC deployments, the health monitor does alert if clocks are out of sync by more than 10 seconds, but you should still check manually. To check time: • FMC: Choose **System > Configuration > Time**. • Devices: Use the **show time** CLI command.
	Check disk space. Run a disk space check for the software upgrade. Without enough free disk space, the upgrade fails. See the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.
	Deploy configurations. Deploying configurations before you upgrade reduces the chance of failure. In some deployments, you may be blocked from upgrade if you have out-of-date configurations. In FMC high availability deployments, you only need to deploy from the active peer. When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device handles traffic, may interrupt traffic until the restart completes. See the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.
	Run readiness checks. If your FMC is running Version 6.1.0+, we recommend compatibility and readiness checks. These checks assess your preparedness for a software upgrade. Version 7.0.0 introduces a new FTD upgrade workflow that prompts you to complete these checks. See Firepower Software Readiness Checks, on page 39.
	Check running tasks. Make sure essential tasks on the device are complete before you upgrade, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. We also recommend you check for tasks that are scheduled to run during the upgrade, and cancel or postpone them.

Upgrade FXOS on a Firepower 4100/9300 with Firepower Threat Defense Logical Devices

On the Firepower 4100/9300, you upgrade FXOS on each chassis independently, even if you have Firepower inter-chassis clustering or high availability pairs configured. You can use the FXOS CLI or Firepower Chassis Manager.

Upgrading FXOS reboots the chassis. Depending on your deployment, traffic can either drop or traverse the network without inspection; see the CiscoFirepower Release Notes for your version.

Upgrade FXOS: FTD Standalone Devices and Intra-chassis Clusters

For a standalone Firepower Threat Defense logical device, or for an FTD intra-chassis cluster (units on the same chassis), first upgrade the FXOS platform bundle then upgrade FTD logical devices. Use the Firepower Management Center to upgrade clustered devices as a unit.

Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster Using Firepower Chassis Manager

This section describes how to upgrade the FXOS platform bundle for a standalone Firepower 4100/9300 chassis.

The section describes the upgrade process for the following types of devices:

- A Firepower 4100 series chassis that is configured with a FTD logical device and is not part of a failover pair or inter-chassis cluster.
- A Firepower 9300 chassis that is configured with one or more standalone FTD logical devices that are not part of a failover pair or inter-chassis cluster.
- A Firepower 9300 chassis that is configured with FTD logical devices in an intra-chassis cluster.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.
- Back up your FXOS and FTD configurations.

Step 1 In Firepower Chassis Manager, choose **System** > **Updates**.
The Available Updates page shows a list of the FXOS platform bundle images and application images that are available on the chassis.

Step 2 Upload the new platform bundle image:

a) Click **Upload Image** to open the Upload Image dialog box.
b) Click **Choose File** to navigate to and select the image that you want to upload.
c) Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.

d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Step 3 After the new platform bundle image has been successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Step 4 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 5 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

Step 6 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.
f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster Using the FXOS CLI

This section describes how to upgrade the FXOS platform bundle for a standalone Firepower 4100/9300 chassis.

The section describes the FXOS upgrade process for the following types of devices:

- A Firepower 4100 series chassis that is configured with a FTD logical device and is not part of a failover pair or inter-chassis cluster.
- A Firepower 9300 chassis that is configured with one or more standalone FTD devices that are not part of a failover pair or inter-chassis cluster.
- A Firepower 9300 chassis that is configured with FTD logical devices in an intra-chassis cluster.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.
- Back up your FXOS and FTD configurations.
- Collect the following information that you will need to download the software image to the Firepower 4100/9300 chassis:
  - IP address and authentication credentials for the server from which you are copying the image.
  - Fully qualified name of the image file.

Step 1 Connect to the FXOS CLI.

Step 2 Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter firmware mode:

Firepower-chassis-a # **scope firmware**

b) Download the FXOS platform bundle software image:

Firepower-chassis-a /firmware # **download image** *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) To monitor the download process:

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 3 If necessary, return to firmware mode:

Firepower-chassis-a /firmware/download-task # **up**

Step 4 Enter auto-install mode:

Firepower-chassis-a /firmware # **scope auto-install**

Step 5 Install the FXOS platform bundle:

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

Step 6 The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter **yes** to confirm that you want to proceed with verification.

Step 7 Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 8 To monitor the upgrade process:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
```

```
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

Step 9 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.
f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Upgrade FXOS: FTD High Availability Pairs

In Firepower Threat Defense high availability deployments, upgrade the FXOS platform bundle on *both chassis* before you upgrade either FTD logical device. To minimize disruption, always upgrade the standby.

In Firepower Management Center deployments, you upgrade the logical devices as a unit:

1. Upgrade FXOS on the standby.
2. Switch roles.
3. Upgrade FXOS on the new standby.
4. Upgrade FTD logical devices.

Upgrade FXOS on an FTD High Availability Pair Using Firepower Chassis Manager

If you have Firepower 9300 or Firepower 4100 series security appliances that have FTD logical devices configured as a high availability pair, use the following procedure to update the FXOS platform bundle on your Firepower 9300 or Firepower 4100 series security appliances:

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.
- Back up your FXOS and FTD configurations.

Step 1 Connect to Firepower Chassis Manager on the Firepower security appliance that contains the *standby* Firepower Threat Defense logical device:

Step 2 In Firepower Chassis Manager, choose **System** > **Updates**.
The Available Updates page shows a list of the FXOS platform bundle images and application images that are available on the chassis.

Step 3 Upload the new platform bundle image:

a) Click **Upload Image** to open the Upload Image dialog box.
b) Click **Choose File** to navigate to and select the image that you want to upload.
c) Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.
d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Step 4 After the new platform bundle image has successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Step 5 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 6 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

Step 7 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.
f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Step 8 Make the unit that you just upgraded the *active* unit so that traffic flows to the upgraded unit:

a) Connect to Firepower Management Center.
b) Choose **Devices** > **Device Management**.
c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ( ).
d) Click **Yes** to immediately make the standby device the active device in the high availability pair.

Step 9 Connect to Firepower Chassis Manager on the Firepower security appliance that contains the *new standby* Firepower Threat Defense logical device:

Step 10 In Firepower Chassis Manager, choose **System** > **Updates**.
The Available Updates page shows a list of the FXOS platform bundle images and application images that are available on the chassis.

Step 11 Upload the new platform bundle image:

a) Click **Upload Image** to open the Upload Image dialog box.
b) Click **Choose File** to navigate to and select the image that you want to upload.
c) Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.
d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Step 12 After the new platform bundle image has successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Step 13 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components. The upgrade process can take up to 30 minutes to complete.

Step 14 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

Step 15 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.
f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Step 16 Make the unit that you just upgraded the *active* unit as it was before the upgrade:

a) Connect to Firepower Management Center.
b) Choose **Devices** > **Device Management**.
c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ( ).
d) Click **Yes** to immediately make the standby device the active device in the high availability pair.

Upgrade FXOS on an FTD High Availability Pair Using the FXOS CLI

If you have Firepower 9300 or Firepower 4100 series security appliances that have FTD logical devices configured as a high availability pair, use the following procedure to update the FXOS platform bundle on your Firepower 9300 or Firepower 4100 series security appliances:

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.
- Back up your FXOS and FTD configurations.
- Collect the following information that you will need to download the software image to the Firepower 4100/9300 chassis:
    - IP address and authentication credentials for the server from which you are copying the image.

- Fully qualified name of the image file.

Step 1 Connect to FXOS CLI on the Firepower security appliance that contains the *standby* Firepower Threat Defense logical device:

Step 2 Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter firmware mode:

Firepower-chassis-a # **scope firmware**

b) Download the FXOS platform bundle software image:

Firepower-chassis-a /firmware # **download image** *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) To monitor the download process:

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 3 If necessary, return to firmware mode:

Firepower-chassis-a /firmware/download-task # **up**

Step 4 Enter auto-install mode:

Firepower-chassis-a /firmware # **scope auto-install**

Step 5 Install the FXOS platform bundle:

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number is the version number of the FXOS platform bundle you are installing; for example, 2.3(1.58).

Step 6 The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter **yes** to confirm that you want to proceed with verification.

Step 7 Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 8 To monitor the upgrade process:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

Step 9 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.
f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Step 10 Make the unit that you just upgraded the *active* unit so that traffic flows to the upgraded unit:

a) Connect to Firepower Management Center.

b) Choose **Devices** > **Device Management**.

c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ( ).

d) Click **Yes** to immediately make the standby device the active device in the high availability pair.

Step 11 Connect to FXOS CLI on the Firepower security appliance that contains the *new standby* Firepower Threat Defense logical device:

Step 12 Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter firmware mode:

Firepower-chassis-a # **scope firmware**

b) Download the FXOS platform bundle software image:

Firepower-chassis-a /firmware # **download image** *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) To monitor the download process:

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 13 If necessary, return to firmware mode:

Firepower-chassis-a /firmware/download-task # **up**

Step 14 Enter auto-install mode:

Firepower-chassis-a /firmware # **scope auto-install**

Step 15 Install the FXOS platform bundle:

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number is the version number of the FXOS platform bundle you are installing; for example, 2.3(1.58).

Step 16 The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter **yes** to confirm that you want to proceed with verification.

Step 17 Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 18 To monitor the upgrade process:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

Step 19 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.
f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Step 20 Make the unit that you just upgraded the *active* unit as it was before the upgrade:

a) Connect to Firepower Management Center.

b) Choose **Devices** > **Device Management**.

c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ( ).

d) Click **Yes** to immediately make the standby device the active device in the high availability pair.

Upgrade FXOS: FTD Inter-chassis Clusters

For Firepower Threat Defense inter-chassis clusters (units on different chassis), upgrade the FXOS platform bundle on *all chassis* before you upgrade the FTD logical devices. To minimize disruption, always upgrade FXOS on an all-data unit chassis. Then, use the Firepower Management Center to upgrade the logical devices as a unit.

For example, for a two-chassis cluster:

1. Upgrade FXOS on the all-data unit chassis.
2. Switch the control module to the chassis you just upgraded.
3. Upgrade FXOS on the new all-data unit chassis.
4. Upgrade FTD logical devices.

Upgrade FXOS on an FTD Inter-chassis Cluster Using Firepower Chassis Manager

If you have Firepower 9300 or Firepower 4100 series security appliances that have FTD logical devices configured as an inter-chassis cluster, use the following procedure to update the FXOS platform bundle on your Firepower 9300 or Firepower 4100 series security appliances:

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.
- Back up your FXOS and FTD configurations.

Step 1 Enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Connect to the FXOS CLI on Chassis #2 (this should be a chassis that does not have the control unit).

b) Enter **top**.

c) Enter **scope ssa**.

d) Enter **show slot**.

e) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

f) Enter **show app-instance**.

g) Verify that the Oper State is `Online` and that the Cluster State is `In Cluster` for any logical devices installed on the chassis. Also verify that the correct FTD software version is shown as the Running Version.

Important Verify that the control unit is not on this chassis. There should not be any Firepower Threat Defense instance with Cluster Role set to `Master`.

h) For any security modules installed on a Firepower 9300 appliance or for the security engine on a Firepower 4100 series appliance, verify that the FXOS version is correct:

scope server 1/*slot_id*, where *slot_id* is 1 for a Firepower 4100 series security engine.

show version.

Step 2 Connect to Firepower Chassis Manager on Chassis #2 (this should be a chassis that does not have the control unit).

Step 3 In Firepower Chassis Manager, choose **System** > **Updates**.
The Available Updates page shows a list of the FXOS platform bundle images and application images that are available on the chassis.

Step 4 Upload the new platform bundle image:

a) Click **Upload Image** to open the Upload Image dialog box.
b) Click **Choose File** to navigate to and select the image that you want to upload.
c) Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.
d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Step 5 After the new platform bundle image has successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Step 6 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 7 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

d) Enter **top**.
e) Enter **scope ssa**.
f) Enter **show slot**.
g) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
h) Enter **show app-instance**.
i) Verify that the Oper State is `Online`, that the Cluster State is `In Cluster` and that the Cluster Role is `Slave` for any logical devices installed on the chassis.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
```

```
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State       Running Version Startup Version Profile Name
Cluster State   Cluster Role
---------- ---------- ----------- ---------------- --------------- --------------- ------------
--------------- ------------
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81                     In
 Cluster      Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81                     In
 Cluster      Slave
ftd        3          Disabled    Not Available                    6.2.2.81                     Not
 Applicable  None
FP9300-A /ssa #
```

Step 8 Set one of the security modules on Chassis #2 as control.

After setting one of the security modules on Chassis #2 to control, Chassis #1 no longer contains the control unit and can now be upgraded.

Step 9 Repeat Steps 1-7 for all other Chassis in the cluster.

Step 10 To return the control role to Chassis #1, set one of the security modules on Chassis #1 as control.

Upgrade FXOS on an FTD Inter-chassis Cluster Using the FXOS CLI

If you have Firepower 9300 or Firepower 4100 series security appliances with FTD logical devices configured as an inter-chassis cluster, use the following procedure to update the FXOS platform bundle on your Firepower 9300 or Firepower 4100 series security appliances:

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.
- Back up your FXOS and FTD configurations.
- Collect the following information that you will need to download the software image to the Firepower 4100/9300 chassis:
  - IP address and authentication credentials for the server from which you are copying the image.
  - Fully qualified name of the image file.

Step 1 Connect to the FXOS CLI on Chassis #2 (this should be a chassis that does not have the control unit).

Step 2 Enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.
f) Verify that the Oper State is `Online` and that the Cluster State is `In Cluster` for any logical devices installed on the chassis. Also verify that the correct FTD software version is shown as the Running Version.

Important Verify that the control unit is not on this chassis. There should not be any Firepower Threat Defense instance with Cluster Role set to `Master`.

g) For any security modules installed on a Firepower 9300 appliance or for the security engine on a Firepower 4100 series appliance, verify that the FXOS version is correct:

scope server 1/*slot_id*, where *slot_id* is 1 for a Firepower 4100 series security engine.

show version.

Step 3 Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter **top**.
b) Enter firmware mode:

Firepower-chassis-a # **scope firmware**

c) Download the FXOS platform bundle software image:

Firepower-chassis-a /firmware # **download image** *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

d) To monitor the download process:

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 4 If necessary, return to firmware mode:

Firepower-chassis-a /firmware/download-task # **up**

Step 5 Enter auto-install mode:

Firepower-chassis /firmware # **scope auto-install**

Step 6 Install the FXOS platform bundle:

Firepower-chassis /firmware/auto-install # **install platform platform-vers** *version_number*

version_number is the version number of the FXOS platform bundle you are installing—for example, 2.3(1.58).

Step 7 The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter **yes** to confirm that you want to proceed with verification.

Step 8 Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 9 To monitor the upgrade process:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

d) Enter **top**.
e) Enter **scope ssa**.
f) Enter **show slot**.

g) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
h) Enter **show app-instance**.
i) Verify that the Oper State is `Online`, that the Cluster State is `In Cluster` and that the Cluster Role is `Slave` for any logical devices installed on the chassis.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State       Running Version Startup Version Profile Name
Cluster State   Cluster Role
---------- ---------- ----------- ---------------- --------------- --------------- ------------
--------------- ------------
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81                    In
 Cluster      Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81                    In
 Cluster      Slave
ftd        3          Disabled    Not Available                    6.2.2.81                    Not
 Applicable  None
FP9300-A /ssa #
```

Step 10 Set one of the security modules on Chassis #2 as control.

After setting one of the security modules on Chassis #2 to control, Chassis #1 no longer contains the control unit and can now be upgraded.

Step 11 Repeat Steps 1-9 for all other Chassis in the cluster.

Step 12 To return the control role to Chassis #1, set one of the security modules on Chassis #1 as control.

Upgrade Firepower Threat Defense with FMC (Version 7.0.0)

The FMC provides a wizard to upgrade FTD. You must still use the System Updates page (**System > Updates**) page to upload or specify the location of upgrade packages. You must also use the System Updates page to upgrade the FMC itself, as well as any older Classic devices.

The wizard walks you through important pre-upgrade stages, including selecting devices to upgrade, copying the upgrade package to the devices, and performing compatibility and readiness checks. As you proceed, the wizard 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 the wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the workflow (unless you logged in with a CAC, in which case your progress is cleared 24 hours after you log out). Your progress is also synchronized between high availability FMCs.

Note In Version 7.0.x, the Device Upgrade page does not correctly display devices in clusters or high availability pairs. Even though you must select and upgrade these devices as a unit, the workflow 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 workflow before you click **Next**.

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. However, with major and maintenance upgrades *from* Version 6.7.0, you can manually cancel failed or in-progress upgrades, and retry failed upgrades; use the Upgrade Status pop-up, accessible from the Device Management page and the Message Center, or use the FTD CLI.

Note that by default, FTD automatically reverts to its pre-upgrade state upon upgrade failure ("auto-cancel"). To be able to *manually* cancel or retry a failed upgrade, disable the auto-cancel option when you initiate the upgrade. Note that auto-cancel is not supported for patches. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. If you have exhausted all options, or if your deployment does not support cancel/retry, contact Cisco TAC.

Before you begin

Complete the pre-upgrade checklist. Make sure the appliances in your deployment are healthy and successfully communicating.

Select devices to upgrade.

Step 1 Choose **Devices > Device Management**.

Step 2 Select the devices you want to upgrade.

You can upgrade multiple devices at once. You must upgrade the members of device clusters and high availability pairs at the same time.

Important Due to performance issues, if you are upgrading a device *to* (not from) Version 6.4.0.x through 6.6.x, we *strongly* recommend upgrading no more than five devices simultaneously.

Step 3 From the **Select Action** or **Select Bulk Action** menu, select **Upgrade Firepower Software**.

The Device Upgrade page appears, indicating how many devices you selected and prompting you to select a target version. The page has two panes: Device Selection on the left, and Device Details on the right. Click a device link in the Device Selection (such as '`4 devices`') to show the Device Details for those devices.

Note that if there is already an upgrade workflow in process, you must first either **Merge Devices** (add the newly selected devices to the previously selected devices and continue) or **Reset** (discard the previous selections and use only the newly selected devices).

Step 4 Verify your device selection.

To select additional devices, go back to the Device Management page—your progress will not be lost. To remove devices, click **Reset** to clear your device selection and start over.

Copy upgrade packages to devices.

Step 5 From the **Upgrade to** menu, select your target version.

The system determines which of your selected devices can be upgraded to that version. If any devices are ineligible, you can click the device link to see why. You do not have to remove ineligible devices if you don't want to; they will just not be included in the next step.

Note that the choices in the **Upgrade to** menu correspond to the device upgrade packages available to the system. If your target version is not listed, go to **System > Updates** and upload or specify the location of the correct upgrade package.

Step 6 For all devices that still need an upgrade package, click **Copy Upgrade Packages**, then confirm your choice.

To upgrade FTD, the software upgrade package must be on the appliance. Copying the upgrade package before upgrade reduces the length of your upgrade maintenance window.

Perform compatibility, readiness, and other final checks.

Step 7 For all devices that need to pass the readiness check, click **Run Readiness Check**, then confirm your choice.

Although you can skip checks by disabling the **Require passing compatibility and readiness checks option**, we recommend against it. Passing all checks greatly reduces the chance of upgrade failure. Do *not* deploy changes to, manually reboot, or shut down a device while running readiness checks. If a device fails the readiness check, correct the issues and run the readiness check again. If the readiness check exposes issues that you cannot resolve, do not begin the upgrade. Instead, contact Cisco TAC.

Note that compatibility checks are automatic. For example, the system alerts you immediately if you need to upgrade FXOS on the Firepower 4100/9300, or if you need to deploy to managed devices.

Step 8 Perform final pre-upgrade checks.

Revisit the pre-upgrade checklist. Make sure you have completed all relevant tasks, especially the final checks.

Step 9 If necessary, return to the Device Upgrade page.

Your progress should have been preserved. If it was not, someone else with Administrator access may have reset, modified, or completed the workflow.

Step 10 Click **Next**.

Upgrade.

Step 11 Verify your device selection and target version.

Step 12 Choose rollback options.

For major and maintenance upgrades, you can **Automatically cancel on upgrade failure and roll back to the previous version**. With this option enabled, the device automatically returns to its pre-upgrade state upon upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

This option is not supported for patches.

Step 13 Click **Start Upgrade**, then confirm that you want to upgrade and reboot the devices.

You can monitor upgrade progress in the Message Center. For information on traffic handling during the upgrade, see the Upgrade the Software chapter in the release notes.

Devices may reboot twice during the upgrade. This is expected behavior.

Verify success and complete post-upgrade tasks.

Step 14 Verify upgrade success.

After the upgrade completes, choose **Devices** > **Device Management** and confirm that the devices you upgraded have the correct software version.

Step 15 (Optional) In high availability/scalability deployments, examine device roles.

The upgrade process switches device roles so that it is always upgrading a standby device or data unit. It does not return devices to the roles they had before upgrade. If you have preferred roles for specific devices, make those changes now.

Step 16 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 17 Complete any post-upgrade configuration changes described in the release notes.

Step 18 Redeploy configurations to the devices you just upgraded.

What to do next

(Optional) Clear the wizard by returning to the Device Upgrade page and clicking **Finish**. Until you do this, the Device Upgrade page continues to display details about the upgrade you just performed.

Upgrade Firepower Threat Defense with FMC (Version 6.0.1–6.7.0)

Use this procedure to upgrade FTD using the FMC's System Updates page. On this page, you can upgrade multiple devices at once only if they use the same upgrade package. You must upgrade the members of device clusters and high availability pairs at the same time.

Before you begin

- Decide whether you want to use this procedure. For FTD upgrades to Version 7.0.x we recommend you use the upgrade wizard instead; see Upgrade Firepower Threat Defense with FMC (Version 7.0.0), on page 74.
- Complete the pre-upgrade checklist. Make sure the appliances in your deployment are healthy and successfully communicating.
- (Optional) Switch the active/standby roles of your high availability device pairs. Choose **Devices** > **Device Management**, click the **Switch Active Peer** icon next to the pair, and confirm your choice.

  The standby device in a high availability pair upgrades first. The devices switch roles, then the new standby upgrades. When the upgrade completes, the devices' roles remain switched. If you want to preserve the active/standby roles, manually switch the roles before you upgrade. That way, the upgrade process switches them back.

Step 1 Choose **System** > **Updates**.

Step 2 Click the Install icon next to the upgrade package you want to use and choose the devices to upgrade.

If the devices you want to upgrade are not listed, you chose the wrong upgrade package.

Note We *strongly* recommend upgrading no more than five devices simultaneously from the System Update page. You cannot stop the upgrade until all selected devices complete the process. If there is an issue with any one device upgrade, all devices must finish upgrading before you can resolve the issue.

Step 3 (Version 6.7.0+) Choose rollback options.

For major and maintenance upgrades, you can **Automatically cancel on upgrade failure and roll back to the previous version**. With this option enabled, the device automatically returns to its pre-upgrade state upon upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. Auto-cancel is not supported for patches.

Step 4 Click **Install**, then confirm that you want to upgrade and reboot the devices.

Some devices may reboot twice during the upgrade; this is expected behavior. Traffic either drops throughout the upgrade or traverses the network without inspection depending on how your devices are configured and deployed. For more information, see the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.

Step 5 Monitor upgrade progress.

Caution Do *not* deploy changes to, manually reboot, or shut down an upgrading device.

In most cases, do *not* restart an upgrade in progress. However, starting with major and maintenance FTD upgrades *from* Version 6.7.0, you can manually cancel failed or in-progress upgrades, and retry failed upgrades; use the Upgrade Status pop-up, accessible from the Device Management page and the Message Center, or use the FTD CLI. Note that by default, FTD automatically reverts to its pre-upgrade state upon upgrade failure ("auto-cancel"). To be able to *manually* cancel or retry a failed upgrade, disable the auto-cancel option when you initiate the upgrade. Note that auto-cancel is not supported for patches. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. If you have exhausted all options, or if your deployment does not support cancel/retry, contact Cisco TAC.

Step 6 Verify upgrade success.

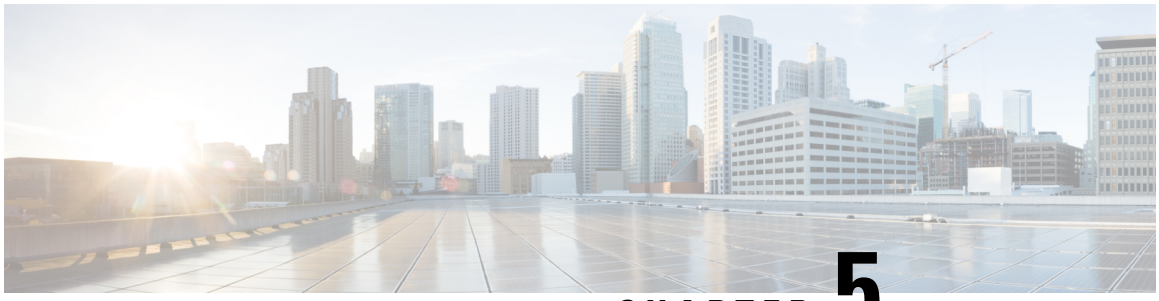
After the upgrade completes, choose **Devices** > **Device Management** and confirm that the devices you upgraded have the correct software version.

Step 7 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 8 Complete any post-upgrade configuration changes described in the release notes.

Step 9 Redeploy configurations to the devices you just upgraded.



CHAPTER 5

Upgrade Firepower 7000/8000 Series and NGIPSv

Upgrade Checklist: Firepower 7000/8000 Series and NGIPSv with FMC

Complete this checklist before you upgrade Firepower 7000/8000 series and NGIPSv devices.

Note At all times during the process, make sure you maintain deployment communication and health. Do *not* restart a device upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 38:

✓	Action/Check
	Plan your upgrade path. This is especially important for multi-appliance deployments, multi-hop upgrades, or situations where you need to upgrade operating systems or hosting environments, all while maintaining deployment compatibility. Always know which upgrade you just performed and which you are performing next. **Note** In FMC deployments, you usually upgrade the FMC, then its managed devices. However, in some cases you may need to upgrade devices first. See Upgrade Paths, on page 10.

✓	Action/Check
	Read *all* upgrade guidelines and plan configuration changes. Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. Start with the release notes, which contain critical and release-specific information, including upgrade warnings, behavior changes, new and deprecated features, and known issues.
	Check appliance access. Devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also able to access the FMC management interface without traversing the device.
	Check bandwidth. Make sure your management network has the bandwidth to perform large data transfers. In FMC deployments, if you transfer an upgrade package to a managed device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. Whenever possible, copy upgrade packages to managed devices before you initiate the device upgrade. See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).
	Schedule maintenance windows. Schedule maintenance windows when they will have the least impact, considering any effect on traffic flow and inspection and the time the upgrade is likely to take. Also consider the tasks you *must* perform in the window, and those you can perform ahead of time. For example, do not wait until the maintenance window to copy upgrade packages to appliances, run readiness checks, perform backups, and so on.

Upgrade Packages

Upgrade packages are available on the Cisco Support & Download site.

Table 39:

✓	Action/Check
	Upload the upgrade package to the FMC. See Upload to the Firepower Management Center, on page 36.
	Copy the upgrade package to the device. If your FMC is running Version 6.2.3+, we recommend you copy (*push*) packages to managed devices before you initiate the device upgrade. See Copy to Managed Devices, on page 38.

Backups

The ability to recover from a disaster is an essential part of any system maintenance plan.

Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your deployment.

Caution We *strongly* recommend you back up to a secure remote location and verify transfer success, both before and after upgrade.

Table 40:

✓	Action/Check
	Back up 7000/8000 series devices. Use the FMC to back up 7000/8000 series devices. Backups are not supported for NGIPSv. Back up before and after upgrade: • Before upgrade: If an upgrade fails catastrophically, you may have to reimage and restore. Reimaging returns most settings to factory defaults, including the system password. If you have a recent backup, you can return to normal operations more quickly. • After upgrade: This creates a snapshot of your freshly upgraded deployment. In FMC deployments, we recommend you back up the FMC after you upgrade its managed devices, so your new FMC backup file 'knows' that its devices have been upgraded.

Associated Upgrades

Because operating system and hosting environment upgrades can affect traffic flow and inspection, perform them in a maintenance window.

Table 41:

✓	Action/Check
	Upgrade virtual hosting. If needed, upgrade the hosting environment for any virtual appliances. If this is required, it is usually because you are running an older version of VMware and are performing a major device upgrade.

Final Checks

A set of final checks ensures you are ready to upgrade.

Table 42:

✓	Action/Check
	Check configurations. Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes.

✓	Action/Check
	Check NTP synchronization. Make sure all appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In FMC deployments, the health monitor does alert if clocks are out of sync by more than 10 seconds, but you should still check manually. To check time: • FMC: Choose **System > Configuration > Time**. • Devices: Use the **show time** CLI command.
	Check disk space. Run a disk space check for the software upgrade. Without enough free disk space, the upgrade fails. See the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.
	Deploy configurations. Deploying configurations before you upgrade reduces the chance of failure. In some deployments, you may be blocked from upgrade if you have out-of-date configurations. In FMC high availability deployments, you only need to deploy from the active peer. When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device handles traffic, may interrupt traffic until the restart completes. See the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.
	Run readiness checks. If your FMC is running Version 6.1.0+, we recommend compatibility and readiness checks. These checks assess your preparedness for a software upgrade. See Firepower Software Readiness Checks, on page 39.
	Check running tasks. Make sure essential tasks on the device are complete before you upgrade, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. We also recommend you check for tasks that are scheduled to run during the upgrade, and cancel or postpone them.

Upgrade Firepower 7000/8000 and NGIPSv with FMC

Use this procedure to upgrade Firepower 7000/8000 series and NGIPSv devices. You can upgrade multiple devices at once if they use the same upgrade package. You must upgrade the members of device stacks and high availability pairs at the same time.

Before you begin

Complete the pre-upgrade checklist. Make sure the appliances in your deployment are healthy and successfully communicating.

Step 1 (Optional) Switch the active/standby roles of your high availability device pairs that perform switching/routing.

If your high availability pairs are deployed to perform access control *only*, the active upgrades first. When the upgrade completes, the active and standby maintain their old roles.

However, in a routed or switched deployment, the standby upgrades first. The devices switch roles, then the new standby upgrades. When the upgrade completes, the devices' roles remain switched. If you want to preserve the active/standby roles, manually switch the roles before you upgrade. That way, the upgrade process switches them back.

Choose **Devices** > **Device Management**, click the **Switch Active Peer** icon next to the pair, and confirm your choice.

Step 2 Choose **System** > **Updates**.

Step 3 Click the Install icon next to the upgrade package you want to use and choose the devices to upgrade.

If the devices you want to upgrade are not listed, you chose the wrong upgrade package.

Note We *strongly* recommend upgrading no more than five devices simultaneously from the System Update page. You cannot stop the upgrade until all selected devices complete the process. If there is an issue with any one device upgrade, all devices must finish upgrading before you can resolve the issue.

Step 4 Click **Install**, then confirm that you want to upgrade and reboot the devices.

Traffic either drops throughout the upgrade or traverses the network without inspection depending on how your devices are configured and deployed. For more information, see the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.

Step 5 Monitor upgrade progress.

Caution Do *not* deploy changes to, manually reboot, or shut down an upgrading device. Do *not* restart a device upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Step 6 Verify upgrade success.

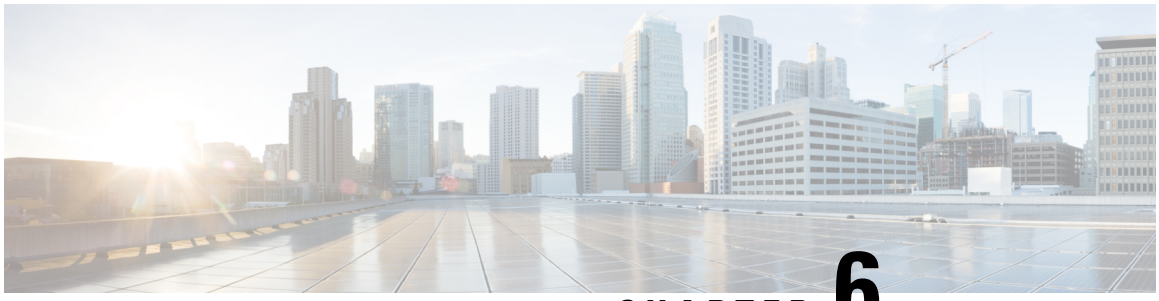
After the upgrade completes, choose **Devices** > **Device Management** and confirm that the devices you upgraded have the correct software version.

Step 7 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 8 Complete any post-upgrade configuration changes described in the release notes.

Step 9 Redeploy configurations to the devices you just upgraded.



CHAPTER 6

Upgrade ASA with FirePOWER Services

Upgrade Checklist: ASA FirePOWER with FMC

Complete this checklist before you upgrade ASA with FirePOWER Services.

Note At all times during the process, make sure you maintain deployment communication and health. Do *not* restart an ASA FirePOWER upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 43:

✓	Action/Check
	Plan your upgrade path. This is especially important for multi-appliance deployments, multi-hop upgrades, or situations where you need to upgrade operating systems or hosting environments, all while maintaining deployment compatibility. Always know which upgrade you just performed and which you are performing next. **Note** In FMC deployments, you usually upgrade the FMC, then its managed devices. However, in some cases you may need to upgrade devices first. See Upgrade Paths, on page 10.

✓	Action/Check
	Read *all* upgrade guidelines and plan configuration changes. Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. Start with the release notes, which contain critical and release-specific information, including upgrade warnings, behavior changes, new and deprecated features, and known issues.
	Check appliance access. Devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also able to access the FMC management interface without traversing the device.
	Check bandwidth. Make sure your management network has the bandwidth to perform large data transfers. In FMC deployments, if you transfer an upgrade package to a managed device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. Whenever possible, copy upgrade packages to managed devices before you initiate the device upgrade. See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).
	Schedule maintenance windows. Schedule maintenance windows when they will have the least impact, considering any effect on traffic flow and inspection and the time the upgrade is likely to take. Also consider the tasks you *must* perform in the window, and those you can perform ahead of time. For example, do not wait until the maintenance window to copy upgrade packages to appliances, run readiness checks, perform backups, and so on.

Upgrade Packages

Upgrade packages are available on the Cisco Support & Download site.

Table 44:

✓	Action/Check
	Upload the upgrade package to the FMC. See Upload to the Firepower Management Center, on page 36.
	Copy the upgrade package to the device. If your FMC is running Version 6.2.3+, we recommend you copy (*push*) packages to managed devices before you initiate the device upgrade. See Copy to Managed Devices, on page 38.

Backups

The ability to recover from a disaster is an essential part of any system maintenance plan.

Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your deployment.

Caution We *strongly* recommend you back up to a secure remote location and verify transfer success, both before and after upgrade.

Table 45:

✓	Action/Check
	Back up ASA. Use ASDM or the ASA CLI to back up configurations and other critical files before and after upgrade, especially if there is an ASA configuration migration.

Associated Upgrades

Because operating system and hosting environment upgrades can affect traffic flow and inspection, perform them in a maintenance window.

Table 46:

✓	Action/Check
	Upgrade ASA. If desired, upgrade ASA. There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues. For standalone ASA devices, upgrade the ASA FirePOWER module just *after* you upgrade ASA and reload. For ASA clusters and failover pairs, to avoid interruptions in traffic flow and inspection, fully upgrade these devices *one at a time*. Upgrade the ASA FirePOWER module just *before* you reload each unit to upgrade ASA. **Note** Before you upgrade ASA, make sure you read all upgrade guidelines and plan configuration changes. Start with the ASA release notes: Cisco ASA Release Notes.

Final Checks

A set of final checks ensures you are ready to upgrade.

Table 47:

✓	Action/Check
	Check configurations. Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes.

✓	Action/Check
	Check NTP synchronization. Make sure all appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In FMC deployments, the health monitor does alert if clocks are out of sync by more than 10 seconds, but you should still check manually. To check time: • FMC: Choose **System > Configuration > Time**. • Devices: Use the **show time** CLI command.
	Check disk space. Run a disk space check for the software upgrade. Without enough free disk space, the upgrade fails. See the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.
	Deploy configurations. Deploying configurations before you upgrade reduces the chance of failure. In some deployments, you may be blocked from upgrade if you have out-of-date configurations. In FMC high availability deployments, you only need to deploy from the active peer. When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device handles traffic, may interrupt traffic until the restart completes. See the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.
	Disable ASA REST API on older devices. Before you upgrade an ASA FirePOWER module *currently* running Version 6.3.0 or earlier, make sure the ASA REST API is disabled. Otherwise, the upgrade could fail. From the ASA CLI: `no rest api agent`. You can reenable after the upgrade: `rest-api agent`.
	Run readiness checks. If your FMC is running Version 6.1.0+, we recommend compatibility and readiness checks. These checks assess your preparedness for a software upgrade. See Firepower Software Readiness Checks, on page 39.
	Check running tasks. Make sure essential tasks on the device are complete before you upgrade, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. We also recommend you check for tasks that are scheduled to run during the upgrade, and cancel or postpone them.

Upgrade the ASA

Use the procedures in this section to upgrade ASA and ASDM for standalone, failover, or clustering deployments.

Upgrade a Standalone Unit

Use the CLI or ASDM to upgrade the standalone unit.

Upgrade a Standalone Unit Using the CLI

This section describes how to install the ASDM and ASA images, and also when to upgrade the ASA FirePOWER module.

Before you begin

This procedure uses FTP. For TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.

Step 1 In privileged EXEC mode, copy the ASA software to flash memory.

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Example:

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asa-9-12-1-smp-k8.bin disk0:/asa-9-12-1-smp-k8.bin
```

Step 2 Copy the ASDM image to flash memory.

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

Example:

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7121.bin disk0:/asdm-7121.bin
```

Step 3 Access global configuration mode.

configure terminal

Example:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Step 4 Show the current boot images configured (up to 4):

show running-config boot system

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

Example:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

Step 5 Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

no boot system disk*n***:/**[*path*/]*asa_image_name*

Example:

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 6 Set the ASA image to boot (the one you just uploaded):

boot system disk*n***:/**[*path*/]*asa_image_name*

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Example:

```
ciscoasa(config)# boot system disk0:/asa-9-12-1-smp-k8.bin
```

Step 7 Set the ASDM image to use (the one you just uploaded):

asdm image disk*n***:/**[*path*/]*asdm_image_name*

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Example:

```
ciscoasa(config)# asdm image disk0:/asdm-7121.bin
```

Step 8 Save the new settings to the startup configuration:

write memory

Step 9 Reload the ASA:

reload

Step 10 If you are upgrading the ASA FirePOWER module, disable the ASA REST API or else the upgrade will fail.

no rest-api agent

You can reenable it after the upgrade:

rest-api agent

Note The ASA 5506-X series does not support the ASA REST API if you are running the FirePOWER module Version 6.0 or later.

Step 11 Upgrade the ASA FirePOWER module.

Upgrade a Standalone Unit from Your Local Computer Using ASDM

The **Upgrade Software from Local Computer** tool lets you upload an image file from your computer to the flash file system to upgrade the ASA.

Step 1 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software** dialog box appears.

Step 2 From the **Image to Upload** drop-down list, choose **ASDM**.

Step 3 In the **Local File Path** field, click **Browse Local Files** to find the file on your PC.

Step 4 In the **Flash File System Path** field, click **Browse Flash** to find the directory or file in the flash file system.

Step 5 Click **Upload Image**.

The uploading process might take a few minutes.

Step 6 You are prompted to set this image as the ASDM image. Click **Yes**.

Step 7 You are reminded to exit ASDM and save the configuration. Click **OK**.

You exit the **Upgrade** tool. **Note:** You will save the configuration and exit and reconnect to ASDM *after* you upgrade the ASA software.

Step 8 Repeat these steps, choosing **ASA** from the **Image to Upload** drop-down list. You can also use this procedure to upload other file types.

Step 9 Choose **Tools** > **System Reload** to reload the ASA.

A new window appears that asks you to verify the details of the reload.

a) Click the **Save the running configuration at the time of reload** radio button (the default).
b) Choose a time to reload (for example, **Now**, the default).
c) Click **Schedule Reload**.

Once the reload is in progress, a **Reload Status** window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

Step 10 After the ASA reloads, restart ASDM.

You can check the reload status from a console port, or you can wait a few minutes and try to connect using ASDM until you are successful.

Step 11 If you are upgrading an ASA FirePOWER module, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api agent**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail. You can reenable it after the upgrade:

rest-api agent

Note The ASA 5506-X series does not support the ASA REST API if you are running the FirePOWER module Version 6.0 or later.

Step 12 Upgrade the ASA FirePOWER module.

Upgrade a Standalone Unit Using the ASDM Cisco.com Wizard

The **Upgrade Software from Cisco.com Wizard** lets you automatically upgrade the ASDM and ASA to more current versions.

In this wizard, you can do the following:

- Choose an ASA image file and/or ASDM image file to upgrade.

Note ASDM downloads the latest image version, which includes the build number. For example, if you are downloading 9.9(1), the download might be 9.9(1.2). This behavior is expected, so you can proceed with the planned upgrade.

- Review the upgrade changes that you have made.
- Download the image or images and install them.
- Review the status of the installation.
- If the installation completed successfully, reload the ASA to save the configuration and complete the upgrade.

Before you begin

Due to an internal change, the wizard is only supported using ASDM 7.10(1) and later; also, due to an image naming change, you must use ASDM 7.12(1) or later to upgrade to ASA 9.10(1) and later. Because ASDM is backwards compatible with earlier ASA releases, you can upgrade ASDM no matter which ASA version you are running.

Step 1 Choose **Tools** > **Check for ASA/ASDM Updates**.

In multiple context mode, access this menu from the System.

The **Cisco.com Authentication** dialog box appears.

Step 2 Enter your Cisco.com username and password, and then click **Login**.

The **Cisco.com Upgrade Wizard** appears.

Note If there is no upgrade available, a dialog box appears. Click **OK** to exit the wizard.

Step 3 Click **Next** to display the **Select Software** screen.

The current ASA version and ASDM version appear.

Step 4 To upgrade the ASA version and ASDM version, perform the following steps:

a) In the **ASA** area, check the **Upgrade to** check box, and then choose an ASA version to which you want to upgrade from the drop-down list.

b) In the **ASDM** area, check the **Upgrade to** check box, and then choose an ASDM version to which you want to upgrade from the drop-down list.

Step 5 Click **Next** to display the **Review Changes** screen.

Step 6 Verify the following items:

- The ASA image file and/or ASDM image file that you have downloaded are the correct ones.
- The ASA image file and/or ASDM image file that you want to upload are the correct ones.
- The correct ASA boot image has been selected.

Step 7 Click **Next** to start the upgrade installation.

You can then view the status of the upgrade installation as it progresses.

The **Results** screen appears, which provides additional details, such as the upgrade installation status (success or failure).

Step 8 If the upgrade installation succeeded, for the upgrade versions to take effect, check the **Save configuration and reload device now** check box to restart the ASA, and restart ASDM.

Step 9 Click **Finish** to exit the wizard and save the configuration changes that you have made.

Note To upgrade to the next higher version, if any, you must restart the wizard.

Step 10 After the ASA reloads, restart ASDM.

You can check the reload status from a console port, or you can wait a few minutes and try to connect using ASDM until you are successful.

Step 11 If you are upgrading an ASA FirePOWER module, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api agent**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail. You can reenable it after the upgrade:

rest-api agent

Note The ASA 5506-X series does not support the ASA REST API if you are running the FirePOWER module Version 6.0 or later.

Step 12 Upgrade the ASA FirePOWER module.

Upgrade an Active/Standby Failover Pair

Use the CLI or ASDM to upgrade the Active/Standby failover pair for a zero downtime upgrade.

Upgrade an Active/Standby Failover Pair Using the CLI

To upgrade the Active/Standby failover pair, perform the following steps.

Before you begin

- Perform these steps on the active unit. For SSH access, connect to the active IP address; the active unit always owns this IP address. When you connect to the CLI, determine the failover status by looking at the ASA prompt; you can configure the ASA prompt to show the failover status and priority (primary or secondary), which is useful to determine which unit you are connected to. See the prompt command. Alternatively, enter the **show failover** command to view this unit's status and priority (primary or secondary).

- This procedure uses FTP. For TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.

Step 1 On the active unit in privileged EXEC mode, copy the ASA software to the active unit flash memory:

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Example:

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin
```

Step 2 Copy the software to the standby unit; be sure to specify the same path as for the active unit:

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Example:

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin
 disk0:/asa9829-15-1-smp-k8.bin
```

Step 3 Copy the ASDM image to the active unit flash memory:

copy ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

Example:

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin disk0:/asdm-77178271417151.bin
```

Step 4 Copy the ASDM image to the standby unit; be sure to specify the same path as for the active unit:

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

Example:

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
 disk0:/asdm-77178271417151.bin
```

Step 5 If you are not already in global configuration mode, access global configuration mode:

configure terminal

Step 6 Show the current boot images configured (up to 4):

show running-config boot system

Example:

```
asa/act(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

Step 7 Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

no boot system disk*n***:/**[*path*/]*asa_image_name*

Example:

```
asa/act(config)# no boot system disk0:/cdisk.bin
asa/act(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 8 Set the ASA image to boot (the one you just uploaded):

boot system disk*n***:/**[*path*/]*asa_image_name*

Example:

```
asa/act(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Step 9 Set the ASDM image to use (the one you just uploaded):

asdm image disk*n***:/**[*path*/]*asdm_image_name*

Example:

```
asa/act(config)# asdm image disk0:/asdm-77178271417151.bin
```

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Step 10 Save the new settings to the startup configuration:

write memory

These configuration changes are automatically saved on the standby unit.

Step 11 If you are upgrading ASA FirePOWER modules, disable the ASA REST API or else the upgrade will fail.

no rest-api agent

Step 12 Upgrade the ASA FirePOWER module on the standby unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *standby* management IP address. Wait for the upgrade to complete.

Step 13 Reload the standby unit to boot the new image:

failover reload-standby

Wait for the standby unit to finish loading. Use the **show failover** command to verify that the standby unit is in the Standby Ready state.

Step 14 Force the active unit to fail over to the standby unit.

no failover active

If you are disconnected from your SSH session, reconnect to the main IP address, now on the new active/former standby unit.

Step 15 Upgrade the ASA FirePOWER module on the former active unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *standby* management IP address. Wait for the upgrade to complete.

Step 16 From the new active unit, reload the former active unit (now the new standby unit).

failover reload-standby

Example:

```
asa/act# failover reload-standby
```

Note If you are connected to the former active unit console port, you should instead enter the **reload** command to reload the former active unit.

Upgrade an Active/Standby Failover Pair Using ASDM

To upgrade the Active/Standby failover pair, perform the following steps.

Before you begin

Place the ASA and ASDM images on your local management computer.

Step 1 Launch ASDM on the *standby* unit by connecting to the standby IP address.

Step 2 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software** dialog box appears.

Step 3 From the **Image to Upload** drop-down list, choose **ASDM**.

Step 4 In the **Local File Path** field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.

Step 5 In the **Flash File System Path** field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

Step 6 Click **Upload Image**. The uploading process might take a few minutes.

When you are prompted to set this image as the ASDM image, click **No**. You exit the Upgrade tool.

Step 7 Repeat these steps, choosing **ASA** from the **Image to Upload** drop-down list.

When you are prompted to set this image as the ASA image, click **No**. You exit the Upgrade tool.

Step 8 Connect ASDM to the *active* unit by connecting to the main IP address, and upload the ASDM software, using the same file location you used on the standby unit.

Step 9 When you are prompted to set the image as the ASDM image, click **Yes**.

You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

Step 10 Upload the ASA software, using the same file location you used for the standby unit.

Step 11 When you are prompted to set the image as the ASA image, click **Yes**.

You are reminded to reload the ASA to use the new image. Click **OK**. You exit the Upgrade tool.

Step 12 Click the **Save** icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the standby unit.

Step 13 If you are upgrading ASA FirePOWER modules, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api enable**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail.

Step 14 Upgrade the ASA FirePOWER module on the standby unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *standby* management IP address. Wait for the upgrade to complete, and then connect ASDM back to the active unit.

Step 15 Reload the standby unit by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Reload Standby**.

Stay on the **System** pane to monitor when the standby unit reloads.

Step 16 After the standby unit reloads, force the active unit to fail over to the standby unit by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Make Standby**.

ASDM will automatically reconnect to the new active unit.

Step 17 Upgrade the ASA FirePOWER module on the former active unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *standby* management IP address. Wait for the upgrade to complete, and then connect ASDM back to the active unit.

Step 18 Reload the (new) standby unit by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Reload Standby**.

Upgrade an Active/Active Failover Pair

Use the CLI or ASDM to upgrade the Active/Active failover pair for a zero downtime upgrade.

Upgrade an Active/Active Failover Pair Using the CLI

To upgrade two units in an Active/Active failover configuration, perform the following steps.

Before you begin

- Perform these steps on the primary unit.
- Perform these steps in the system execution space.
- This procedure uses FTP. For TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.

Step 1 On the primary unit in privileged EXEC mode, copy the ASA software to flash memory:

copy ftp://[[*user*[**:***password*]**@**]*server*[/*path*]/*asa_image_name* **disk***n***:**/[*path*/]*asa_image_name*

Example:

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin
disk0:/asa9829-15-1-smp-k8.bin
```

Step 2 Copy the software to the secondary unit; be sure to specify the same path as for the primary unit:

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[/*path*]/*asa_image_name* **disk***n***:**/[*path*/]*asa_image_name*

Example:

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin
 disk0:/asa9829-15-1-smp-k8.bin
```

Step 3 Copy the ASDM image to the primary unit flash memory:

copy ftp://[[*user*[**:***password*]**@**]*server*[/*path*]/*asdm_image_name* **disk***n***:**/[*path*/]*asdm_image_name*

Example:

```
asa/act/pri# ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
disk0:/asdm-77178271417151.bin
```

Step 4 Copy the ASDM image to the secondary unit; be sure to specify the same path as for the primary unit:

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[/*path*]/*asdm_image_name* **disk***n***:**/[*path*/]*asdm_image_name*

Example:

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
 disk0:/asdm-77178271417151.bin
```

Step 5 If you are not already in global configuration mode, access global configuration mode:

configure terminal

Step 6 Show the current boot images configured (up to 4):

show running-config boot system

Example:

```
asa/act/pri(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

Step 7 Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

no boot system disk*n*:/[*path*/]*asa_image_name*

Example:

```
asa/act/pri(config)# no boot system disk0:/cdisk.bin
asa/act/pri(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 8 Set the ASA image to boot (the one you just uploaded):

boot system disk*n*:/[*path*/]*asa_image_name*

Example:

```
asa/act/pri(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Step 9 Set the ASDM image to use (the one you just uploaded):

asdm image disk*n*:/[*path*/]*asdm_image_name*

Example:

```
asa/act/pri(config)# asdm image disk0:/asdm-77178271417151.bin
```

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Step 10 Save the new settings to the startup configuration:

write memory

These configuration changes are automatically saved on the secondary unit.

Step 11 If you are upgrading ASA FirePOWER modules, disable the ASA REST API or else the upgrade will fail.

no rest-api agent

Step 12 Make both failover groups active on the primary unit:

failover active group 1

failover active group 2

Example:

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

Step 13 Upgrade the ASA FirePOWER module on the secondary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 *standby* management IP address. Wait for the upgrade to complete.

Step 14 Reload the secondary unit to boot the new image:

failover reload-standby

Wait for the secondary unit to finish loading. Use the **show failover** command to verify that both failover groups are in the Standby Ready state.

Step 15 Force both failover groups to become active on the secondary unit:

no failover active group 1

no failover active group 2

Example:

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

If you are disconnected from your SSH session, reconnect to the failover group 1 IP address, now on the secondary unit.

Step 16 Upgrade the ASA FirePOWER module on the primary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 *standby* management IP address. Wait for the upgrade to complete.

Step 17 Reload the primary unit:

failover reload-standby

Example:

```
asa/act/sec# failover reload-standby
```

Note If you are connected to the primary unit console port, you should instead enter the **reload** command to reload the primary unit.

You may be disconnected from your SSH session.

Step 18 If the failover groups are configured with the **preempt** command, they automatically become active on their designated unit after the preempt delay has passed.

Upgrade an Active/Active Failover Pair Using ASDM

To upgrade two units in an Active/Active failover configuration, perform the following steps.

Before you begin

- Perform these steps in the system execution space.
- Place the ASA and ASDM images on your local management computer.

Step 1 Launch ASDM on the *secondary* unit by connecting to the management address in failover group 2.

Step 2 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software** dialog box appears.

Step 3 From the **Image to Upload** drop-down list, choose **ASDM**.

Step 4 In the **Local File Path** field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.

Step 5 In the **Flash File System Path** field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

Step 6 Click **Upload Image**. The uploading process might take a few minutes.

When you are prompted to set this image as the ASDM image, click **No**. You exit the Upgrade tool.

Step 7 Repeat these steps, choosing **ASA** from the **Image to Upload** drop-down list.

When you are prompted to set this image as the ASA image, click **No**. You exit the Upgrade tool.

Step 8 Connect ASDM to the *primary* unit by connecting to the management IP address in failover group 1, and upload the ASDM software, using the same file location you used on the secondary unit.

Step 9 When you are prompted to set the image as the ASDM image, click **Yes**.

You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

Step 10 Upload the ASA software, using the same file location you used for the secondary unit.

Step 11 When you are prompted to set the image as the ASA image, click **Yes**.

You are reminded to reload the ASA to use the new image. Click **OK**. You exit the Upgrade tool.

Step 12 Click the **Save** icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the secondary unit.

Step 13 If you are upgrading ASA FirePOWER modules, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api enable**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail.

Step 14 Make both failover groups active on the primary unit by choosing **Monitoring** > **Failover** > **Failover Group #**, where **#** is the number of the failover group you want to move to the primary unit, and clicking **Make Active**.

Step 15 Upgrade the ASA FirePOWER module on the secondary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 *standby* management IP address. Wait for the upgrade to complete, and then connect ASDM back to the primary unit.

Step 16 Reload the secondary unit by choosing **Monitoring** > **Failover** > **System**, and clicking **Reload Standby**.

Stay on the **System** pane to monitor when the secondary unit reloads.

Step 17 After the secondary unit comes up, make both failover groups active on the secondary unit by choosing **Monitoring** > **Failover** > **Failover Group #**, where **#** is the number of the failover group you want to move to the secondary unit, and clicking **Make Standby**.

ASDM will automatically reconnect to the failover group 1 IP address on the secondary unit.

Step 18 Upgrade the ASA FirePOWER module on the primary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 *standby* management IP address. Wait for the upgrade to complete, and then connect ASDM back to the secondary unit.

Step 19 Reload the primary unit by choosing **Monitoring** > **Failover** > **System**, and clicking **Reload Standby**.

Step 20 If the failover groups are configured with Preempt Enabled, they automatically become active on their designated unit after the preempt delay has passed. ASDM will automatically reconnect to the failover group 1 IP address on the primary unit.

Upgrade an ASA Cluster

Use the CLI or ASDM to upgrade the ASA Cluster for a zero downtime upgrade.

Upgrade an ASA Cluster Using the CLI

To upgrade all units in an ASA cluster, perform the following steps. This procedure uses FTP. For TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.

Before you begin

- Perform these steps on the control unit. If you are also upgrading the ASA FirePOWER module, then you need console or ASDM access on each data unit. You can configure the ASA prompt to show the cluster unit and state (control or data), which is useful to determine which unit you are connected to. See the prompt command. Alternatively, enter the **show cluster info** command to view each unit's role.
- You must use the console port; you cannot enable or disable clustering from a remote CLI connection.
- Perform these steps in the system execution space for multiple context mode.

Step 1 On the control unit in privileged EXEC mode, copy the ASA software to all units in the cluster.

cluster exec copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]/*asa_image_name* **disk***n***:**/[*path/*]*asa_image_name*

Example:

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin
```

Step 2 Copy the ASDM image to all units in the cluster:

cluster exec copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]/*asdm_image_name*
disk*n***:**/[*path/*]*asdm_image_name*

Example:

```
asa/unit1/master# cluster exec copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
 disk0:/asdm-77178271417151.bin
```

Step 3 If you are not already in global configuration mode, access it now.

configure terminal

Example:

```
asa/unit1/master# configure terminal
asa/unit1/master(config)#
```

Step 4 Show the current boot images configured (up to 4).

show running-config boot system

Example:

```
asa/unit1/master(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

Step 5 Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

no boot system disk*n***:/**[*path*/]*asa_image_name*

Example:

```
asa/unit1/master(config)# no boot system disk0:/cdisk.bin
asa/unit1/master(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 6 Set the ASA image to boot (the one you just uploaded):

boot system disk*n***:/**[*path*/]*asa_image_name*

Example:

```
asa/unit1/master(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Step 7 Set the ASDM image to use (the one you just uploaded):

asdm image disk*n***:/**[*path*/]*asdm_image_name*

Example:

```
asa/unit1/master(config)# asdm image disk0:/asdm-77178271417151.bin
```

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Step 8 Save the new settings to the startup configuration:

write memory

These configuration changes are automatically saved on the data units.

Step 9 If you are upgrading ASA FirePOWER modules, disable the ASA REST API or else the ASA FirePOWER module upgrade will fail.

no rest-api agent

Step 10 If you are upgrading ASA FirePOWER modules that are managed by ASDM, you will need to connect ASDM to the *individual* management IP addresses, so you need to note the IP addresses for each unit.

show running-config interface *management_interface_id*

Note the **cluster-pool** poolname used.

show ip[**v6**] **local pool** *poolname*

Note the cluster unit IP addresses.

Example:

```
asa/unit2/slave# show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.86.118.1 255.255.252.0 cluster-pool inside-pool
asa/unit2/slave# show ip local pool inside-pool
Begin           End             Mask            Free     Held     In use
10.86.118.16    10.86.118.17    255.255.252.0       0        0        2

Cluster Unit                    IP Address Allocated
unit2                           10.86.118.16
unit1                           10.86.118.17
asa1/unit2/slave#
```

Step 11 Upgrade the data units.

Choose the procedure below depending on whether you are also upgrading ASA FirePOWER modules. The ASA FirePOWER procedures minimize the number of ASA reloads when also upgrading the ASA FirePOWER module. You can choose to use the data Console or ASDM for these procedures. You may want to use ASDM instead of the Console if you do not have ready access to all of the console ports but can reach ASDM over the network.

Note During the upgrade process, never use the **cluster master unit** command to force a data unit to become control; you can cause network connectivity and cluster stability-related problems. You must upgrade and reload all data units first, and then continue with this procedure to ensure a smooth transition from the current control unit to a new control unit.

If you do not have ASA FirePOWER module upgrades:

a) On the control unit, to view member names, enter **cluster exec unit ?**, or enter the **show cluster info** command.

b) Reload a data unit.

cluster exec unit *data-unit* **reload noconfirm**

Example:

```
asa/unit1/master# cluster exec unit unit2 reload noconfirm
```

c) Repeat for each data unit.

To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, enter **show cluster info**.

If you also have ASA FirePOWER module upgrades (using the data Console):

a) Connect to the console port of a data unit, and enter global configuration mode.

enable

configure terminal

Example:

```
asa/unit2/slave> enable
Password:
asa/unit2/slave# configure terminal
asa/unit2/slave(config)#
```

b) Disable clustering.

cluster group *name*

no enable

Do not save this configuration; you want clustering to be enabled when you reload. You need to disable clustering to avoid multiple failures and rejoins during the upgrade process; this unit should only rejoin after all of the upgrading and reloading is complete.

Example:

```
asa/unit2/slave(config)# cluster group cluster1
asa/unit2/slave(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable
 clustering or remove cluster group configuration.

Cluster unit unit2 transitioned from SLAVE to DISABLED
asa/unit2/ClusterDisabled(cfg-cluster)#
```

c) Upgrade the ASA FirePOWER module on this data unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *individual* management IP address that you noted earlier. Wait for the upgrade to complete.

d) Reload the data unit.

reload noconfirm

e) Repeat for each data unit.

To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, enter **show cluster info**.

If you also have ASA FirePOWER module upgrades (using ASDM):

a) Connect ASDM to the *individual* management IP address of this data unit that you noted earlier.
b) Choose **Configuration** > **Device ManagementHigh Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** > **.**
c) Uncheck the **Participate in ASA cluster** check box.

You need to disable clustering to avoid multiple failures and rejoins during the upgrade process; this unit should only rejoin after all of the upgrading and reloading is complete.

Do not uncheck the **Configure ASA cluster settings** check box; this action clears all cluster configuration, and also shuts down all interfaces including the management interface to which ASDM is connected. To restore connectivity in this case, you need to access the CLI at the console port.

Note Some older versions of ASDM do not support disabling the cluster on this screen; in this case, use the **Tools** > **Command Line Interface** tool, click the **Multiple Line** radio button, and enter **cluster group** *name* and **no enable**. You can view the cluster group name in the **Home** > **Device Dashboard** > **Device Information** > **ASA Cluster** area.

d) Click **Apply**.
e) You are prompted to exit ASDM. Reconnect ASDM to the same IP address.
f) Upgrade the ASA FirePOWER module.

Wait for the upgrade to complete.

g) In ASDM, choose **Tools** > **System Reload**.
h) Click the **Reload without saving the running configuration** radio button.

You do not want to save the configuration; when this unit reloads, you want clustering to be enabled on it.

i) Click **Schedule Reload**.
j) Click **Yes** to continue the reload.
k) Repeat for each data unit.

To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, see the **Monitoring** > **ASA Cluster** > **Cluster Summary** pane on the control unit.

Step 12 Upgrade the control unit.

a) Disable clustering.

cluster group *name*

no enable

Wait for 5 minutes for a new control unit to be selected and traffic to stabilize.

Do not save this configuration; you want clustering to be enabled when you reload.

We recommend manually disabling cluster on the control unit if possible so that a new control unit can be elected as quickly and cleanly as possible.

Example:

```
asa/unit1/master(config)# cluster group cluster1
asa/unit1/master(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable
 clustering or remove cluster group configuration.

Cluster unit unit1 transitioned from MASTER to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

b) Upgrade the ASA FirePOWER module on this unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *individual* management IP address that you noted earlier. The main cluster IP address now belongs to the new control unit; this former control unit is still accessible on its individual management IP address.

Wait for the upgrade to complete.

c) Reload this unit.

reload noconfirm

When the former control unit rejoins the cluster, it will be a data unit.

Upgrade an ASA Cluster Using ASDM

To upgrade all units in an ASA cluster, perform the following steps.

Before you begin

- Perform these steps on the control unit. If you are also upgrading the ASA FirePOWER module, then you need ASDM access to each data unit.
- Perform these steps in the system execution space for multiple context mode.
- Place the ASA and ASDM images on your local management computer.

Step 1 Launch ASDM on the *control* unit by connecting to the main cluster IP address.

This IP address always stays with the control unit.

Step 2 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software from Local Computer** dialog box appears.

Step 3 Click the **All devices in the cluster** radio button.

The **Upgrade Software** dialog box appears.

Step 4 From the **Image to Upload** drop-down list, choose **ASDM**.

Step 5 In the **Local File Path** field, click **Browse Local Files** to find the file on your computer.

Step 6 (Optional) In the **Flash File System Path** field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

By default, this field is prepopulated with the following path: **disk0:**/*filename*.

Step 7 Click **Upload Image**. The uploading process might take a few minutes.

Step 8 You are prompted to set this image as the ASDM image. Click **Yes**.

Step 9 You are reminded to exit ASDM and save the configuration. Click **OK**.

You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

Step 10 Repeat these steps, choosing **ASA** from the **Image to Upload** drop-down list.

Step 11 Click the **Save** icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the data units.

Step 12 Take note of the individual management IP addresses for each unit on **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Members** so that you can connect ASDM directly to data units later.

Step 13 If you are upgrading ASA FirePOWER modules, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api enable**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail.

Step 14 Upgrade the data units.

Choose the procedure below depending on whether you are also upgrading ASA FirePOWER modules. The ASA FirePOWER procedure minimizes the number of ASA reloads when also upgrading the ASA FirePOWER module.

Note During the upgrade process, never change the control unit using the **Monitoring** > **ASA Cluster** > **Cluster Summary** page to force a data unit to become control; you can cause network connectivity and cluster stability-related problems. You must reload all data units first, and then continue with this procedure to ensure a smooth transition from the current control unit to a new control unit.

If you do not have ASA FirePOWER module upgrades:

a) On the control unit, choose **Tools** > **System Reload**.
b) Choose a data unit name from the **Device** drop-down list.
c) Click **Schedule Reload**.
d) Click **Yes** to continue the reload.
e) Repeat for each data unit.

   To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, see the **Monitoring** > **ASA Cluster** > **Cluster Summary** pane.

If you also have ASA FirePOWER module upgrades:

a) On the control unit, choose **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Members**.
b) Select the data unit that you want to upgrade, and click **Delete**.
c) Click **Apply**.
d) Exit ASDM, and connect ASDM to the data unit by connecting to its *individual* management IP address that you noted earlier.
e) Upgrade the ASA FirePOWER module.

   Wait for the upgrade to complete.

f) In ASDM, choose **Tools** > **System Reload**.
g) Click the **Reload without saving the running configuration** radio button.

   You do not want to save the configuration; when this unit reloads, you want clustering to be enabled on it.

h) Click **Schedule Reload**.
i) Click **Yes** to continue the reload.
j) Repeat for each data unit.

   To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, see the **Monitoring** > **ASA Cluster** > **Cluster Summary** pane.

Step 15 Upgrade the control unit.

a) In ASDM on the control unit, choose **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** pane.

b) Uncheck the **Participate in ASA cluster** check box, and click **Apply**.

You are prompted to exit ASDM.

c) Wait for up to 5 minutes for a new control unit to be selected and traffic to stabilize.

When the former control unit rejoins the cluster, it will be a data unit.

d) Re-connect ASDM to the former control unit by connecting to its *individual* management IP address that you noted earlier.

The main cluster IP address now belongs to the new control unit; this former control unit is still accessible on its individual management IP address.

e) Upgrade the ASA FirePOWER module.

Wait for the upgrade to complete.

f) Choose **Tools** > **System Reload**.

g) Click the **Reload without saving the running configuration** radio button.

You do not want to save the configuration; when this unit reloads, you want clustering to be enabled on it.

h) Click **Schedule Reload**.

i) Click **Yes** to continue the reload.

You are prompted to exit ASDM. Restart ASDM on the main cluster IP address; you will reconnect to the new control unit.

Upgrade an ASA FirePOWER Module with FMC

Use this procedure to upgrade an ASA FirePOWER module managed by an FMC. When you upgrade the module depends on whether you are upgrading ASA, and on your ASA deployment.

- Standalone ASA devices: If you are also upgrading ASA, upgrade the ASA FirePOWER module just *after* you upgrade ASA and reload.
- ASA clusters and failover pairs: To avoid interruptions in traffic flow and inspection, fully upgrade these devices *one at a time*. If you are also upgrading ASA, upgrade the ASA FirePOWER module just *before* you reload each unit to upgrade ASA.

For more information, see Upgrade Path: ASA FirePOWER, on page 21 and the ASA upgrade procedures.

Before you begin

Complete the pre-upgrade checklist. Make sure the appliances in your deployment are healthy and successfully communicating.

Step 1 Choose **System** > **Updates**.

Step 2 Click the Install icon next to the upgrade package you want to use and choose the devices to upgrade.

If the devices you want to upgrade are not listed, you chose the wrong upgrade package.

Note We *strongly* recommend upgrading no more than five devices simultaneously from the System Update page. You cannot stop the upgrade until all selected devices complete the process. If there is an issue with any one device upgrade, all devices must finish upgrading before you can resolve the issue.

Step 3 Click **Install**, then confirm that you want to upgrade and reboot the devices.

Traffic either drops throughout the upgrade or traverses the network without inspection depending on how your devices are configured and deployed. For more information, see the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.

Step 4 Monitor upgrade progress.

Caution Do *not* deploy changes to, manually reboot, or shut down an upgrading device. Do *not* restart a device upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Step 5 Verify upgrade success.

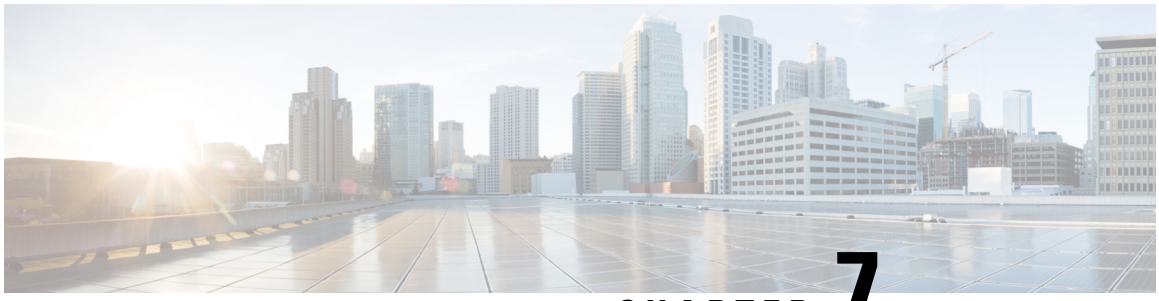
After the upgrade completes, choose **Devices** > **Device Management** and confirm that the devices you upgraded have the correct software version.

Step 6 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 7 Complete any post-upgrade configuration changes described in the release notes.

Step 8 Redeploy configurations to the devices you just upgraded.



CHAPTER 7

Uninstall a Patch

You can uninstall most patches. If you need to return to an earlier major or maintenance release, you must reimage.

Uninstalling a patch returns you to the version you upgraded from, and does not change configurations. Because the FMC must run the same or newer version as its managed devices, uninstall patches from devices first. Uninstall is not supported for hotfixes.

Patches That Support Uninstall

Uninstalling specific patches can cause issues, *even when the uninstall itself succeeds*. These issues include:

- Inability to deploy configuration changes after uninstall.
- Incompatibilities between the operating system and the software.
- FSIC (file system integrity check) failure when the appliance reboots, if you patched with security certifications compliance enabled (CC/UCAPL mode).

Caution If security certifications compliance is enabled and the FSIC fails, the software does not start, remote SSH access is disabled, and you can access the appliance only via local console. If this happens, contact Cisco TAC.

Version 7.0 Patches That Support Uninstall

Uninstall is currently supported for all Version 7.0 patches.

Version 6.7 Patches That Support Uninstall

Uninstall is currently supported for all Version 6.7 patches.

Version 6.6 Patches That Support Uninstall

Uninstall is currently supported for all Version 6.6 patches.

Version 6.5 Patches That Support Uninstall

This table lists supported uninstall scenarios for Version 6.5 patches. Uninstalling returns you to the patch level you upgraded from. If uninstall will take you farther back than what is supported, we recommend you reimage and then upgrade to your desired patch level.

Table 48: Version 6.5.0 Patches That Support Uninstall

Current Version	Farthest Back You Should Uninstall		
	FTD/FTDv	ASA FirePOWER NGIPSv	FMC/FMCv
6.5.0.2+	6.5.0	6.5.0	6.5.0.1
6.5.0.1	6.5.0	6.5.0	—

Version 6.4 Patches That Support Uninstall

This table lists supported uninstall scenarios for Version 6.4 patches. Uninstalling returns you to the patch level you upgraded from. If uninstall will take you farther back than what is supported, we recommend you reimage and then upgrade to your desired patch level.

Table 49: Version 6.4.0 Patches That Support Uninstall

Current Version	Farthest Back You Should Uninstall		
	FTD/FTDv	Firepower 7000/8000 ASA FirePOWER NGIPSv	FMC/FMCv
6.4.0.5+	6.4.0.4	6.4.0.4	6.4.0.4
6.4.0.4	—	—	—
6.4.0.3	6.4.0	—	—
6.4.0.2	6.4.0	—	—
6.4.0.1	6.4.0	6.4.0	6.4.0

Version 6.3 Patches That Support Uninstall

This table lists supported uninstall scenarios for Version 6.3 patches. Uninstalling returns you to the patch level you upgraded from. If uninstall will take you farther back than what is supported, we recommend you reimage and then upgrade to your desired patch level.

Table 50: Version 6.3.0 Patches That Support Uninstall

Current Version	Farthest Back You Should Uninstall
6.3.0.5	—
6.3.0.1 through 6.3.0.4	6.3.0

Version 6.2.3 Patches That Support Uninstall

This table lists supported uninstall scenarios for Version 6.2.3 patches. Uninstalling returns you to the patch level you upgraded from. If uninstall will take you farther back than what is supported, we recommend you reimage and then upgrade to your desired patch level.

Table 51: Version 6.2.3 Patches That Support Uninstall

Current Version	Farthest Back You Should Uninstall		
	FTD/FTDv	Firepower 7000/8000 ASA FirePOWER NGIPSv	FMC/FMCv
6.2.3.16+	6.2.3.15	6.2.3.15	6.2.3.15
6.2.3.15	—	—	—
6.2.3.12 through 6.2.3.14	6.2.3	6.2.3.11	6.2.3.11
6.2.3.11	6.2.3	—	—
6.2.3.8 through 6.2.3.10	6.2.3	6.2.3.7	6.2.3.7
6.2.3.7	6.2.3	—	—
6.2.3.1 through 6.2.3.6	6.2.3	6.2.3	6.2.3

Version 6.2.2 Patches That Support Uninstall

This table lists supported uninstall scenarios for Version 6.2.2 patches. Uninstalling returns you to the immediately preceding patch, even if you upgraded from an earlier patch. If uninstall will take you farther back than what is supported, we recommend you reimage and then upgrade to your desired patch level.

Table 52: Version 6.2.2 Patches That Support Uninstall

Current Version	Farthest Back You Should Uninstall
6.2.2.3 through 6.2.2.5	6.2.2.2
6.2.2.2	—
6.2.2.1	6.2.2

Uninstall Order for High Availability/Scalability

In high availability/scalability deployments, minimize disruption by uninstalling from one appliance at a time. Unlike upgrade, the system does not do this for you. Wait until the patch has fully uninstalled from one unit before you move on to the next.

Table 53: Uninstall Order for FMC High Availability

Configuration	Uninstall Order
FMC high availability	With synchronization paused, which is a state called *split-brain*, uninstall from peers one at a time. Do not make or deploy configuration changes while the pair is split-brain. **1.** Pause synchronization (enter split-brain). **2.** Uninstall from the standby. **3.** Uninstall from the active. **4.** Restart synchronization (exit split-brain).

Table 54: Uninstall Order for FTD High Availability and Clusters

Configuration	Uninstall Order
FTD high availability	You cannot uninstall a patch from devices configured for high availability. You must break high availability first. **1.** Break high availability. **2.** Uninstall from the former standby. **3.** Uninstall from the former active. **4.** Reestablish high availability.
FTD cluster	Uninstall from one unit at a time, leaving the control unit for last. Clustered units operate in maintenance mode while the patch uninstalls. **1.** Uninstall from the data modules one at a time. **2.** Make one of the data modules the new control module. **3.** Uninstall from the former control.

Table 55: Uninstall Order for ASA with FirePOWER Services in ASA Failover Pairs/Clusters

Configuration	Uninstall Order
ASA active/standby failover pair, with ASA FirePOWER	Always uninstall from the standby. 1. Uninstall from the ASA FirePOWER module on the standby ASA device. 2. Fail over. 3. Uninstall from the ASA FirePOWER module on the new standby ASA device.
ASA active/active failover pair, with ASA FirePOWER	Make both failover groups active on the unit you are not uninstalling. 1. Make both failover groups active on the primary ASA device. 2. Uninstall from the ASA FirePOWER module on the secondary ASA device. 3. Make both failover groups active on the secondary ASA device. 4. Uninstall from the ASA FirePOWER module on the primary ASA device.
ASA cluster, with ASA FirePOWER	Disable clustering on each unit before you uninstall. Uninstall from one unit at a time, leaving the control unit for last. 1. On a data unit, disable clustering. 2. Uninstall from the ASA FirePOWER module on that unit. 3. Reenable clustering. Wait for the unit to rejoin the cluster. 4. Repeat for each data unit. 5. On the control unit, disable clustering. Wait for a new control unit to take over. 6. Uninstall from the ASA FirePOWER module on the former control unit. 7. Reenable clustering.

Uninstall Device Patches with FMC

Use the Linux shell (*expert mode*) to uninstall patches. You must have access to the device shell as the `admin` user for the device, or as another local user with CLI configuration access. You cannot use an FMC user account. If you disabled shell access, contact Cisco TAC to reverse the lockdown.

Caution Do not make or deploy configuration changes during uninstall. Even if the system appears inactive, do not manually reboot, shut down, or restart an uninstall in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the uninstall, including a failed uninstall or unresponsive appliance, contact Cisco TAC.

Before you begin

- Break FTD high availability pairs; see Uninstall Order for High Availability/Scalability, on page 114.
- Make sure your deployment is healthy and successfully communicating.

Step 1 If the device's configurations are out of date, deploy now from the FMC.

Deploying before you uninstall reduces the chance of failure. Make sure the deployment and other essential tasks complete. Tasks running when the uninstall begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

Step 2 Access the Firepower CLI on the device. Log in as `admin` or another CLI user with configuration access.

You can either SSH to the device's management interface (hostname or IP address) or use the console. If you use the console, some devices default to the operating system CLI and require an extra step to access the Firepower CLI, as listed in the following table.

Firepower 1000 series	`connect ftd`
Firepower 2100 series	`connect ftd`
Firepower 4100/9300	`connect module` *`slot_number`* `console`, then `connect ftd` (first login only)
ASA FirePOWER	`session sfr`

Step 3 Use the `expert` command to access the Linux shell.

Step 4 Verify the uninstall package is in the upgrade directory.

```
ls /var/sf/updates
```

Patch uninstallers are named like upgrade packages, but have `Patch_Uninstaller` instead of `Patch` in the file name. When you patch a device, the uninstaller for that patch is automatically created in the upgrade directory. If the uninstaller is not there, contact Cisco TAC.

Step 5 Run the uninstall command, entering your password when prompted.

```
sudo install_update.pl --detach /var/sf/updates/uninstaller_name
```

Caution The system does *not* ask you to confirm. Entering this command starts the uninstall, which includes a device reboot. Interruptions in traffic flow and inspection during an uninstall are the same as the interruptions that occur during an upgrade. Make sure you are ready. Note that using the `--detach` option ensures the uninstall process is not killed if your SSH session times out, which can leave the device in an unstable state.

Step 6 Monitor the uninstall until you are logged out.

For a detached uninstall, use `tail` or `tailf` to display logs:

- FTD: `tail /ngfw/var/log/sf/update.status`
- ASA FirePOWER and NGIPSv: `tail /var/log/sf/update.status`

Otherwise, monitor progress in the console or terminal.

Step 7 Verify uninstall success.

After the uninstall completes, confirm that the devices have the correct software version. On the FMC, choose **Devices** > **Device Management**.

Step 8 In high availability/scalability deployments, repeat steps 2 through 6 for each unit.

For clusters, never uninstall from the control unit. After you uninstall from all the data units, make one of them the new control, then uninstall from the former control.

Step 9 Redeploy configurations.

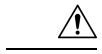
Exception: Do not deploy to mixed-version high availability pairs or device clusters. Deploy before you uninstall from the first device, but not again until you have uninstalled the patch from all group members.

What to do next

- For high availability, reestablish high availability.
- For clusters, if you have preferred roles for specific devices, make those changes now.

Uninstall Standalone FMC Patches

We recommend you use the web interface to uninstall FMC patches. If you cannot use the web interface, you can use the Linux shell as either the `admin` user for the shell, or as an external user with shell access. If you disabled shell access, contact Cisco TAC to reverse the lockdown.



Caution Do not make or deploy configuration changes during uninstall. Even if the system appears inactive, do not manually reboot, shut down, or restart an uninstall in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the uninstall, including a failed uninstall or unresponsive appliance, contact Cisco TAC.

Before you begin

- If uninstalling will put the FMC at a lower patch level than its managed devices, uninstall patches from the devices first.
- Make sure your deployment is healthy and successfully communicating.

Step 1 Deploy to managed devices whose configurations are out of date.

Deploying before you uninstall reduces the chance of failure.

Step 2 Under Available Updates, click the **Install** icon next to the uninstall package, then choose the FMC.

Patch uninstallers are named like upgrade packages, but have `Patch_Uninstaller` instead of `Patch` in the file name. When you patch the FMC, the uninstaller for that patch is automatically created. If the uninstaller is not there, contact Cisco TAC.

Step 3 Click **Install**, then confirm that you want to uninstall and reboot.

You can monitor uninstall progress in the Message Center until you are logged out.

Step 4 Log back in when you can and verify uninstall success.

If the system does not notify you of the uninstall's success when you log in, choose **Help** > **About** to display current software version information.

Step 5 Redeploy configurations to all managed devices.

Uninstall High Availability FMC Patches

We recommend you use the web interface to uninstall FMC patches. If you cannot use the web interface, you can use the Linux shell as either the `admin` user for the shell, or as an external user with shell access. If you disabled shell access, contact Cisco TAC to reverse the lockdown.

Uninstall from high availability peers one at a time. With synchronization paused, first uninstall from the standby, then the active. When the standby starts the uninstall, its status switches from standby to active, so that both peers are active. This temporary state is called *split-brain* and is *not* supported except during upgrade and uninstall.

Caution Do not make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you restart synchronization. Do not make or deploy configuration changes during uninstall. Even if the system appears inactive, do not manually reboot, shut down, or restart an uninstall in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the uninstall, including a failed uninstall or unresponsive appliance, contact Cisco TAC.

Before you begin

- If uninstalling will put the FMCs at a lower patch level than their managed devices, uninstall patches from the devices first.
- Make sure your deployment is healthy and successfully communicating.

Step 1 On the active FMC, deploy to managed devices whose configurations are out of date.

Deploying before you uninstall reduces the chance of failure.

Step 2 On the active FMC, pause synchronization.

a) Choose **System** > **Integration**.
b) On the **High Availability** tab, click **Pause Synchronization**.

Step 3 Uninstall the patch from peers one at a time — first the standby, then the active.

Follow the instructions in Uninstall Standalone FMC Patches , on page 117, but omit the initial deploy, stopping after you verify uninstall success on each peer. In summary, for each peer:

a) On the **System** > **Updates** page, uninstall the patch.
b) Monitor progress until you are logged out, then log back in when you can.

c) Verify uninstall success.

Step 4 On the FMC you want to make the active peer, restart synchronization.

a) Choose **System** > **Integration**.
b) On the **High Availability** tab, click **Make-Me-Active**.
c) Wait until synchronization restarts and the other FMC switches to standby mode.

Step 5 Redeploy configurations to all managed devices.