Cisco Firepower Management Center Upgrade Guide

First Published: 2018-03-29

Last Modified: 2021-07-07

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

This guide explains how to prepare for and complete a successful upgrade of a Firepower Management Center deployment.

Is This Guide for You?

This guide explains how to prepare for and complete a successful upgrade of a *Firepower Management Center* deployment, including any managed devices.

If you cannot or do not want to upgrade, you can freshly install major and maintenance versions of the Firepower software. This is also called *reimaging*. If you think you might need to reimage, see the Cisco Firepower Release Notes for your version and review the fresh install chapter for scenarios, important guidelines, and links to the installation instructions for the various Firepower deployment types.

The following tables provide links to other Firepower upgrade resources.

Table 1: Upgrade Firepower Software

Manager	Devices	Guide
FMC: Firepower Management Center	FTD only NGIPS only NGIPS and FTD	Cisco Firepower Management Center Upgrade Guide: This guide.
FDM: Firepower Device Manager	FTD	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager: To upgrade the Firepower software. See the *System Management* chapter in the guide for the FTD version you are currently running, not the version you are upgrading to. Cisco Firepower 4100/9300 Upgrade Guide: To upgrade FXOS on a Firepower 4100/9300.

Manager	Devices	Guide
CDO: Cloud Defense Orchestrator	FTD	Managing FTD with Cisco Defense Orchestrator: To upgrade the Firepower software. Cisco Firepower 4100/9300 Upgrade Guide: To upgrade FXOS on a Firepower 4100/9300.
ASDM: Adaptive Security Device Manager	ASA FirePOWER	Cisco ASA Upgrade Guide

Table 2: Upgrade Other Components

Platform	Component	Guide
Firepower Management Center	BIOS and firmware	Cisco Firepower Hotfix Release Notes
ISA 3000, ASA 5506-X, 5508-X, and 5516-X	ROMMON image	Cisco ASA and Firepower Threat Defense Reimage Guide See the *Upgrade the ROMMON Image* section. You should always make sure you have the latest image. This applies to both Firepower Threat Defense and ASA FirePOWER deployments.

Firepower Software Upgrade Feature History

Upgrade Feature History: Firepower Management Center Deployments

Table 3:

Feature	Version	Details
Improved FTD upgrade performance and status reporting	7.0.0	Firepower Threat Defense 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	Version	Details
Easy-to-follow upgrade workflow for FTD devices	7.0.0	A new device upgrade page (**Devices** > **Upgrade**) on the Version 7.0.0 Firepower Management Center provides an easy-to-follow wizard for upgrading Version 6.4.0+ Firepower Threat Defense 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 the System Updates page (**System** > **Updates**) page to upload or specify the location of Firepower Threat Defense upgrade packages. You must also use the System Updates page to upgrade the Firepower Management Center itself, as well as all non-Firepower Threat Defense managed devices. **Note** In Version 7.0.0/7.0.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 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	Version	Details
Upgrade more FTD devices at once	7.0.0	The Firepower Threat Defense 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 6.7.0+ 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 Firepower Threat Defense 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.

Feature	Version	Details
Improved FTD upgrade status reporting and cancel/retry options	6.7.0	You can now view the status of FTD device upgrades and readiness checks in progress on the Device Management page, as well as a 7-day history of upgrade success/failures. The Message Center also provides enhanced status and error messages. A new Upgrade Status pop-up, accessible from both Device Management and the Message Center with a single click, shows detailed upgrade information, including percentage/time remaining, specific upgrade stage, success/failure data, upgrade logs, and so on. Also on this pop-up, you can manually cancel failed or in-progress upgrades (**Cancel Upgrade**), or retry failed upgrades (**Retry Upgrade**). Canceling an upgrade reverts the device to its pre-upgrade state. **Note** To be able to manually cancel or retry a failed upgrade, you must disable the new auto-cancel option, which appears when you use the FMC to upgrade an FTD device: **Automatically cancel on upgrade failure and roll back to the previous version**. With the option enabled, the device automatically reverts to its pre-upgrade state upon upgrade failure. Auto-cancel is not supported for patches. In an HA or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. New/modified screens: • **System** > **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	6.7.0	To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. Upgrades now remove locally stored PCAP files.

Feature	Version	Details
Get FTD upgrade packages from an internal web server	6.6.0	FTD devices can now get upgrade packages from your own internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC. **Note** This feature is supported only for FTD devices running Version 6.6.0+. It is not supported for upgrades *to* Version 6.6.0, nor is it supported for the FMC or Classic devices. New/modified screens: **System > Updates > Upload Update** button **> Specify software update source** option
FMC upgrades postpone scheduled tasks	6.7.0 6.6.3 6.4.0.10	FMC upgrades now postpone 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.
Copy upgrade packages to managed devices before the upgrade	6.2.3	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

This table summarizes the upgrade planning process. For full checklists, see the upgrade procedures.

Table 4: Upgrade Planning Phases

Phase	Includes
Planning and Feasibility Careful planning and preparation can help you avoid missteps.	Assess your deployment. Plan your upgrade path. Read *all* upgrade guidelines and plan configuration changes. Check appliance access. Check bandwidth. Schedule maintenance windows.
Upgrade Packages Upgrade packages are available on the Cisco Support & Download site.	Download upgrade packages from Cisco. Upload upgrade packages to appliances or place them somewhere the appliances can acccess during the upgrade process.
Backups The ability to recover from a disaster is an essential part of any system maintenance plan.	Back up Firepower software. Back up FXOS on the Firepower 4100/9300.

Phase	Includes
Associated Upgrades Because operating system and hosting environment upgrades can affect traffic flow and inspection, perform them in a maintenance window.	Upgrade virtual hosting in virtual deployments. Upgrade FXOS on the Firepower 4100/9300. Upgrade ASA on ASA with FirePOWER Services.
Final Checks A set of final checks ensures you are ready to upgrade.	Check configurations. Check NTP synchronization. Check disk space. Deploy configurations. Disable ASA REST API on older devices. 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 5:

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.

Note In Firepower Management Center deployments, you upgrade the Firepower Management Center, then its managed devices. However, in some cases you may need to upgrade devices first.

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 8.

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 Compatibility, on page 111.

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 Firepower Management Center and device upgrades, consider reimaging older devices instead of upgrading. First, remove the devices from the Firepower Management Center. Then, upgrade the Firepower Management Center, reimage the devices, and re-add them to the Firepower Management Center.

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: Firepower Management Center-Device Compatibility, on page 111

- Can I maintain FXOS compatibility with logical devices, for the Firepower 4100/9300: Firepower 4100/9300 Compatibility with ASA and FTD, on page 117
- Can I maintain ASA compatibility with ASA FirePOWER modules, for ASA with FirePOWER services: ASA 5500-X Series and ISA 3000 with FirePOWER Services, on page 128

Upgrade Path: Firepower Management Centers

This table provides upgrade paths for Firepower Management Centers, 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 listed in the table. In those cases, the upgrade quickly fails and displays an error explaining that there are data store incompatibilities between the two versions. The Cisco Firepower Release Notes for both your current and target version list any specific restrictions. The Cisco Firepower Management Center New Features by Release lists all relevant release dates.

Table 6: FMC Direct Upgrades

Current Version	Target Version
7.0.0 7.0.x (maintenance releases)	Any of: → Any later 7.0.x maintenance release
6.7.0 6.7.x (maintenance releases)	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 (maintenance releases) 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
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.

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 Firepower 4100/9300 Compatibility with ASA and FTD, on page 117.

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 7: 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 Hitless upgrades of FTD high availability pairs require a preinstallation package: Firepower System Release Notes Version 6.1.0 Preinstallation Package.

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.

Note With some older Firepower Threat Defense versions, hitless upgrades have some additional requirements. See Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300, on page 233.

Table 8: FXOS + FTD Upgrade Order

Deployment	Upgrade Order
Standalone device Cluster, units on the same chassis (Firepower 9300 only)	1. Upgrade FXOS. 2. Upgrade Firepower software.

Deployment	Upgrade Order
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 Firepower software.
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 Firepower software.

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 a Firepower Management Center, 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 9: 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 (maintenance releases)	→ Any later 7.0.x maintenance release
6.7.0 6.7.x (maintenance releases)	Any of: → 7.0.0 or any 7.0.x maintenance release → Any later 6.7.x maintenance release

Current Version	Target Version
6.6.0 6.6.x (maintenance releases) 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
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

Current Version	Target Version
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 Hitless upgrades of FTD high availability pairs require a preinstallation package: Firepower System Release Notes Version 6.1.0 Preinstallation Package.

Upgrade Path: Firepower 7000/8000 Series

This table provides upgrade paths for Firepower 7000/8000 series devices, managed by a Firepower Management Center.

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

Table 10: 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.

Current Version	Target Version
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
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 a Firepower Management Center.

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 22.

Table 11: Upgrade Paths: ASA FirePOWER with FMC

Current Version	Target Version
7.0.0 7.0.x (maintenance releases)	Any of: → Any later 7.0.x maintenance release
6.7.0 6.7.x (maintenance releases)	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 (maintenance releases) 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
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

Current Version	Target Version
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
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 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 ASA 5500-X Series and ISA 3000 with FirePOWER Services, on page 128.

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 87.

Table 12: ASA + ASA FirePOWER Upgrade Order

ASA Deployment	Upgrade Order
Standalone device	**1.** Upgrade ASA, including reload. **2.** Upgrade ASA FirePOWER.
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 Deployment	Upgrade Order
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 13: Upgrade Paths: ASA for ASA FirePOWER

Current Version	Target Version
9.15(x)	Any of: → **9.16(x)**
9.14(x) Last ASA FirePOWER support for ASA 5525-X, ASA 5545-X, and ASA 5555-X, with Firepower Version 6.6.0/6.6.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 a Firepower Management Center.

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

Table 14: Upgrade Paths: NGIPSv with FMC

Current Version	Target Version
7.0.0 7.0.x (maintenance releases)	Any of: → Any later 7.0.x maintenance release

Current Version	Target Version
6.7.0 6.7.x (maintenance releases)	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 (maintenance releases)	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.

Download Upgrade Packages

Download upgrade packages from 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

Firepower software 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 a Firepower software upgrade package, select or search for your Firepower appliance model, then browse to the Firepower 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 Firepower models in a family or series. Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), and Firepower version. Maintenance releases use the upgrade package type.

For example:

- Package: `Cisco_Firepower_Mgmt_Center_Upgrade-7.0.0-999.sh.REL.tar`
- Platform: Firepower Management Center
- Package type: Upgrade
- Version and build: 7.0.0-999
- File extension: sh.REL.tar

So that Firepower 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 15:

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 16: 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 17: 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 Firepower Management Center high availability deployments, you must upload the Firepower Management Center 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 72. 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.

Do not manually reboot or shut down an appliance running readiness checks. The time required to run a readiness check varies depending on appliance model and database size. Later releases also have faster readiness checks.

Tip For all device upgrades to Version 6.2.3–6.6.x, you can reduce the amount of time it takes to run readiness checks by copying (pushing) upgrade packages to devices before you begin. Readiness checks for FTD device upgrades to Version 6.7.0+ no longer require the upgrade package to reside on the device. Although we still recommend you copy 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.

Support by Firepower Management Center Version

Table 18:

Current FMC Version	Readiness Check Support
5.4.x – 6.0.0	Not supported.
6.0.1	Supported, with a preinstallation package. 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 its managed devices. See the Firepower System Release Notes Version 6.1.0 Pre-Installation Package.

Current FMC Version	Readiness Check Support
6.1 – 6.6.x	You can use a Version 6.1–6.6.x Firepower Management Center to perform the readiness check on itself and its standalone managed devices. 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.
6.7.0+	You can use a Version 6.7.0+ Firepower Management Center to perform the readiness check on itself and the devices it manages, including FTD devices configured for high availability and scalability. Starting with Version 6.7.0, FMCs and FTD devices must also pass pre-upgrade compatibility checks before you can run more complex readiness checks or attempt to upgrade. This check catches issues that *will* cause your upgrade to fail—but we now catch them earlier and block you from proceeding.
7.0.0+	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 72. For the FMC itself and other managed devices, continue to run the readiness checks separately as described in the next topics.

Run Readiness Checks (Version 7.0.0+ FTD with FMC)

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 72.

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 (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 72. You must still use this procedure to run readiness checks on the FMC and on any Classic devices (7000/8000 series, ASA FirePOWER, NGIPSv).

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 (Version 6.1.0–6.6.x with FMC), on page 37.
- 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 (Version 6.1.0–6.6.x with FMC)

This procedure is valid for FMCs *currently* running Version 6.1.0–6.6.x, and their standalone managed devices.

Note You can use this procedure to run readiness checks on a Version 6.0.1 → 6.1.0 upgrade, but you must first install the Version 6.1.0 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.

Before you begin

- 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.

PART I

Upgrade Firepower Appliances

CHAPTER 3

Upgrade Firepower Management Centers

Upgrade Checklist: Firepower Management Center

Complete this checklist before you upgrade aFirepower Management Center, 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. And, know what to do in case of an unresponsive upgrade. See General Guidelines, on page 145.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 19:

✓	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 Firepower Management Center deployments, you usually upgrade the Firepower Management Center, then its managed devices. However, in some cases you may need to upgrade devices first. See Upgrade Paths , on page 8.

✓	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 Firepower Management Center 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 20:

✓	Action/Check
	Upload the Firepower upgrade package. In Firepower Management Center high availability deployments, you must upload the Firepower Management Center 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 32.

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 Firepower product.

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

Table 21:

✓	Action/Check
	Back up the Firepower Management Center. 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 Firepower Management Center deployments, we recommend you back up the Firepower Management Center after you upgrade its managed devices, so your new Firepower Management Center 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 22:

✓	Action/Check
	Upgrade FMCv 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 Firepower upgrade.

Final Checks

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

Table 23:

✓	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 Firepower appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In Firepower Management Center 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: • Firepower Management Center: Choose **System** > **Configuration** > **Time**. • Devices: Use the **show time** CLI command.
	Check disk space. Run a disk space check for the Firepower software upgrade. Without enough free disk space, the upgrade fails. See Time Tests and Disk Space Requirements, on page 183.
	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 Firepower Management Center 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 Traffic Flow, Inspection, and Device Behavior, on page 233.
	Run Firepower software readiness checks. If your Firepower Management Center is running Version 6.1.0+, we recommend compatibility and readiness checks. These checks assess your preparedness for a Firepower software upgrade. See Firepower Software Readiness Checks, on page 35.
	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 Firepower Management Centers 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* deploy changes to or from, manually reboot, or shut down an upgrading appliance. In most cases, 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, there may be something you can do — see the General Guidelines, on page 145.

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 Firepower Management Centers 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* deploy changes to or from, manually reboot, or shut down an upgrading appliance. In most cases, 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, there may be something you can do — see the General Guidelines, on page 145.

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 Firepower Management Center high availability deployments, you must upload the Firepower Management Center 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 45, 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 Firepower Management Center 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 Firepower Management Center switches to standby mode.

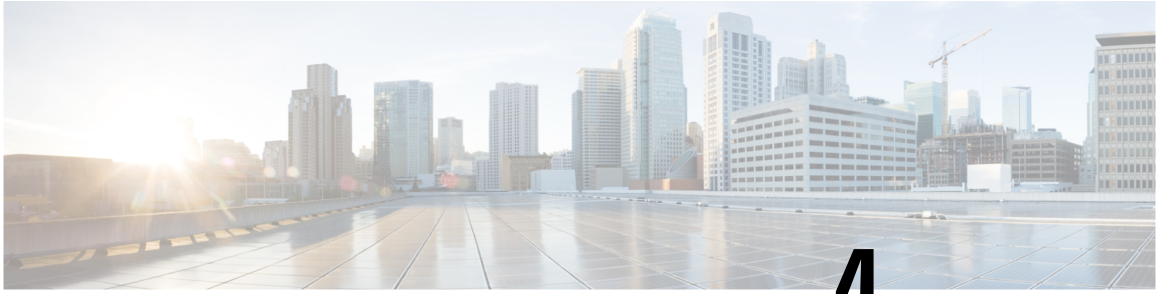
Step 5 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

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. And, know what to do in case of an unresponsive upgrade. See General Guidelines, on page 145.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 24:

✓	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 Firepower Management Center deployments, you usually upgrade the Firepower Management Center, then its managed devices. However, in some cases you may need to upgrade devices first. See Upgrade Paths , on page 8.

✓	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. Firepower devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade a Firepower device, 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 Firepower Management Center 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 25:

✓	Action/Check
	Upload the Firepower Threat Defense upgrade package to the Firepower Management Center or internal web server. In Version 6.6.0+ you can configure an internal web server instead of the Firepower Management Center as the source for Firepower Threat Defense upgrade packages. This is useful if you have limited bandwidth between the Firepower Management Center and its devices, and saves space on the Firepower Management Center. See Upload to an Internal Server (Version 6.6.0+ FTD with FMC), on page 33.

✓	Action/Check
	Copy the Firepower Threat Defense 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 to the device from the Firepower Management Center. • Version 6.6.0 adds the ability to manually copy upgrade packages from an internal web server to Firepower Threat Defense devices. • Version 7.0.0 adds a Firepower Threat Defense upgrade workflow that prompts you to copy the upgrade package to Firepower Threat Defense devices. **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 34.

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 Firepower product.

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

Table 26:

✓	Action/Check
	Back up Firepower Threat Defense. Use the Firepower Management Center to back up devices. Not all Firepower Threat Defenseplatforms 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 Firepower Management Center deployments, we recommend you back up the Firepower Management Center after you upgrade its managed devices, so your new Firepower Management Center backup file 'knows' that its devices have been upgraded.

✓	Action/Check
	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 27:

✓	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 Firepower upgrade.
	Upgrade FXOS on the Firepower 4100/9300. If needed, upgrade FXOS before you upgrade the Firepower software. 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 Firepower Threat Defense 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 28:

✓	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 Firepower appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In Firepower Management Center 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: • Firepower Management Center: Choose **System** > **Configuration** > **Time**. • Devices: Use the **show time** CLI command.
	Check disk space. Run a disk space check for the Firepower software upgrade. Without enough free disk space, the upgrade fails. See Time Tests and Disk Space Requirements, on page 183.
	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 Firepower Management Center 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 Traffic Flow, Inspection, and Device Behavior, on page 233.
	Run Firepower software readiness checks. If your Firepower Management Center is running Version 6.1.0+, we recommend compatibility and readiness checks. These checks assess your preparedness for a Firepower software upgrade. Version 7.0.0 introduces a new Firepower Threat Defense upgrade workflow that prompts you to complete these checks for Firepower Threat Defense devices. See Firepower Software Readiness Checks, on page 35.
	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 Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300, on page 233.

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 (see FXOS Packages, on page 30).
- Back up your FXOS and FTD configurations.

Note The upgrade process typically takes between 20 and 30 minutes. Traffic will not traverse through the device while it is upgrading.

Step 1 In Firepower Chassis Manager, choose **System** > **Updates**.

The Available Updates page shows a list of the Firepower eXtensible Operating System 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 Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components. The upgrade process can take up to 30 minutes to complete.

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 (see FXOS Packages, on page 30).
- 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.

Note The upgrade process typically takes between 20 and 30 minutes. Traffic will not traverse through the device while it is upgrading.

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 Firepower eXtensible Operating 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 (see FXOS Packages, on page 30).
- Back up your FXOS and FTD configurations.

Note The upgrade process typically takes between 20 and 30 minutes per chassis.

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 Firepower eXtensible Operating System 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 Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components. The upgrade process can take up to 30 minutes to complete.

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 Firepower eXtensible Operating System 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 Firepower eXtensible Operating 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 (see FXOS Packages, on page 30).
- 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.

Note The upgrade process typically takes between 20 and 30 minutes per chassis.

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 Firepower eXtensible Operating 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 Firepower eXtensible Operating 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 (see FXOS Packages, on page 30).
- Back up your FXOS and FTD configurations.

Note The upgrade process typically takes between 20 and 30 minutes per chassis.

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 Firepower eXtensible Operating System 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 Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components. The upgrade process can take up to 30 minutes to complete.

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 (see FXOS Packages, on page 30).
- 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.

Note The upgrade process typically takes between 20 and 30 minutes per chassis.

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 Firepower eXtensible Operating 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+)

If your Firepower Management Center is running Version 7.0.0+, you can use a wizard to upgrade Firepower Threat Defense. Upgrades performed with this wizard are faster, more reliable, and take up less disk space.

Note You must still use the System Updates page (**System** > **Updates**) page to upload or specify the location of upgrade packages, to upgrade the Firepower Management Center itself, and to upgrade 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.

Important In Version 7.0.0/7.0.x, to avoid possible time-consuming upgrade failures, *manually* ensure all group members are ready to move on to the next step before you click **Next**.

This is because 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 system 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.

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 On the Firepower Management Center, 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 back 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 Firepower software, the software upgrade package must be on the appliance. Copying the upgrade package before upgrade reduces the length of your upgrade maintenance window.

Run compatibility and readiness checks.

Step 7 Click **Next**.

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. However, you must manually run readiness checks.

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.

Step 8 For all devices that still need to pass the readiness check, click **Run Readiness Check**, then confirm your choice.

Do not manually reboot, or shut down an appliance running readiness checks. If your appliance 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.

Perform other final checks and pre-upgrade actions.

Step 9 (Optional, high availability only) Switch the active/standby roles of your high availability device pairs.

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.

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

Step 10 Perform final pre-upgrade checks.

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

Upgrade.

Step 11 If necessary, return to the Device Upgrade page (**Devices** > **Upgrade**).

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

Step 12 Click **Next**.

Step 13 Verify your device selection and target version.

Step 14 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.

Step 15 Click **Start Upgrade**, then confirm that you want to upgrade and reboot the devices.

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 Traffic Flow, Inspection, and Device Behavior, on page 233.

Step 16 Monitor upgrade progress.

Caution Do *not* deploy changes to or from, manually reboot, or shut down an upgrading appliance. In most cases, 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, there may be something you can do — see the General Guidelines, on page 145.

Verify success and complete post-upgrade tasks.

Step 17 Verify upgrade success.

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

Step 18 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 19 Complete any post-upgrade configuration changes described in the release notes.

Step 20 Redeploy configurations to the devices you just upgraded.

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

Use this procedure to upgrade Firepower Threat Defense using the Firepower Management Center'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

- Complete the pre-upgrade checklist. Make sure the appliances in your deployment are healthy and successfully communicating.
- Decide whether you want to use this procedure. For Firepower Threat Defense upgrades to Version 7.0.0+ we recommend you use the upgrade wizard instead; see Upgrade Firepower Threat Defense with FMC (Version 7.0.0+), on page 72.

Step 1 (Optional, high availability only) Switch the active/standby roles of your high availability device pairs.

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.

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 (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.

Step 5 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 Traffic Flow, Inspection, and Device Behavior, on page 233.

Step 6 Monitor upgrade progress.

Caution Do *not* deploy changes to or from, manually reboot, or shut down an upgrading appliance. In most cases, 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, there may be something you can do — see the General Guidelines, on page 145.

Step 7 Verify upgrade success.

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

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 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. And, know what to do in case of an unresponsive upgrade. See General Guidelines, on page 145.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 29:

✓	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 Firepower Management Center deployments, you usually upgrade the Firepower Management Center, then its managed devices. However, in some cases you may need to upgrade devices first. See Upgrade Paths , on page 8.

✓	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. Firepower devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade a Firepower device, 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 Firepower Management Center 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 30:

✓	Action/Check
	Upload the Firepower upgrade package to the Firepower Management Center. See Upload to the Firepower Management Center, on page 32.
	Copy the Firepower upgrade package to the device. If your Firepower Management Center 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 34.

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 Firepower product.

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

Table 31:

✓	Action/Check
	Back up 7000/8000 series devices. Use the Firepower Management Center 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 Firepower Management Center deployments, we recommend you back up the Firepower Management Center after you upgrade its managed devices, so your new Firepower Management Center 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 32:

✓	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 Firepower upgrade.

Final Checks

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

Table 33:

✓	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 Firepower appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In Firepower Management Center 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: • Firepower Management Center: Choose **System** > **Configuration** > **Time**. • Devices: Use the **show time** CLI command.
	Check disk space. Run a disk space check for the Firepower software upgrade. Without enough free disk space, the upgrade fails. See Time Tests and Disk Space Requirements, on page 183.
	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 Firepower Management Center 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 Traffic Flow, Inspection, and Device Behavior, on page 233.
	Run Firepower software readiness checks. If your Firepower Management Center is running Version 6.1.0+, we recommend compatibility and readiness checks. These checks assess your preparedness for a Firepower software upgrade. See Firepower Software Readiness Checks, on page 35.
	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, high availability only) 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 Traffic Flow, Inspection, and Device Behavior, on page 233.

Step 5 Monitor upgrade progress.

Caution Do *not* deploy changes to or from, manually reboot, or shut down an upgrading appliance. In most cases, 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, there may be something you can do — see the General Guidelines, on page 145.

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. And, know what to do in case of an unresponsive upgrade. See General Guidelines, on page 145.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 34:

✓	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 Firepower Management Center deployments, you usually upgrade the Firepower Management Center, then its managed devices. However, in some cases you may need to upgrade devices first. See Upgrade Paths , on page 8.

✓	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. Firepower devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade a Firepower device, 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 Firepower Management Center 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 35:

✓	Action/Check
	Upload the Firepower upgrade package to the Firepower Management Center. See Upload to the Firepower Management Center, on page 32.
	Copy the Firepower upgrade package to the device. If your Firepower Management Center 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 34.

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 Firepower product.

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

Table 36:

✓	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 37:

✓	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 38:

✓	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 Firepower appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In Firepower Management Center 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: • Firepower Management Center: Choose **System** > **Configuration** > **Time**. • Devices: Use the **show time** CLI command.
	Check disk space. Run a disk space check for the Firepower software upgrade. Without enough free disk space, the upgrade fails. See Time Tests and Disk Space Requirements, on page 183.
	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 Firepower Management Center 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 Traffic Flow, Inspection, and Device Behavior, on page 233.
	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 Firepower software readiness checks. If your Firepower Management Center is running Version 6.1.0+, we recommend compatibility and readiness checks. These checks assess your preparedness for a Firepower software upgrade. See Firepower Software Readiness Checks, on page 35.

✓	Action/Check
	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 Firepower Management Center. 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 19 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 ASA FirePOWER Upgrade Behavior, on page 240.

Step 4 Monitor upgrade progress.

Caution Do *not* deploy changes to or from, manually reboot, or shut down an upgrading appliance. In most cases, 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, there may be something you can do — see the General Guidelines, on page 145.

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.

PART II

Reference

CHAPTER 7

Compatibility

For general Firepower compatibility information see:

- Cisco Firepower Compatibility Guide: Detailed compatibility information for all supported Firepower versions, including versions and builds of bundled operating systems and other components, as well as links to end-of-sale and end-of-life announcements for deprecated platforms.
- Cisco NGFW Product Line Software Release and Sustaining Bulletin: Support timelines for the Cisco Next Generation Firewall product line, including management platforms and operating systems.

For compatibility information relevant to the upgrade process, see:

- Firepower Management Centers, on page 111
- Firepower Devices, on page 116

Firepower Management Centers

Firepower Management Center-Device Compatibility

A Firepower Management Center must run the *same or newer* version as its managed devices. This means:

- You *can* manage older devices with a newer FMC, usually a few major versions back.

  For example, a Version 7.0.0 FMC can manage a Version 6.4.0 device.

- You *cannot* upgrade a device past the FMC.

  For example, a Version 7.0.0 FMC can manage a Version 6.4.0 device.

  Before you upgrade an FMC, make sure the upgraded FMC will be able to manage its current devices. For example, a Version 7.0.1 FMC could manage a Version 7.0.0 device, but not a Version 7.0.2 device.

Below, we list FMC versions and the devices they can manage. Find your current version in the first column, then read across to determine which devices you can manage. Remember, within a major version, the FMC must be running the same or newer maintenance (third-digit) release as its managed devices.

Table 39: FMC Management Capability: Version 6.2.3 through 7.0.x

FMC Version	Can Manage: Device Version										
	7.0.x	**6.7.x**	**6.6.x**	**6.5.0**	**6.4.0**	**6.3.0**	**6.2.3**	**6.2.2**	**6.2.1**	**6.2.0**	**6.1.0**
7.0.x	**YES**	**YES**	**YES**	**YES**	**YES**	—	—	—	—	—	—
6.7.x	—	**YES**	**YES**	**YES**	**YES**	**YES**	—	—	—	—	—
6.6.x	—	—	**YES**	**YES**	**YES**	**YES**	**YES**	—	—	—	—
6.5.0	—	—	—	**YES**	**YES**	**YES**	**YES**	—	—	—	—
6.4.0	—	—	—	—	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
6.3.0	—	—	—	—	—	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
6.2.3	—	—	—	—	—	—	**YES**	**YES**	**YES**	**YES**	**YES**

Table 40: FMC Management Capability: Version 5.4.0 through 6.2.2

FMC Version	Can Manage: Device Version							
	6.2.2	**6.2.1**	**6.2.0**	**6.1.0**	**6.0.1**	**6.0.0**	**5.4.1**	**5.4.0**
6.2.2	**YES**	**YES**	**YES**	**YES**	—	—	—	—
6.2.1	—	**YES**	**YES**	**YES**	—	—	—	—
6.2.0	—	—	**YES**	**YES**	—	—	—	—
6.1.0	—	—	—	**YES**	**YES**	**YES**	**YES** *	**YES** *
6.0.1	—	—	—	—	**YES**	**YES**	**YES** *	**YES** *
6.0.0	—	—	—	—	—	**YES**	**YES** *	**YES** *
5.4.1	—	—	—	—	—	—	**YES**	**YES**
5.4.0	—	—	—	—	—	—	—	**YES**

* A device must be running at least Version 5.4.0.2/5.4.1.1 to be managed by a Version 6.0, 6.0.1, or 6.1 FMC.

Firepower Management Centers: Physical

Table 41: Firepower Management Center Compatibility

Firepower Version	FMC 1600 FMC 2600 FMC 4600	FMC 1000 FMC 2500 FMC 4500	FMC 2000 FMC 4000	FMC 750 FMC 1500 FMC 3500	DC 500 DC 1000 DC 3000
7.0.x	YES	YES	—	—	—
6.7.x	YES	YES	—	—	—
6.6.x	YES	YES	YES	—	—
6.5.0	YES	YES	YES	—	—
6.4.0	YES	YES	YES	YES	—
6.3.0	YES	YES	YES	YES	—
6.2.3	—	YES	YES	YES	—
6.2.2	—	YES	YES	YES	—
6.2.1	—	YES	YES	YES	—
6.2.0	—	YES	YES	YES	—
6.1.0	—	—	YES	YES	—
6.0.1	—	—	YES	YES	—
6.0.0	—	—	YES	YES	—
5.4.1	—	—	YES	YES	YES
5.4.0 *	—	—	YES	YES	YES

* 5.4.0 only. Use 5.4.1.x Defense Centers to manage 5.4.x devices.

Firepower Management Centers: Virtual

These tables lists Firepower compatibility and virtual hosting environment requirements for FMCv. Note that support for FMCv300 for VMware begins in Version 6.5.0.

Table 42: FMCv for VMware Compatibility: Firepower Version 6.2.3 through 7.0.x

Firepower Version	VMware vSphere/VMware ESXi					
	7.0	6.7	6.5	6.0	5.5	5.1
7.0.x	YES	YES	YES	—	—	—

Firepower Version	VMware vSphere/VMware ESXi					
	7.0	6.7	6.5	6.0	5.5	5.1
6.7.x	—	YES	YES	YES	—	—
6.6.x	—	YES	YES	YES	—	—
6.5.0	—	YES	YES	YES	—	—
6.4.0	—	—	YES	YES	—	—
6.3.0	—	—	YES	YES	—	—
6.2.3	—	—	YES	YES	YES	—

Table 43: FMCv for VMware Compatibility: Firepower Version 5.4 through 6.2.2

Firepower Version	VMware vSphere/VMware ESXi				VMware vCloud Director
	6.0	5.5	5.1	5.0	
6.2.2	YES	YES	—	—	—
6.2.1	YES	YES	—	—	—
6.2.0	YES	YES	—	—	—
6.1.0	YES	YES	—	—	—
6.0.1	—	YES	YES	—	—
6.0.0	—	YES	YES	—	—
5.4.1	—	YES	YES	YES	YES
5.4.0 *	—	YES	YES	YES	YES

* 5.4.0 only; use 5.4.1.x Defense Centers to manage 5.4.x devices.

Table 44: FMCv Compatibility: Other Hypervisors

Firepower Version	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Cisco HyperFlex (HyperFlex)	Kernel-Based Virtual Machine (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack	Oracle Cloud Infrastructure (OCI)
7.0.x	YES	YES	YES	YES	YES	YES	YES	YES
6.7.x	YES	YES	YES	—	YES	—	—	YES
6.6.x	YES	YES	—	—	YES	—	—	—
6.6.x	YES	YES	—	—	YES	—	—	—

Firepower Version	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Cisco HyperFlex (HyperFlex)	Kernel-Based Virtual Machine (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack	Oracle Cloud Infrastructure (OCI)
6.5.0	**YES**	**YES**		—	**YES**	—	—	—
6.4.0	**YES**	**YES**	—	—	**YES**	—	—	—
6.3.0	**YES**	—	—	—	**YES**	—	—	—
6.2.3	**YES**	—	—	—	**YES**	—	—	—
6.2.2	**YES**	—	—	—	**YES**	—	—	—
6.2.1	**YES**	—	—	—	**YES**	—	—	—
6.2.0	**YES**	—	—	—	**YES**	—	—	—
6.1.0	**YES**	—	—	—	**YES**	—	—	—
6.0.1	**YES**	—	—	—	—	—	—	—

BIOS and Firmware for FMCs

We provide updates for BIOS and RAID controller firmware on Firepower Management Center hardware. If your FMC does not meet the requirements, apply the appropriate hotfix. If your FMC model and version are not listed and you think you need to update, contact Cisco TAC.

Table 45: BIOS and Firmware Minimum Requirements

Platform	Firepower Version	BIOS	RAID Controller Firmware	CIMC Firmware	Hotfix
FMC 1600, 2600, 4600	6.3.0 to 6.7.x	C220M5.4.1.1c.0	51.10.0-2978	4.1(1f)	BIOS Update Hotfix EI
FMC 1000, 2500, 4500	6.2.3 to 6.7.x	C22M4.4.0.2d.0	24.12.1-0433	4.0(2d)	BIOS Update Hotfix EI
FMC 2000, 4000	6.2.3 to 6.6.x	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)	BIOS Update Hotfix EI
FMC 750, 1500, 3500	6.2.3 to 6.4.0	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)	BIOS Update Hotfix EI

Hotfixing is the only way to update the BIOS and RAID controller firmware. Upgrading the Firepower software does not accomplish this task, nor does reimaging to a later version. If the FMC is already up to date, the hotfix has no effect.

Tip

These hotfixes also update the CIMC firmware; for resolved issues see Release Notes for Cisco UCS Rack Server Software. Note that in general, we do not support changing configurations on the FMC using CIMC. However, to enable logging of invalid CIMC usernames, apply Hotfix EI then follow the instructions in the *Viewing Faults and Logs* chapter in the Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Version 4.0 or later.

Use the regular upgrade process to apply hotfixes. For hotfix release notes, which include quicklinks to the Cisco Support & Download site, see the Cisco Firepower Hotfix Release Notes.

Note

The Firepower Management Center web interface may display these hotfixes with a version that is different from the current Firepower software version; for example, *Hotfix EI: Version 7.0.0*. This is expected behavior and the hotfixes are safe to apply.

Determining BIOS and Firmware Versions

To determine the current versions on an FMC, run these commands from the Linux shell/expert mode:

- BIOS: **sudo dmidecode -t bios -q**
- RAID controller firmware (FMC 4500): **sudo MegaCLI -AdpAllInfo -aALL | grep "FW Package"**
- RAID controller firmware (all other models): **sudo storcli /c0 show | grep "FW Package"**

Firepower Devices

Firepower 1000/2100 Series with FTD

Firepower 1000 and Firepower 2100 series devices use the FXOS operating system. Upgrading Firepower Threat Defense automatically upgrades FXOS.

These devices can also run ASA instead of FTD. For more information, see Cisco ASA Compatibility.

Table 46: Firepower 1000/2100 Series Compatibility

Firepower Version	Firepower 2110 Firepower 2120 Firepower 2130 Firepower 2140	Firepower 1010 Firepower 1120 Firepower 1140	Firepower 1150
7.0.x	**YES**	**YES**	**YES**
6.7.x	**YES**	**YES**	**YES**
6.6.x	**YES**	**YES**	**YES**

Firepower Version	Firepower 2110 Firepower 2120 Firepower 2130 Firepower 2140	Firepower 1010 Firepower 1120 Firepower 1140	Firepower 1150
6.5.0	**YES**	**YES**	**YES**
6.4.0	**YES**	**YES**	—
6.3.0	**YES**	—	—
6.2.3	**YES**	—	—
6.2.2	**YES**	—	—
6.2.1	**YES**	—	—

Firepower 4100/9300 Compatibility with ASA and FTD

The following table lists compatibility between the ASA or FTD applications with FXOS and Firepower models.

The FXOS versions with (EoL) appended have reached their end of life (EoL), or end of support.

Note The **bold** versions listed below are specially-qualified companion releases. You should use these software combinations whenever possible because Cisco performs enhanced testing for these combinations.

Note Firepower 1000 and 2100 series appliances utilize FXOS only as an underlying operating system that is included in the ASA and Firepower Threat Defense unified image bundles.

Table 47: ASA or FTD, and Firepower 4100/9300 Compatibility

FXOS Version	Firepower Model	ASA Version	FTD Version

2.10(1.159)+
Note FXOS 2.10(1.159)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.10(1.159)+, such as 9.13 or 9.12, are not affected.
	Firepower 4112	**9.16(1)** (recommended)
		9.15(1)
		9.14(x)
			7.0.0 (recommended)
			6.7.0
			6.6.x

	Firepower 4145
	Firepower 4125
	Firepower 4115
		9.16(1) (recommended)
		9.15(1)
		9.14(x)
		9.13(1)
		9.12(x)
			7.0.0 (recommended)
			6.7.0
			6.6.x
			6.5.0
			6.4.0

	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

	Firepower 4150
	Firepower 4140
	Firepower 4120
	Firepower 4110
		9.16(1) (recommended)
		9.15(1)
		9.14(x)
		9.13(x)
		9.12(x)
		9.10(x)
		9.9(x)
		9.8(x)
			7.0.0 (recommended)
			6.7.0
			6.6.x
			6.5.0
			6.4.0
			6.3.0

	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Firepower Model	ASA Version	FTD Version

2.9(1.131)+
Note FXOS 2.9(1.131)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.9(1.131)+, such as 9.13 or 9.12, are not affected.
	Firepower 4112	**9.15(1)** (recommended)
		9.14(x)
			6.7.0 (recommended)
			6.6.x

	Firepower 4145
	Firepower 4125
	Firepower 4115
		9.15(1) (recommended)
		9.14(x)
		9.13(1)
		9.12(x)
			6.7.0 (recommended)
			6.6.x
			6.5.0
			6.4.0

	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

	Firepower 4150
	Firepower 4140
	Firepower 4120
	Firepower 4110
		9.15(1) (recommended)
		9.14(x)
		9.13(x)
		9.12(x)
		9.10(x)
		9.9(x)
		9.8(x)
			6.7.0 (recommended)
			6.6.x
			6.5.0
			6.4.0
			6.3.0

	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Firepower Model	ASA Version	FTD Version
2.8(1.105)+ **Note** FXOS 2.8(1.125)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.8(1.125)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	**9.14(x)**	**6.6.x** **Note** 6.6.1+ requires FXOS 2.8(1.125)+.

	Firepower 4145
	Firepower 4125
	Firepower 4115
		9.14(x) (recommended)
		9.13(1)
		9.12(x)
		Note Firepower 9300 SM-56 requires ASA 9.12(2)+
			6.6.x (recommended)
			Note 6.6.1+ requires FXOS 2.8(1.125)+.
			6.5.0
			6.4.0

	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

	Firepower 4150
	Firepower 4140
	Firepower 4120
	Firepower 4110
		9.14(x) (recommended)
		9.13(x)
		9.12(x)
		9.10(x)
		9.9(x)
		9.8(x)
		9.6(4)
			6.6.x (recommended)
			Note 6.6.1+ requires FXOS 2.8(1.125)+.
			6.5.0
			6.4.0
			6.3.0
			6.2.3
			6.2.0

	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

2.7(1.92)+	Firepower 4145
	Firepower 4125
	Firepower 4115
		9.13(1) (recommended)
		9.12(x)
		Note Firepower 9300 SM-56 requires ASA 9.12.2+
			6.5.0 (recommended)
			6.4.0

	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

	Firepower 4150
	Firepower 4140
	Firepower 4120
	Firepower 4110
		9.13(1) (recommended)
		9.12(x)
		9.10(1)
		9.9(x)
		9.8(x)
		9.6(4)
			6.5.0 (recommended)
			6.4.0
			6.3.0
			6.2.3
			6.2.2
			6.2.0

	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Firepower Model	ASA Version	FTD Version
2.6(1.157)+ **Note** You can now run ASA 9.12+ and FTD 6.4+ on separate modules in the same Firepower 9300 chassis	Firepower 4145 Firepower 4125 Firepower 4115	**9.12(x)** **Note** Firepower 9300 SM-56 requires ASA 9.12.2+	**6.4.0**
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

	Firepower 4150
	Firepower 4140
	Firepower 4120
	Firepower 4110
		9.12(x) (recommended)
		9.10(1)
		9.9(x)
		9.8(x)
		9.6(4)
		Note 9.7(x) is not supported.
			6.4.0 (recommended)
			6.3.0
			6.2.3
			6.2.2
			6.2.0
			6.1.0

	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	**9.12(x)**	Not supported

	Firepower 4150
	Firepower 4140
	Firepower 4120
	Firepower 4110
		9.12(x) (recommended)
		9.10(1)
		9.9(x)
		9.8(x)
		9.6(4)
		Note 9.7(x) is not supported.	

	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

2.4(1.214)+
Note FXOS 2.4(1.238)+ is required for hardware bypass. For more information, see the Important Notes section of the Cisco Firepower 4100/9300 FXOS Release Notes, 2.4(1).
	Firepower 4150
	Firepower 4140
	Firepower 4120
	Firepower 4110
		9.10(1) (recommended)
		9.9(x)
		9.8(x)
		9.6(3), 9.6(4)
		Note 9.7(x) is not supported.
			6.3.0 (recommended)
			6.2.3
			6.2.2
			6.2.0
			6.1.0

	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Firepower Model	ASA Version	FTD Version

2.4(1.101)	Firepower 4150
	Firepower 4140
	Firepower 4120
	Firepower 4110
		9.10(1) (recommended)
		9.9(x)
		9.8(x)
		9.6(3), 9.6(4)
		Note 9.7(x) is not supported.
			Not supported

	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

2.3(1.73)+	Firepower 4150
	Firepower 4140
	Firepower 4120
	Firepower 4110
		9.9(x) (recommended)
		9.8(x)
		9.7(x)
		9.6(3), 9.6(4)
		Note 9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+.
			6.2.3 (recommended)
			Note 6.2.3.16+ requires FXOS 2.3.1.157+
			6.2.2
			6.2.0
			6.1.0
			Note 6.2.2.2+ is required for flow offload when running FXOS 2.3(1.130)+.

	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

2.3(1.66)
2.3(1.58)
2.3(1.56)
Note FXOS 2.3(1.56), which was briefly available on Cisco.com, is no longer supported. For more information, see the Cisco FXOS Release Notes, 2.3(1).
	Firepower 4150
	Firepower 4140
	Firepower 4120
	Firepower 4110
		9.9(x) (recommended)
		9.8(x)
		9.7(x)
		9.6(3), 9.6(4)
		Note 9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+.
			6.2.2 (recommended)
			6.2.2
			6.2.0
			6.1.0
			Note 6.2.2.2+ is required for flow offload when running FXOS 2.3(1.130)+.

	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Firepower Model	ASA Version	FTD Version
2.2(2)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.8(x)** (recommended)	**6.2.2** (recommended) 6.2.0 **Note** 6.2.2+ is required for flow offload when running FXOS 2.2(2.91)+.
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

2.2(1)	Firepower 4150
	Firepower 4140
	Firepower 4120
	Firepower 4110
		9.8(1) (recommended)
		9.7(x)
		Note 9.7(1.15)+ is required for flow offload.
			6.2.0 (recommended)
			Note 6.2.0.3+ is required for flow offload.

	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

2.1(1) (EoL)	Firepower 4150
	Firepower 4140
	Firepower 4120
	Firepower 4110
		9.7(x) (recommended)
		9.6(2), 9.6(3), 9.6(4)
			6.2.0 (recommended)
			6.1.0

	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

2.0(1)	Firepower 4150
	Firepower 4140
	Firepower 4120
	Firepower 4110
		9.6(2), 9.6(3), 9.6(4) (recommended)
		9.6(1)
			6.1.0 (recommended)
			6.0.1

	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Firepower Model	ASA Version	FTD Version
1.1(4)	Firepower 4140 Firepower 4120 Firepower 4110	**9.6(1)**	**6.0.1** (recommended)

	Firepower 9300 SM-36
	Firepower 9300 SM-24
		9.6(1) (recommended)
		9.5(2), 9.5(3)	

1.1(3)	Firepower 9300 SM-36
	Firepower 9300 SM-24
		9.5(2), 9.5(3) (recommended)
		9.4(2)
			Not supported

1.1(2)	Firepower 9300 SM-36
	Firepower 9300 SM-24
		9.4(2) (recommended)
		9.4(1)
			Not supported

1.1(1) (EoL)	Firepower 9300 SM-36 Firepower 9300 SM-24	**9.4(1)** (recommended)	Not supported

Radware DefensePro Compatibility

The following table lists the supported Radware DefensePro version for each Firepower security appliance and associated logical device.

Table 48: Radware DefensePro Compatibility

FXOS Version	ASA	Firepower Threat Defense	Radware DefensePro	Firepower Models
1.1(4)	9.6(1)	not supported	1.1(2.32-3)	9300

2.0(1)	9.6(1)
	9.6(2)
	9.6(3)
	9.6(4)
		not supported	8.10.01.16-5	Firepower 9300
				Firepower 4120
				Firepower 4140
				Firepower 4150

2.1(1)	9.6(2)
	9.6(3)
	9.6(4)
	9.7(1)
		not supported	8.10.01.16-5	Firepower 9300
				Firepower 4120
				Firepower 4140
				Firepower 4150

2.2(1)	9.7(1)
	9.8(1)
		6.2.0	8.10.01.17-2	Firepower 9300
				Firepower 4110 (Firepower Threat Defense only)
				Firepower 4120
				Firepower 4140
				Firepower 4150

FXOS Version	ASA	Firepower Threat Defense	Radware DefensePro	Firepower Models

2.2(2)	9.8(1)
	9.8(2)
	9.8(3)
		6.2.0
		6.2.2
			8.10.01.17-2	Firepower 9300
				Firepower 4110 (Firepower Threat Defense only)
				Firepower 4120
				Firepower 4140
				Firepower 4150

2.3(1)	9.9(1)
	9.9(2)
		6.2.2
		6.2.3
			8.13.01.09-2	Firepower 9300
				Firepower 4110 (Firepower Threat Defense only)
				Firepower 4120
				Firepower 4140
				Firepower 4150

2.4(1)	9.9(2)
	9.10(1)
		6.2.3
		6.3
			8.13.01.09-2	Firepower 9300
				Firepower 4110
				Firepower 4120
				Firepower 4140
				Firepower 4150

2.6(1)	9.12(1)
	9.10(1)
		6.4.0
		6.3.0
			8.13.01.09-3	Firepower 9300
				Firepower 4110
				Firepower 4115
				Firepower 4120
				Firepower 4125
				Firepower 4140
				Firepower 4145
				Firepower 4150

2.7(1)	9.13(1)	6.5	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

FXOS Version	ASA	Firepower Threat Defense	Radware DefensePro	Firepower Models
2.8.1	9.14(1)	6.6.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.9.1	9.15(1)	6.7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.10.1	9.16(1)	7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

Firepower Threat Defense Virtual

These tables list Firepower compatibility and virtual hosting environment requirements for FTDv.

Table 49: FTDv for VMware Compatibility

Firepower Version	VMware vSphere/VMware ESXi					
	7.0	6.7	6.5	6.0	5.5	5.1
7.0.x	YES	YES	YES	—	—	—
6.7.x	—	YES	YES	YES	—	—
6.6.x	—	YES	YES	YES	—	—
6.5.0	—	YES	YES	YES	—	—
6.4.0	—	—	YES	YES	—	—
6.3.0	—	—	YES	YES	—	—
6.2.3	—	—	YES	YES	YES	—
6.2.2	—	—	—	YES	YES	—
6.2.1	—	—	—	—	—	—
6.2.0	—	—	—	YES	YES	—
6.1.0	—	—	—	YES	YES	—
6.0.1	—	—	—	—	YES	YES

Table 50: FTDv Compatibility: Other Hypervisors

Firepower Version	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Cisco HyperFlex (HyperFlex)	Kernel-Based Virtual Machine (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack	Oracle Cloud Infrastructure (OCI)
7.0.x	YES	YES	YES	YES	YES	YES	YES	YES
6.7.x	YES	YES	YES	—	YES	—	—	YES
6.6.x	YES	YES	—	—	YES	—	—	—
6.5.0	YES	YES	—	—	YES	—	—	—
6.4.0	YES	YES	—	—	YES	—	—	—
6.3.0	YES	YES	—	—	YES	—	—	—
6.2.3	YES	YES	—	—	YES	—	—	—
6.2.2	YES	YES	—	—	YES	—	—	—
6.2.1	—	—	—	—	—	—	—	—
6.2.0	YES	YES	—	—	YES	—	—	—

Firepower Version	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Cisco HyperFlex (HyperFlex)	Kernel-Based Virtual Machine (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack	Oracle Cloud Infrastructure (OCI)
6.1.0	**YES**	—	—	—	**YES**	—	—	—
6.0.1	**YES**	—	—	—	—	—	—	—

Firepower 7000/8000 Series and Legacy Devices

This table lists Firepower compatibility with 7000/8000 series devices, AMP models, and legacy device platforms.

Table 51: Firepower 7000/8000 Series Compatibility

Firepower Version	7000/8000 Series (Includes AMP)	Series 2 (Legacy)	Cisco NGIPS for Blue Coat X-Series (Legacy)
6.4.0	**YES**	—	—
6.3.0	**YES**	—	—
6.2.3	**YES**	—	—
6.2.2	**YES**	—	—
6.2.1	—	—	—
6.2.0	**YES**	—	—
6.1.0	**YES**	—	—
6.0.0	**YES**	—	—
5.4.0	**YES**	**YES**	5.4.0 and 5.4.0.2 - 5.4.0.5 only Requires XOS 9.7.2.x or 10.x

ASA 5500-X Series and ISA 3000 with FirePOWER Services

The ASA FirePOWER module runs on the separately upgraded ASA operating system. There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues.For example, the Firepower captive portal feature requires at least ASA FirePOWER Version 6.0.0 *and* ASA 9.5(2).

Compatibility Table

The following table shows the ASA, ASDM, and ASA FirePOWER support. If you are using an FMC to manage ASA FirePOWER, you can ignore the ASDM requirements.

Note that:

- ASA 9.14(x)/ASDM 7.14(x)/FirePOWER 6.6.0/6.6.x is the final version for the ASA FirePOWER module on the ASA 5525-X, 5545-X, and 5555-X.
- ASA 9.12(x)/ASDM 7.12(x)/FirePOWER 6.4.0 is the final version for the ASA FirePOWER module on the ASA 5515-X and 5585-X.
- ASA 9.9(x)/ASDM 7.9(2)/FirePOWER 6.2.3 is the final version for the ASA FirePOWER module on the ASA 5506-X series and 5512-X.

ASDM versions are backwards compatible with all previous ASA versions, unless otherwise stated. For example, ASDM 7.13(1) can manage an ASA 5516-X on ASA 9.10(1). ASDM 7.13(1) and ASDM 7.14(1) did not support ASA 5512-X, 5515-X, 5585-X, and ASASM; you must upgrade to ASDM 7.13(1.101) or 7.14(1.48) to restore ASDM support.

Table 52: ASA and ASA FirePOWER Compatibility

ASA FirePOWER Version	ASDM Version (for local mgmt)	ASA Version	ASA Model						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X (See below for SSP notes)	ISA 3000
7.0.x	ASDM 7.16(1)	ASA 9.16(x) ASA 9.15(x) ASA 9.14(x) ASA 9.13(x) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)	—	**YES**	—	—	—	—	**YES**

ASA FirePOWER Version	ASDM Version (for local mgmt)	ASA Version	ASA Model						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X (See below for SSP notes)	ISA 3000
6.7.x	ASDM 7.15(1)	ASA 9.16(x) ASA 9.15(x) ASA 9.14(x) ASA 9.13(x) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)	—	**YES**	—	—	—	—	**YES**
6.6.x	ASDM 7.14(1)	ASA 9.16(x) (No 5525-X, 5545-X, 5555-X) ASA 9.15(x) (No 5525-X, 5545-X, 5555-X) ASA 9.14(x) ASA 9.13(x) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)	—	**YES**	—	—	**YES**	—	**YES**

ASA FirePOWER Version	ASDM Version (for local mgmt)	ASA Version	ASA Model						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X (See below for SSP notes)	ISA 3000
6.5.0	ASDM 7.13(1)	ASA 9.16(x) (No 5525-X, 5545-X, 5555-X) ASA 9.15(x) (No 5525-X, 5545-X, 5555-X) ASA 9.14(x) ASA 9.13(x) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)	—	**YES**	—	—	**YES**	—	**YES**

ASA FirePOWER Version	ASDM Version (for local mgmt)	ASA Version	ASA Model						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X (See below for SSP notes)	ISA 3000
6.4.0	ASDM 7.12(1)	ASA 9.16(x) (No 5515-X, 5525-X, 5545-X, 5555-X, 5585-X) ASA 9.15(x) (No 5515-X, 5525-X, 5545-X, 5555-X, 5585-X) ASA 9.14(x) (No 5515-X, 5585-X) ASA 9.13(x) (No 5515-X, 5585-X) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)	—	**YES**	—	**YES**	**YES**	**YES**	**YES**

ASA FirePOWER Version	ASDM Version (for local mgmt)	ASA Version	ASA Model						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X (See below for SSP notes)	ISA 3000
6.3.0	ASDM 7.10(1)	ASA 9.16(x) (No 5515-X, 5525-X, 5545-X, 5555-X, 5585-X) ASA 9.15(x) (No 5515-X, 5525-X, 5545-X, 5555-X, 5585-X) ASA 9.14(x) (No 5515-X, 5585-X) ASA 9.13(x) (No 5515-X, 5585-X) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3)	—	**YES**	—	**YES**	**YES**	**YES**	**YES**

ASA FirePOWER Version	ASDM Version (for local mgmt)	ASA Version	ASA Model						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X (See below for SSP notes)	ISA 3000
6.2.3	ASDM 7.9(2)	ASA 9.16(x) (No 5506-X, 5512-X,5515-X, 5525-X, 5545-X, 5555-X, 5585-X) ASA 9.15(x) (No 5506-X, 5512-X,5515-X, 5525-X, 5545-X, 5555-X, 5585-X) ASA 9.14(x) (No 5506-X, 5512-X, 5515-X, 5585-X) ASA 9.13(x) (No 5506-X, 5512-X, 5515-X, 5585-X) ASA 9.12(x) (No 5506-X, 5512-X) ASA 9.10(x) (No 5506-X, 5512-X) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3) (No 5506-X)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—

ASA FirePOWER Version	ASDM Version (for local mgmt)	ASA Version	ASA Model						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X (See below for SSP notes)	ISA 3000
6.2.2	ASDM 7.8(2)	ASA 9.16(x) (No 5506-X, 5512-X,5515-X, 5525-X, 5545-X, 5555-X, 5585-X) ASA 9.15(x) (No 5506-X, 5512-X,5515-X, 5525-X, 5545-X, 5555-X, 5585-X) ASA 9.14(x) (No 5506-X, 5512-X, 5515-X, 5585-X) ASA 9.13(x) (No 5506-X, 5512-X, 5515-X, 5585-X) ASA 9.12(x) (No 5506-X, 5512-X) ASA 9.10(x) (No 5506-X, 5512-X) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3) (No 5506-X)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—

ASA FirePOWER Version	ASDM Version (for local mgmt)	ASA Version	ASA Model						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X (See below for SSP notes)	ISA 3000
6.2.0	ASDM 7.7(1)	ASA 9.16(x) (No 5506-X, 5512-X,5515-X, 5525-X, 5545-X, 5555-X, 5585-X) ASA 9.15(x) (No 5506-X, 5512-X,5515-X, 5525-X, 5545-X, 5555-X, 5585-X) ASA 9.14(x) (No 5506-X, 5512-X, 5515-X, 5585-X) ASA 9.13(x) (No 5506-X, 5512-X, 5515-X, 5585-X) ASA 9.12(x) (No 5506-X, 5512-X) ASA 9.10(x) (No 5506-X, 5512-X) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3) (No 5506-X)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—

ASA FirePOWER Version	ASDM Version (for local mgmt)	ASA Version	ASA Model						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X (See below for SSP notes)	ISA 3000
6.1.0	ASDM 7.6(2)	ASA 9.16(x) (No 5506-X, 5512-X,5515-X, 5525-X, 5545-X, 5555-X, 5585-X) ASA 9.15(x) (No 5506-X, 5512-X,5515-X, 5525-X, 5545-X, 5555-X, 5585-X) ASA 9.14(x) (No 5506-X, 5512-X, 5515-X, 5585-X) ASA 9.13(x) (No 5506-X, 5512-X, 5515-X, 5585-X) ASA 9.12(x) (No 5506-X, 5512-X) ASA 9.10(x) (No 5506-X, 5512-X) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3) (No 5506-X)	YES	YES	YES	YES	YES	YES	—
6.0.1	ASDM 7.6(1) (no ASA 9.4(x) support with ASDM; only FMC)	ASA 9.6(x) ASA 9.5(1.5), 9.5(2), 9.5(3) ASA 9.4(x) Due to CSCuv91730, we recommend that you upgrade to 9.4(2) and later.	YES	YES	YES	YES	YES	YES	—

ASA FirePOWER Version	ASDM Version (for local mgmt)	ASA Version	ASA Model						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X (See below for SSP notes)	ISA 3000
6.0.0	ASDM 7.5(1.112) (no ASA 9.4(x) support with ASDM; only FMC)	ASA 9.6(x) ASA 9.5(1.5), 9.5(2), 9.5(3) ASA 9.4(x) Due to CSCuv91730, we recommend that you upgrade to 9.4(2) and later.	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—

ASA FirePOWER Version	ASDM Version (for local mgmt)	ASA Version	ASA Model						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X (See below for SSP notes)	ISA 3000
5.4.1.7+	ASDM 7.5(1.112) (no ASA 9.4(x) support with ASDM; only FMC)	ASA 9.16(x) (No 5506-X, 5512-X,5515-X, 5525-X, 5545-X, 5555-X, 5585-X) ASA 9.15(x) (No 5506-X, 5512-X,5515-X, 5525-X, 5545-X, 5555-X, 5585-X) ASA 9.14(x) (No 5506-X) ASA 9.13(x) (No 5506-X) ASA 9.12(x) (No 5506-X) ASA 9.10(x) (No 5506-X) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(2), 9.5(3) ASA 9.4(x) ASA 9.4(1.225) (ISA 3000 only) ASA 9.3(2), 9.3(3) (no 5508-X or 5516-X) Due to CSCuv91730, we recommend that you upgrade to 9.3(3.8) or 9.4(2) and later.	**YES**	**YES**	**—**	—	—	—	**YES**

ASA FirePOWER Version	ASDM Version (for local mgmt)	ASA Version	ASA Model						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X (See below for SSP notes)	ISA 3000
5.4.1	ASDM 7.3(3)	ASA 9.16(x) (No 5506-X) ASA 9.15(x) (No 5506-X) ASA 9.14(x) (No 5506-X) ASA 9.13(x) (No 5506-X) ASA 9.12(x) (No 5506-X) ASA 9.10(x) (No 5506-X) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(1.5), 9.5(2), 9.5(3) ASA 9.4(x) ASA 9.3(2), 9.3(3) (5506-X only) Due to CSCuv91730, we recommend that you upgrade to 9.3(3.8) or 9.4(2) and later.	**YES**	**YES**	—	—	—	—	—

ASA FirePOWER Version	ASDM Version (for local mgmt)	ASA Version	ASA Model						
			5506-X Series	5508-X 5516-X	5512-X	5515-X	5525-X 5545-X 5555-X	5585-X (See below for SSP notes)	ISA 3000
5.4.0.2+	—	ASA 9.14(x) (No 5512-X, 5515-X, 5585-X) ASA 9.13(x) (No 5512-X, 5515-X, 5585-X) ASA 9.12(x) ASA 9.10(x) ASA 9.9(x) ASA 9.8(x) ASA 9.7(x) ASA 9.6(x) ASA 9.5(1.5), 9.5(2), 9.5(3) ASA 9.4(x) ASA 9.3(2), 9.3(3) Due to CSCuv91730, we recommend that you upgrade to 9.3(3.8) or 9.4(2) and later.	—	—	YES	YES	YES	YES	—
5.4.0.1	—	ASA 9.2(2.4), 9.2(3), 9.2(4) Due to CSCuv91730, we recommend that you upgrade to 9.2(4.5) and later.	—	—	YES	YES	YES	YES	—
5.3.1	—	ASA 9.2(2.4), 9.2(3), 9.2(4) Due to CSCuv91730, we recommend that you upgrade to 9.2(4.5) and later.	—	—	YES	YES	YES	YES	—

ASA 5585-X SSP Compatibility

Same level SSPs

ASA FirePOWER SSP -10, -20, -40, and -60

Requirements: Install in slot 1, with matching-level ASA SSP in slot 0

Mixed level SSPs

Support for the following combinations starts with version 5.4.0.1.

- ASA SSP-10/ASA FirePOWER SSP-40
- ASA SSP-20/ASA FirePOWER SSP-60
- ASA SSP-40/ASA FirePOWER SSP-60

Requirements: ASA SSP in slot 0, ASA FirePOWER SSP in slot 1

Note For the SSP40/60 combination, you might see an error message that this combination is not supported. You can ignore the message.

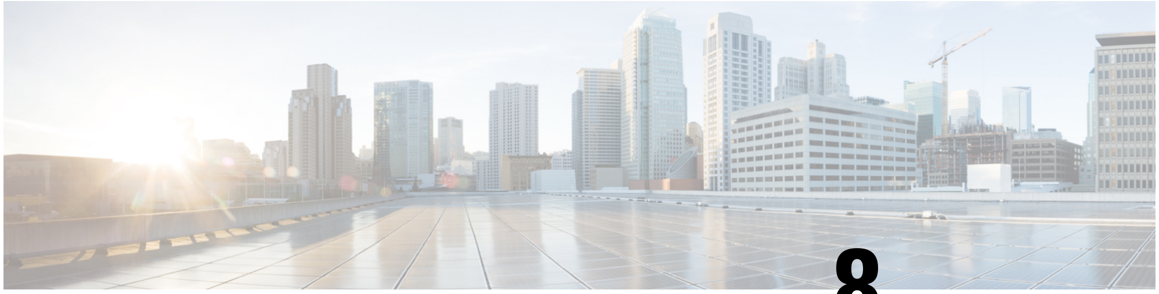
NGIPSv

This table lists Firepower compatibility and virtual hosting environment requirements for NGIPSv (virtual NGIPS devices running on VMware).

Table 53: NGIPSv Compatibility

Firepower Version	VMware vSphere/VMware ESXi							VMware vCloud Director
	7.0	6.7	6.5	6.0	5.5	5.1	5.0	5.1
7.0.x	YES	YES	YES	—	—	—	—	—
6.7.x	—	YES	YES	YES	—	—	—	—
6.6.x	—	YES	YES	YES	—	—	—	—
6.5.0	—	YES	YES	YES	—	—	—	—
6.4.0	—	—	YES	YES	—	—	—	—
6.3.0	—	—	YES	YES	—	—	—	—
6.2.3	—	—	YES	YES	YES	—	—	—
6.2.2	—	—	—	YES	YES	—	—	—
6.2.1	—	—	—	—	—	—	—	—
6.2.0	—	—	—	YES	YES	—	—	—

Firepower Version	VMware vSphere/VMware ESXi							VMware vCloud Director
	7.0	6.7	6.5	6.0	5.5	5.1	5.0	5.1
6.1.0	—	—	—	**YES**	**YES**	—	—	—
6.0.1	—	—	—	—	**YES**	**YES**	—	—
6.0.0	—	—	—	—	**YES**	**YES**	—	—
5.4.0	—	—	—	—	**YES**	**YES**	**YES**	**YES**



CHAPTER 8

Firepower Software Upgrade Guidelines

For your convenience, this guide lists the same version-specific Firepower software upgrade guidelines as the Cisco Firepower Release Notes .

If your upgrade skips versions, guidelines for intermediate releases can apply. The checklists in this chapter help you identify all applicable guidelines—just follow the cross references/links to read about them. In this chapter, upgrade guidelines appear under the version where they *first* apply.

Important This list of guidelines does *not* replace the release notes. You *must* read the Firepower release notes for additional critical and version-specific information. For example, new and deprecated features can require pre- or post-upgrade configuration changes, or even prevent upgrade. Or, known issues (bugs) can affect upgrade. In addition, this guide is updated less frequently.

General Guidelines

Deployment Health and Communication

At all times during the process, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported.

Unresponsive Upgrades

In most cases, 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, there may be something you can do.

Starting with major and maintenance Firepower Threat Defense device upgrades *from* Version 6.7.0, you can manually cancel failed or in-progress upgrades, and retry failed upgrades. On the Firepower Management Center, use the Upgrade Status pop-up, accessible from the Device Management page and the Message Center. You can also use the Firepower Threat Defense CLI.

Note By default, an Firepower Threat Defense device will automatically revert 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.

Version 7.0.x Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 7.0.0.

Table 54: Version 7.0.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Reconnect with Cisco Threat Grid for HA FMCs, on page 147	FMC	6.4.0 through 6.7.x	7.0.0+

This checklist contains older upgrade guidelines.

Table 55: Version 7.0.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 148	Firepower 1010	6.4.0 through 6.6.x	6.7.0+
	FMCv Requires 28 GB RAM for Upgrade, on page 150	FMCv	6.2.3 through 6.5.0.x	6.6.0+
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 152	Firepower 1000 series	6.4.0.x	6.5.0+
	New URL Categories and Reputations, on page 153	Any	6.2.3 through 6.4.0.x	6.5.0+

Reconnect with Cisco Threat Grid for HA FMCs

Deployments: FMC high availability/AMP for Networks (malware detection) deployments where you submit files for dynamic analysis

Upgrading from: Version 6.4.0 through 6.7.x

Directly to: Version 7.0+

Related bug: CSCvu35704

Firepower Version 7.0 fixes an issue with FMC high availability where, after failover, the system stopped submitting files for dynamic analysis. For the fix to take effect, you must reassociate with the Cisco Threat Grid public cloud.

After you upgrade the HA pair, on the primary FMC:

1. Select **AMP** > **Dynamic Analysis Connections**.
2. Click **Associate** in the table row corresponding to the Cisco Threat Grid public cloud.

   A Cisco Threat Grid portal window opens. You do not have to sign in. The reassociation happens in the background, within a few minutes.

Version 6.7.x Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 6.7.0.

Table 56: Version 6.7.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 148	Firepower 1010	6.4.0 through 6.6.x	6.7.0+

This checklist contains older upgrade guidelines.

Table 57: Version 6.7.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: FMC with Email Alerting for Intrusion Events, on page 149	FMC	6.2.3 through 6.7.0.x	6.7.0 6.6.0, 6.6.1, or 6.6.3 All patches to these releases
	FMCv Requires 28 GB RAM for Upgrade, on page 150	FMCv	6.2.3 through 6.5.0.x	6.6.0+
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 152	Firepower 1000 series	6.4.0.x	6.5.0+

✓	Guideline	Platforms	Upgrading From	Directly To
	New URL Categories and Reputations, on page 153	Any	6.2.3 through 6.4.0.x	6.5.0+
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 161	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4.0+

Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs

Deployments: Firepower 1010

Upgrading from: Version 6.4.0 through 6.6.x

Directly to: Version 6.7.0+

For the Firepower 1010, FTD upgrades to Version 6.7.0+ will fail if you configured switch ports with a VLAN ID in the 3968–4047 range. These IDs are for internal use only.

Version 6.6.x Guidelines

There are no new upgrade guidelines for Version 6.6.x maintenance releases.

This checklist contains upgrade guidelines that are new or specific to Version 6.6.0.

Table 58: Version 6.6.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: FMC with Email Alerting for Intrusion Events, on page 149	FMC	6.2.3 through 6.7.0.x	6.7.0 6.6.0, 6.6.1, or 6.6.3 All patches to these releases
	FMCv Requires 28 GB RAM for Upgrade, on page 150	FMCv	6.2.3 through 6.5.0.x	6.6.0+

This checklist contains older upgrade guidelines.

Table 59: Version 6.6.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 152	Firepower 1000 series	6.4.0.x	6.5.0+
	New URL Categories and Reputations, on page 153	Any	6.2.3 through 6.4.0.x	6.5.0+

✓	Guideline	Platforms	Upgrading From	Directly To
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 161	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4.0+
	Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv, on page 164	FMC NGIPSv	6.1.0 through 6.1.0.6 6.2.0 through 6.2.0.6 6.2.1 6.2.2 through 6.2.2.4 6.2.3 through 6.2.3.4	6.3.0+
	RA VPN Default Setting Change Can Block VPN Traffic, on page 165	FTD with FMC	6.2.0 through 6.2.3.x	6.3.0+
	Security Intelligence Enables Application Identification, on page 166	FMC deployments	6.1.0 through 6.2.3.x	6.3.0+
	Update VDB after Upgrade to Enable CIP Detection, on page 166	Any	6.1.0 through 6.2.3.x	6.3.0+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 167	Any	6.1.0 through 6.2.3.x	6.3.0+

Upgrade Failure: FMC with Email Alerting for Intrusion Events

Deployments: Firepower Management Center

Upgrading from: Version 6.2.3 through 6.7.0.x

Directly to: Version 6.6.0, 6.6.1, 6.6.3, or 6.7.0, as well as any patches to these releases

Related bugs: CSCvw38870, CSCvx86231

If you configured email alerting for individual intrusion events, fully disable it before you upgrade a Firepower Management Center to any of the versions listed above. Otherwise, the upgrade will fail.

You can reenable this feature after the upgrade. If you already experienced an upgrade failure due to this issue, contact Cisco TAC.

To fully disable intrusion email alerting:

1. On the Firepower Management Center, choose **Policies** > **Actions** > **Alerts**, then click **Intrusion Email**.
2. Set the **State** to **off**.
3. Next to **Rules**, click **Email Alerting per Rule Configuration** and deselect any rules.

Note which rules you deselected so you can reselect them after the upgrade.

Tip If reselecting rules would be too time consuming, contact Cisco TAC *before* you upgrade. They can guide you through saving your selections, so you can quickly reimplement them post-upgrade.

4. Save your configurations.

FMCv Requires 28 GB RAM for Upgrade

Deployments: FMCv

Upgrading from: Version 6.2.3 through 6.5.0.x

Directly to: Version 6.6.0+

All FMCv implementations now have the same RAM requirements: 32 GB recommended, 28 GB required (64 GB for FMCv 300). Upgrades to Version 6.6.0+ will fail if you allocate less than 28 GB to the virtual appliance. After upgrade, the health monitor will alert if you lower the memory allocation.

These new memory requirements enforce uniform requirements across all virtual environments, improve performance, and allow you to take advantage of new features and functionality. We recommend you do not decrease the default settings. To improve performance, you can increase a virtual appliance's memory and number of CPUs, depending on your available resources. For details on FMCv memory requirements, see the Cisco Firepower Management Center Virtual Getting Started Guide.

Note As of the Version 6.6.0 release, lower-memory instance types for cloud-based FMCv deployments (AWS, Azure) are fully deprecated. You cannot create new FMCv instances using them, even for earlier Firepower versions. You can continue running existing instances.

This table summarizes pre-upgrade requirements for lower-memory FMCv deployments.

Table 60: FMCv Memory Requirements for Version 6.6.0+ Upgrades

Platform	Pre-Upgrade Action	Details
VMware	Allocate 28 GB minimum/32 GB recommended.	Power off the virtual machine first. For instructions, see the VMware documentation.
KVM	Allocate 28 GB minimum/32 GB recommended.	For instructions, see the documentation for your KVM environment.

Platform	Pre-Upgrade Action	Details
AWS	Resize instances: • **From** c3.xlarge **to** c3.4xlarge. • **From** c3.2.xlarge **to** c3.4xlarge. • **From** c4.xlarge **to** c4.4xlarge. • **From** c4.2xlarge **to** c4.4xlarge. We also offer a c5.4xlarge instance for new deployments.	Stop the instance before you resize. Note that when you do this, data on the instance store volume is lost, so migrate your instance store-backed instance first. Additionally, if your management interface does not have an Elastic IP address, its public IP address is released. For instructions, see the documentation on changing your instance type in the AWS user guide for Linux instances.
Azure	Resize instances: • **From** Standard_D3_v2 **to** Standard_D4_v2.	Use the Azure portal or PowerShell. You do not need to stop the instance before you resize, but stopping may reveal additional sizes. Resizing restarts a running virtual machine. For instructions, see the Azure documentation on resizing a Windows VM.

Version 6.5.0 Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 6.5.0.

Table 61: Version 6.5.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 152	Firepower 1000 series	6.4.0.x	6.5.0+
	Disable Egress Optimization for Version 6.5.0, on page 152	FTD	6.2.3 through 6.4.0.x	6.5.0 only
	New URL Categories and Reputations, on page 153	Any	6.2.3 through 6.4.0.x	6.5.0+

This checklist contains older upgrade guidelines.

Table 62: Version 6.5.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: Insufficient Disk Space on Container Instances, on page 160	Firepower 4100/9300	6.3.0 through 6.4.0.x	6.3.0.1 through 6.5.0
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 161	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4.0+

✓	Guideline	Platforms	Upgrading From	Directly To
	Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv, on page 164	FMC Firepower 7000/8000 series NGIPSv	6.1.0 through 6.1.0.6 6.2.0 through 6.2.0.6 6.2.1 6.2.2 through 6.2.2.4 6.2.3 through 6.2.3.4	6.3.0+
	RA VPN Default Setting Change Can Block VPN Traffic, on page 165	FTD with FMC	6.2.0 through 6.2.3.x	6.3.0+
	Security Intelligence Enables Application Identification, on page 166	FMC deployments	6.1.0 through 6.2.3.x	6.3.0+
	Update VDB after Upgrade to Enable CIP Detection, on page 166	Any	6.1.0 through 6.2.3.x	6.3.0+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 167	Any	6.1.0 through 6.2.3.x	6.3.0+

Firepower 1000 Series Devices Require Post-Upgrade Power Cycle

Deployments: Firepower 1000 series

Upgrading from: Version 6.4.0.x

Directly to: Version 6.5.0+

Version 6.5.0 introduces an FXOS CLI 'secure erase' feature for Firepower 1000/2100 and Firepower 4100/9300 series devices.

For Firepower 1000 series devices, you must power cycle the device after you upgrade to Version 6.5.0+ for this feature to work properly. The automatic reboot is not sufficient. Other supported devices do not require the power cycle.

Disable Egress Optimization for Version 6.5.0

Deployments: FTD

Upgrading from: Version 6.2.3 through 6.4.0.x

Directly to: Version 6.5.0 only

To mitigate CSCvq34340, patching an FTD device to Version 6.4.0.7+ or Version 6.5.0.2+ turns off egress optimization processing. This happens regardless of whether the egress optimization feature is enabled or disabled.

Upgrading to Version 6.5.0:

- From Version 6.2.3.x: Enables and turns on egress optimization.
- From Version 6.3.0.x: Enables and turns on egress optimization.
- From Version 6.4.0.x: Respects your current settings. However, if the Version 6.4.0.x patch turned off egress optimization but the feature is still enabled, the upgrade to Version 6.5.0 turns it on again.

Note We recommend you patch to Version 6.5.0.2+ or upgrade to Version 6.6.0. If you remain at Version 6.5.0 or 6.5.0.1, you should manually disable egress optimization from the FTD CLI: **no asp inspect-dp egress-optimization**.

This issue is fixed in Version 6.6.0, where egress optimization works as expected. For more information, see the software advisory: FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature.

New URL Categories and Reputations

Deployments: Any

Upgrading from: Version 6.2.3 through 6.4.0.x

Directly to: Version 6.5.0+

Cisco Talos Intelligence Group (Talos) has introduced new categories and renamed reputations to classify and filter URLs. For detailed lists of category changes, see the Cisco Firepower Release Notes, Version 6.5.0. For descriptions of the new URL categories, see the Talos Intelligence Categories site.

Also new are the concepts of uncategorized and reputationless URLs, although rule configuration options stay the same:

- *Uncategorized URLs* can have a Questionable, Neutral, Favorable, or Trusted reputation.

  You can filter **Uncategorized** URLs but you cannot further constrain by reputation. These rules will match all uncategorized URLs, regardless of reputation.

  Note that there is no such thing as an Untrusted rule with no category. Otherwise uncategorized URLs with an Untrusted reputation are automatically assigned to the new Malicious Sites threat category.

- *Reputationless URLs* can belong to any category.

  You cannot filter reputationless URLs. There is no option in the rule editor for 'no reputation.' However, you can filter URLs with **Any** reputation, which includes reputationless URLs. These URLs must also be constrained by category. There is no utility to an Any/Any rule.

The following table summarizes the changes on upgrade. Although they are designed for minimal impact and will not prevent post-upgrade deploy for most customers, we *strongly* recommend you review these release notes and your current URL filtering configuration. Careful planning and preparation can help you avoid missteps, as well as reduce the time you spend troubleshooting post-upgrade.

Table 63: Deployment Changes on Upgrade

Change	Details
Modifies URL rule categories.	The upgrade modifies URL rules to use the nearest equivalents in the new category set, in the following policies: • Access control • SSL • QoS (FMC only) • Correlation (FMC only) These changes may create redundant or preempted rules, which can slow performance. If your configuration includes merged categories, you may experience minor changes to the URLs that are allowed or blocked.
Renames URL rule reputations.	The upgrade modifies URL rules to use the new reputation names: **1.** Untrusted (was *High Risk*) **2.** Questionable (was *Suspicious sites*) **3.** Neutral (was *Benign sites with security risks*) **4.** Favorable (was *Benign sites*) **5.** Trusted (was *Well Known*)
Clears the URL cache.	The upgrade clears the URL cache, which contains results that the system previously looked up in the cloud. Your users may temporarily experience slightly longer access times for URLs that are not in the local data set.
Labels 'legacy' events.	For already-logged events, the upgrade labels any associated URL category and reputation information as `Legacy`. These legacy events will age out of the database over time.

Pre-Upgrade Actions for URL Categories and Reputations

Before upgrade, take the following actions.

Table 64: Pre-Upgrade Actions

Action	Details
Make sure your appliances can reach Talos resources.	The system must be able to communicate with the following Cisco resources after the upgrade: • https://regsvc.sco.cisco.com/ — Registration • https://est.sco.cisco.com/ — Obtain certificates for secure communications • https://updates-talos.sco.cisco.com/ — Obtain client/server manifests • http://updates.ironport.com/ — Download database (note: uses port 80) • https://v3.sds.cisco.com/ — Cloud queries The cloud query service also uses the following IP address blocks: • IPv4 cloud queries: • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 • IPv6 cloud queries: • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
Identify potential rule issues.	Understand the upcoming changes. Examine your current URL filtering configuration and determine what post-upgrade actions you will need to take (see the next section). **Note** You may want to modify URL rules that use deprecated categories now. Otherwise, rules that use them will prevent deploy after the upgrade. In FMC deployments, we recommend you generate an *access control policy report*, which provides details on the policy's current saved configuration, including access control rules and rules in subordinate policies (such as SSL). For each URL rule, you can see the current categories, reputations, and associated rule actions. On the FMC, choose **Policies** > **Access Control** , then click the report icon (📋) next to the appropriate policy.

Post-Upgrade Actions for URL Categories and Reputations

After upgrade, you should reexamine your URL filtering configuration and take the following actions as soon as possible. Depending on deployment type and the changes made by the upgrade, some — but not all — issues may be marked in the GUI. For example, in access control policies on FMC/FDM, you can click **Show Warnings** (FMC) or **Show Problem Rules** (FDM).

Table 65: Post-Upgrade Actions

Action	Details
Remove **deprecated categories** from rules. Required.	The upgrade does not modify URL rules that use deprecated categories. Rules that use them will prevent deploy. On the FMC, these rules are marked.
Create or modify rules to include the **new categories**.	Most of the new categories identify threats. We strongly recommend you use them. On the FMC, these new categories are not marked after *this* upgrade, but Talos may add additional categories in the future. When that happens, new categories are marked.
Evaluate rules changed as a result of **merged categories**.	Each rule that included any of the affected categories now include all of the affected categories. If the original categories were associated with different reputations, the new rule is associated with the broader, more inclusive reputation. To filter URLs as before, you may have to modify or delete some configurations; see Guidelines for Rules with Merged URL Categories, on page 156. Depending on what changed and how your platform handles rule warnings, changes may be marked. For example, the FMC marks wholly redundant and wholly preempted rules, but not rules that have partial overlap.
Evaluate rules changed as a result of **split categories**.	The upgrade replaces each old, single category in URL rules with *all* the new categories that map to the old one. This will not change the way you filter URLs, but you can modify affected rules to take advantage of the new granularity. These changes are not marked.
Understand which categories were **renamed** or are **unchanged**.	Although no action is required, you should be aware of these changes. These changes are not marked.
Evaluate how you handle **uncategorized** and **reputationless** URLs.	Even though it is now possible to have uncategorized and reputationless URLs, you cannot still cannot filter uncategorized URLs by reputation, nor can you filter reputationless URLs. Make sure that rules that filter by the **Uncategorized** category, or by **Any** reputation, will behave as you expect.

Guidelines for Rules with Merged URL Categories

When you examine your URL filtering configuration before the upgrade, determine which of the following scenarios and guidelines apply to you. This will ensure that your post-upgrade configuration is as you expect, and that you can take quick action to resolve any issues.

Table 66: Guidelines for Rules with Merged URL Categories

Guideline	Details
Rule Order Determines Which Rule Matches Traffic	When considering rules that include the same category, remember that traffic matches the first rule in the list that includes the condition.
Categories in the Same Rule vs Categories in Different Rules	Merging categories in a single rule will merge into a single category in the rule. For example, if Category A and Category B are merging to become Category AB, and you have a rule with both Category A and Category B, then after merge the rule will have a single Category AB. Merging categories in different rules will result in separate rules with the same category in each rule after the merge. For example, if Category A and Category B are merging to become Category AB, and you have Rule 1 with Category A and Rule 2 with Category B, then after merge Rule 1 and Rule 2 will each include Category AB. How you choose to resolve this situation depends on the rule order, on the actions and reputation levels associated with the rules, on the other URL categories included in the rule, and on the non-URL conditions that are included in the rule.
Associated Action	If merged categories in different rules were associated with different actions, then after merge you may have two or more rules with different actions for the same category.
Associated Reputation Level	If a single rule includes categories that were associated with different reputation levels before merging, the merged category will be associated with the more inclusive reputation level. For example, if Category A was associated in a particular rule with **Any reputation** and Category B was associated in the same rule with reputation level **3 - Benign sites with security risks**, then after merge Category AB in that rule will be associated with **Any reputation**.
Duplicate and Redundant Categories and Rules	After merge, different rules may have the same category associated with different actions and reputation levels. Redundant rules may not be exact duplicates, but they may no longer match traffic if another rule earlier in the rule order matches instead. For example, if you have pre-merge Rule 1 with Category A that applies to Any Reputation, and Rule 2 with Category B that applies only to Reputation 1-3, then after merge, both Rule 1 and Rule 2 will have Category AB, but Rule 2 will never match if Rule 1 is higher in the rule order. On the FMC, rules with an identical category and reputation will show a warning. However, these warnings will not indicate rules that include the same category but a different reputation. Caution: Consider all conditions in the rule when determining how to resolve duplicate or redundant categories.
Other URL Categories in a Rule	Rules with merged URLs may also include other URL categories. Therefore, if a particular category is duplicated after merge, you may want to modify rather than delete these rules.

Guideline	Details
Non-URL Conditions in a Rule	Rules with merged URL categories may also include other rule conditions, such as application conditions. Therefore, if a particular category is duplicated after merge, you may want to modify rather than delete these rules.

The examples in the following table use Category A and Category B, now merged into Category AB. In two-rule examples, Rule 1 comes before Rule 2.

Table 67: Examples of Rules with Merged URL Categories

Scenario	Before Upgrade	After Upgrade
Merged categories in the same rule	Rule 1 has Category A and Category B.	Rule 1 has Category AB.
Merged categories in different rules	Rule 1 has Category A. Rule 2 has Category B.	Rule 1 has Category AB. Rule 2 has Category AB. The specific result varies by the rules' order in the list, reputation levels, and associated actions. You should also consider all other conditions in the rule when determining how to resolve any redundancy.
Merged categories in different rules have different actions (Reputation is the same)	Rule 1 has Category A set to Allow. Rule 2 has Category B set to Block. (Reputation is the same)	Rule 1 has Category AB set to Allow. Rule 2 has Category AB set to Block. Rule 1 will match all traffic for this category. Rule 2 will never match traffic, and will display a warning indicator if you show warnings after merge, because both category and reputation are the same.
Merged categories in the same rule have different reputation levels	Rule 1 includes: Category A with Reputation Any Category B with Reputation 1-3	Rule 1 includes Category AB with Reputation Any.
Merged categories in different rules have different reputation levels	Rule 1 includes Category A with Reputation Any. Rule 2 includes Category B with Reputation 1-3.	Rule 1 includes Category AB with Reputation Any. Rule 2 includes Category AB with Reputation 1-3. Rule 1 will match all traffic for this category. Rule 2 will never match traffic, but you will not see a warning indicator because the reputations are not identical.

Version 6.4.0 Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 6.4.0.

Table 68: Version 6.4.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic, on page 160	Firepower 1010	6.4.0	6.4.0.3 through 6.4.0.5
	Upgrade Failure: Insufficient Disk Space on Container Instances, on page 160	Firepower 4100/9300	6.3.0 through 6.4.0.x	6.3.0.1 through 6.5.0
	Upgrade Failure: NGIPS Devices Previously at Version 6.2.3.12, on page 160	Firepower 7000/8000 series ASA FirePOWER NGIPSv	6.2.3 through 6.3.0.x	6.4.0 only
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 161	Firepower 2100 series Firepower 4100/9300	6.1.0 through 6.3.0.x	6.4.0+

This checklist contains older upgrade guidelines.

Table 69: Version 6.4.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv, on page 164	FMC Firepower 7000/8000 series NGIPSv	6.1.0 through 6.1.0.6 6.2.0 through 6.2.0.6 6.2.1 6.2.2 through 6.2.2.4 6.2.3 through 6.2.3.4	6.3.0+
	RA VPN Default Setting Change Can Block VPN Traffic, on page 165	FTD with FMC	6.2.0 through 6.2.3.x	6.3.0+
	Security Intelligence Enables Application Identification, on page 166	FMC deployments	6.1.0 through 6.2.3.x	6.3.0+

✓	Guideline	Platforms	Upgrading From	Directly To
	Update VDB after Upgrade to Enable CIP Detection, on page 166	Any	6.1.0 through 6.2.3.x	6.3.0+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 167	Any	6.1.0 through 6.2.3.x	6.3.0+
	Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade, on page 169	FTD clusters	6.1.0.x	6.2.3 through 6.4.0
	Access Control Can Get Latency-Based Performance Settings from SRUs, on page 170	FMC	6.1.0.x	6.2.0 through 6.4.0
	'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 171	FTD with FMC	6.1.0.x	6.2.0 through 6.4.0

EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic

Deployments: Firepower 1010 with FTD

Affected Versions: Version 6.4.0 to 6.4.0.5

Related Bug: CSCvq81354

We *strongly* recommend you do not configure EtherChannels on Firepower 1010 devices running FTD Version 6.4.0 to Version 6.4.0.5. (Note that Versions 6.4.0.1 and 6.4.0.2 are not supported on this model.)

Due to an internal traffic hashing issue, some EtherChannels on Firepower 1010 devices may blackhole some egress traffic. The hashing is based on source/destination IP address so the behavior will be consistent for a given source/destination IP pair. That is, some traffic consistently works and some consistently fails.

This issue is fixed in Version 6.4.0.6 and Version 6.5.0.

Upgrade Failure: Insufficient Disk Space on Container Instances

Deployments: Firepower 4100/9300 with FTD

Upgrading from: Version 6.3.0 through 6.4.0.x

Directly to: Version 6.3.0.1 through Version 6.5.0

Most often during major upgrades — but possible while patching — FTD devices configured with container instances can fail in the precheck stage with an erroneous insufficient-disk-space warning.

If this happens to you, you can try to free up more disk space. If that does not work, contact Cisco TAC.

Upgrade Failure: NGIPS Devices Previously at Version 6.2.3.12

Deployments: 7000/8000 series, ASA FirePOWER, NGIPSv

Related bug: CSCvp42398

Upgrading from: Version 6.2.3 through 6.3.0.x

Directly to: Version 6.4.0 only

You cannot upgrade an NGIPS device to Version 6.4.0 if:

- The device previously ran Version 6.2.3.12, and then
- You uninstalled the Version 6.2.3.12 patch, or upgraded to Version 6.3.0.x.

  This also includes scenarios where you uninstalled the Version 6.2.3.12 patch *and then* upgraded to Version 6.3.0.x.

If this is your current situation, contact Cisco TAC.

TLS Crypto Acceleration Enabled/Cannot Disable

Deployments: Firepower 2100 series, Firepower 4100/9300 chassis

Upgrading from: Version 6.1.0 through 6.3.x

Directly to: Version 6.4.0+

SSL hardware acceleration has been renamed *TLS crypto acceleration*.

Depending on the device, TLS crypto acceleration might be performed in software or in hardware. The upgrade automatically enables acceleration on all eligible devices, even if you previously disabled the feature manually. In most cases you cannot configure this feature; it is automatically enabled and you cannot disable it.

Upgrading to Version 6.4.0: If you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can use the FXOS CLI to enable TLS crypto acceleration for *one* container instance per module/security engine. Acceleration is disabled for other container instances, but enabled for native instances.

Upgrading to Version 6.5.0+: If you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can use the FXOS CLI to enable TLS crypto acceleration for multiple container instances (up to 16) on a Firepower 4100/9300 chassis. New instances have this feature enabled by default. However, the upgrade does *not* enable acceleration on existing instances. Instead, use the **config hwCrypto enable** CLI command.

Version 6.3.0 Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 6.3.0.

Table 70: Version 6.3.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Renamed Upgrade and Installation Packages, on page 163	FMC Firepower 7000/8000 series NGIPSv	Any	6.3.0+

✓	Guideline	Platforms	Upgrading From	Directly To
	Reimaging to Version 6.3+ Disables LOM on Most Appliances, on page 164	FMC (physical) Firepower 7000/8000 series	Any	6.3.0+
	Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv, on page 164	FMC Firepower 7000/8000 series NGIPSv	6.2.3 through 6.2.3.4 6.2.2 through 6.2.2.4 6.2.1 6.2.0 through 6.2.0.6 6.1.0 through 6.1.0.6	6.3.0+
	RA VPN Default Setting Change Can Block VPN Traffic, on page 165	FTD with FMC	6.2.0 through 6.2.3.x	6.3.0+
	TLS/SSL Hardware Acceleration Enabled on Upgrade, on page 165	Firepower 2100 series Firepower 4100/9300	6.1.0 through 6.2.3.x	6.3.0 only
	Upgrade Failure: Version 6.3.0-83 Upgrades to FMC and ASA FirePOWER, on page 166	FMC ASA FirePOWER with ASDM	6.1.0 through 6.2.3.x	6.3.0 only
	Security Intelligence Enables Application Identification, on page 166	FMC deployments	6.1.0 through 6.2.3.x	6.3.0+
	Update VDB after Upgrade to Enable CIP Detection, on page 166	Any	6.1.0 through 6.2.3.x	6.3.0+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 167	Any	6.1.0 through 6.2.3.x	6.3.0+
	Firepower 4100/9300 Requires FTD Push Before FXOS Upgrade, on page 167	Firepower 4100/9300	6.1.0.x	6.3.0 only

This checklist contains older upgrade guidelines.

Table 71: Version 6.3.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade, on page 169	FTD clusters	6.1.0.x	6.2.3 through 6.4.0

✓	Guideline	Platforms	Upgrading From	Directly To
	Access Control Can Get Latency-Based Performance Settings from SRUs, on page 170	FMC	6.1.0.x	6.2.0 through 6.4.0
	'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 171	FTD with FMC	6.1.0.x	6.2.0 through 6.4.0

Renamed Upgrade and Installation Packages

Deployments: FMC, 7000/8000 series, NGIPSv

Upgrading from: Version 6.1.0 through 6.2.3.x

Directly to: Version 6.3+

The naming scheme (that is, the first part of the name) for upgrade, patch, hotfix, and installation packages changed starting with Version 6.3.0, on select platforms.

Note This change causes issues with reimaging older *physical* appliances: DC750, 1500, 2000, 3500, and 4000, as well as 7000/8000 series devices and AMP models. If you are currently running Version 5.x and need to freshly install Version 6.3.0 or 6.4.0 on one of these appliances, rename the installation package to the "old" name after you download it from the Cisco Support & Download site. You cannot reimage these appliances to Version 6.5+.

Table 72: Naming Schemes: Upgrade, Patch, and Hotfix Packages

Platform	Naming Schemes
FMC	**New:** Cisco_Firepower_Mgmt_Center **Old:** Sourcefire_3D_Defense_Center_S3
Firepower 7000/8000 series	**New:** Cisco_Firepower_NGIPS_Appliance **Old:** Sourcefire_3D_Device_S3
NGIPSv	**New:** Cisco_Firepower_NGIPS_Virtual **Old:** Sourcefire_3D_Device_VMware **Old:** Sourcefire_3D_Device_Virtual64_VMware

Table 73: Naming Schemes: Installation Packages

Platform	Naming Schemes
FMC (physical)	**New:** Cisco_Firepower_Mgmt_Center **Old:** Sourcefire_Defense_Center_M4 **Old:** Sourcefire_Defense_Center_S3

Platform	Naming Schemes
FMCv: VMware	**New:** Cisco_Firepower_Mgmt_Center_Virtual_VMware **Old:** Cisco_Firepower_Management_Center_Virtual_VMware
FMCv: KVM	**New:** Cisco_Firepower_Mgmt_Center_Virtual_KVM **Old:** Cisco_Firepower_Management_Center_Virtual
Firepower 7000/8000 series	**New:** Cisco_Firepower_NGIPS_Appliance **Old:** Sourcefire_3D_Device_S3
NGIPSv	**New:** Cisco_Firepower_NGIPSv_VMware **Old:** Cisco_Firepower_NGIPS_VMware

Reimaging to Version 6.3+ Disables LOM on Most Appliances

Deployments: Physical FMCs, 7000/8000 series devices

Reimaging from: Version 6.0+

Directly to: Version 6.3+

Freshly installing Version 6.3+ now automatically deletes Lights-Out Management (LOM) settings on most appliances, for security reasons. On a few older FMC models, you have the option of retaining LOM settings along with your management network settings.

If you delete network settings during a Version 6.3+ reimage, you *must* make sure you have physical access to the appliance to perform the initial configuration. You cannot use LOM. After you perform the initial configuration, you can reenable LOM and LOM users.

Table 74: Reimage Effect on LOM Settings

Platform	Reimage to Version 6.2.3 or earlier	Reimage to Version 6.3+
MC1600, 2600, 4600 MC1000, 2500, 4500 MC2000, 4000	Never deleted	Always deleted
MC750, 1500, 3500	Deleted if you delete network settings	Deleted if you delete network settings
7000/8000 series	Always deleted	Always deleted

Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv

Deployments: FMC, 7000/8000 series devices, NGIPSv

Upgrading from: Version 6.1.0 through 6.1.0.6, Version 6.2.0 through 6.2.0.6, Version 6.2.1, Version 6.2.2 through 6.2.2.4, and Version 6.2.3 through 6.2.3.4

Directly to: Version 6.3.0+

You cannot run the readiness check on the listed models when upgrading from one of the listed Firepower versions. This occurs because the readiness check process is incompatible with newer upgrade packages.

Table 75: Patches with Readiness Checks for Version 6.3.0+

Readiness Check Not Supported	First Patch with Fix
6.1.0 through 6.1.0.6	6.1.0.7
6.2.0 through 6.2.0.6	6.2.0.7
6.2.1	None. Upgrade to Version 6.2.3.5+.
6.2.2 through 6.2.2.4	6.2.2.5
6.2.3 through 6.2.3.4	6.2.3.5

RA VPN Default Setting Change Can Block VPN Traffic

Deployments: Firepower Threat Defense configured for remote access VPN

Upgrading from: Version 6.2.x

Directly to: Version 6.3+

Version 6.3 changes the default setting for a hidden option, **sysopt connection permit-vpn**. Upgrading can cause your remote access VPN to stop passing traffic. If this happens, use either of these techniques:

- Create a FlexConfig object that configures the **sysopt connection permit-vpn** command. The new default for this command is **no sysopt connection permit-vpn**.

  This is the more secure method to allow traffic in the VPN, because external users cannot spoof IP addresses in the remote access VPN address pool. The downside is that the VPN traffic will not be inspected, which means that intrusion and file protection, URL filtering, or other advanced features will not be applied to the traffic.

- Create access control rules to allow connections from the remote access VPN address pool.

  This method ensures that VPN traffic is inspected and advanced services can be applied to the connections. The downside is that it opens the possibility for external users to spoof IP addresses and thus gain access to your internal network.

TLS/SSL Hardware Acceleration Enabled on Upgrade

Deployments: Firepower 2100 series, Firepower 4100/9300 chassis

Upgrading from: Version 6.1.0 through 6.2.3.x

Directly to: Version 6.3.0 only

The upgrade process automatically enables TLS/SSL hardware acceleration (sometimes called *TLS crypto acceleration*) on eligible devices. When it was introduced in Version 6.2.3, this feature was disabled by default on Firepower 4100/9300 chassis, and was not available on Firepower 2100 series devices.

Using TLS/SSL hardware acceleration on a managed device that is not decrypting traffic can affect performance. In Version 6.3.0.x, we recommend you disable this feature on devices that are not decrypting traffic.

To disable, use this CLI command:

```
system support ssl-hw-offload disable
```

Upgrade Failure: Version 6.3.0-83 Upgrades to FMC and ASA FirePOWER

Deployments: Firepower Management Center, ASA FirePOWER (locally managed)

Upgrading from: Version 6.1.0 through 6.2.3.x

Directly to: Version 6.3.0-83

Some Firepower Management Centers and locally (ASDM) managed ASA FirePOWER modules experienced upgrade failures with Version 6.3.0, build 83. This issue was limited to a subset of customers who upgraded from Version 5.4.x. For more information, see CSCvn62123 in the Cisco Bug Search Tool.

A new upgrade package is now available. If you downloaded the Version 6.3.0-83 upgrade package, do not use it. If you already experienced an upgrade failure due to this issue, contact Cisco TAC.

Security Intelligence Enables Application Identification

Deployments: Firepower Management Center

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

In Version 6.3, Security Intelligence configurations enable application detection and identification. If you disabled discovery in your current deployment, the upgrade process may enable it again. Disabling discovery if you don't need it (for example, in an IPS-only deployment) can improve performance.

To disable discovery you must:

- Delete all rules from your network discovery policy.
- Use only simple network-based conditions to perform access control: zone, IP address, VLAN tag, and port. Do not perform any kind of application, user, URL, or geolocation control.
- **(NEW)** Disable network and URL-based Security Intelligence by deleting all whitelists and blacklists from your access control policy's Security Intelligence configuration, including the default Global lists.
- **(NEW)** Disable DNS-based Security Intelligence by deleting or disabling all rules in the associated DNS policy, including the default Global Whitelist for DNS and Global Blacklist for DNS rules.

Update VDB after Upgrade to Enable CIP Detection

Deployments: Any

Upgrading from: Version 6.1.0 through 6.2.3.x, with VDB 299+

Directly to: Version 6.3.0+

If you upgrade while using vulnerability database (VDB) 299 or later, an issue with the upgrade process prevents you from using CIP detection post-upgrade. This includes every VDB released from June 2018 to now, even the latest VDB.

Although we always recommend you update the vulnerability database (VDB) to the latest version after you upgrade, it is especially important in this case.

To check if you are affected by this issue, try to configure an access control rule with a CIP-based application condition. If you cannot find any CIP applications in the rule editor, manually update the VDB.

Invalid Intrusion Variable Sets Can Cause Deploy Failure

Deployments: Any

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3.0+

For network variables in an intrusion variable set, any IP addresses you *exclude* must be a subset of the IP addresses you *include*. This table shows you examples of valid and invalid configurations.

Valid	Invalid
Include: 10.0.0.0/8 Exclude: 10.1.0.0/16	Include: 10.1.0.0/16 Exclude: 172.16.0.0/12 Exclude: 10.0.0.0/8

Before Version 6.3.0, you could successfully save a network variable with this type of invalid configuration. Now, these configurations block deploy with the error: `Variable set has invalid excluded values`.

If this happens, identify and edit the incorrectly configured variable set, then redeploy. Note that you may have to edit network objects and groups referenced by your variable set.

Firepower 4100/9300 Requires FTD Push Before FXOS Upgrade

Deployments: Firepower 4100/9300 with FTD

Upgrading from: Version 6.1.x on FXOS 2.0.1, 2.1.1, or 2.3.1

Directly to: Version 6.3.0 on FXOS 2.4.1

If your Firepower Management Center is running Version 6.2.3+, we strongly recommend you copy (*push*) Firepower upgrade packages to managed devices before you upgrade. This helps reduce the length of your upgrade maintenance window. For Firepower 4100/9300 with FTD, best practice is to copy before you begin the required companion FXOS upgrade.

Note We recommend that you not upgrade from Version 6.1.0 → 6.3.0. If you are running Version 6.1.0, we recommend upgrading to Version 6.2.3 on FXOS 2.3.1, and proceeding from there. If you do choose to perform this Version 6.1.0 → 6.3.0 upgrade, a push from the FMC before you upgrade FXOS is *required*.

This is because upgrading FXOS to Version 2.4.1 while still running Firepower 6.1.0 causes the device management port to flap, which in turn causes intermittent communication problems between the device and the FMC. Until you upgrade the Firepower software, you may continue to experience management port flaps. You may see 'sftunnel daemon exited' alarms, and any task that involves sustained communications—such as pushing a large upgrade package—may fail.

To upgrade Firepower 4100/9300 with FTD, always follow this sequence:

1. Upgrade the FMC to the target version.
2. Obtain the device upgrade package from the Cisco Support & Download site and upload it to the FMC.
3. Use the FMC to push the upgrade package to the device.
4. After the push completes, upgrade FXOS to the target version.
5. Immediately, use the FMC to upgrade the Firepower software on the device.

Version 6.2.3 Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 6.2.3.

Table 76: Version 6.2.3 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Edit/Resave Access Control Policies After Upgrade, on page 168	Any	6.1.0 through 6.2.2.x	6.2.3 only
	Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade, on page 169	FTD clusters	6.1.0.x	6.2.3 through 6.4.0

This checklist contains older upgrade guidelines.

Table 77: Version 6.2.3 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Access Control Can Get Latency-Based Performance Settings from SRUs, on page 170	FMC	6.1.0.x	6.2.0 through 6.4.0
	'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 171	FTD with FMC	6.1.0.x	6.2.0 through 6.4.0

Edit/Resave Access Control Policies After Upgrade

Deployments: Any

Upgrading from: Version 6.1 through 6.2.2.x

Directly to: Version 6.2.3 only

If you configured network or port objects that are used *only* in intrusion policy variable sets, deploying associated access control policies after the upgrade fails. If this happens, edit the access control policy, make a change (such as editing the description), save, and redeploy.

Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade

Deployments: Firepower Threat Defense clusters

Upgrading from: Version 6.1.x

Directly to: Version 6.2.3 through 6.4.0

Firepower Threat Defense Version 6.1.x clusters do not support inter-site clustering (you can configure inter-site features using FlexConfig starting in Version 6.2.0).

If you deployed or redeployed a Version 6.1.x cluster in FXOS 2.1.1, and you entered a value for the (unsupported) site ID, remove the site ID (set to `0`) on each unit in FXOS before you upgrade. Otherwise, the units cannot rejoin the cluster after the upgrade.

If you already upgraded, remove the site ID from each unit, then reestablish the cluster. To view or change the site ID, see the Cisco FXOS CLI Configuration Guide.

Version 6.2.2 Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 6.2.2.

Table 78: Version 6.2.2 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Security Enhancement: Signed Upgrade Packages, on page 169	Any	Any	6.2.2+
	Version 6.2.2.1+ Required for 8000 Series Security Certs Compliance, on page 170	Firepower 8000 series	6.2.0.x	6.2.2 only

Security Enhancement: Signed Upgrade Packages

Deployments: Any

Upgrading from: Version 6.2.1+

Directly to: Version 6.2.2+

So that Firepower can verify that you are using the correct files, upgrade packages from (and hotfixes to) Version 6.2.1+ are *signed* tar archives (.tar). Upgrades from earlier versions continue to use unsigned packages.

When you manually download upgrade packages from the Cisco Support & Download site—for example, for a major upgrade or in an air-gapped deployment—make sure you download the correct package. Do not untar signed (.tar) packages.

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

Version 6.2.2.1+ Required for 8000 Series Security Certs Compliance

Deployments: Firepower 8000 series devices

Upgrading from: Version 6.2.0.x

Directly to: Version 6.2.2 only

Enabling security certifications compliance (CC/UCAPL mode) on 8000 series devices running Version 6.2.2 can cause a FSIC (file system integrity check) failure. Wait until you upgrade the device to Version 6.2.2.1+.

⚠ **Caution** Because the FSIC fails, Firepower 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 6.2.0 Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 6.2.0.

Table 79: Version 6.2.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Access Control Can Get Latency-Based Performance Settings from SRUs, on page 170	FMC	6.1.0.x	6.2.0 through 6.4.0
	'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 171	FTD with FMC	6.1.0.x	6.2.0 through 6.4.0
	IAB 'All Applications' Option Removed on Upgrade, on page 171	FMC ASA FirePOWER with ASDM	6.1.0.3 or later patch	6.2.0 only
	URL Filtering Sub-site Lookups for Low-Memory Devices Disabled on Upgrade , on page 172	Any	6.1.0.1 or later patch	6.2.0 only

Access Control Can Get Latency-Based Performance Settings from SRUs

Deployments: FMC

Upgrading from: 6.1.x

Directly to: 6.2.0+

New access control policies in Version 6.2.0+ *by default* get their latency-based performance settings from the latest intrusion rule update (SRU). This behavior is controlled by a new **Apply Settings From** option. To configure this option, edit or create an access control policy, click **Advanced**, and edit the Latency-Based Performance Settings.

When you upgrade to Version 6.2.0+, the new option is set according to your current (Version 6.1.x) configuration. If your current settings are:

- Default: The new option is set to **Installed Rule Update**. When you deploy after the upgrade, the system uses the latency-based performance settings from the latest SRU. It is possible that traffic handling could change, depending on what the latest SRU specifies.
- Custom: The new option is set to **Custom**. The system retains its current performance settings. There should be no behavior change due to this option.

We recommend you review your configurations before you upgrade. From the Version 6.1.x FMC web interface, view your policies' Latency-Based Performance Settings as described earlier, and see whether the **Revert to Defaults** button is dimmed. If the button is dimmed, you are using the default settings. If it is active, you have configured custom settings.

'Snort Fail Open' Replaces 'Failsafe' on FTD

Deployments: FTD with FMC

Upgrading from: Version 6.1.x

Directly to: Version 6.2+

In Version 6.2, the Snort Fail Open configuration replaces the Failsafe option on FMC-managed Firepower Threat Defense devices. While Failsafe allows you to drop traffic when Snort is busy, traffic automatically passes without inspection when Snort is down. Snort Fail Open allows you to drop this traffic.

When you upgrade an FTD device, its new Snort Fail Open setting depends on its old Failsafe setting, as follows. Although the new configuration should not change traffic handling, we still recommend that you consider whether to enable or disable Failsafe before you upgrade.

Table 80: Migrating Failsafe to Snort Fail Open

Version 6.1 Failsafe	Version 6.2 Snort Fail Open	Behavior
Disabled (default behavior)	**Busy**: Disabled **Down**: Enabled	New and existing connections drop when the Snort process is busy and pass without inspection when the Snort process is down.
Enabled	**Busy**: Enabled **Down**: Enabled	New and existing connections pass without inspection when the Snort process is busy or down.

Note that Snort Fail Open requires Version 6.2 on the device. If you are managing a Version 6.1.x device, the FMC web interface displays the Failsafe option.

IAB 'All Applications' Option Removed on Upgrade

Deployments: FMC, ASA FirePOWER with ASDM

Upgrading from: 6.1.0.3 or later patch

Directly to: 6.2.0 only

The Intelligent Application Bypass (IAB) option '**All applications including unidentified applications**' trusts any application that exceeds any flow bypass threshold, regardless of application type, if one of the IAB inspection performance thresholds is met. The option is available in the following versions:

- Version 6.0.1.4 and later patches
- Version 6.1.0.3 and later patches
- Version 6.2.0.1 and later patches
- Version 6.2.2 and all later patches and major versions

If you upgrade from a version where the option is supported to one where it is not, the option is *removed*. Also, if you actually enabled the option and your access control policy does not contain IAB bypassable application and filter configurations, the upgraded user interface exhibits the following unexpected behaviors:

- IAB is enabled, but the **All applications including unidentified applications option** is no longer present.
- The IAB configuration page displays `1 Applications/Filters`, incorrectly indicating that you have configured one application or filter.
- The Selected Applications and Filters window in the applications and filters editor displays either `deleted` (FMC) or `Any Application` (ASDM). We recommend you delete this selection.

To restore the option, apply any Version 6.2.0.x patch, or upgrade to Version 6.2.2+ (recommended).

URL Filtering Sub-site Lookups for Low-Memory Devices Disabled on Upgrade

Deployments: Lower-memory devices performing URL filtering

Upgrading from: Version 6.1.0.3 or later patch

Directly to: Version 6.2.0 only

Due to memory limitations, some device models perform URL filtering with a smaller database of categories and reputations. This can become an issue if a URL's subsites have different URL categories and reputations than the parent site, but the device only has the parent site's data.

In Version 6.1.0.3, we changed the system's behavior so that instead of relying on the parent URL's category and reputation, the device considers these subsites to have an 'unknown' category and reputation. This forces the device to perform a cloud lookup for the subsite's data (and cache the results for next time).

Version 6.2.0 discontinues support for these subsite cloud lookups. Affected devices are:

- Firepower 7010, 7020, and 7030
- ASA 5506-X series, 5508-X, 5516-X
- ASA 5512-X, 5515-X, 5525-X

Support is reintroduced in Version 6.2.0.1.

Version 6.1.0 Guidelines

Disable the ASA REST API Before Upgrading ASA FirePOWER Modules

Deployments: ASA FirePOWER

Upgrading from: Version 6.1.0 through 6.3.0.x

Directly to: Version 6.1.0.x through 6.3.0.x

Before you upgrade a ASA FirePOWER module, use the ASA CLI to disable the ASA REST API:

no rest-api agent

If you do not disable the REST API, the upgrade fails. You can reenable it after the upgrade:

rest-api agent

ASA 5506-X series devices do not support the ASA REST API if you are also running Version 6.0.0+ of the ASA FirePOWER module.

STIG Mode Changed to UCAPL Mode

Deployments: Firepower Management Center

In Version 6.1.0, the security certifications compliance mode known as Security Technical Implementation Guide (STIG) mode is renamed to Unified Capabilities Approved Products List (UCAPL) mode. After the upgrade, a Firepower appliance that was in STIG mode will be in UCAPL mode. All of the restrictions and changes in system functionality associated with UCAPL mode will be in effect.

For more information, including information on hardening your system for UCAPL compliance, see the Security Certifications Compliance chapter of the Firepower Management Center Configuration Guide, and the guidelines for this product provided by the certifying entity.

Restore Classic Licenses After Upgrade

Deployments: Firepower Management Center

Upgrading the Firepower Management Center to Version 6.1.0 may delete or disable Classic licenses for managed NGIPSv, ASA FirePOWER, and 7000/8000 series devices. Before you begin the update, contact Cisco TAC for a script you can run to prevent this issue.

If you do not run the pre-upgrade script, after the update:

- Check and reinstall deleted licenses: Choose **System** > **Licenses** > **Classic Licenses**.
- Edit affected devices and reenable licenses: Choose **Devices** > **Device Management**.

Version 6.0.0 Guidelines

Terminology and Branding

Version 6.0.0 has major terminology and branding changes, including:

- FireSIGHT System → Firepower
- FireSIGHT Defense Center → Firepower Management Center (FMC)
- Series 3 device → 7000 series device *or* 8000 series device
- virtual managed device → NGIPSv

For more information, see the Cisco Firepower Terminology Guide.

Version 6.0.0 Preinstallation Package

For upgrades from Version 5.4.x to Version 6.0.0, Cisco provides a preinstallation package that optimizes the upgrade.

In some cases you *must* use the preinstallation package, as listed in the following table. And even when it is not required, we *strongly* recommend you include and use the Version 6.0.0 preinstallation package in your upgrade path. For more information, see FireSIGHT System Release Notes Version 6.0.0 Preinstallation.

Platform	Min. Version to Upgrade	Package Required	Package Recommended
FireSIGHT Defense Center (FMC)	5.4.1.1	5.4.1.1 to 5.4.1.5	5.4.1.6+
7000/8000 series	5.4.0.2	5.4.0.2 to 5.4.0.6	5.4.0.7+
NGIPSv	5.4.0.2	5.4.0.2 to 5.4.0.6	5.4.0.7+
ASA FirePOWER: 5.4.1.x	5.4.1.1	5.4.1.1 to 5.4.1.5	5.4.1.6+
ASA FirePOWER: 5.4.0.x	5.4.0.2	5.4.0.2 to 5.4.0.6	5.4.0.7+

Upgrade Memory for DC750, DC1500, DC3500 and Virtual Defense Center

The following FireSIGHT Defense Center models may require additional memory to run Version 6.0.0:

- DC750
- DC1500
- DC3500
- Virtual Defense Center

Because the increase in memory is driven by Cisco product requirements, Cisco makes memory upgrade kits available at no cost for customers who are entitled to run Version 6.0.0 on a qualifying DC750 or DC1500:

- Order the kit—See Field Notice: FN - 64077 - Cisco FireSIGHT and Sourcefire Defense Center Management Appliances - Memory Upgrade Required for FirePOWER Software V6.0.0 and Later
- Upgrade the memory—See Memory Upgrade Instructions for Firepower Management Centers in the *Firepower Management Center Installation Guide*.

Break Defense Center High Availability Pairs

Version 6.0.0 and Version 6.0.1 do not support high availability for Firepower Management Centers.

You cannot upgrade a Version 5.4.x high availability pair of Defense Centers to a Version 6.0.0 high availability pair of Firepower Management Centers. You must break the pair and upgrade each Defense Center individually. You can reestablish high availability with Version 6.1.0.

Disable "Retry URL Cache Miss Lookup" Option

Upgrading a Firepower Management Center to Version 6.0.0 when you are managing devices running Version 5.4.0.6, Version 5.4.1.5, or earlier may cause traffic outages and system issues.

Before you upgrade the Defense Center, disable the **Retry URL cache miss lookup** option, which you set on the Advanced tab in the access control policies deployed to your devices. Then, redeploy. You can reenable the option after you upgrade your managed devices to Version 5.4.0.7+ or Version 5.4.1.6+ (or Version 6.0.0).

Update Defense Center HTTPS Certificates

If you upgrade a Version 5.4.x Defense Center that is using one of these HTTPS certificates to a Version 6.0.0 Firepower Management Center, you will not be able to log in and must contact Cisco TAC:

- Certificates generated with an RSASSA-PSS signature algorithm.

  Before you upgrade, replace with a certificate generated with either a sha1WithRSAEncryption algorithm or sha256WithRSAEncryption algorithm, or with the Defense Center default certificate. Reboot.

- Certificates generated using a public server key larger than 2048 bits.

  Before you upgrade, replace with a certificate generated with a server certificate request (CSR). Reboot.

Also, do *not* upload either of these types of certificates after you upgrade. To generate a certificate on a Version 5.4.x appliance, see Using Custom HTTPS Certificates in the *FireSIGHT System User Guide*, Version 5.4.1.

No Private AMP Cloud Support

Version 6.0.0 does not support AMP for Firepower signature lookups with the private AMP cloud. In Version 6.0.0, the system automatically submits SHA-256 signatures to the public AMP cloud. If you have a private AMP cloud and are receiving events from endpoints, the Version 6.0.0 Defense Center will continue to receive those events without any additional changes to your configuration.

Patch Guidelines by Version

These checklists contain important upgrade guidelines and warnings for Firepower patches.

Version 6.7.x.x Guidelines

This checklist contains upgrade guidelines for Version 6.7.x patches.

Table 81: Version 6.7.x.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: FMC with Email Alerting for Intrusion Events, on page 149	FMC	6.2.3 through 6.7.0.x	6.7.0 6.6.0, 6.6.1, or 6.6.3 All patches to these releases

Version 6.6.x.x Guidelines

This checklist contains upgrade guidelines for Version 6.6.x patches.

Table 82: Version 6.6.x.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: FMC with Email Alerting for Intrusion Events, on page 149	FMC	6.2.3 through 6.7.0.x	6.7.0 6.6.0, 6.6.1, or 6.6.3 All patches to these releases
	Version 6.6.0.1 FTD Upgrade with FDM Suspends HA, on page 176	FTD with FDM	6.6.0	6.6.0.1

Version 6.6.0.1 FTD Upgrade with FDM Suspends HA

Deployments: FTD with FDM, configured as a high availability pair

Upgrading from: Version 6.6.0

Directly to: Version 6.6.0.1

Related bug: CSCvv45500

After you upgrade an FDM-managed FTD device in high availability (HA) to Version 6.6.0.1, the device enters Suspended mode after the post-upgrade reboot. You must manually resume HA.

FMC deployments are not affected.

To upgrade an FDM-managed FTD HA pair to Version 6.6.0.1:

1. Upgrade the standby device.

2. When the upgrade completes and the device reboots, manually resume HA. You can use FDM or the CLI:

    - FDM: Click **Device** > **High Availability**, then select **Resume HA** from the gear menu (⚙).
    - CLI: **configure high-availability resume**

The HA status of the freshly upgraded device should return to normal, as the standby unit, after the unit negotiates with the peer.

3. Switch the active and standby peers (force failover) so the freshly upgraded device is now the active peer.
4. Repeat this procedure for the new standby peer.

For more information on configuring and managing high availability with FDM, see the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

Version 6.4.0.x Guidelines

This checklist contains upgrade guidelines for Version 6.4.0 patches.

Table 83: Version 6.4.0.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: Insufficient Disk Space on Container Instances, on page 160	Firepower 4100/9300	6.3.0 through 6.4.0.x	6.3.0.1 through 6.5.0
	EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic, on page 160	Firepower 1010	6.4.0 only	6.4.0.3 through 6.4.0.5
	Upgrade Caution: Firepower 7000/8000 Series to Version 6.4.0.9–6.4.0.11, on page 177	Firepower 7000/8000 series	6.4.0 through 6.4.0.10	6.4.0.9 through 6.4.0.11

Upgrade Caution: Firepower 7000/8000 Series to Version 6.4.0.9–6.4.0.11

Deployments: Firepower 7000/8000 series

Upgrading From: Version 6.4.0 through 6.4.0.10

Directly To: Version 6.4.0.9 through 6.4.0.11

Related Bug: CSCvw01028

If your Firepower 7000/8000 series device *ever* ran a version older than Version 6.4.0, do not upgrade to Version 6.4.0.9, 6.4.0.10, or 6.4.0.11. Otherwise, your device may become unresponsive and you will be forced to reimage. Instead, upgrade to Version 6.4.0.12+.

If you are already running one of the affected versions and you are vulnerable to this issue, you should contact Cisco TAC for a hotfix, then upgrade to Version 6.4.0.12 as soon as possible. You can also reimage and upgrade.

Version 6.3.0.x Guidelines

This checklist contains upgrade guidelines for Version 6.3.0 patches.

Table 84: Version 6.3.0.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: Insufficient Disk Space on Container Instances, on page 160	Firepower 4100/9300	6.3.0 through 6.4.0.x	6.3.0.1 through 6.5.0

Version 6.2.3.x Guidelines

This checklist contains upgrade guidelines for Version 6.2.3 patches.

Table 85: Version 6.2.3.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure, on page 178	FTD	6.2.3 through 6.2.3.9	6.2.3.10 only
	Version 6.2.3.3 FTD Device Cannot Switch to Local Management, on page 178	FTD with FMC	6.2.3 through 6.2.3.2	6.2.3.3
	Hotfix Before Upgrading Version 6.2.3-88 FMCs, on page 179	FMC	6.2.3-88	6.2.3.1 through 6.2.3.3

Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure

Deployments: Firepower Threat Defense

Upgrading from: Version 6.2.3 through 6.2.3.9

Directly to: Version 6.2.3.10 only

Known issue: CSCvo39052

Upgrading an FTD device to Version 6.2.3.10 with CC mode enabled causes a FSIC (file system integrity check) failure when the device reboots.

⚠

Caution If security certifications compliance is enabled and the FSIC fails, Firepower 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.

If your FTD deployment requires security certifications compliance (CC mode), we recommend you upgrade directly to Version 6.2.3.13+. For Firepower 4100/9300 devices, we also recommend that you upgrade to FXOS 2.3.1.130+.

Version 6.2.3.3 FTD Device Cannot Switch to Local Management

Deployments: FTD wth FMC

Upgrading from: Version 6.2.3 through Version 6.2.3.2

Directly to: Version 6.2.3.3 only

In Version 6.2.3.3, you cannot switch Firepower Threat Defense device management from FMC to FDM. This happens even if you uninstall the Version 6.2.3.3 patch. If you want to switch to local management at that point, either freshly install Version 6.2.3, or contact Cisco TAC.

As a workaround, switch management before you upgrade to Version 6.2.3.3. Or, upgrade to the latest patch. Keep in mind that you lose device configurations when you switch management.

Note that you can switch management from FDM to FMC in Version 6.2.3.3.

Hotfix Before Upgrading Version 6.2.3-88 FMCs

Deployments: FMC

Upgrading from: Version 6.2.3-88

Directly to: Version 6.2.3.1, Version 6.2.3.2, or Version 6.2.3.3

Sometimes Cisco releases updated builds of Firepower upgrade packages. Version 6.2.3-88 has been replaced by a later build. If you upgrade an FMC running Version 6.2.3-88 to Version 6.2.3.1, Version 6.2.3.2, or Version 6.2.3.3, the SSE cloud connection continuously drops and generates errors. Uninstalling the patch does not resolve the issue.

If you are running Version 6.2.3-88, install Hotfix T before you upgrade.

Version 6.2.2.x Guidelines

This checklist contains upgrade guidelines for Version 6.2.2 patches.

Table 86: Version 6.2.2.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Cannot Upgrade Firepower 2100 Series HA Pair from Version 6.2.2 to 6.2.2.4, on page 179	Firepower 2100 series HA pair	6.2.2 only	6.2.2.4 only

Cannot Upgrade Firepower 2100 Series HA Pair from Version 6.2.2 to 6.2.2.4

Deployments: Firepower 2100 series devices configured as an FTD high availability pair

Upgrading from: Version 6.2.2 only

Directly to: Version 6.2.2.4 only

The upgrade from Version 6.2.2 to Version 6.2.2.4 fails for Firepower 2100 devices in high availability. If you are running Version 6.2.2 and really need to be at Version 6.2.2.4, upgrade to Version 6.2.2.1 first. Otherwise, we recommend you skip this version.

If you already started the upgrade and it has failed, we recommend you reimage.

Version 6.2.0.x Guidelines

This checklist contains upgrade guidelines for Version 6.2.0 patches.

Table 87: Version 6.2.0.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Apply Hotfix BH to Version 6.2.0.3 FMCs, on page 180	FMC	6.2.0 through 6.2.0.2	6.2.0.3 only

Apply Hotfix BH to Version 6.2.0.3 FMCs

Deployments: FMC

Upgrading from: Version 6.2 through 6.2.0.2

Directly to: Version 6.2.0.3 only

Resolves: CSCvg32885

After you upgrade to Version 6.2.0.3, you must apply Hotfix BH. If you do not apply Hotfix BH, you cannot edit access control rules or deploy configuration changes.

For more information, see the Firepower Hotfix Release Notes.

Date-Based Guidelines

Sometimes Cisco issues date-based upgrade guidelines and warnings.

Expired CA Certificates for Dynamic Analysis

Deployments: AMP for Networks (malware detection) deployments where you submit files for dynamic analysis

Affected Versions: Version 6.0+

Resolves: CSCvj07038

On June 15, 2018, some Firepower deployments stopped being able to submit files for dynamic analysis. This occurred due to an expired CA certificate that was required for communications with the AMP Threat Grid cloud. Version 6.3.0 is the first major version with the new certificate.

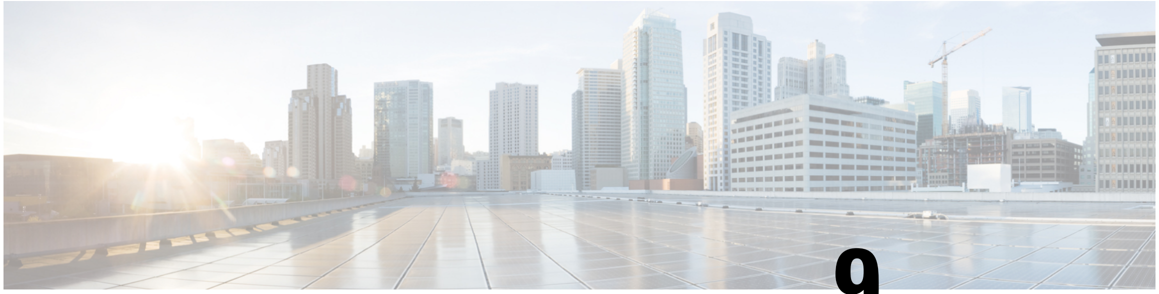
Note If you do not want to upgrade to Version 6.3.0+, you must patch or hotfix to obtain the new certificate and reenable dynamic analysis. However, subsequently upgrading a patched or hotfixed deployment to either Version 6.2.0 or Version 6.2.3 reverts to the old certificate and you must patch or hotfix again.

If this is your first time installing the patch or hotfix, make sure your firewall allows outbound connections to `fmc.api.threatgrid.com` (replacing `panacea.threatgrid.com`) from both the FMC and its managed devices. Managed devices submit files to the cloud for dynamic analysis; the FMC queries for results.

This table lists the versions with the old certificates, as well as the patches and hotfixes that contain the new certificates, for each major version sequence and platform. Patches and hotfixes are available on the Cisco Support & Download site.

Table 88: Patches and Hotfixes with New CA Certificates

Versions with Old Cert	First Patch with New Cert	Hotfix with New Cert	
6.2.3 through 6.2.3.3	6.2.3.4	Hotfix G	FTD devices
		Hotfix H	FMC, NGIPS devices
6.2.2 through 6.2.2.3	6.2.2.4	Hotfix BN	All platforms
6.2.1	None. You must upgrade.	None. You must upgrade.	
6.2.0 through 6.2.0.5	6.2.0.6	Hotfix BX	FTD devices
		Hotfix BW	FMC, NGIPS devices
6.1.0 through 6.1.0.6	6.1.0.7	Hotfix EM	All platforms
6.0.x	None. You must upgrade.	None. You must upgrade.	



CHAPTER 9

Time Tests and Disk Space Requirements

To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. You must also have enough time to perform the upgrade. We provide reports of in-house time and disk space tests for reference purposes.

About Time Tests

Time values are based on in-house tests.

Although we report the *slowest* time of all upgrades tested for a particular platform/series, your upgrade will likely take longer than the provided times for multiple reasons, as follows.

Table 89: Time Test Conditions

Condition	Details
Deployment	Values are from tests in a Firepower Management Center deployment. 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.
Models	In most cases, we test on the lowest-end models in each series, and sometimes on multiple models in a series.
Virtual settings	We test with the default settings for memory and resources.
High availability and 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. Note that stacked 8000 series devices upgrade simultaneously, with the stack operating in limited, mixed-version state until all devices complete the upgrade. This should not take significantly 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.

Condition	Details
Components	Values represent *only* the time it takes for the Firepower software upgrade script. They do not include time for: • Operating system upgrades. • Transferring upgrade packages. • Readiness checks. • VDB and intrusion rule (SRU/LSP) updates. • Deploying configurations. • Reboots, although reboot time may be provided separately.

About Disk Space Requirements

Space estimates are the *largest* reported for all Firepower software upgrades. For releases after early 2020, they are:

- Not rounded up (under 1 MB).
- Rounded up to the next 1 MB (1 MB - 100 MB).
- Rounded up to the next 10 MB (100 MB - 1GB).
- Rounded up to the next 100 MB (greater than 1 GB).

Values represent *only* the space needed to upload and run the Firepower software upgrade script. They do not include values for operating system upgrades, VDB or intrusion rule (SRU/LSP) updates, and so on.

Note When you use the Firepower Management Center to upgrade a managed device, the Firepower Management Center requires additional disk space in /Volume for the device upgrade package (unless you configure an internal web server where your devices can get the package; requires Firepower Threat Defense Version 6.6.0+) .

Checking Disk Space

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.

To check disk space for the Firepower Management Center and its managed devices, use the **System** > **Monitoring** > **Statistics** page on the FMC. After you select the appliance you want to check, under Disk Usage, expand the By Partition details.

Version 7.0.0 Time and Disk Space

Table 90: Version 7.0.0 Time and Disk Space

Platform	Local Space	Space on FMC	Upgrade Time	Reboot Time
FMC	14 GB in /Volume 70 MB in /	—	41 min	7 min
FMCv	16 GB in /Volume 72 MB in /	—	28 min	4 min
Firepower 1000 series	420 MB in /ngfw/var 7.6 GB	890 MB	12 min	14 min
Firepower 2100 series	480 MB in /ngfw/Volume 7.7 GB in /ngfw	950 MB	11 min	13 min
Firepower 9300	45 MB in /ngfw/Volume 11.1 GB in /ngfw	830 MB	11 min	11 min
Firepower 4100 series	40 MB in /ngfw/Volume 8.4 GB in /ngfw	830 MB	8 min	9 min
Firepower 4100 series container instance	36 MB in /ngfw/Volume 9.7 GB in /ngfw	830 MB	8 min	7 min
ASA 5500-X series with FTD	5.3 GB in /ngfw/Volume 95 KB in /ngfw	1.1 GB	25 min	12 min
FTDv	6.6 GB in /ngfw/Volume 23 KB in /ngfw	1.1 GB	11 min	6 min
ASA FirePOWER	9.5 GB in /var 64 MB in /	1.1 GB	69 min	8 min
NGIPSv	5 GB in /var 54 MB in /	720 MB	8 min	4 min

Version 6.7.0.2 Time and Disk Space

Table 91: Version 6.7.0.2 Time and Disk Space

Platform	Local Space		Space on FMC	Upgrade Time from 6.7.0	Reboot Time
FMC	2.3 GB 20 MB	in /Volume in /	—	35 min	7 min
FMCv: VMware 6.0	2.4 GB 23 MB	in /Volume in /	—	28 min	2 min
Firepower 1000 series	3 GB	in /ngfw	610 MB	8 min	13 min
Firepower 2100 series	3GB	in /ngfw	660 MB	6 min	14 min
Firepower 9300	2.6 GB	in /ngfw	410 MB	5 min	7 min
Firepower 4100 series	2.4 GB	in /ngfw	410 MB	4 min	7 min
Firepower 4100 series container instance	2.3 GB	in /	410 MB	5 min	4 min
ASA 5500-X series with FTD	2.2 GB 110 MB	in /ngfw/Volume in /ngfw	370 MB	10 min	7 min
ISA 3000 with FTD	2.3 GB 110 MB	in /ngfw/Volume in /ngfw	370 MB	17 min	9 min
FTDv: VMware 6.0	2.2 GB 110 MB	in /ngfw/Volume in /ngfw	370 MB	6 min	4 min
FTDv: KVM	2.2 GB 110 MB	in /ngfw/Volume in /ngfw	370 MB	6 min	8 min
ASA FirePOWER	3 GB 21 MB	in /var in /	430 MB	73 min	4 min
NGIPSv: VMware 6.0	930 MB 19 MB	in /var in /	290 MB	5 min	3 min

Version 6.7.0.1 Time and Disk Space

Table 92: Version 6.7.0.1 Time and Disk Space

Platform	Local Space		Space on FMC	Upgrade Time from 6.7.0	Reboot Time
FMC	1.8 GB 20 MB	in /Volume in /	—	32 min	7 min
FMCv: VMware 6.0	1.4 GB 23 MB	in /Volume in /	—	28 min	5 min
Firepower 1000 series	1.4 GB	in /ngfw	340 MB	7 min	12 min
Firepower 2100 series	1.4 GB	in /ngfw	400 MB	7 min	12 min
Firepower 9300	710 MB	in /ngfw	130 MB	5 min	7 min
Firepower 4100 series	700 MB	in /ngfw	130 MB	4 min	5 min
Firepower 4100 series container instance	480 MB	in /	130 MB	5 min	2 min
ASA 5500-X series with FTD	540 MB 110 MB	in /ngfw/Volume in /ngfw	88 MB	10 min	12 min
ISA 3000 with FTD	540 MB 110 MB	in /ngfw/Volume in /ngfw	88 MB	13 min	7 min
FTDv: VMware 6.0	530 MB 110 MB	in /ngfw/Volume in /ngfw	88 MB	6 min	4 min
FTDv: KVM	550 MB 110 MB	in /ngfw/Volume in /ngfw	88 MB	7 min	3 min
ASA FirePOWER	1.2 GB 21 MB	in /var in /	41 MB	66 min	2 min
NGIPSv: VMware 6.0	82 MB 18 MB	in /var in /	9 MB	6 min	3 min

Version 6.7.0 Time and Disk Space

Table 93: Version 6.7.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time	Reboot Time
FMC	13.6 GB	70 MB	—	46 min	9 min
FMCv: VMware 6.0	15.5 GB	64 MB	—	35 min	8 min
Firepower 1000 series	430 MB	11 GB	2 GB	17 min	16 min
Firepower 2100 series	500 MB	11 GB	1.1 GB	15 min	16 min
Firepower 9300	64 MB	11.1 GB	1.1 GB	13 min	12 min
Firepower 4100 series	10 MB	10 GB	1.1 GB	10 min	12 min
Firepower 4100 series container instance	8 MB	9.5 GB	1.1 GB	10 min	9 min
ASA 5500-X series with FTD	8.7 GB	96 KB	1.1 GB	26 min	13 min
FTDv: VMware 6.0	8.1 GB	26 KB	1.1 GB	14 min	18 min
ASA FirePOWER	10.3 GB	64 MB	1.3 GB	62 min	11 min
NGIPSv: VMware 6.0	5.5 GB	54 MB	840 MB	10 min	6 min

Version 6.6.4 Time and Disk Space

Table 94: Version 6.6.4 Time and Disk Space

Platform	Local Space		Space on FMC	Upgrade Time	Reboot Time
FMC	15.1 GB 23 MB	in /Volume in /	—	60 min	28 min
FMCv: VMware 6.0	23.7 GB 29 MB	in /var in /	—	43 min	8 min

Platform	Local Space		Space on FMC	Upgrade Time	Reboot Time
Firepower 1000 series	9.7 GB 400 MB	in /ngfw/var in /ngfw	1 GB	21 min	16 min
Firepower 2100 series	10.1 GB 450 MB	in /ngfw/var in /ngfw	1 GB	21 min	13 min
Firepower 9300	10.1 GB 11 MB	in /ngfw/var in /ngfw	970 MB	14 min	10 min
Firepower 4100 series	8.9 GB 11 MB	in /ngfw/var in /ngfw	970 MB	11 min	9 min
Firepower 4100 series container instance	10.9 GB 10 MB	in /ngfw/var in /ngfw	970 MB	10 min	7 min
ASA 5500-X series with FTD	8.5 GB 756 KB	in /ngfw/var in /ngfw	1.2 GB	20 min	19 min
FTDv: VMware 6.0	7.7 GB 756 KB	in /ngfw/var in /ngfw	1.2 GB	19 min	12 min
ASA FirePOWER	11.4 GB 26 MB	in /var in /	1.3 GB	59 min	16 min
NGIPSv: VMware 6.0	7.4 GB 21 MB	in /var in /	870 MB	13 min	8 min

Version 6.6.3 Time and Disk Space

Table 95: Version 6.6.3 Time and Disk Space

Platform	Local Space		Space on FMC	Upgrade Time	Reboot Time
FMC	15.1 GB 23 MB	in /Volume in /	—	60 min	28 min
FMCv: VMware 6.0	23.7 GB 29 MB	in /var in /	—	43 min	8 min
Firepower 1000 series	9.7 GB 400 MB	in /ngfw/var in /ngfw	1 GB	21 min	16 min

Platform	Local Space		Space on FMC	Upgrade Time	Reboot Time
Firepower 2100 series	10.1 GB 450 MB	in /ngfw/var in /ngfw	1 GB	21 min	13 min
Firepower 9300	10.1 GB 11 MB	in /ngfw/var in /ngfw	970 MB	14 min	10 min
Firepower 4100 series	8.9 GB 11 MB	in /ngfw/var in /ngfw	970 MB	11 min	9 min
Firepower 4100 series container instance	10.9 GB 10 MB	in /ngfw/var in /ngfw	970 MB	10 min	7 min
ASA 5500-X series with FTD	8.5 GB 756 KB	in /ngfw/var in /ngfw	1.2 GB	20 min	19 min
FTDv: VMware 6.0	7.7 GB 756 KB	in /ngfw/var in /ngfw	1.2 GB	19 min	12 min
ASA FirePOWER	11.4 GB 26 MB	in /var in /	1.3 GB	59 min	16 min
NGIPSv: VMware 6.0	7.4 GB 21 MB	in /var in /	870 MB	13 min	8 min

Version 6.6.1 Time and Disk Space

Table 96: Version 6.6.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time	Reboot Time
FMC	18.6 GB	23 MB	—	54 min	14 min
FMCv: VMware 6.0	15.8 GB	58 MB	—	56 min	13 min
Firepower 1000 series	10.8 GB	400 MB	1.1 GB	20 min	17 min
Firepower 2100 series	10.9 GB	450 MB	1.1 GB	16 min	21 min
Firepower 9300	9.8 GB	11 MB	1 GB	15 min	15 min
Firepower 4100 series	9.7 GB	10 MB	1 GB	15 min	14 min
Firepower 4100 series container instance	11.2 GB	9 MB	1 GB	10 min	13 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time	Reboot Time
ASA 5500-X series with FTD	9.3 GB	1 MB	1.2 GB	21 min	24 min
FTDv: VMware 6.0	9.3 GB	1 MB	1.2 GB	18 min	19 min
ASA FirePOWER	12.3 GB	26 MB	1.4 GB	72 min	23 min
NGIPSv: VMware 6.0	7.1 GB	54 MB	860 MB	14 min	20 min

Version 6.6.0.1 Time and Disk Space

In this table, the upgrade time includes reboot.

Table 97: Version 6.6.0.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.6.0
FMC	31 MB	20 MB	—	22 min
FMCv: VMware 6.0	1.1 GB	23 MB	—	17 min
Firepower 1000 series	450 MB	450 MB	240 MB	21 min
Firepower 2100 series	260 MB	260 MB	270 MB	17 min
Firepower 9300	460 MB	460 MB	46 MB	33 min
Firepower 4100 series	470 MB	470 MB	46 MB	11 min
ASA 5500-X series with FTD	440 MB	120 MB	46 MB	17 min
ISA 3000 with FTD	440 MB	120 MB	46 MB	21 min
FTDv: VMware 6.0	430 MB	120 MB	46 MB	11 min
ASA FirePOWER	80 MB	20 MB	15 MB	18 min
NGIPSv: VMware 6.0	64 MB	28 MB	15 MB	9 min

Version 6.6.0 Time and Disk Space

Note For ASA 5545-X with FirePOWER Services, if the SRU on the device is the *same as* or *newer than* the SRU in the Version 6.6.0 upgrade package (2020-01-16-001-vrt), the upgrade can take longer than expected—more than an hour longer. To determine if this will affect you, log into the Firepower CLI on the device and use the **show version** command to display the **Rules update version**.

Table 98: Version 6.6.0 Time and Disk Space

Platform	Local Space		Space on FMC	Upgrade Time	Reboot Time
FMC	16.5 GB 71 MB	in /Volume in /	—	46 min	15 min
FMCv: VMware 6.0	16.7 GB 57 MB	in /var in /	—	36 min	7 min
Firepower 1000 series	410 MB 11.5 GB	in /ngfw/var in /ngfw	1.1 GB	20 min	17 min
Firepower 2100 series	470 MB 10.3 GB	in /ngfw/var in /ngfw	1 GB	14 min	14 min
Firepower 9300	64 MB 8.7 GB	in /ngfw/var in /ngfw	980 MB	15 min	12 min
Firepower 4100 series	61 MB 9.3 GB	in /ngfw/var in /ngfw	980 MB	11 min	9 min
Firepower 4100 series container instance	46 MB 11.3 GB	in /ngfw/var in /ngfw	980 MB	11 min	6 min
ASA 5500-X series with FTD	8.7 GB 70 KB	in /ngfw/var in /ngfw	1.2 GB	23 min	26 min
FTDv: VMware 6.0	8.7 GB 70 KB	in /ngfw/var in /ngfw	1.2 GB	14 min	17 min
ASA FirePOWER	11.4 GB 63 MB	in /var in /	1.4 GB	93 min	10 min
NGIPSv: VMware 6.0	6.1 GB 53 MB	in /var in /	860 MB	10 min	5 min

Version 6.5.0.5 Time and Disk Space

Table 99: Version 6.5.0.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.5.0	Reboot Time
FMC	4.4 GB	28 MB	—	47 min	8 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.5.0	Reboot Time
FMCv: VMware 6.0	4.2 GB	25 MB	—	36 min	4 min
Firepower 1000 series	2.6 GB	2.6 GB	510 MB	9 min	11 min
Firepower 2100 series	2.5 GB	2.5 GB	530 MB	7 min	10 min
Firepower 4100 series	2.6 GB	2.6 GB	360 MB	5 min	8 min
Firepower 9300	2.6 GB	2.6 GB	360 MB	5 min	8 min
ASA 5500-X series with FTD	1.9 GB	120 MB	310 MB	9 min	8 min
FTDv: VMware 6.0	2.2 GB	120 MB	310 MB	7 min	6 min
ASA FirePOWER	4.3 GB	32 MB	610 MB	52 min	6 min
NGIPSv: VMware 6.0	2.2 GB	420 MB	470 MB	6 min	4 min

Version 6.5.0.4 Time and Disk Space

Table 100: Version 6.5.0.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.5.0
Firepower 1000 series	2.6 GB	2.6 GB	500 MB	20 min
Firepower 2100 series	2.5 GB	2.5 GB	530 MB	18 min
Firepower 4100 series	2.5 GB	2.5 GB	360 MB	13 min
Firepower 9300	2.5 GB	2.5 GB	360 MB	17 min
ASA 5500-X series with FTD	1.9 GB	110 MB	310 MB	16 min
FTDv: VMware 6.0	1.9 GB	110 MB	310 MB	9 min
ASA FirePOWER	2.6 GB	20 MB	340 MB	72 min
NGIPSv: VMware 6.0	740 MB	20 MB	230 MB	8 min

Version 6.5.0.3 Time and Disk Space

Version 6.5.0.3 was removed from the Cisco Support & Download site on 2019-02-04 (for FMCs) and 2020-03-02 (for devices). If you are running this version, it is safe to continue.

Version 6.5.0.2 Time and Disk Space

Table 101: Version 6.5.0.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.5.0
FMC	2.6 GB	20 MB	—	42 min
FMCv: VMware 6.0	2.7 GB	23 MB	—	34 min
Firepower 1000 series	2.5 GB	2.5 GB	480 MB	12 min
Firepower 2100 series	2.3 GB	2.3 GB	500 MB	17 min
Firepower 4100 series	2.3 GB	2.3 GB	340 MB	13 min
Firepower 9300	2.3 GB	2.3 GB	340 MB	17 min
ASA 5500-X series with FTD	1.9 GB	110 MB	280 MB	22 min
FTDv: VMware 6.0	1.7 GB	110 MB	280 MB	10 min
ASA FirePOWER	2.5 GB	20 MB	320 MB	56 min
NGIPSv: VMware 6.0	680 MB	18 MB	210 MB	9 min

Version 6.5.0.1 Time and Disk Space

Version 6.5.0.1 was removed from the Cisco Support & Download site on 2019-12-19. If you are running this version, we recommend you upgrade.

Version 6.5.0 Time and Disk Space

Table 102: Version 6.5.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	18.6 GB	24 MB	—	47 min
FMCv: VMware 6.0	18.7 GB	30 MB	—	35 min
Firepower 1000 series	1.0 GB	11.3 GB	1.1 GB	10 min
Firepower 2100 series	1.1 GB	12.3 GB	1.0 GB	12 min
Firepower 4100 series	20 MB	10.8 GB	990 MB	8 min
Firepower 9300	23 MB	10.9 GB	990 MB	8 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
ASA 5500-X series with FTD	10.4 GB	120 KB	1.1 GB	17 min
FTDv: VMware 6.0	10 GB	120 KB	1.1 GB	10 min
ASA FirePOWER	12.2 GB	26 MB	1.3 GB	81 min
NGIPSv: VMware 6.0	6.6 GB	22 MB	870 MB	9 min

Version 6.4.0.12 Time and Disk Space

Table 103: Version 6.4.0.12 Time and Disk Space

Platform	Local Space		Space on FMC	Upgrade Time from 6.4.0	Reboot Time
FMC	3.8 GB 170 MB	in /Volume in /	—	25 min	8 min
FMCv: VMware 6.0	3.8 GB 170 MB	in /Volume in /	—	27 min	4 min
Firepower 1000 series	2.9 GB	in /ngfw	530 MB	10 min	13 min
Firepower 2100 series	2.5 GB	in /ngfw	510 MB	8 min	32 min
Firepower 9300	2.5 GB	in /ngfw	440 MB	4 min	8 min
Firepower 4100 series	2.5 GB	in /ngfw	440 MB	4 min	9 min
ASA 5500-X series with FTD	1.9 GB 110 MB	in /ngfw/Volume in /ngfw	290 MB	12 min	40 min
FTDv: VMware 6.0	1.9 GB 110 MB	in /ngfw/Volume in /ngfw	290 MB	7 min	5 min
Firepower 7000/8000 series	3.7 GB 170 MB	in /var in /	660 MB	10 min	15 min
ASA FirePOWER	4.2 GB 37 MB	in /var in /	600 MB	47 min	51 min
NGIPSv: VMware 6.0	2.2 GB 150 MB	in /var in /	460 MB	7 min	5 min

Version 6.4.0.11 Time and Disk Space

Table 104: Version 6.4.0.11 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0	Reboot Time
FMC	3.8 GB	170 MB	—	30 min	8 min
FMCv: VMware 6.0	4.1 GB	170 MB	—	27 min	7 min
Firepower 1000 series	3.0 GB	3.0 GB	530 MB	14 min	9 min
Firepower 2100 series	2.5 GB	2.5 GB	510 MB	9 min	6 min
Firepower 4100 series	1.8 GB	1.8 GB	310 MB	8 min	7 min
Firepower 9300	1.8 GB	1.8 GB	310 MB	9 min	9 min
ASA 5500-X series with FTD	1.6 GB	110 MB	290 MB	12 min	12 min
FTDv: VMware 6.0	4.4 GB	170 MB	290 MB	28 min	4 min
Firepower 7000/8000 series	3.6 GB	170 MB	680 MB	11 min	97 min
ASA FirePOWER	4.2 GB	36 MB	630 MB	54 min	51 min
NGIPSv: VMware 6.0	2.4 GB	150 MB	470 MB	11 min	15 min

Version 6.4.0.10 Time and Disk Space

Table 105: Version 6.4.0.10 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0	Reboot Time
FMC	3.8 GB	170 MB	—	30 min	8 min
FMCv: VMware 6.0	4.1 GB	170 MB	—	27 min	7 min
Firepower 1000 series	2.9 GB	2.9 GB	560 MB	11 min	14 min
Firepower 2100 series	2.5 GB	2.5 GB	530 MB	8 min	13 min
Firepower 4100 series	1.8 GB	1.8 GB	330 MB	5 min	11 min
Firepower 9300	1.8 GB	1.8 GB	330 MB	5 min	17 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0	Reboot Time
ASA 5500-X series with FTD	1.9 GB	110 MB	310 MB	12 min	31 min
FTDv: VMware 6.0	2.0 GB	110 MB	310 MB	8 min	8 min
Firepower 7000/8000 series	3.6 GB	170 MB	680 MB	11 min	97 min
ASA FirePOWER	4.2 GB	36 MB	630 MB	54 min	51 min
NGIPSv: VMware 6.0	2.4 GB	150 MB	470 MB	11 min	15 min

Version 6.4.0.9 Time and Disk Space

Table 106: Version 6.4.0.9 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0	Reboot Time
FMC	3.7 GB	170 MB	—	41 min	10 min
FMCv: VMware 6.0	3.7 GB	170 MB	—	28 min	6 min
Firepower 1000 series	2.9 GB	2.9 GB	530 MB	11 min	14 min
Firepower 2100 series	2.6 GB	2.6 GB	510 MB	10 min	13 min
Firepower 4100 series	1.8 GB	1.8 GB	310 MB	4 min	10 min
Firepower 9300	1.8 GB	1.8 GB	310 MB	4 min	10 min
ASA 5500-X series with FTD	1.9 GB	290 MB	290 MB	12 min	42 min
FTDv: VMware 6.0	1.9 GB	290 MB	290 MB	7 min	9 min
Firepower 7000/8000 series	3.7 GB	170 MB	650 MB	20 min	6 min
ASA FirePOWER	4.2 GB	36 MB	600 MB	48 min	48 min
NGIPSv: VMware 6.0	2.1 GB	150 MB	450 MB	6 min	4 min

Version 6.4.0.8 Time and Disk Space

Table 107: Version 6.4.0.8 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMC	5.0 GB	170 MB	—	44 min
FMCv: VMware 6.0	5.1 GB	170 MB	—	32 min
Firepower 1000 series	3.0 GB	3.0 GB	530 MB	18 min
Firepower 2100 series	2.5 GB	2.5 GB	510 MB	18 min
Firepower 4100 series	1.8 GB	1.8 GB	310 MB	14 min
Firepower 9300	2.0 GB	2.0 GB	310 MB	11 min
ASA 5500-X series with FTD	1.8 GB	110 MB	290 MB	17 min
FTDv: VMware 6.0	1.9 GB	110 MB	290 MB	12 min
Firepower 7000/8000 series	3.7 GB	190 MB	650 MB	25 min
ASA FirePOWER	2.2 GB	110 MB	590 MB	16 min
NGIPSv: VMware 6.0	2.1 GB	150 MB	450 MB	9 min

Version 6.4.0.7 Time and Disk Space

Table 108: Version 6.4.0.7 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMC	4.9 GB	170 MB	—	41 min
FMCv: VMware 6.0	5.1 GB	170 MB	—	32 min
Firepower 1000 series	2.9 GB	2.9 GB	530 MB	17 min
Firepower 2100 series	2.4 GB	2.4 GB	500 MB	17 min
Firepower 4100 series	1.7 GB	1.7 GB	310 MB	15 min
Firepower 9300	2.4 GB	2.4 GB	310 MB	12 min
ASA 5500-X series with FTD	1.9 GB	110 MB	290 MB	18 min
FTDv: VMware 6.0	1.8 GB	110 MB	290 MB	9 min
Firepower 7000/8000 series	3.7 GB	190 MB	650 MB	28 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
ASA FirePOWER	4.2 GB	36 MB	590 MB	54 min
NGIPSv: VMware 6.0	2.3 GB	150 MB	450 MB	9 min

Version 6.4.0.6 Time and Disk Space

Version 6.4.0.6 was removed from the Cisco Support & Download site on 2019-12-19. If you are running this version, we recommend you upgrade.

Version 6.4.0.5 Time and Disk Space

Table 109: Version 6.4.0.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMC	5.0 GB	170 MB	—	39 min
FMCv: VMware 6.0	3.7 GB	170 MB	—	27 min
Firepower 1000 series	2.9 GB	2.9 GB	530 MB	26 min
Firepower 2100 series	2.5 GB	2.5 GB	500 MB	16 min
Firepower 4100 series	1.8 GB	1.8 GB	310 MB	12 min
Firepower 9300	1.8 GB	1.8 GB	310 MB	11 min
ASA 5500-X series with FTD	1.8 GB	110 MB	290 MB	20 min
FTDv: VMware 6.0	1.8 GB	110 MB	290 MB	10 min
Firepower 7000/8000 series	3.6 GB	170 MB	650 MB	26 min
ASA FirePOWER	4.1 GB	36 MB	590 MB	45 min
NGIPSv: VMware 6.0	2.1 GB	150 MB	450 MB	10 min

Version 6.4.0.4 Time and Disk Space

Table 110: Version 6.4.0.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMC	4.4 GB	170 MB	—	35 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMCv: VMware 6.0	4.8 GB	170 MB	—	31 min
Firepower 1000 series	2.9 GB	2.9 GB	520 MB	28 min
Firepower 2100 series	2.4 GB	2.4 GB	500 MB	10 min
Firepower 4100 series	2.0 GB	2.0 GB	310 MB	12 min
Firepower 9300	1.7 GB	1.7 GB	310 MB	10 min
ASA 5500-X series with FTD	1.8 GB	110 MB	290 MB	29 min
FTDv: VMware 6.0	1.8 GB	110 MB	290 MB	8 min
Firepower 7000/8000 series	3.6 GB	170 MB	650 MB	24 min
ASA FirePOWER	4.2 GB	36 MB	600 MB	55 min
NGIPSv: VMware 6.0	2.1 GB	150 MB	550 MB	10 min

Version 6.4.0.3 Time and Disk Space

Table 111: Version 6.4.0.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMC	3.2 GB	24 MB	—	34 min
FMCv: VMware 6.0	2.5 GB	23 MB	—	25 min
Firepower 1000 series	2.9 GB	2.9 GB	520 MB	22 min
Firepower 2100 series	2.4 GB	2.4 GB	500 MB	19 min
Firepower 4100 series	1.7 GB	1.7 GB	310 MB	12 min
Firepower 9300	1.7 GB	1.7 GB	310 MB	14 min
ASA 5500-X series with FTD	1.8 GB	110 MB	290 MB	18 min
FTDv: VMware 6.0	1.8 GB	110 MB	290 MB	12 min
Firepower 7000/8000 series	1.9 GB	21 MB	370 MB	20 min
ASA FirePOWER	2.5 GB	2.5 GB	320 MB	28 min
NGIPSv: VMware 6.0	690 MB	21 MB	210 MB	8 min

Version 6.4.0.2 Time and Disk Space

Table 112: Version 6.4.0.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMC	3.1 GB	24 MB	—	39 min
FMCv: VMware 6.0	2.5 GB	23 MB	—	24 min
Firepower 2100 series	1.9 GB	1.9 GB	480 MB	19 min
Firepower 4100 series	2.3 GB	2.3 GB	290 MB	11 min
Firepower 9300	1.7 GB	1.7 GB	290 MB	11 min
ASA 5500-X series with FTD	1.8 GB	110 MB	270 MB	21 min
FTDv: VMware 6.0	1.2 GB	110 MB	270 MB	10 min
Firepower 7000/8000 series	1.9 GB	36 MB	350 MB	20 min
ASA FirePOWER	2.0 GB	21 MB	300 MB	34 min
NGIPSv: VMware 6.0	630 MB	21 MB	190 MB	10 min

Version 6.4.0.1 Time and Disk Space

Table 113: Version 6.4.0.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMC	1.8 GB	24 MB	—	50 min
FMCv: VMware 6.0	1.8 GB	23 MB	—	20 min
Firepower 2100 series	1.4 GB	1.4 GB	300 MB	17 min
Firepower 4100 series	1.1 GB	1.1 GB	95 MB	9 min
Firepower 9300	1.1 GB	1.1 GB	95 MB	10 min
ASA 5500-X series with FTD	550 MB	110 MB	76 MB	16 min
FTDv: VMware 6.0	550 MB	110 MB	76 MB	15 min
Firepower 7000/8000 series	59 MB	21 MB	2 MB	14 min
ASA FirePOWER	85 MB	20 MB	2 MB	30 min
NGIPSv: VMware 6.0	45 MB	21 MB	2 MB	10 min

Version 6.4.0 Time and Disk Space

Table 114: Version 6.4.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	13.3 GB	26 MB	—	41 min
FMCv: VMware 6.0	13.6 GB	29 MB	—	30 min
Firepower 2100 series	12 MB	8.9 GB	950 MB	20 min
Firepower 4100 series	10 MB	7.5 GB	920 MB	6 min
Firepower 9300	10 MB	7.7 GB	920 MB	7 min
ASA 5500-X series with FTD	9.0 GB	110 KB	1.1 GB	24 min
FTDv: VMware 6.0	7.5 GB	100 KB	1.1 GB	12 min
Firepower 7000/8000 series	7.7 GB	19 MB	980 MB	34 min
ASA FirePOWER	11.5 GB	22 MB	1.3 GB	66 min
NGIPSv: VMware 6.0	6.5 GB	19 MB	840 MB	16 min

Version 6.3.0.5 Time and Disk Space

Table 115: Version 6.3.0.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.3.0
FMC	4.9 GB	200 MB	—	46 min
FMCv: VMware 6.0	4.5 GB	180 MB	—	41 min
Firepower 2100 series	2.3 GB	2.3 GB	480 MB	21 min
Firepower 4100 series	1.6 GB	1.6 GB	280 MB	13 min
Firepower 9300	1.6 GB	1.6 GB	280 MB	17 min
ASA 5500-X series with FTD	1.7 GB	110 MB	270 MB	26 min
FTDv: VMware 6.0	1.7 GB	110 MB	270 MB	17 min
Firepower 7000/8000 series	2.6 GB	210 MB	600 MB	23 min
ASA FirePOWER	3.6 GB	47 MB	540 MB	74 min
NGIPSv: VMware 6.0	2.1 GB	160 MB	440 MB	17 min

Version 6.3.0.4 Time and Disk Space

Table 116: Version 6.3.0.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.3.0
FMC	3.4 GB	180 MB	—	34 min
FMCv: VMware 6.0	4.4 GB	180 MB	—	38 min
Firepower 2100 series	2.3 GB	2.3 GB	480 MB	17 min
Firepower 4100 series	1.6 GB	1.6 GB	280 MB	12 min
Firepower 9300	1.8 GB	1.8 GB	280 MB	12 min
ASA 5500-X series with FTD	1.7 GB	110 MB	270 MB	23 min
FTDv: VMware 6.0	1.7 GB	110 MB	270 MB	18 min
Firepower 7000/8000 series	3.3 GB	170 MB	600 MB	21 min
ASA FirePOWER	3.5 GB	31 MB	530 MB	48 min
NGIPSv: VMware 6.0	2.1 GB	160 MB	430 MB	16 min

Version 6.3.0.3 Time and Disk Space

Table 117: Version 6.3.0.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.3.0
FMC	3.7 GB	180 MB	—	33 min
FMCv: VMware 6.0	3.2 GB	180 MB	—	24 min
Firepower 2100 series	1.2 GB	1.2 GB	290 MB	18 min
Firepower 4100 series	990 MB	990 MB	99 MB	11 min
Firepower 9300	990 MB	990 MB	99 MB	12 min
ASA 5500-X series with FTD	620 MB	110 MB	79 MB	18 min
FTDv: VMware 6.0	240 MB	110 MB	79 MB	7 min
Firepower 7000/8000 series	2.6 GB	170 MB	400 MB	20 min
ASA FirePOWER	2.9 GB	30 MB	340 MB	45 min
NGIPSv: VMware 6.0	1.5 GB	160 MB	250 MB	4 min

Version 6.3.0.2 Time and Disk Space

Table 118: Version 6.3.0.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.3.0
FMC	3.5 GB	180 MB	—	53 min
FMCv: VMware 6.0	3.2 GB	180 MB	—	28 min
Firepower 2100 series	1.2 GB	1.2 GB	100 MB	17 min
Firepower 4100 series	970 MB	970 MB	100 MB	12 min
Firepower 9300	970 MB	970 MB	100 MB	11 min
ASA 5500-X series with FTD	570 MB	110 MB	80 MB	12 min
FTDv: VMware 6.0	600 MB	110 MB	80 MV	10 min
Firepower 7000/8000 series	2.5 GB	170 MB	400 MB	20 min
ASA FirePOWER	3.0 GB	30 MB	340 MB	45 min
NGIPSv: VMware 6.0	1.5 GB	160 MB	250 MB	10 min

Version 6.3.0.1 Time and Disk Space

Table 119: Version 6.3.0.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.3.0
FMC	3.0 GB	170 MB	—	31 min
FMCv: VMware 6.0	2.4 GB	170 MB	—	25 min
Firepower 2100 series	1.2 GB	1.2 GB	290 MB	18 min
Firepower 4100 series	740 MB	740 MB	100 MB	12 min
Firepower 9300	740 MB	740 MB	100 MB	12 min
ASA 5500-X series with FTD	400 MB	150 MB	72 MB	17 min
FTDv: VMware 6.0	400 MB	150 MB	72 MB	10 min
Firepower 7000/8000 series	2.1 GB	170 MB	350 MB	20 min
ASA FirePOWER	2.4 GB	28 MB	270 MB	44 min
NGIPSv: VMware 6.0	1.5 GB	150 MB	350 MB	10 min

Version 6.3.0 Time and Disk Space

Table 120: Version 6.3.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	12.7 GB	29 MB	—	47 min
FMCv on: VMware 6.0	12.7 GB	29 MB	—	29 min
Firepower 2100 series	13 MB	8.8 GB	930 MB	20 min
Firepower 4100/9300 chassis	10 MB	7.6 GB	930 MB	6 min
ASA 5500-X series with FTD	7.9 GB	100 KB	1.1 GB	25 min
FTDv: VMware 6.0	7.3 GB	100 KB	1.1 GB	12 min
Firepower 7000/8000 series	7.0 GB	19 MB	920 MB	32 min
ASA FirePOWER	11.3 GB	22 MB	1.2 GB	63 min
NGIPSv	5.7 GB	19 MB	810 MB	16 min

Version 6.2.3.17 Time and Disk Space

Table 121: Version 6.2.3.17 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3	Reboot Time
FMC	3.4 GB	300 MB	—	32 min	7 min
FMCv: VMware 6.0	4.1 GB	230 MB	—	23 min	5 min
Firepower 2100 series	2.7 GB	2.7 GB	600 MB	12 min	12 min
Firepower 4100 series	1.7 GB	1.7 GB	390 MB	5 min	6 min
Firepower 9300	1.7 GB	1.7 GB	390 MB	5 min	7 min
ASA 5500-X series with FTD	2.1 GB	200 MB	420 MB	18 min	37 min
FTDv: VMware 6.0	2.1 GB	190 MB	420 MB	7 min	5 min
Firepower 7000/8000 series	3.5 GB	200 MB	640 MB	10 min	15 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3	Reboot Time
ASA FirePOWER	3.8 GB	58 MB	580 MB	72 min	61 min
NGIPSv: VMware 6.0	2.5 GB	180 MB	480 MB	5 min	4 min

Version 6.2.3.16 Time and Disk Space

Table 122: Version 6.2.3.16 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3	Reboot Time
FMC	3.6 GB	250 MB	—	40 min	9 min
FMCv: VMware 6.0	3.3 GB	220 MB	—	25 min	4 min
Firepower 2100 series	2.6 GB	2.6 GB	620 MB	11 min	12 min
Firepower 4100 series	1.7 GB	1.7 GB	410 MB	5 min	5 min
Firepower 9300	1.8 GB	1.8 GB	410 MB	5 min	9 min
ASA 5500-X series with FTD	2.0 GB	200 MB	430 MB	18 min	33 min
FTDv: VMware 6.0	2.0 GB	190 MB	430 MB	8 min	5 min
Firepower 7000/8000 series	3.5 GB	200 MB	670 MB	31 min	14 min
ASA FirePOWER	3.8 GB	58 MB	600 MB	74 min	77 min
NGIPSv: VMware 6.0	2.3 GB	180 MB	500 MB	6 min	4 min

Version 6.2.3.15 Time and Disk Space

Table 123: Version 6.2.3.15 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.7 GB	260 MB	—	50 min
FMCv: VMware 6.0	4.7 GB	210 MB	—	Hardware dependent
Firepower 2100 series	2.3 GB	2.3 GB	590 MB	27 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
Firepower 4100 series	1.7 GB	1.7 GB	390 MB	10 min
Firepower 9300	2.4 GB	2.4 GB	390 MB	11 min
ASA 5500-X series with FTD	2.0 GB	190 MB	410 MB	38 min
FTDv: VMware 6.0	2.4 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.5 GB	210 MB	640 MB	19 min
ASA FirePOWER	3.9 GB	56 MB	580 MB	100 min
NGIPSv: VMware 6.0	2.7 GB	180 MB	470 MB	Hardware dependent

Version 6.2.3.14 Time and Disk Space

Table 124: Version 6.2.3.14 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.5 GB	260 MB	—	58 min
FMCv: VMware 6.0	4.7 GB	190 MB	—	Hardware dependent
Firepower 2100 series	1.9 GB	1.9 GB	590 MB	23 min
Firepower 4100 series	1.7 GB	1.7 GB	390 MB	11 min
Firepower 9300	1.7 GB	1.7 GB	390 MB	10 min
ASA 5500-X series with FTD	2.0 GB	200 MB	410 MB	32 min
FTDv: VMware 6.0	2.4 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.4 GB	200 MB	630 MB	19 min
ASA FirePOWER	3.7 GB	53 MB	560 MB	106 min
NGIPSv: VMware 6.0	2.6 GB	190 MB	470 MB	Hardware dependent

Version 6.2.3.13 Time and Disk Space

Table 125: Version 6.2.3.13 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.7 GB	290 MB	—	50 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMCv: VMware 6.0	4.6 GB	190 MB	—	Hardware dependent
Firepower 2100 series	2.6 GB	2.6 GB	590 MB	25 min
Firepower 4100 series	1.7 GB	1.7 GB	390 MB	11 min
Firepower 9300	1.8 GB	1.8 GB	390 MB	11 min
ASA 5500-X series with FTD	2.4 GB	190 MB	410 MB	32 min
FTDv: VMware 6.0	2.3 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.8 GB	190 MB	620 MB	18 min
ASA FirePOWER	3.7 GB	51 MB	560 MB	105 min
NGIPSv: VMware 6.0	2.6 GB	180 MB	470 MB	Hardware dependent

Version 6.2.3.12 Time and Disk Space

Table 126: Version 6.2.3.12 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	3.9 GB	220 MB	—	49 min
FMCv: VMware 6.0	4.6 GB	160 MB	—	Hardware dependent
Firepower 2100 series	1.9 GB	1.9 GB	390 MB	21 min
Firepower 4100 series	970 MB	970 MB	190 MB	14 min
Firepower 9300	1.7 GB	1.7 GB	190 MB	11 min
ASA 5500-X series with FTD	1.4 GB	96 MB	210 MB	30 min
FTDv: VMware 6.0	2.4 GB	200 MB	210 MB	Hardware dependent
Firepower 7000/8000 series	3.6 GB	160 MB	540 MB	19 min
ASA FirePOWER	3.5 GB	31 MB	480 MB	104 min
NGIPSv: VMware 6.0	2.6 GB	130 MB	400 MB	Hardware dependent

Version 6.2.3.11 Time and Disk Space

Table 127: Version 6.2.3.11 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.5 GB	250 MB	—	39 min
FMCv: VMware 6.0	4.6 GB	35 MB	—	Hardware dependent
Firepower 2100 series	2.8 GB	2.8 GB	590 MB	40 min
Firepower 4100 series	2.0 GB	2.0 GB	380 MB	10 min
Firepower 9300	1.6 GB	1.6 GB	380 MB	11 min
ASA 5500-X series with FTD	1.8 GB	230 MB	410 MB	33 min
FTDv: VMware 6.0	2.2 GB	230 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.3 GB	170 MB	600 MB	23 min
ASA FirePOWER	3.6 GB	50 MB	530 MB	110 min
NGIPSv: VMware 6.0	2.6 GB	130 MB	450 MB	Hardware dependent

Version 6.2.3.10 Time and Disk Space

Table 128: Version 6.2.3.10 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.2 GB	200 MB	—	40 min
FMCv	4.5 GB	230 MB	—	Hardware dependent
Firepower 2100 series	1.8GB	1.8 GB	390 MB	21 min
Firepower 4100/9300 chassis	1.3 GB	1.3 GB	190 MB	11 min
ASA 5500-X series with FTD	1.3 GB	140 MB	210 MB	25 min
FTDv	1.6 GB	140 MB	210 MB	Hardware dependent
Firepower 7000/8000 series	3.2 GB	190 MB	560 MB	25 min
ASA FirePOWER	3.4 GB	31 MB	480 MB	100 min
NGIPSv	2.1 GB	160 MB	400 MB	Hardware dependent

Version 6.2.3.9 Time and Disk Space

Table 129: Version 6.2.3.9 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	3630 MB	190 MB	—	35 min
FMCv	3596 MB	172 MB	—	Hardware dependent
Firepower 2100 series	1677 MB	1677 MB	385 MB	21 min
Firepower 4100/9300 chassis	779 MB	779 MB	184 MB	9 min
ASA 5500-X series with FTD	1105 MB	130 MB	206 MB	12 min
ISA 3000 with FTD	1071 MB	130 MB	206 MB	25 min
FTDv	1094 MB	130 MB	206 MB	Hardware dependent
Firepower 7000/8000 series	2975 MB	161 MB	538 MB	30 min
ASA FirePOWER	3211 MB	27 MB	462 MB	38 min
NGIPSv	1883 MB	146 MB	378 MB	Hardware dependent

Version 6.2.3.8 Time and Disk Space

Version 6.2.3.8 was removed from the Cisco Support & Download site on 2019-01-07. If you are running this version, we recommend you upgrade.

Version 6.2.3.7 Time and Disk Space

Table 130: Version 6.2.3.7 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	2909 MB	137 MB	—	25 min
FMCv	3972 MB	211 MB	—	Hardware dependent
Firepower 2100 series	1668 MB	1668 MB	384 MB	19 min
Firepower 4100/9300 chassis	795 MB	795 MB	183 MB	8 min
ASA 5500-X series with FTD	1067 MB	130 MB	205 MB	9 min
ISA 3000 with FTD	1080 MB	130 MB	205 MB	20 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FTDv	1146 MB	130 MB	205 MB	Hardware dependent
Firepower 7000/8000 series	3300 MB	136 MB	477 MB	20 min
ASA FirePOWER	2291 MB	26 MB	411 MB	80 min
NGIPSv	1588 MB	121 MB	327 MB	Hardware dependent

Version 6.2.3.6 Time and Disk Space

Table 131: Version 6.2.3.6 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	2524 MB	47 MB	—	30 min
FMCv	2315 MB	101 MB	—	Hardware dependent
Firepower 2100 series	1673 MB	1673 MB	383 MB	10 min
Firepower 4100/9300 chassis	790 MB	790 MB	182 MB	17 min
ASA 5500-X series with FTD	1220 MB	130 MB	205 MB	21 min
ISA 3000 with FTD	1087 MB	130 MB	205 MB	21 min
FTDv	1133 MB	130 MB	205 MB	Hardware dependent
Firepower 7000/8000 series	1196 MB	17 MB	204 MB	30 min
ASA FirePOWER	1844 MB	16 MB	226 MB	106 min
NGIPSv	364 MB	17 MB	142 MB	Hardware dependent

Version 6.2.3.5 Time and Disk Space

Table 132: Version 6.2.3.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1566 MB	24 MB	—	28 min
FMCv	2266 MB	80 MB	—	Hardware dependent
Firepower 2100 series	1001 MB	1001MB	257 MB	20 min
Firepower 4100/9300 chassis	370 MB	370 MB	56 MB	7 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
ASA 5500-X series with FTD	587 MB	130 MB	78 MB	20 min
ISA 3000 with FTD	379 MB	130 MB	78 MB	20 min
Firepower 7000/8000 series	806 MB	17 MB	78 MB	22 min
ASA FirePOWER	1465 MB	15 MB	100 MB	70 min
NGIPSv	120 MB	17 MB	16 MB	Hardware dependent

Version 6.2.3.4 Time and Disk Space

Table 133: Version 6.2.3.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	2191 MB	107 MB	—	80 min
FMCv	1760 MB	35 MB	—	Hardware dependent
Firepower 2100 series	1014 MB	1014 MB	261 MB	17 min
Firepower 4100/9300 chassis	334 MB	334 MB	59 MB	7 min
ASA 5500-X series with FTD	411 MB	128 MB	82 MB	20 min
ISA 3000 with FTD	393 MB	128 MB	82 MB	20 min
FTDv	411 MB	128 MB	82 MB	Hardware dependent
Firepower 7000/8000 series	800 MB	17 MB	82 MB	23 min
ASA FirePOWER	1385 MB	15 MB	103 MB	25 min
NGIPSv	191 MB	17 MB	20 MB	Hardware dependent

Version 6.2.3.3 Time and Disk Space

Table 134: Version 6.2.3.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1879 MB	88 MB	—	26 min
FMCv	2093 MB	90 MB	—	Hardware dependent
Firepower 2100 series	987 MB	987 MB	255 MB	15 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
Firepower 4100/9300 chassis	313 MB	313 MB	54 MB	5 min
ASA 5500-X series with FTD	553 MB	128 MB	77 MB	16 min
ISA 3000 with FTD	307 MB	90 MB	77 MB	15 min
FTDv	307 MB	90 MB	77 MB	Hardware dependent
Firepower 7000/8000 series	825 MB	17 MB	77 MB	15 min
ASA FirePOWER	634 MB	16 MB	98 MB	40 min
NGIPSv	102 MB	17 MB	77 MB	Hardware dependent

Version 6.2.3.2 Time and Disk Space

Table 135: Version 6.2.3.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1743 MB	27 MB	—	24 min
FMCv	1976 MB	70 MB	—	Hardware dependent
Firepower 2100 series	977 MB	977 MB	252 MB	17 min
Firepower 4100/9300 chassis	374 MB	374 MB	51 MB	4 min
ASA 5500-X series with FTD	585 MB	126 MB	73 MB	16 min
ISA 3000 with FTD	676 MB	126 MB	73 MB	17 min
FTDv	585 MB	126 MB	73 MB	Hardware dependent
Firepower 7000/8000 series	688 MB	11 MB	76 MB	13 min
ASA FirePOWER	1440 MB	15 MB	98 MB	40 min
NGIPSv	96 MB	17 MB	14 MB	Hardware dependent

Version 6.2.3.1 Time and Disk Space

Table 136: Version 6.2.3.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1361.8 MB	59.67 MB	—	25 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMCv	1240.8 MB	40.8 MB	—	Hardware dependent
Firepower 2100 series	948.3 MB	948.3 MB	246 MB	81 min
Firepower 4100/9300 chassis	278 MB	278 MB	45 MB	8 min
ASA 5500-X series with FTD	275.5 MB	89.9 MB	68 MB	16 min
ISA 3000 with FTD	343.4 MB	127.5 MB	68 MB	15 min
FTDv	275.5 MB	89.9 MB	67 MB	Hardware dependent
Firepower 7000/8000 series	99.8 MB	36 MB	10 MB	19 min
ASA FirePOWER	867.9 MB	15.45 MB	32 MB	60 min
NGIPSv	101.9 MB	17.18 MB	9 MB	Hardware dependent

Version 6.2.3 Time and Disk Space

Table 137: Version 6.2.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	From 6.1.0: 7415 MB From 6.2.0: 8863 MB From 6.2.1: 8263 MB From 6.2.2: 11860 MB	From 6.1.0: 17 MB From 6.2.0: 24 MB From 6.2.1: 23 MB From 6.2.2: 24 MB	—	From 6.1.0: 38 min From 6.2.0: 43 min From 6.2.1: 37 min From 6.2.2: 37 min
FMCv	From 6.1.0: 7993 MB From 6.2.0: 9320 MB From 6.2.1: 11571 MB From 6.2.2: 11487 MB	From 6.1.0: 23 MB From 6.2.0: 28 MB From 6.2.1: 24 MB From 6.2.2: 24 MB	—	Hardware dependent
Firepower 2100 series	From 6.2.1: 7356 MB From 6.2.2: 11356 MB	From 6.2.1: 7356 MB From 6.2.2: 11356 MB	1000 MB	From 6.2.1: 15 min From 6.2.2: 15 min
Firepower 4100/9300 chassis	From 6.1.0: 5593 MB From 6.2.0: 5122 MB From 6.2.2: 7498 MB	From 6.1.0: 5593 MB From 6.2.0: 5122 MB From 6.2.2: 7498 MB	795 MB	From 6.1.0: 10 min From 6.2.0: 12 min From 6.2.2: 15 min
ASA 5500-X series with FTD	From 6.1.0: 4322 MB From 6.2.0: 6421 MB From 6.2.2: 6450 MB	From 6.1.0: .088 MB From 6.2.0: .092 MB From 6.2.2: .088 MB	1000 MB	From 6.1.0: 54 min From 6.2.0: 53 min From 6.2.2: 50 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FTDv	From 6.1.0: 4225 MB From 6.2.0: 5179 MB From 6.2.2: 6450 MB	From 6.1.0: .076 MB From 6.2.0: .092 MB From 6.2.2: .092 MB	1000 MB	Hardware dependent
Firepower 7000/8000 series	From 6.1.0: 5145 MB From 6.2.0: 5732 MB From 6.2.2: 6752 MB	From 6.1.0: 18 MB From 6.2.0: 18 MB From 6.2.2: 18 MB	840 MB	From 6.1.0: 29 min From 6.2.0: 31 min From 6.2.2: 31 min
ASA FirePOWER	From 6.1.0: 7286 MB From 6.2.0: 7286 MB From 6.2.2: 10748 MB	From 6.1.0: 16 MB From 6.2.0: 16 MB From 6.2.2: 16 MB	From 6.1.0: 1200 MB From 6.2.0: 1200 MB	From 6.1.0: 94 min From 6.2.0: 104 min From 6.2.2: 96 min
NGIPSv	From 6.1.0: 4115 MB From 6.2.0: 5505 MB From 6.2.2: 5871 MB	From 6.1.0: 18 MB From 6.2.0: 19 MB From 6.2.2: 19 MB	741 MB	Hardware dependent

Version 6.2.2.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	5271 MB	25 MB	—	From 6.2.2: 60 min From 6.2.2.4: 42 min
FMCv	5292 MB	33 MB	—	Hardware dependent
Firepower 2100 series	9113 MB	9113 MB	2.0 GB	From 6.2.2: 87 min From 6.2.2.4: 32 min
Firepower 4100/9300	3325 MB	3325 MB	612 MB	From 6.2.2: 28 min From 6.2.2.4: 12 min
ASA 5500-X series with FTD	3809 MB	226 MB	724 MB	From 6.2.2: 49 min From 6.2.2.4: 25 min
FTDv	3809 MB	226 MB	724 MB	Hardware dependent
Firepower 7000/8000 series	566 MB	28 MB	419 MB	From 6.2.2: 54 min From 6.2.2.4: 12 min
ASA FirePOWER	3714 MB	28 MB	432 MB	From 6.2.2: 215 min From 6.2.2.4: 105 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
NGIPSv	3799 MB	24 MB	98 MB	Hardware dependent

Version 6.2.2.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	4435 MB	217 MB	—	From 6.2.2: 85 min From 6.2.2.3: 42 min
FMCv	3691 MB	48 MB	—	Hardware dependent
Firepower 2100 series	6965 MB	6965 MB	1 GB	From 6.2.2: 58 min From 6.2.2.3: 34 min
Firepower 4100/9300	1676 MB	1676 MB	339 MB	From 6.2.2: 24 min From 6.2.2.3: 13 min
ASA 5500-X series with FTD	1695 MB	225 MB	427 MB	From 6.2.2: 142 min From 6.2.2.3: 68 min
FTDv	1695 MB	225 MB	427 MB	Hardware dependent
Firepower 7000/8000 series	3343 MB	36 MB	414 MB	From 6.2.2: 45 min From 6.2.2.3: 19 min
ASA FirePOWER	3192 MB	27 MB	405 MB	From 6.2.2: 182 min From 6.2.2.3: 80 min
NGIPSv	444 MB	28 MB	94 MB	Hardware dependent

Version 6.2.2.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	3766.6 MB	205 MB	—	From 6.2.2: 66 min From 6.2.2.2: 41 min
FMCv	3485 MB	17.5 MB	—	Hardware dependent
Firepower 2100 series	4486.64 MB	4486.64 MB	132 MB	From 6.2.2: 61 min From 6.2.2.2: 36 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
Firepower 4100/9300	811.7 MB	811.7 MB	132 MB	From 6.2.2: 20 min From 6.2.2.2: 12 min
ASA 5500-X series with FTD	1636.6 MB	125.1 MB	199 MB	From 6.2.2: 35 min From 6.2.2.2: 20 min
FTDv	1810.7 MB	125 MB	199 MB	Hardware dependent
Firepower 7000/8000 series	2775 MB	17 MB	339 MB	From 6.2.2: 80 min From 6.2.2.2: 42 min
ASA FirePOWER	2301.5 MB	15.69 MB	308 MB	From 6.2.2: 184 min From 6.2.2.2: 100 min
NGIPSv	576.3 MB	17.5 MB	20 MB	Hardware dependent

Version 6.2.2.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	1656 MB	18 MB	—	From 6.2.2: 34 min From 6.2.2.1: 27 min
FMCv	2356 MB	19 MB	—	Hardware dependent
Firepower 2100 series	2377 MB	2377 MB	497 MB	From 6.2.2: 41 min From 6.2.2.1: 20 min
Firepower 4100/9300	561 MB	561 MB	41 MB	From 6.2.2: 21 min From 6.2.2.1: 13 min
ASA 5500-X series with FTD	984 MB	122 MB	136 MB	From 6.2.2: 110 min From 6.2.2.1: 70 min
FTDv	984 MB	122 MB	136 MB	Hardware dependent
Firepower 7000/8000 series	1706 MB	16 MB	310 MB	From 6.2.2: 56 min From 6.2.2.1: 40 min
ASA FirePOWER	1602 MB	15 MB	190 MB	From 6.2.2: 113 min From 6.2.2.1: 80 min
NGIPSv	170 MB	17 MB	16 MB	Hardware dependent

Version 6.2.2.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.2
FMC	480 MB	18 MB	—	52 min
FMCv	775 MB	30 MB	—	Hardware dependent
Firepower 2100 series	1003 MB	1003 MB	47 MB	28 min
Firepower 4100/9300	299 MB	299 MB	47 MB	35 min
ASA 5500-X series with FTD	674 MB	121 MB	69 MB	72 min
FTDv	674 MB	121 MB	69 MB	Hardware dependent
Firepower 7000/8000 series	664 MB	14 MB	61 MB	33 min
ASA FirePOWER	758 MB	15 MB	83 MB	90 min
NGIPSv	106 MB	17 MB	10 MB	Hardware dependent

Version 6.2.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	From 6.2.0: 6467 MB From 6.2.1: 6916 MB	From 6.2.0: 22 MB From 6.2.1: 21 MB	—	From 6.2.0: 52 min From 6.2.1: 61 min
FMCv	From 6.2.0: 6987 MB From 6.2.1: 5975 MB	From 6.2.0: 24 MB From 6.2.1: 24 MB	—	Hardware dependent
Firepower 2100 series	5613 MB	5613 MB	925 MB	57 min
Firepower 4100/9300	4635 MB	4635 MB	743 MB	14 min
FTDv	3586 MB	.92 MB	987 MB	Hardware dependent
ASA 5500-X series with FTD	3683 MB	.16 MB	987 MB	80 min
Firepower 7000/8000 series	6745 MB	18 MB	1300 MB	27 min
ASA FirePOWER	7021 MB	16 MB	1200 MB	131 min
NGIPSv	7261 MB	18 MB	1300 MB	Hardware dependent

Version 6.2.0.6 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	8547 MB	104 MB	—	From 6.2.0: 97 min From 6.2.0.5: 36 min
FMCv	8543 MB	30 MB	—	Hardware dependent
Firepower 4100/9300	4085 MB	4085 MB	789 MB	From 6.2.0: 23 min From 6.2.0.5: 13 min
FTDv	4526 MB	226 MB	918 MB	Hardware dependent
ASA 5500-X series with FTD	4960 MB	227 MB	918 MB	From 6.2.0: 56 min From 6.2.0.5:27 min
Firepower 7000/8000 series	7464 MB	29 MB	944 MB	From 6.2.0: 60 min From 6.2.0.5: 24 min
ASA FirePOWER	7191 MB	28 MB	878 MB	From 6.2.0: 75 min From 6.2.0.5: 49 min
NGIPSv	1658 MB	29 MB	284 MB	Hardware dependent

Version 6.2.0.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	6009 MB	180 MB	—	From 6.2.0: 72 min From 6.2.0.4: 34 min
FMCv	6943 MB	20 MB	—	Hardware dependent
Firepower 4100/9300	3009 MB	3009 MB	441 MB	From 6.2.0: 28 min From 6.2.0.4: 16 min
FTDv	2805 MB	135 MB	548 MB	Hardware dependent
ASA 5500-X series with FTD	4316 MB	135 MB	548 MB	From 6.2.0: 46 min From 6.2.0.4: 22 min
Firepower 7000/8000 series	5806 MB	18 MB	693 MB	From 6.2.0: 51 min From 6.2.0.4: 18 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
ASA FirePOWER	5945 MB	16 MB	703 MB	From 6.2.0: 66 min From 6.2.0.4: 27 min
NGIPSv	1301 MB	18 MB	211 MB	Hardware dependent

Version 6.2.0.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	5271 MB	167 MB	—	From 6.2.0: 84 min From 6.2.0.3: 50 min
FMCv	5346 MB	20 MB	—	Hardware dependent
Firepower 4100/9300	1828 MB	1828 MB	325 MB	From 6.2.0: 23 min From 6.2.0.3: 12 min
ASA 5500-X series with FTD	3593 MB	134 MB	448 MB	From 6.2.0: 2 hr 28 min From 6.2.0.3: 69 min
FTDv	275 MB	136 MB	448 MB	Hardware dependent
Firepower 7000/8000 series	4614 MB	18 MB	608 MB	From 6.2.0: 45 min From 6.2.0.3: 17 min
ASA FirePOWER	4585 MB	16 MB	597 MB	From 6.2.0: 3 hr 34 min From 6.2.0.3: 83 min
NGIPSv	1067 MB	18 MB	208 MB	Hardware dependent

Version 6.2.0.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	3352 MB	18 MB	—	From 6.2.0: 75 min From 6.2.0.2: 37 min
FMCv	3342 MB	19 MB	—	Hardware dependent
Firepower 4100/9300	—	1355 MB	319 MB	From 6.2.0: 18 min From 6.2.0.2: 12 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
ASA 5500-X series with FTD	131 MB	2302 MB	384 MB	From 6.2.0: 118 min From 6.2.0.2: 76 min
FTDv	842 MB	17 MB	384 MB	Hardware dependent
Firepower 7000/8000 series	3526 MB	17 MB	554 MB	From 6.2.0: 38 min From 6.2.0.2: 19 min
ASA FirePOWER	15 MB	3361 MB	521 MB	From 6.2.0: 3 hr From 6.2.0.2: 97 min
NGIPSv	842 MB	17 MB	202 MB	Hardware dependent

Version 6.2.0.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	1665 MB	35 MB	—	From 6.2.0: 36 min From 6.2.0.1: 30 min
FMCv	2834 MB	21 MB	—	Hardware dependent
Firepower 4100/9300	1060 MB	1060 MB	274 MB	From 6.2.0: 12 min From 6.2.0.1: 9 min
ASA 5500-X series with FTD	1808 MB	144 MB	295 MB	From 6.2.0: 95 min From 6.2.0.1: 59 min
FTDv	998 MB	143 MB	295 MB	Hardware dependent
Firepower 7000/8000 series	2110 MB	17 MB	458 MB	From 6.2.0: 54 min From 6.2.0.1: 35 min
ASA FirePOWER	2014 MB	17 MB	383 MB	From 6.2.0: 40 min From 6.2.0.1: 80 min
NGIPSv	612 MB	19 MB	195 MB	Hardware dependent

Version 6.2.0.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.0
FMC	1237 MB	50 MB	—	28 min
FMCv	1488 MB	23 MB	—	Hardware dependent
Firepower 4100/9300	524 MB	524 MB	137 MB	12 min
ASA 5500-X series with FTD	945 MB	144 MB	159 MB	62 min
FTDv	144 MB	10 MB	159 MB	Hardware dependent
Firepower 7000/8000 series	1134 MB	18 MB	186 MB	22 min
ASA FirePOWER	97 MB	17 MB	206 MB	69 min
NGIPSv	721 MB	19 MB	98 MB	Hardware dependent

Version 6.2.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	10207 MB	17 MB	—	57 min
FMCv	10207 MB	17 MB	—	Hardware dependent
Firepower 4100/9300	5234 MB	5234 MB	734 MB	21 min
ASA 5500-X series with FTD	5213 MB	.096 MB	938 MB	83 min
FTDv	5663 MB	1 MB	936 MB	Hardware dependent
Firepower 7000/8000 series	6129 MB	17 MB	1200 MB	27 min
ASA FirePOWER	6619 MB	16 MB	1100 MB	165 min
NGIPSv	7028 MB	18 MB	1300 MB	Hardware dependent

Version 6.1.0.7 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	1941 MB	187 MB	—	From 6.1.0: 111 min From 6.1.0.5: 41 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMCv	12435 MB	218 MB	—	Hardware dependent
Firepower 4100/9300	9881 MB	9881 MB	1400 MB	From 6.1.0: 43 min From 6.1.0.5: 13 min
ASA 5500-X series with FTD	8846 MB	1033 MB	1480 MB	From 6.1.0: 251 min From 6.1.0.5: 75 min
FTDv	1339 MB	185 MB	1480 MB	Hardware dependent
Firepower 7000/8000 series	5896 MB	33 MB	159 MB	From 6.1.0: 39 min From 6.1.0.5: 25 min
ASA FirePOWER	13061 MB	45 MB	1390 MB	From 6.1.0: 156 min From 6.1.0.5: 28 min
NGIPSv	5477 MB	185 MB	717 MB	Hardware dependent

Version 6.1.0.6 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	10503 MB	215 MB	—	From 6.1.0: 66 min From 6.1.0.5: 27 min
FMCv	1367 MB	196 MB	—	Hardware dependent
Firepower 4100/9300	8140 MB	8140 MB	1126 MB	From 6.1.0: 270 min From 6.1.0.5: 75 min
ASA 5500-X series with FTD	8540 MB	1034 MB	1229 MB	From 6.1.0: 40 min From 6.1.0.5: 15 min
FTDv	7414 MB	1033 MB	1229 MB	Hardware dependent
Firepower 7000/8000 series	12725 MB	237 MB	1434 MB	From 6.1.0: 136 min From 6.1.0.5: 34 min
ASA FirePOWER	11189 MB	31 MB	1131 MB	From 6.1.0: 257 min From 6.1.0.5: 60 min
NGIPSv	4606 MB	196 MB	644 MB	Hardware dependent

Version 6.1.0.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	7673 MB	46 MB	—	From 6.1.0: 56 min From 6.1.0.4: 28 min
FMCv	10790 MB	216 MB	—	Hardware dependent
Firepower 4100/9300	7680 MB	7680 MB	1060 MB	From 6.1.0: 30 min From 6.1.0.4: 10 min
ASA 5500-X series with FTD	7952 MB	137 MB	1141 MB	From 6.1.0: 186 min From 6.1.0.4: 70 min
FTDv	7453 MB	1140 MB	1141 MB	Hardware dependent
Firepower 7000/8000 series	11877 MB	259 MB	1403 MB	From 6.1.0: 115 min From 6.1.0.4: 25 min
ASA FirePOWER	8955 MB	34 MB	1217 MB	From 6.1.0: 208 min From 6.1.0.4: 105 min
NGIPSv	4298 MB	215 MB	640 MB	Hardware dependent

Version 6.1.0.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	6739516 MB	218808 MB	—	From 6.1.0: 65 min From 6.1.0.3: 30 min
FMCv	675984 MB	200748 MB	—	Hardware dependent
Firepower 4100/9300	6010092 MB	6010092 MB	1020 MB	From 6.1.0: 26 min From 6.1.0.3: 10 min
ASA 5500-X series with FTD	6155828 MB	1058968 MB	1100 MB	From 6.1.0: 49 min From 6.1.0.3: 20 min
FTDv	1059632 MB	1059632 MB	1100 MB	Hardware dependent
Firepower 7000/8000 series	8713068 MB	240940 MB	1200 MB	From 6.1.0: 48 min From 6.1.0.3: 17 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
ASA FirePOWER	7442808 MB	31740 MB	1100 MB	From 6.1.0: 63 min From 6.1.0.3: 45 min
NGIPSv	3367536 MB	20120 MB	636 MB	Hardware dependent

Version 6.1.0.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	5537816 MB	218676 MB	—	From 6.1.0: 46 min From 6.1.0.2: 35 min
FMCv	6611148 MB	200904 MB	—	Hardware dependent
Firepower 4100/9300	5014020 MB	5014020 MB	929 MB	From 6.1.0: 22 min From 6.1.0.2: 13 min
ASA 5500-X series with FTD	1057776 MB	1057776 MB	1000 MB	From 6.1.0: 40 min From 6.1.0.2: 23 min
FTDv	1059932 MB	1059932 MB	1000 MB	Hardware dependent
Firepower 7000/8000 series	7357340 MB	228728 MB	1100 MB	From 6.1.0: 43 min From 6.1.0.2: 25 min
ASA FirePOWER	4782384 MB	31792 MB	1000 MB	From 6.1.0: 160 min From 6.1.0.2: 80 min
NGIPSv	2710540 MB	200896 MB	635 MB	Hardware dependent

Version 6.1.0.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	3872 MB	235 MB	—	From 6.1.0: 44 min From 6.1.0.1: 22 min
FMCv	3871 MB	219 MB	—	Hardware dependent
Firepower 4100/9300	4046 MB	4046 MB	886 MB	From 6.1.0: 20 min From 6.1.0.1: 14 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
ASA 5500-X series with FTD	2291 MB	96 MB	918 MB	From 6.1.0: 74 min From 6.1.0.1: 106 min
FTDv	2797 MB	1137 MB	918 MB	Hardware dependent
Firepower 7000/8000 series	4130 MB	260 MB	965 MB	From 6.1.0: 62 min From 6.1.0.1: 24 min
ASA FirePOWER	4549 MB	40 MB	816 MB	From 6.1.0: 139 min From 6.1.0.1: 34 min
NGIPSv	2710540 MB	200896 MB	635 MB	Hardware dependent

Version 6.1.0.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.1.0
FMC	1893 MB	140 MB	—	23 min
FMCv	2144 MB	207 MB	—	Hardware dependent
Firepower 4100 series	2580 MB	580 MB	600 MB	15 min
Firepower 9300	1877 MB	1877 MB	600 MB	20 min
ASA 5500-X series with FTD	1377 MB	846 MB	600 MB	10 min
FTDv	1377 MB	846 MB	600 MB	Hardware dependent
Firepower 7000/8000 series	2094 MB	156 MB	513 MB	47 min
ASA FirePOWER	1728 MB	34 MB	433 MB	76 min
NGIPSv	793 MB	130 MB	295 MB	Hardware dependent

Version 6.1.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	10722 MB	18 MB	—	47 min
FMCv	10128 MB	17 MB	—	Hardware dependent
ASA 5500-X series with FTD	5213 MB	.096 MB	914 MB	21 min
FTDv	5403 MB	.096 MB	914 MB	Hardware dependent

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
Firepower 7000/8000 series	7108 MB	61 MB	1740 MB	39 min
ASA FirePOWER	8392 MB	47 MB	1300 MB	59 min
NGIPSv	6368 MB	54 MB	1229 MB	Hardware dependent

Version 6.0.1.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	3428 MB	201 MB	—	From 6.0.0: 92 min From 6.0.1.3: 39 min
FMCv	3108 MB	95 MB	—	Hardware dependent
Firepower 4100 series	5237 MB	5237 MB	1000 MB	From 6.0.0: 30 min From 6.0.1.3: 18 min
Firepower 9300	1360 MB	5434 MB	1000 MB	From 6.0.0: 26 min From 6.0.1.3: 14 min
ASA 5500-X series with FTD	3416 MB	1017 MB	1000 MB	From 6.0.0: 26 min From 6.0.1.3: 14 min
FTDv	3619 MB	1020 MB	1000 MB	Hardware dependent
Firepower 7000/8000 series	7891 MB	222 MB	1270 MB	From 6.0.0: 47 min From 6.0.1.3: 23 min
ASA FirePOWER	6049 MB	45 MB	990 MB	From 6.0.0: 95 min From 6.0.1.3: 43 min
NGIPSv	2916 MB	192 MB	990 MB	Hardware dependent

Version 6.0.1.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	2419 MB	110 MB	—	58 min
FMCv	2419 MB	101 MB	—	Hardware dependent
Firepower 4100/9300	2781 MB	2781 MB	473 MB	22 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
ASA 5500-X series with FTD	2641 MB	813 MB	473 MB	24 min
FTDv	2651 MB	813 MB	473 MB	Hardware dependent
Firepower 7000/8000 series	4757 MB	125 MB	926 MB	55 min
ASA FirePOWER	3883 MB	58 MB	685 MB	184 min
NGIPSv	1695 MB	107 MB	430 MB	Hardware dependent

Version 6.0.1.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	272 MB	54 MB	—	7 min
FMCv	368 MB	54 MB	—	Hardware dependent
Firepower 4100/9300	2101 MB	56 MB	302 MB	16 min
ASA 5500-X series with FTD	740 MB	807 MB	302 MB	13 min
FTDv	2101 MB	56 MB	302 MB	Hardware dependent
Firepower 7000/8000 series	3190 MB	63 MB	412 MB	17 min
ASA FirePOWER	2027 MB	54 MB	577 MB	99 min
NGIPSv	602 MB	56 MB	243 MB	Hardware dependent

Version 6.0.1.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.0.1
FMC	14 MB	54 MB	—	23 min
FMCv	14 MB	54 MB	—	Hardware dependent
Firepower 4100/9300	54 MB	54 MB	2 MB	6 min
ASA 5500-X series with FTD	54 MB	54 MB	2 MB	7 min
FTDv	14 MB	54 MB	2 MB	Hardware dependent
Firepower 7000/8000 series	944 MB	61 MB	166 MB	39 min
ASA FirePOWER	824 MB	54 MB	84 MB	46 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.0.1
NGIPSv	54 MB	56 MB	1 MB	Hardware dependent

Version 6.0.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	8959 MB	18 MB	—	66 min
FMCv	—	—	—	—
Firepower 7000/8000 series	3683 MB	227 MB	614 MB	30 min
ASA FirePOWER	2966 MB	54 MB	429 MB	91 min
NGIPSv	2090 MB	196 MB	3050 MB	Hardware dependent

Version 6.0.0.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.0.0
FMC	976 MB	120 MB	—	25 min
FMCv	969 MB	119 MB	—	Hardware dependent
Firepower 7000/8000 series	1568 MB	134 MB	273 MB	25 min
ASA FirePOWER	1101 MB	56 MB	181 MB	56 min
NGIPSv	929 MB	26 MB	174 MB	Hardware dependent

Version 6.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	8022 MB	16 MB	—	58 min
FMCv	8022 MB	16 MB	—	Hardware dependent
Firepower 7000/8000 series	6496 MB	16 MB	1200 MB	94 min
ASA FirePOWER	7644 MB	32 MB	1200 MB	41 min
NGIPSv	6046 MB	17 MB	102000 MB	Hardware dependent

CHAPTER 10

Traffic Flow, Inspection, and Device Behavior

You must identify potential interruptions in traffic flow and inspection during the upgrade. This can occur:

- When a device is rebooted.
- When you upgrade the operating system or virtual hosting environment on a device.
- When you upgrade the Firepower software on a device.
- When you uninstall or revert the Firepower software on a device.
- When you deploy configuration changes as part of the upgrade or uninstall process (Snort process restarts).

Device type, deployment type (standalone, high availability, clustered), and interface configurations (passive, IPS, firewall, and so on) determine the nature of the interruptions. We *strongly* recommend performing these tasks in a maintenance window or at a time when any interruption will have the least impact on your deployment.

Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300

This section describes device and traffic behavior when you upgrade a Firepower 4100/9300 chassis with FTD.

These scenarios also apply to patch uninstall.

Firepower 4100/9300 Chassis: FXOS Upgrade

Upgrade FXOS on each chassis independently, even if you have inter-chassis clustering or high availability pairs configured. How you perform the upgrade determines how your devices handle traffic during the FXOS upgrade.

Table 138: Traffic Behavior During FXOS Upgrade

Deployment	Method	Traffic Behavior
Standalone	—	Dropped.
High availability	**Best Practice:** Update FXOS on the standby, switch active peers, upgrade the new standby.	Unaffected.
	Upgrade FXOS on the active peer before the standby is finished upgrading.	Dropped until one peer is online.
Inter-chassis cluster (6.2+)	**Best Practice:** Upgrade one chassis at a time so at least one module is always online.	Unaffected.
	Upgrade chassis at the same time, so all modules are down at some point.	Dropped until at least one module is online.
Intra-chassis cluster (Firepower 9300 only)	Hardware bypass enabled: **Bypass: Standby** or **Bypass-Force**. (6.1+)	Passed without inspection.
	Hardware bypass disabled: **Bypass: Disabled**. (6.1+)	Dropped until at least one module is online.
	No hardware bypass module.	Dropped until at least one module is online.

Standalone FTD Device: Firepower Software Upgrade

Firepower devices/security modules operate in maintenance mode while they upgrade. Entering maintenance mode at the beginning of the upgrade causes a 2-3 second interruption in traffic inspection. Interface configurations determine how a standalone device handles traffic both then and during the upgrade.

This table also applies to device revert, regardless of your high availability/scalability configuration.

Table 139: Traffic Behavior During Firepower Software Upgrade: Standalone FTD Device

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force** (6.1+).	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby** (6.1+).	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: **Bypass: Disabled** (6.1+).	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

High Availability Pairs: Firepower Software Upgrade

You should not experience interruptions in traffic flow or inspection while upgrading the Firepower software on devices in high availability pairs. To ensure continuity of operations, they upgrade one at a time. Devices operate in maintenance mode while they upgrade.

The standby device 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.

Clusters: Firepower Software Upgrade

You should not experience interruptions in traffic flow or inspection while upgrading the Firepower software on devices in Firepower Threat Defense clusters. To ensure continuity of operations, they upgrade one at a time. The data security module or modules upgrade first, then the control module. Security modules operate in maintenance mode while they upgrade.

During the control security module upgrade, although traffic inspection and handling continues normally, the system stops logging events. Events for traffic processed during the logging downtime appear with out-of-sync timestamps after the upgrade is completed. However, if the logging downtime is significant, the system may prune the oldest events before they can be logged.

Note Upgrading an inter-chassis cluster from Version 6.2.0, 6.2.0.1, or 6.2.0.2 causes a 2-3 second traffic interruption in traffic inspection when each module is removed from the cluster.

High Availability and Clustering Hitless Upgrade Requirements

Performing hitless upgrades have the following additional requirements.

Flow Offload: 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. To perform a hitless upgrade in a high availability or clustered deployment, you must make sure you are always running 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/FTD 6.2.2.0, and you want to upgrade to FXOS 2.6.1/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.

Version 6.1.0 Upgrades: Performing a hitless upgrade of an FTD high availability pair to Version 6.1.0 requires a preinstallation package. For more information, see Firepower System Release Notes Version 6.1.0 Preinstallation Package.

Traffic Behavior During Deployment

You deploy configurations multiple times during the upgrade process. Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection on all Firepower devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 140: Traffic Behavior During FTD Deployment

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, **Failsafe** enabled or disabled (6.0.1–6.1).	Passed without inspection. A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
	Inline set, **Snort Fail Open: Down**: disabled (6.2+).	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled (6.2+).	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Firepower Threat Defense Upgrade Behavior: Other Devices

This section describes device and traffic behavior when you upgrade Firepower Threat Defense, with the exception of the Firepower 4100/9300.

These scenarios also apply to patch uninstall.

Standalone FTD Device: Firepower Software Upgrade

Firepower devices operate in maintenance mode while they upgrade. Entering maintenance mode at the beginning of the upgrade causes a 2-3 second interruption in traffic inspection. Interface configurations determine how a standalone device handles traffic both then and during the upgrade.

This table also applies to device revert, regardless of your high availability/scalability configuration.

Table 141: Traffic Behavior During Firepower Software Upgrade: Standalone FTD Device

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force** (Firepower 2100 series, 6.3+).	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby** (Firepower 2100 series, 6.3+).	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: **Bypass: Disabled** (Firepower 2100 series, 6.3+).	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

High Availability Pairs: Firepower Software Upgrade

You should not experience interruptions in traffic flow or inspection while upgrading the Firepower software on devices in high availability pairs. To ensure continuity of operations, they upgrade one at a time. Devices operate in maintenance mode while they upgrade.

The standby device 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.

Traffic Behavior During Deployment

You deploy configurations multiple times during the upgrade process. Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection on all Firepower devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 142: Traffic Behavior During FTD Deployment

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, **Failsafe** enabled or disabled (6.0.1–6.1).	Passed without inspection. A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
	Inline set, **Snort Fail Open: Down**: disabled (6.2+).	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled (6.2+).	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Firepower 7000/8000 Series Upgrade Behavior

The following sections describe device and traffic behavior when you upgrade Firepower 7000/8000 series devices.

Standalone 7000/8000 Series: Firepower Software Upgrade

Interface configurations determine how a standalone device handles traffic during the upgrade.

Table 143: Traffic Behavior During Upgrade: Standalone 7000/8000 Series

Interface Configuration	Traffic Behavior
Inline, hardware bypass enabled (**Bypass Mode: Bypass**)	Passed without inspection, although traffic is interrupted briefly at two points: • At the beginning of the upgrade process as link goes down and up (flaps) and the network card switches into hardware bypass. • After the upgrade finishes as link flaps and the network card switches out of bypass. Inspection resumes after the endpoints reconnect and reestablish link with the device interfaces.
Inline, no hardware bypass module,or hardware bypass disabled (**Bypass Mode: Non-Bypass**)	Dropped
Inline, tap mode	Egress packet immediately, copy not inspected
Passive	Uninterrupted, not inspected
Routed, switched	Dropped

7000/8000 Series High Availability Pairs: Firepower Software Upgrade

You should not experience interruptions in traffic flow or inspection while upgrading devices (or device stacks) in high availability pairs. To ensure continuity of operations, they upgrade one at a time. Devices operate in maintenance mode while they upgrade.

Which peer upgrades first depends on your deployment:

- Routed or switched: 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.
- Access control only: Active upgrades first. When the upgrade completes, the active and standby maintain their old roles.

8000 Series Stacks: Firepower Software Upgrade

In an 8000 series stack, devices upgrade simultaneously. Until the primary device completes its upgrade and the stack resumes operation, traffic is affected as if the stack were a standalone device. Until all devices complete the upgrade, the stack operates in a limited, mixed-version state.

Traffic Behavior During Deployment

You deploy configurations multiple times during the upgrade process. Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection on all Firepower devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 144: Traffic Behavior During Deployment: 7000/8000 Series

Interface Configuration	Traffic Behavior
Inline, **Failsafe** enabled or disabled	Passed without inspection A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
Inline, tap mode	Egress packet immediately, copy bypasses Snort
Passive	Uninterrupted, not inspected
Routed, switched	Dropped

ASA FirePOWER Upgrade Behavior

Your ASA service policies for redirecting traffic to the ASA FirePOWER module determine how the module handles traffic during the Firepower software upgrade, including when you deploy certain configurations that restart the Snort process.

Table 145: Traffic Behavior During ASA FirePOWER Upgrade

Traffic Redirection Policy	Traffic Behavior
Fail open (**sfr fail-open**)	Passed without inspection
Fail closed (**sfr fail-close**)	Dropped
Monitor only (**sfr {fail-close}|{fail-open} monitor-only**)	Egress packet immediately, copy not inspected

Traffic Behavior During ASA FirePOWER Deployment

Traffic behavior while the Snort process restarts is the same as when you upgrade the ASA FirePOWER module.

You deploy configurations multiple times during the upgrade process. Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection. Your service policies determine whether traffic drops or passes without inspection during the interruption.

NGIPSv Upgrade Behavior

This section describes device and traffic behavior when you upgrade NGIPSv.

Firepower Software Upgrade

Interface configurations determine how NGIPSv handles traffic during the upgrade.

Table 146: Traffic Behavior During NGIPSv Upgrade

Interface Configuration	Traffic Behavior
Inline	Dropped
Inline, tap mode	Egress packet immediately, copy not inspected
Passive	Uninterrupted, not inspected

Traffic Behavior During Deployment

You deploy configurations multiple times during the upgrade process. Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 147: Traffic Behavior During NGIPSv Deployment

Interface Configuration	Traffic Behavior
Inline, **Failsafe** enabled or disabled	Passed without inspection A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
Inline, tap mode	Egress packet immediately, copy bypasses Snort
Passive	Uninterrupted, not inspected