Planning Your Upgrade

Upgrade Planning Phases

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

Table 1: Upgrade Planning Phases

Planning Phase	Includes
Planning and Feasibility	Assess your deployment. Plan your upgrade path. Read *all* upgrade guidelines and plan configuration changes. Check appliance access. Check bandwidth. Schedule maintenance windows.
Backups	Back up the software. Back up FXOS on the Firepower 4100/9300. Back up ASA for ASA FirePOWER.
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.

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

Current Version and Model Information

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

Table 2:

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

Upgrade Paths

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

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

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 2.

Where Am I Going?

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

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

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

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

How Do I Get There?

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

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

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

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

Can I Maintain Deployment Compatibility?

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

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

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

Upgrade Path: Firepower Management Centers

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

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

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

Table 3: FMC Direct Upgrades

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

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

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

Upgrade Path: Firepower 4100/9300 with FTD Logical Devices

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

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

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

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

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

Table 4: Upgrade Paths: Firepower 4100/9300 with FTD Logical Devices

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

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

Upgrading FXOS with FTD Logical Devices in Clusters or HA Pairs

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

Table 5: FXOS + FTD Upgrade Order

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

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

With older versions, hitless upgrades have some additional requirements.

Table 6: Hitless Upgrades in Older Versions

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

Note on Downgrades

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

Upgrade Path: Other FTD Devices

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

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

Table 7: Upgrade Paths: Firepower 1000/2100 series, ASA 5500-X series, ISA 3000, and Firepower Threat Defense Virtual with FMC

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

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

Upgrade Path: Firepower 7000/8000 Series

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

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

Table 8: Upgrade Paths: Firepower 7000/8000 Series with FMC

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

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

Upgrade Path: ASA FirePOWER

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

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

If desired, you can also upgrade ASA. There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues. For ASA upgrade paths, see Upgrade Path: ASA for ASA FirePOWER, on page 17.

Table 9: Upgrade Paths: ASA FirePOWER with FMC

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

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

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

Upgrading ASA

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

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

Table 10: ASA + ASA FirePOWER Upgrade Order

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

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

Upgrade Path: ASA for ASA FirePOWER

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

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

Table 11: Upgrade Paths: ASA for ASA FirePOWER

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

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

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

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

Upgrade Path: NGIPSv

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

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

Table 12: Upgrade Paths: NGIPSv with FMC

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

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

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

Unresponsive Upgrades

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

Unresponsive FMC or Classic Device Upgrade

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

Unresponsive FTD Upgrade

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

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

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

Time and Disk Space Tests

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

Time Tests

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

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive Upgrades, on page 22.

Table 13: Time Test Conditions for Software Upgrades

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

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

Disk Space Tests

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

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

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

Without enough free disk space, the upgrade fails.

Table 14: Checking Disk Space

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

Download Upgrade Packages

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

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

Firepower Software Packages

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

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

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

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

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

For example:

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

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

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

Firepower Software Upgrade Packages

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

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

Step 2 Click **Upload Update**.

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

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

Step 4 Click **Choose File**.

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

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

Starting with Version 6.6.0, Firepower Threat Defense devices can get upgrade packages from an internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC.

Note This feature is supported only for FTD devices running Version 6.6.0+. It is not supported for upgrades *to* Version 6.6.0, nor is it supported for the FMC or Classic devices.

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

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

Before you begin

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

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

Step 2 Click **Upload Update**.

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

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

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

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

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

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

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

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

Step 6 Click **Save**.

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

Copy to Managed Devices

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

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

Support varies by Firepower version:

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

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

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

  This reduces the length of your upgrade maintenance window.

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

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

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

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

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

Before you begin

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

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

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

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

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

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

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

Step 4 Push the package

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

Firepower Software Readiness Checks

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

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

Run Readiness Checks with FMC (Version 7.0.0+ FTD)

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

See the next topics if you are:

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

Run Readiness Checks with FMC (Version 6.7.0+)

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

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

Before you begin

- Upgrade the FMC to at least Version 6.7.0. If your FMC is currently running an older version, see Run Readiness Checks with FMC (Version 6.0.1–6.6.x), on page 32.
- Upload the upgrade package to the FMC, for the appliance you want to check. If you want to check Version 6.6.0+ FTD devices, you can also specify the upgrade package location on an internal web server. This is required because readiness checks are included in upgrade packages.
- (Optional) If you are upgrading a Classic device to any version, or an FTD device to Version 6.3.0.1–6.6.x, copy the upgrade package to the device. This can reduce the time required to run the readiness check. If you are upgrading an FTD device to Version 6.7.0+, you can skip this step. Although we still recommend you push the upgrade package to the device before you begin the upgrade itself, you no longer have to do so before you run the readiness check.

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

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

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

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

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

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

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

What to do next

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

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

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

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

Before you begin

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

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

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

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

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