

Upgrade the Software

This chapter provides critical and release-specific information.

- Planning Your Upgrade, on page 1
- Minimum Version to Upgrade, on page 2
- Upgrade Guidelines for Version 6.7 Patches, on page 2
- Unresponsive Upgrades, on page 3
- Firepower Threat Defense Upgrade Behavior: Other Devices, on page 4
- Time and Disk Space Tests, on page 11
- Upgrade Instructions, on page 15

Planning Your Upgrade

Careful planning and preparation can help you avoid missteps. This table summarizes the upgrade planning process. For detailed checklists and procedures, see the the appropriate upgrade or configuration guide for full instructions: Upgrade Instructions, on page 15.

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.

Minimum Version to Upgrade

Patches can change the fourth digit *only*. You cannot upgrade directly to a patch from a previous major or maintenance release.

Upgrade Guidelines for Version 6.7 Patches

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

Table 2: Version 6.7.x.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: FMC with Email Alerting for Intrusion Events, on page 2	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

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.

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:

- FMC: Use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page, and from the Message Center.
- FDM: Use the System Upgrade panel.

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/scalability 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.

Firepower Threat Defense Upgrade Behavior: Other Devices

Software Upgrades for Standalone Devices

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.

Table 3: Traffic Behavior: Software Upgrades for Standalone Devices

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.
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.

Software Upgrades for High Availability/Scalability

You should not experience interruptions in traffic flow or inspection while upgrading high availability devices.

- Firepower Threat Defense with FMC: For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.
- Firepower Threat Defense with FDM: For high availability pairs, upgrade the standby, manually switch roles, then upgrade the new standby.

Software Uninstall (Patches)

In Version 6.2.3 and later, uninstalling a patch returns you to the version you upgraded from, and does not change configurations.

- FTD with FMC: For standalone devices, interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In high availability/scalability deployments, you must explicitly plan an uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.
- FTD with FDM: Not supported.

Software Revert (Major/Maintenance Releases)

Reverting returns FTD to its state just before the last major or maintenance upgrade. Regardless of deployment — even for high availability/scalability — you should expect interruptions to traffic flow and inspection. This is because revert is more successful when all units are reverted simultaneously. Simultaneous revert means that interruptions to traffic flow and inspection depend on interface configurations only, as if every device were standalone.

Support for revert begins in Version 6.7.0 for FTD with FDM. It is not supported for FTD with FMC.

Deploying Configuration Changes

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 devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 4: Traffic Behavior: Deploying Configuration Changes

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.
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.

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 5: 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 6: 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

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 7: 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 devices, including those configured

for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 8: 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

Traffic Flow and Inspection

Interruptions in traffic flow and inspection can occur when you:

- Reboot a device.
- Upgrade the device software, operating system, or virtual hosting environment.
- Uninstall or revert the device software.
- Move a device between domains.
- Deploy configuration changes (Snort process restarts).

Device type, high availability/scalibility configurations, and interface configurations 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

FXOS Upgrades

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 9: Traffic Behavior: FXOS Upgrades

Deployment	Method	Traffic Behavior
Standalone	—	Dropped.

Deployment	Method	Traffic Behavior
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.

Software Upgrades for Standalone Devices

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.

Table 10: Traffic Behavior: Software Upgrades for Standalone Devices

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.

Software Upgrades for High Availability/Scalability

You should not experience interruptions in traffic flow or inspection while upgrading high availability or clustered devices.

- FTD with FMC: For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.

  For clusters, the data security module or modules upgrade first, then the control module. 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.

- FTD with FDM: For high availability pairs, upgrade the standby, manually switch roles, then upgrade the new standby.

Software Uninstall (Patches)

In Version 6.2.3 and later, uninstalling a patch returns you to the version you upgraded from, and does not change configurations.

- FTD with FMC: For standalone devices, interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In high availability/scalability deployments, you must explicitly plan an uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.

- FTD with FDM: Not supported.

Software Revert (Major/Maintenance Releases)

Reverting returns FTD to its state just before the last major or maintenance upgrade. Regardless of deployment — even for high availability/scalability — you should expect interruptions to traffic flow and inspection. This

is because revert is more successful when all units are reverted simultaneously. Simultaneous revert means that interruptions to traffic flow and inspection depend on interface configurations only, as if every device were standalone.

Support for revert begins in Version 6.7.0 for FTD with FDM. It is not supported for FTD with FMC.

Deploying Configuration Changes

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 devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 11: Traffic Behavior: Deploying Configuration Changes

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.
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.

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.

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 3.

Table 12: 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.
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 13: 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.
FTD with FDM	Use the **show disk** CLI command.

Time and Disk Space for Version 6.7.0.3

Table 14: Time and Disk Space for Version 6.7.0.3

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	2.9 GB in /var	34 MB in /	—	38 min	7 min
FMCv: VMware	2.6 GB in /var	39 MB in /	—	30 min	5 min
Firepower 1000 series	—	3.3 GB in /ngfw	650 MB	9 min	13 min
Firepower 2100 series	—	3.2 GB in /ngfw	700 MB	7 min	14 min
Firepower 4100 series	—	2.5 GBin /ngfw	450 MB	5 min	7 min
Firepower 4100 series container instance	—	2.4 GB in /ngfw	450 MB	6 min	4 min
Firepower 9300	—	3.1 GB in /ngfw	450 MB	4 min	8 min
ASA 5500-X series with FTD	2.3 GB in /ngfw/Volume	110 MB in /ngfw	380 MB	13 min	9 min
ISA 3000 with FTD	2.2 GB in /ngfw/Volume	110 MB in /ngfw	380 MB	19 min	8 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FTDv: VMware	2.3 GB in /ngfw/Volume	110 MBin /ngfw	380 MB	6 min	5 min
FTDv: KVM	2.3 GB in /ngfw/Volume	110 MB in /ngfw	380 MB	8 min	5 min
ASA FirePOWER	3.1 GB in /var	36 MB in /	450 MB	64 min	6 min
NGIPSv	970 MB in /var	34 MB in /	300 MB	5 min	4 min

Time and Disk Space for Version 6.7.0.2

Table 15: Time and Disk Space for Version 6.7.0.2

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	2.3 GB in /var	20 MB in /	—	35 min	7 min
FMCv: VMware	2.4 GB in /var	23 MB in /	—	28 min	2 min
Firepower 1000 series	—	3.0 GB in /ngfw	610 MB	8 min	13 min
Firepower 2100 series	—	3.0 GB 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 /ngfw	410 MB	5 min	4 min
ASA 5500-X series with FTD	2.2 GB in /ngfw/Volume	110 MB in /ngfw	370 MB	10 min	7 min
ISA 3000 with FTD	2.3 GB in /ngfw/Volume	110 MB in /ngfw	370 MB	17 min	9 min
FTDv: VMware	2.2 GB in /ngfw/Volume	110 MB in /ngfw	370 MB	6 min	4 min
FTDv: KVM	2.2 GB in /ngfw/Volume	110 MB in /ngfw	370 MB	6 min	8 min
ASA FirePOWER	3.0 GB in /var	21 MB in /	430 MB	73 min	4 min
NGIPSv	930 MB in /var	19 MB in /	290 MB	5 min	3 min

Time and Disk Space for Version 6.7.0.1

Table 16: Time and Disk Space for Version 6.7.0.1

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	1.8 GB in /var	20 MB in /	—	32 min	7 min
FMCv: VMware	1.4 GB in /var	23 MB 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 /ngfw	130 MB	5 min	2 min
ASA 5500-X series with FTD	540 MB in /ngfw/Volume	110 MB in /ngfw	88 MB	10 min	12 min
ISA 3000 with FTD	540 MB in /ngfw/Volume	110 MB in /ngfw	88 MB	13 min	7 min
FTDv: VMware	530 MB in /ngfw/Volume	110 MB in /ngfw	88 MB	6 min	4 min
FTDv: KVM	550 MB in /ngfw/Volume	110 MB in /ngfw	88 MB	7 min	3 min
ASA FirePOWER	1.2 GB in /var	21 MB in /	41 MB	66 min	2 min
NGIPSv	82 MB in /var	18 MB in /	9 MB	6 min	3 min

Upgrade Instructions

The release notes do not contain upgrade instructions. After you read the guidelines and warnings in these release notes, see one of the following documents.

Table 17: Firepower Upgrade Instructions

Task	Guide
Upgrade in Firepower Management Center deployments.	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
Upgrade Firepower Threat Defense with Firepower Device Manager.	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager See the *System Management* chapter in the guide for the Firepower Threat Defense version you are currently running—not the version you are upgrading to.
Upgrade FXOS on a Firepower 4100/9300 chassis.	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
Upgrade ASA FirePOWER modules with ASDM.	Cisco ASA Upgrade Guide
Upgrade the ROMMON image on the ISA 3000, ASA 5508-X, and ASA 5516-X.	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.