



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 6.5.0.x Patches](#), on page 2
- [Unresponsive Upgrades](#), on page 2
- [Traffic Flow and Inspection](#), on page 2
- [Time and Disk Space Tests](#), on page 9
- [Upgrade Instructions](#), on page 12

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 12.

Table 1: Upgrade Planning Phases

Planning Phase	Includes
Planning and Feasibility	Assess your deployment. Plan your upgrade path. Read <i>all</i> 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 6.5.0.x Patches

There are no upgrade guidelines that apply specifically to Version 6.5.0 patches.

Unresponsive Upgrades

Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot, shut down, or 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, contact Cisco TAC.

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 the device software.
- Move a device between domains.

- Deploy configuration changes (Snort process restarts).

Device type, high availability/scalability 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 2: Traffic Behavior: FXOS Upgrades

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.

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 (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.

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.

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 5: 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.

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 6: 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.

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 7: 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 8: 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 9: 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

Time and Disk Space Tests

For reference purposes, we provide reports of in-house time and disk space tests for the FTD and FMC software.

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

Even if the system appears inactive, do not manually reboot, shut down, or 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, contact Cisco TAC.

Table 10: Time Test Conditions for Software Upgrades

Condition	Details
Deployment	Times for FTD 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 <i>only</i> . 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 /var) for the device upgrade package. 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.

Table 11: 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.

Version 6.5.0.5 Time and Disk Space

Table 12: Version 6.5.0.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time	Reboot Time
FMC	4.4 GB	28 MB	—	47 min	8 min
FMCv: VMware	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	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	2.2 GB	420 MB	470 MB	6 min	4 min

Version 6.5.0.4 Time and Disk Space

Table 13: Version 6.5.0.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
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	1.9 GB	110 MB	310 MB	9 min
ASA FirePOWER	2.6 GB	20 MB	340 MB	72 min
NGIPSv	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 14: Version 6.5.0.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	2.6 GB	20 MB	—	42 min
FMCv: VMware	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	1.7 GB	110 MB	280 MB	10 min
ASA FirePOWER	2.5 GB	20 MB	320 MB	56 min
NGIPSv	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.

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 15: 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 <i>System Management</i> 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 <i>Upgrade the ROMMON Image</i> section. You should always make sure you have the latest image.