Upgrade the Software

This chapter provides critical and release-specific information.

Upgrade Checklist

This pre-upgrade checklist highlights actions that can prevent common issues. However, we still recommend you refer to the appropriate upgrade or configuration guide for full instructions: Upgrade Instructions, on page 28.

Important At all times during the process, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported. Do not deploy changes to or from, manually reboot, or shut down an upgrading appliance. Do not restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 1:

✓	Action/Check
	Assess your deployment. Determine the current state of your deployment. Understanding where you are determines how you get to where you want to go. 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.
	Plan your upgrade path. This is especially important for multi-appliance deployments, multi-hop upgrades, or situations where you need to upgrade operating systems or hosting environments, all while maintaining deployment compatibility. Always know which upgrade you just performed and which you are performing next. **Note** In FMC deployments, you usually upgrade the FMC, then its managed devices. However, in some cases you may need to upgrade devices first.
	Read ***all*** upgrade guidelines and plan configuration changes. Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. Upgrade guidelines can appear in multiple places. Make sure you read them all. They include: • Upgrade Guidelines for Version 6.2.3.x Patches, on page 6: Important upgrade guidelines that are new or specific to this release. • Known Issues: Be prepared to work around any bugs that affect upgrade. • Features and Functionality: New and deprecated features can require pre- or post-upgrade configuration changes, or even prevent upgrade.
	Check appliance access. Devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also able to access the FMC management interface without traversing the device.
	Check bandwidth. Make sure your management network has the bandwidth to perform large data transfers. In FMC deployments, if you transfer an upgrade package to a managed device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. Whenever possible, copy upgrade packages to managed devices before you initiate the device upgrade. See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).
	Schedule maintenance windows. Schedule maintenance windows when they will have the least impact, considering any effect on traffic flow and inspection and the time the upgrade is likely to take. Also consider the tasks you must perform in the window, and those you can perform ahead of time. For example, do not wait until the maintenance window to copy upgrade packages to appliances, run readiness checks, perform backups, and so on.

Upgrade Packages

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

Table 2:

✓	Action/Check
	Upload upgrade packages. In FMC deployments, upload all upgrade packages—including for managed devices—to the FMC. 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.
	Copy upgrade packages to managed devices. In FMC deployments, we recommend you copy (push) upgrade packages to managed devices before you initiate the device upgrade. **Note** For the Firepower 4100/9300, we recommend (and sometimes require) you copy the upgrade package before you begin the required companion FXOS upgrade.

Backups

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

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

⚠

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

Table 3:

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

✓	Action/Check
	Back up FXOS on the Firepower 4100/9300. Use the Firepower Chassis Manager or the FXOS CLI to export chassis configurations before and after upgrade, including logical device and platform configuration settings.
	Back up ASA for ASA with FirePOWER Services. Use ASDM or the ASA CLI to back up configurations and other critical files before and after upgrade, especially if there is an ASA configuration migration.

Associated Upgrades

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

Table 4:

✓	Action/Check
	Upgrade virtual hosting. If needed, upgrade the hosting environment for any virtual appliances. If this is required, it is usually because you are running an older version of VMware and are performing a major device upgrade.
	Upgrade FXOS on the Firepower 4100/9300. If needed, upgrade FXOS before you upgrade FTD. This is usually a requirement for major upgrades, but very rarely for patches. To avoid interruptions in traffic flow and inspection, upgrade FXOS in FTD high availability pairs and inter-chassis clusters one chassis at a time. **Note** Before you upgrade FXOS, make sure you read all upgrade guidelines and plan configuration changes. Start with the FXOS release notes: Cisco Firepower 4100/9300 FXOS Release Notes.
	Upgrade ASA on ASA with FirePOWER Services. If desired, upgrade ASA. There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues. For standalone ASA devices, upgrade the ASA FirePOWER module just after you upgrade ASA and reload. For ASA clusters and failover pairs, to avoid interruptions in traffic flow and inspection, fully upgrade these devices one at a time. Upgrade the ASA FirePOWER module just before you reload each unit to upgrade ASA. **Note** Before you upgrade ASA, make sure you read all upgrade guidelines and plan configuration changes. Start with the ASA release notes: Cisco ASA Release Notes.

Final Checks

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

Table 5:

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

Upgrade Guidelines for Version 6.2.3.x Patches

This checklist contains upgrade guidelines for Version 6.2.3 patches.

Table 6: Version 6.2.3.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure, on page 6	FTD	6.2.3 through 6.2.3.9	6.2.3.10 only
	Version 6.2.3.3 FTD Device Cannot Switch to Local Management, on page 6	FTD with FMC	6.2.3 through 6.2.3.2	6.2.3.3
	Expired CA Certificates for Dynamic Analysis, on page 7	Any	6.2.3 through 6.2.3.2	6.2.3.1 through 6.2.3.3
	Upgrade Can Unregister FTD/FDM from CSSM, on page 8	FTD with FDM	6.2.3 through 6.2.3.1	6.2.3.2 through 6.2.3.5
	Hotfix Before Upgrading Version 6.2.3-88 FMCs, on page 8	FMC	6.2.3-88	6.2.3.1 through 6.2.3.3

Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure

Deployments: Firepower Threat Defense

Upgrading from: Version 6.2.3 through 6.2.3.9

Directly to: Version 6.2.3.10 only

Known issue: CSCvo39052

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

⚠

Caution If security certifications compliance is enabled and the FSIC fails, the software does not start, remote SSH access is disabled, and you can access the appliance only via local console. If this happens, contact Cisco TAC.

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

Version 6.2.3.3 FTD Device Cannot Switch to Local Management

Deployments: FTD wth FMC

Upgrading from: Version 6.2.3 through Version 6.2.3.2

Directly to: Version 6.2.3.3 only

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

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

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

Expired CA Certificates for Dynamic Analysis

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

Affected Versions: Version 6.0.0+

Resolves: CSCvj07038

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

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

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

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

Table 7: Patches and Hotfixes with New CA Certificates

Versions with Old Cert	First Patch with New Cert	Hotfix with New Cert	
6.2.3 through 6.2.3.3	6.2.3.4	Hotfix G	FTD devices
		Hotfix H	FMC, NGIPS devices
6.2.2 through 6.2.2.3	6.2.2.4	Hotfix BN	All platforms
6.2.1	None. You must upgrade.	None. You must upgrade.	

Versions with Old Cert	First Patch with New Cert	Hotfix with New Cert	
6.2.0 through 6.2.0.5	6.2.0.6	Hotfix BX	FTD devices
		Hotfix BW	FMC, NGIPS devices
6.1.0 through 6.1.0.6	6.1.0.7	Hotfix EM	All platforms
6.0.x	None. You must upgrade.	None. You must upgrade.	

Upgrade Can Unregister FTD/FDM from CSSM

Deployments: FTD with FDM

Upgrading from: Version 6.2.3 or 6.2.3.1

Directly to: 6.2.3.2 through 6.2.3.5

Upgrading a Firepower Threat Defense device managed by Firepower Device Manager may unregister the device from the Cisco Smart Software Manager. After the upgrade completes, check your license status.

Step 1 Click Device, then click View Configuration in the Smart License summary.

Step 2 If the device is not registered, click Register Device.

Hotfix Before Upgrading Version 6.2.3-88 FMCs

Deployments: FMC

Upgrading from: Version 6.2.3-88

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

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

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

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.

Note For the Firepower 4100/9300 with FTD, Firepower 6.2.3.16+ requires FXOS 2.3.1.157 or later build. Upgrade FXOS first.

Time and Disk Space Tests

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

About Time Tests

Time values are based on in-house tests.

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

Table 8: Time Test Conditions

Condition	Details
Deployment	Values are from tests in a Firepower Management Center deployment. Raw upgrade times for remotely and locally managed devices are similar, given similar conditions.
Versions	For major and maintenance releases, we test upgrades from all eligible previous major versions. For patches, we test upgrades from the base version.
Models	In most cases, we test on the lowest-end models in each series, and sometimes on multiple models in a series.
Virtual settings	We test with the default settings for memory and resources.
High availability and scalability	Unless otherwise noted, we test on standalone devices. In a high availability or clustered configuration, devices upgrade one at a time to preserve continuity of operations, with each device operating in maintenance mode while it upgrades. Upgrading a device pair or entire cluster, therefore, takes longer than upgrading a standalone device. Note that stacked 8000 series devices upgrade simultaneously, with the stack operating in limited, mixed-version state until all devices complete the upgrade. This should not take significantly longer than upgrading a standalone device.
Configurations	We test on appliances with minimal configurations and traffic load. Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how those things are affected by the upgrade. For example, if you use a lot of access control rules and the upgrade needs to make a backend change to how those rules are stored, the upgrade can take longer.

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

About Disk Space Requirements

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

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

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

Note When you use the Firepower Management Center to upgrade a managed device, the Firepower Management Center requires additional disk space in /Volume for the device upgrade package .

Checking Disk Space

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

To check disk space:

- Firepower Management Center and its managed devices: Use the System > Monitoring > Statistics page on the FMC. After you select the appliance you want to check, under Disk Usage, expand the By Partition details.
- Firepower Threat Defense with Firepower Device Manager: Use the show disk CLI command.
- ASA FirePOWER with ASDM: Use the Monitoring > ASA FirePOWER Monitoring > Statistics page. Under Disk Usage, expand the By Partition details.

Version 6.2.3.18 Time and Disk Space

Table 9: Version 6.2.3.18 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3	Reboot Time
FMC	3.4 GB	290 MB	—	40 min	9 min
FMCv: VMware 6.0	3.5 GB	250 MB	—	24 min	4 min
Firepower 2100 series	—	2.7 GB	600 MB	13 min	12 min
Firepower 4100 series	—	1.8 GB	400 MB	6 min	6 min
Firepower 9300	—	1.7 GB	400 MB	5 min	9 min
ASA 5500-X series with FTD	2.1 GB	200 MB	420 MB	15 min	53 min
FTDv: VMware 6.0	2.0 GB	200 MB	420 MB	8 min	5 min
Firepower 7000/8000 series	3.5 GB	200 MB	650 MB	10 min	83 min
ASA FirePOWER	3.8 GB	59 MB	580 MB	74 min	59 min
NGIPSv: VMware 6.0	2.3 GB	180 MB	480 MB	6 min	4 min

Version 6.2.3.17 Time and Disk Space

Table 10: Version 6.2.3.17 Time and Disk Space

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

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3	Reboot Time
FTDv: VMware 6.0	2.1 GB	190 MB	420 MB	7 min	5 min
Firepower 7000/8000 series	3.5 GB	200 MB	640 MB	10 min	15 min
ASA FirePOWER	3.8 GB	58 MB	580 MB	72 min	61 min
NGIPSv: VMware 6.0	2.5 GB	180 MB	480 MB	5 min	4 min

Version 6.2.3.16 Time and Disk Space

Table 11: Version 6.2.3.16 Time and Disk Space

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

Version 6.2.3.15 Time and Disk Space

Table 12: Version 6.2.3.15 Time and Disk Space

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

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
Firepower 2100 series	—	2.3 GB	590 MB	27 min
Firepower 4100 series	—	1.7 GB	390 MB	10 min
Firepower 9300	—	2.4 GB	390 MB	11 min
ASA 5500-X series with FTD	2.0 GB	190 MB	410 MB	38 min
FTDv: VMware 6.0	2.4 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.5 GB	210 MB	640 MB	19 min
ASA FirePOWER	3.9 GB	56 MB	580 MB	100 min
NGIPSv: VMware 6.0	2.7 GB	180 MB	470 MB	Hardware dependent

Version 6.2.3.14 Time and Disk Space

Table 13: Version 6.2.3.14 Time and Disk Space

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

Version 6.2.3.13 Time and Disk Space

Table 14: Version 6.2.3.13 Time and Disk Space

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

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

Version 6.2.3.12 Time and Disk Space

Table 15: Version 6.2.3.12 Time and Disk Space

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

Version 6.2.3.11 Time and Disk Space

Table 16: Version 6.2.3.11 Time and Disk Space

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

Version 6.2.3.10 Time and Disk Space

Table 17: Version 6.2.3.10 Time and Disk Space

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

Version 6.2.3.9 Time and Disk Space

Table 18: Version 6.2.3.9 Time and Disk Space

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

Version 6.2.3.8 Time and Disk Space

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

Version 6.2.3.7 Time and Disk Space

Table 19: Version 6.2.3.7 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	2909 MB	137 MB	—	25 min
FMCv	3972 MB	211 MB	—	Hardware dependent
Firepower 2100 series	—	1668 MB	384 MB	19 min
Firepower 4100/9300	—	795 MB	183 MB	8 min
ASA 5500-X series with FTD	1067 MB	130 MB	205 MB	9 min
ISA 3000 with FTD	1080 MB	130 MB	205 MB	20 min
FTDv	1146 MB	130 MB	205 MB	Hardware dependent
Firepower 7000/8000 series	3300 MB	136 MB	477 MB	20 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
ASA FirePOWER	2291 MB	26 MB	411 MB	80 min
NGIPSv	1588 MB	121 MB	327 MB	Hardware dependent

Version 6.2.3.6 Time and Disk Space

Table 20: Version 6.2.3.6 Time and Disk Space

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

Version 6.2.3.5 Time and Disk Space

Table 21: Version 6.2.3.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1566 MB	24 MB	—	28 min
FMCv	2266 MB	80 MB	—	Hardware dependent
Firepower 2100 series	—	1001MB	257 MB	20 min
Firepower 4100/9300	—	370 MB	56 MB	7 min
ASA 5500-X series with FTD	587 MB	130 MB	78 MB	20 min
ISA 3000 with FTD	379 MB	130 MB	78 MB	20 min
Firepower 7000/8000 series	806 MB	17 MB	78 MB	22 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
ASA FirePOWER	1465 MB	15 MB	100 MB	70 min
NGIPSv	120 MB	17 MB	16 MB	Hardware dependent

Version 6.2.3.4 Time and Disk Space

Table 22: Version 6.2.3.4 Time and Disk Space

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

Version 6.2.3.3 Time and Disk Space

Table 23: Version 6.2.3.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1879 MB	88 MB	—	26 min
FMCv	2093 MB	90 MB	—	Hardware dependent
Firepower 2100 series	—	987 MB	255 MB	15 min
Firepower 4100/9300	—	313 MB	54 MB	5 min
ASA 5500-X series with FTD	553 MB	128 MB	77 MB	16 min
ISA 3000 with FTD	307 MB	90 MB	77 MB	15 min
FTDv	307 MB	90 MB	77 MB	Hardware dependent

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
Firepower 7000/8000 series	825 MB	17 MB	77 MB	15 min
ASA FirePOWER	634 MB	16 MB	98 MB	40 min
NGIPSv	102 MB	17 MB	77 MB	Hardware dependent

Version 6.2.3.2 Time and Disk Space

Table 24: Version 6.2.3.2 Time and Disk Space

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

Version 6.2.3.1 Time and Disk Space

Table 25: Version 6.2.3.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1361.8 MB	59.67 MB	—	25 min
FMCv	1240.8 MB	40.8 MB	—	Hardware dependent
Firepower 2100 series	—	948.3 MB	246 MB	81 min
Firepower 4100/9300	—	278 MB	45 MB	8 min
ASA 5500-X series with FTD	275.5 MB	89.9 MB	68 MB	16 min
ISA 3000 with FTD	343.4 MB	127.5 MB	68 MB	15 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FTDv	275.5 MB	89.9 MB	67 MB	Hardware dependent
Firepower 7000/8000 series	99.8 MB	36 MB	10 MB	19 min
ASA FirePOWER	867.9 MB	15.45 MB	32 MB	60 min
NGIPSv	101.9 MB	17.18 MB	9 MB	Hardware dependent

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/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 26: 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.

Deployment	Method	Traffic Behavior
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 27: 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.

- Firepower Threat Defense 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.

- Firepower Threat Defense with FDM: Not supported.

Note Upgrading an inter-chassis cluster from Version 6.2.0, 6.2.0.1, or 6.2.0.2 causes a 2-3 second traffic interruption in traffic inspection when each module is removed from the cluster. Upgrading high availability or clustered devices from Version 6.0.1 through 6.2.2.x may have additional upgrade path requirements; see the upgrade path information in the planning chapter of the Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.

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.

- Firepower Threat Defense 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.

- Firepower Threat Defense 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 28: 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 29: 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 (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: Not supported.

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.

- Firepower Threat Defense 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.
- Firepower Threat Defense 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 30: 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 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 31: 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

Interface Configuration	Traffic Behavior
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 32: Traffic Behavior During Deployment: 7000/8000 Series

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

ASA FirePOWER Upgrade Behavior

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

Table 33: 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 34: 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 35: 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

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 36: 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 5506-X, 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.

Upgrade 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
- 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.

For example:

- Package: `Cisco_Firepower_Mgmt_Center_Patch-6.2.3.1-999.sh.REL.tar`
- Platform: Firepower Management Center
- Package type: Patch
- Version and build: 6.2.3.1-999
- 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.

Software Upgrade Packages

Table 37:

Platform	Package
FMC/FMCv	Sourcefire_3D_Defense_Center_S3
Firepower 2100 series	Cisco_FTD_SSP-FP2K
Firepower 4100/9300	Cisco_FTD_SSP
ASA 5500-X series with FTD ISA 3000 with FTD FTDv	Cisco_FTD
Firepower 7000/8000 series AMP models	Sourcefire_3D_Device_S3
ASA FirePOWER	Cisco_Network_Sensor
NGIPSv	Sourcefire_3D_Device_VMware

ASA and FXOS Upgrade Packages

For information on operating system upgrade packages, see the planning topics in the following guides:

- Cisco ASA Upgrade Guide, for ASA OS
- 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, for FXOS