# 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 18.

**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. In most cases, do not restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, there may be something you can do — see the Note on Unresponsive Upgrades.

### Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

*Table 1:*

| ✓ | Action/Check |
|---|---|
| | Assess your deployment.<br><br>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.<br><br>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.<br><br>**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.<br><br>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:<br><br>• Upgrade Guidelines for Version 6.7.x.x Patches, on page 6: Important upgrade guidelines that are new or specific to this release.<br><br>• Known Issues: Be prepared to work around any bugs that affect upgrade.<br><br>• Features and Functionality: New and deprecated features can require pre- or post-upgrade configuration changes, or even prevent upgrade. |
| | Check appliance access.<br><br>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.<br><br>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.<br><br>See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote). |
| | Schedule maintenance windows.<br><br>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.<br>In FMC deployments, upload FMC and all Classic device (ASA FirePOWER, NGIPSv) upgrade packages to the FMC. For FTD, you can either upload upgrade packages to the FMC, or configure your own internal web server as the source for upgrade packages.<br>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.<br>In FMC deployments, we recommend you copy (push) upgrade packages to managed devices before you initiate the device upgrade.<br>**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.<br>Back up before and after upgrade, when supported:<br>• 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.<br>• 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.<br>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.<br>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.<br>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.<br>If needed, upgrade FXOS before you upgrade FTD. This is usually a requirement for major upgrades, but very rarely for maintenance releases and patches. To avoid interruptions in traffic flow and inspection, upgrade FXOS in FTD high availability pairs and inter-chassis clusters one chassis at a time.<br>**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.<br>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.<br>For standalone ASA devices, upgrade the ASA FirePOWER module just after you upgrade ASA and reload.<br>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.<br>**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.<br><br>Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes. |
| | Check NTP synchronization.<br><br>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.<br><br>To check time:<br><br>• FMC: Choose System > Configuration > Time.<br><br>• Devices: Use the show time CLI command. |
| | Check disk space.<br><br>Run a disk space check for the software upgrade. Without enough free disk space, the upgrade fails.<br><br>See the Upgrade the Software chapter in the Cisco Firepower Release Notes for your target version. |
| | Deploy configurations.<br><br>Deploying configurations before you upgrade reduces the chance of failure. In some deployments, you may be blocked from upgrade if you have out-of-date configurations. In FMC high availability deployments, you only need to deploy from the active peer.<br><br>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.<br><br>See the Upgrade the Software chapter in the Cisco Firepower Release Notes for your target version. |
| | Check running tasks.<br><br>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.<br><br>**Note** In some deployments, upgrades automatically postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot.<br><br>This feature is currently supported for FMCs running Version 6.4.0.10 and later patches, Version 6.6.3 and later maintenance releases, and Version 6.7.0+. Note that this feature is supported for all upgrades from a supported version. This feature is not supported for upgrades to a supported version from an unsupported version. |
| | Run readiness checks.<br><br>We recommend compatibility and readiness checks. These checks assess your preparedness for a software upgrade. |

### Note on Unresponsive Upgrades

Starting with major and maintenance FTD upgrades from Version 6.7.0, you can manually cancel failed or in-progress upgrades, and retry failed upgrades:

- FMC deployments: Use the Upgrade Status pop-up, accessible from the Device Management page and the Message Center.
- FDM deployments: 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. Note that auto-cancel is not supported for patches. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

If you have exhausted all options, or if your deployment does not support cancel/retry, contact Cisco TAC.

# Upgrade Guidelines for Version 6.7.x.x Patches

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

***Table 6: Version 6.7.x.x Guidelines***

| ✓ | Guideline | Platforms | Upgrading From | Directly To |
|---|---|---|---|---|
| | Upgrade Failure: FMC with Email Alerting for Intrusion Events, on page 6 | FMC | 6.2.3 through 6.7.0.x | 6.7.0<br>6.6.0, 6.6.1, or 6.6.3<br>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.

# 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.

# 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 7: Time Test Conditions***

| Condition | Details |
|---|---|
| Deployment | Values are from tests in a Firepower Management Center deployment.<br>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.<br>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. |

| Condition | Details |
|---|---|
| High availability and scalability | Unless otherwise noted, we test on standalone devices.<br>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.<br>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 | Values represent only the time it takes for the software upgrade script to run. This does not include:<br>• Operating system upgrades.<br>• Transferring upgrade packages.<br>• Readiness checks.<br>• VDB and intrusion rule (SRU/LSP) updates.<br>• Deploying configurations.<br>• 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/LSP) updates, and so on.

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

### Checking Disk Space

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

To check disk space:

- 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 6.7.0.3 Time and Disk Space

***Table 8: Version 6.7.0.3 Time and Disk Space***

| Platform | Space in /Volume | Space in / | Space on FMC | Upgrade Time from 6.7.0 | 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 |
| 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 |

# Version 6.7.0.2 Time and Disk Space

*Table 9: Version 6.7.0.2 Time and Disk Space*

| Platform | Space in /Volume | Space in / | Space on FMC | Upgrade Time from 6.7.0 | 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 |

# Version 6.7.0.1 Time and Disk Space

*Table 10: Version 6.7.0.1 Time and Disk Space*

| Platform | Space in /Volume | Space in / | Space on FMC | Upgrade Time from 6.7.0 | 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 |

| Platform | Space in /Volume | Space in / | Space on FMC | Upgrade Time from 6.7.0 | Reboot Time |
|---|---|---|---|---|---|
| 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 |

# 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 11: 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 12: Traffic Behavior: Software Upgrades for Standalone Devices***

| Interface Configuration | | Traffic Behavior |
|---|---|---|
| Firewall interfaces | Routed or switched including EtherChannel, redundant, subinterfaces.<br>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.

- 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: 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.

- 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.

### 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 Firepower Device Manager deployments, and in Version 7.1.0 for Firepower Management Center deployments.

### 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 13: Traffic Behavior: Deploying Configuration Changes***

| Interface Configuration | | Traffic Behavior |
|---|---|---|
| Firewall interfaces | Routed or switched including EtherChannel, redundant, subinterfaces.<br>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.<br>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 14: Traffic Behavior: Software Upgrades for Standalone Devices*

| Interface Configuration | | Traffic Behavior |
|---|---|---|
| Firewall interfaces | Routed or switched including EtherChannel, redundant, subinterfaces.<br>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.

- 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.

### 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 Firepower Device Manager deployments, and in Version 7.1.0 for Firepower Management Center deployments.

### 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 15: Traffic Behavior: Deploying Configuration Changes***

| Interface Configuration | | Traffic Behavior |
|---|---|---|
| Firewall interfaces | Routed or switched including EtherChannel, redundant, subinterfaces.<br>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.<br>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 16: 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 17: 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 18: Traffic Behavior During NGIPSv Deployment*

| Interface Configuration | Traffic Behavior |
|---|---|
| Inline, Failsafe enabled or disabled | Passed without inspection<br>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 19: 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<br>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<br>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
- ASA with FirePOWER Services (ASA 5500-X series): https://www.cisco.com/go/asa-firepower-sw
- ASA with FirePOWER Services (ISA 3000): https://www.cisco.com/go/isa3000-software
- NGIPSv: https://www.cisco.com/go/ngipsv-software

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

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

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

For example:

- Package: `Cisco_Firepower_Mgmt_Center_Patch-6.7.0.1-999.sh.REL.tar`
- Platform: Firepower Management Center
- Package type: Patch
- Version and build: 6.7.0.1-999
- 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 20:***

| Platform | Package |
|---|---|
| FMC/FMCv | Cisco_Firepower_Mgmt_Center |
| Firepower 1000 series | Cisco_FTD_SSP-FP1K |

| Platform | Package |
|---|---|
| Firepower 2100 series | Cisco_FTD_SSP-FP2K |
| Firepower 4100/9300 | Cisco_FTD_SSP |
| ASA 5500-X series with FTD<br>ISA 3000 with FTD<br>FTDv | Cisco_FTD |
| ASA FirePOWER | Cisco_Network_Sensor |
| NGIPSv | Cisco_Firepower_NGIPS_Virtual |

### 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