# Upgrade to Version 6.2.3

These topics provide critical and release-specific information for Version 6.2.3.

# Guidelines and Warnings for Version 6.2.3

These important upgrade guidelines and warnings are *new* for Version 6.2.3.

**Note** If your upgrade path skips one or more major versions—that is, you are not upgrading from the last major version or one of its patches—you must also review Previously Published Guidelines and Warnings, on page 4.

Use the table as a checklist by printing, then marking the column next to the guidelines that apply to you.

*Table 1: Version 6.2.3 Guidelines*

| ✓ | Platforms | Upgrading From | Directly To | Guideline |
|---|---|---|---|---|
|  | FTD clusters | 6.1.x | 6.2.3+ | Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade, on page 2 |
|  | FMC | 6.1.0 through 6.2.2.x | 6.2.3+ | Changes to Result Limits in Reports, on page 2 |
|  | FTD with FDM | 6.2.0 through 6.2.2.x | 6.2.3+ | Upgrade Can Unregister FTD/FDM from CSSM, on page 3 |

| ✓ | Platforms | Upgrading From | Directly To | Guideline |
|---|---|---|---|---|
| | Any | 6.1.0+ | 6.2.3+ | Sharing Data with Cisco During and After Upgrade, on page 3 |
| | Any | 6.1.0 through 6.2.2.x | 6.2.3 only | Edit/Resave Access Control Policies After Upgrade, on page 3 |
| | FTD with FDM | 6.2.0 through 6.2.2.x | 6.2.3 only | Edit/Resave Realms After FTD/FDM Upgrade, on page 4 |
| | Firepower 2100 series with FDM | 6.2.2.5 | 6.2.3 only | Firepower 2100 Series Upgrade from Version 6.2.2.5 Can Fail, on page 4 |

# Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade

**Deployments:** Firepower Threat Defense clusters

**Upgrading from:** Version 6.1.x

**Directly to:** Version 6.2.3+

Firepower Threat Defense Version 6.1.x clusters do not support inter-site clustering (you can configure inter-site features using FlexConfig starting in Version 6.2.0).

If you deployed or redeployed a Version 6.1.x cluster in FXOS 2.1.1, and you entered a value for the (unsupported) site ID, remove the site ID (set to 0) on each unit in FXOS before you upgrade. Otherwise, the units cannot rejoin the cluster after the upgrade.

If you already upgraded, remove the site ID from each unit, then reestablish the cluster. To view or change the site ID, see the Cisco FXOS CLI Configuration Guide.

# Changes to Result Limits in Reports

**Deployments:** Firepower Management Center

**Upgrading from:** Version 6.1 through 6.2.2.x

**Directly to:** Version 6.2.3+

Version 6.2.3 limits the number of results you can use or include in a report section, as follows. For table and detail views, you can include fewer records in a PDF report than in an HTML/CSV report.

*Table 2: New Result Limits in Reports*

| Report Section Type | Max Records: HTML/CSV Report Section | Max Records: PDF Report Section |
|---|---|---|
| Bar chart<br>Pie chart | 100 (top or bottom) | 100 (top or bottom) |
| Table view | 400,000 | 100,000 |
| Detail view | 1,000 | 500 |

If, before you upgrade a Firepower Management Center, a section in a report template specifies a larger number of results than the HTML/CSV maximum, the upgrade process lowers the setting to the new maximum value.

For report templates that generate PDF reports, if you exceed the PDF limit in any template section, the upgrade process changes the output format to HTML. To continue generating PDFs, lower the results limit to the PDF maximum. If you do this after the upgrade, set the output format back to PDF.

## Upgrade Can Unregister FTD/FDM from CSSM

**Deployments:** FTD with FDM

**Upgrading from:** Version 6.2 through 6.2.2.x

**Directly to:** Version 6.2.3+

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**.

## Sharing Data with Cisco During and After Upgrade

**Deployments:** Any

**Upgrading from:** Version 6.1.0+

**Directly to:** Version 6.2.3+

Features in Version 6.2.3+ involve sharing data with Cisco.

*Cisco Network Participation* and *Cisco Success Network* send usage information and statistics to Cisco, which are essential to provide you with technical support. During the upgrade, you accept or decline participation in these programs. You can also opt in or out at any time.

*Web analytics tracking* sends non-personally-identifiable usage data to Cisco, including but not limited to pages viewed, the time spent on a page, browser versions, product versions, user location, and management IP addresses or hostnames of your FMCs.

## Edit/Resave Access Control Policies After Upgrade

**Deployments:** Any

**Upgrading from:** Version 6.1 through 6.2.2.x

**Directly to:** Version 6.2.3 only

If you configured network or port objects that are used *only* in intrusion policy variable sets, deploying associated access control policies after the upgrade fails. If this happens, edit the access control policy, make a change (such as editing the description), save, and redeploy.

# Edit/Resave Realms After FTD/FDM Upgrade

**Deployments:** FTD with FDM

**Upgrading from:** Version 6.2.0 through Version 6.2.2.x

**Directly to:** Version 6.2.3 only

Before Version 6.2.3, users were not automatically logged out after 24 hours of inactivity. After you upgrade Firepower Threat Defense to Version 6.2.3 when using Firepower Device Manager, if you are using identity policies with active authentication, update your realm before you deploy configurations. Choose **Objects** > **Identity Realm**, edit the realm (no changes are needed), and save it. Then, deploy.

# Firepower 2100 Series Upgrade from Version 6.2.2.5 Can Fail

**Deployments:** Firepower 2100 series with FTD, managed by FDM

**Upgrading from:** Version 6.2.2.5

**Directly to:** Version 6.2.3 only

If you change the DNS settings on a Firepower 2100 series device running Version 6.2.2.5, and then upgrade to Version 6.2.3 without an intermediate deployment, the upgrade fails. You must deploy or execute an action that triggers a deployment, such as an SRU update, before you upgrade the device.

# Previously Published Guidelines and Warnings

You can upgrade to Version 6.2.3 from several previous major versions; see Minimum Version to Upgrade, on page 9. If your upgrade path skips one or more major versions, review these previously published guidelines and warnings. Use the table as a checklist by printing, then marking the column next to the guidelines that apply to you.

*Table 3: Previously Published Guidelines*

| ✓ | Platforms | Upgrading From | Guideline |
|---|---|---|---|
| | Any | 6.1.0 through 6.2.2.x | Patch/Hotfix for Dynamic Analysis CA Certificates, on page 7 |
| | FMC | 6.1.x | EOS: Nested Correlation Rules, on page 5 |
| | FMC | 6.1.x | Access Control Can Get Latency-Based Performance Settings from SRUs, on page 5 |
| | FTD with FMC | 6.1.x | 'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 6 |
| | FTD with FDM | 6.2.0 only | FDM Upgrades from Version 6.2.0 Can Fail, on page 4 |

## FDM Upgrades from Version 6.2.0 Can Fail

**Deployments:** FTD with FDM, running on a lower-memory ASA 5500-X series device

**Upgrading from:** Version 6.2.0

**Directly to:** Version 6.2.2+

If you are upgrading from Version 6.2.0, the upgrade may fail with an error of: `Uploaded file is not a valid system upgrade file`. This can occur even if you are using the correct file.

If this happens, you can try the following workarounds:

- Try again.
- Use the CLI to upgrade.
- Upgrade to 6.2.0.1 first.

## EOS: Nested Correlation Rules

**Deployments:** FMC

**Upgrading from:** Version 6.1.x

**Directly to:** Version 6.2+

Version 6.2 ends support for nested correlation rules. Before you upgrade to Version 6.2+, make sure that any nested correlation rules can be "flattened." Otherwise, the upgrade will fail.

### What are Nested Correlation Rules?

A correlation rule is nested if it serves as a trigger for *another correlation rule*. For example, if you create Rule A and Rule B, which both trigger on an intrusion event, you can use 'Rule A is true' as a constraint for Rule B. In this configuration, Rule A is nested inside Rule B.

### Automatic Configuration Changes

The upgrade process flattens certain nested correlation rules by copying settings from the nested correlation rule (Rule A) to the nesting correlation rule (Rule B) and deleting the nested rule. The upgrade also copies the host profile/user qualifications and the snooze/inactive periods from the nested rule to the nesting rule.

For all of these settings except inactive periods, the system can copy the settings from the nested rule to the nesting rule only if the settings are absent from the nesting rule. When the system copies inactive periods from the nested rule to the nesting rule, it retains inactive periods from the nesting rule, so that the resulting rule uses settings from both rules originally involved in the nesting configuration.

### Avoiding Upgrade Failure

The upgrade cannot flatten nested rules if the nested and nesting rule have specific types of conflict. To avoid upgrade failure, modify your correlation rules as follows before you run the upgrade:

- Remove the host profile qualification, user qualification, and snooze period settings from either the nested rule or the nesting rule, so that only one rule in the nested configuration specifies these settings.
- Remove connection trackers from any nested rules.
- Remove host profile qualifications, user qualifications, snooze periods, and inactive periods from nested rules that do not have to be true; that is, remove those elements from nested rules that are linked to other rule conditions using the OR operator, within the nesting rule.

## Access Control Can Get Latency-Based Performance Settings from SRUs

**Deployments:** FMC

**Upgrading from:** 6.1.x

**Directly to:** 6.2+

New access control policies in Version 6.2+ *by default* get their latency-based performance settings from the latest intrusion rule update (SRU). This behavior is controlled by a new **Apply Settings From** option. To configure this option, edit or create an access control policy, click **Advanced**, and edit the Latency-Based Performance Settings.

When you upgrade to Version 6.2+, the new option is set according to your current (Version 6.1.x) configuration. If your current settings are:

- Default: The new option is set to **Installed Rule Update**. When you deploy after the upgrade, the system uses the latency-based performance settings from the latest SRU. It is possible that traffic handling could change, depending on what the latest SRU specifies.
- Custom: The new option is set to **Custom**. The system retains its current performance settings. There should be no behavior change due to this option.

We recommend you review your configurations before you upgrade. From the Version 6.1.x FMC web interface, view your policies' Latency-Based Performance Settings as described earlier, and see whether the **Revert to Defaults** button is dimmed. If the button is dimmed, you are using the default settings. If it is active, you have configured custom settings.

## 'Snort Fail Open' Replaces 'Failsafe' on FTD

**Deployments:** FTD with FMC

**Upgrading from:** Version 6.1.x

**Directly to:** Version 6.2+

In Version 6.2, the Snort Fail Open configuration replaces the Failsafe option on FMC-managed Firepower Threat Defense devices. While Failsafe allows you to drop traffic when Snort is busy, traffic automatically passes without inspection when Snort is down. Snort Fail Open allows you to drop this traffic.

When you upgrade an FTD device, its new Snort Fail Open setting depends on its old Failsafe setting, as follows. Although the new configuration should not change traffic handling, we still recommend that you consider whether to enable or disable Failsafe before you upgrade.

*Table 4: Migrating Failsafe to Snort Fail Open*

| Version 6.1 Failsafe | Version 6.2 Snort Fail Open | Behavior |
|---|---|---|
| Disabled (default behavior) | **Busy**: Disabled<br>**Down**: Enabled | New and existing connections drop when the Snort process is busy and pass without inspection when the Snort process is down. |
| Enabled | **Busy**: Enabled<br>**Down**: Enabled | New and existing connections pass without inspection when the Snort process is busy or down. |

Note that Snort Fail Open requires Version 6.2 on the device. If you are managing a Version 6.1.x device, the FMC web interface displays the Failsafe option.

## Patch/Hotfix for Dynamic Analysis CA Certificates

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

**Affected Versions:** Version 6.0+

**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.

The following 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. For release notes, see Firepower Release Notes.

*Table 5: 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. | |
| 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. | |

# Blacklisted FlexConfig Commands for FTD

Some Firepower Threat Defense features are configured using ASA configuration commands. Beginning with Version 6.2, you can use Smart CLI or FlexConfig to manually configure various ASA features that are not otherwise supported in the web interface.

FTD upgrades can add GUI or Smart CLI support for features that you previously configured using FlexConfig. This can blacklist FlexConfig commands that you are currently using. Although your existing configurations continue to work and you can still deploy, you cannot assign or create FlexConfig objects using the newly blacklisted commands.

After the upgrade, examine your FlexConfig policies and objects. If any contain commands that are now blacklisted, messages indicate the problem. We recommend you redo your configuration. After you are satisfied with the new configuration, you can delete the problematic FlexConfig objects or commands.

For full lists, see the FlexConfig topics in your configuration guide or online help.

# Guidelines and Limitations for All Upgrades

These important guidelines and limitations apply to every upgrade.

### Appliance Access

Before you upgrade a Firepower device, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In Firepower Management Center deployments, you should also able to access the FMC management interface without traversing the device. This is because Firepower devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails.

### Signed Upgrade Packages

So that Firepower can verify that you are using the correct files, upgrade packages from (and hotfixes to) Version 6.2.1+ are *signed* tar archives (.tar). Upgrades from earlier versions continue to use unsigned packages.

When you manually download upgrade packages from the Cisco Support & Download site—for example, for a major upgrade or in an air-gapped deployment—make sure you download the correct package. Do not untar signed (.tar) packages.

**Note** After you upload a signed upgrade package, the GUI can take several minutes to load as the system verifies the package. Remove signed packages after you no longer need them to speed up the display.

### Sharing Data with Cisco During and After Upgrade

Features in Version 6.2.3+ involve sharing data with Cisco.

*Cisco Network Participation* and *Cisco Success Network* send usage information and statistics to Cisco, which are essential to provide you with technical support. During upgrades, you may be asked to accept or decline participation in these programs. You can also opt in or out at any time.

*Web analytics tracking* sends non-personally-identifiable usage data to Cisco, including but not limited to pages viewed, the time spent on a page, browser versions, product versions, user location, and management IP addresses or hostnames of your FMCs.

### Unresponsive Upgrades

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.

# Minimum Version to Upgrade

You can upgrade directly to Version 6.2.3 from several previous major version sequences. You do not need to be running the latest patch of any previous version to upgrade.

***Table 6: Minimum Version to Upgrade Firepower Software to Version 6.2.3***

| Platform | Minimum Version |
|---|---|
| Firepower Management Center<br>All managed devices in FMC deployments | 6.1.0 |
| Firepower Threat Defense with Firepower Device Manager | 6.2.0 |
| ASA FirePOWER with ASDM | 6.2.0 |

# Time Tests and Disk Space Requirements

To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. When you use the Firepower Management Center to upgrade a managed device, the FMC requires additional disk space in its /Volume partition, for the device upgrade package. You must also have enough time to perform the upgrade.

For reference purposes, we provide reports of in-house time and disk space tests.

## About Time Tests

Time values given here 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 (provided below).

### Basic Test Conditions

- Deployment: Values are from tests in a Firepower Management Center deployment. This is because raw upgrade times for remotely and locally managed devices are similar, given similar conditions.
- Versions: For major upgrades, we test upgrades from all eligible previous major versions. For patches, we test upgrades from the base version and from the immediately preceding patch.
- 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.

### Push and Reboot Not Included

Values represent *only* the time it took for the Firepower upgrade script itself to run. Values do not include the time required to upload upgrade packages to a locally managed device or to the FMC, nor the time to copy (*push*) upgrade packages from the FMC to a managed device.

In FMC deployments, insufficient bandwidth between the FMC and managed devices can extend upgrade time or even cause the upgrade to time out. Make sure you have the bandwidth to perform a large data transfer from the FMC to its devices. For more information, see Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).

Values also do not include reboots, readiness checks, operating system upgrades, or configuration deploys.

### Time Is For Single Devices

Values are *per device*. 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.

### Affected Configurations and Data

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.

## About Disk Space Requirements

Space estimates are the *largest* reported for all upgrades, and starting with the Version 6.2.3.10 results, 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).

## Version 6.2.3 Time and Disk Space

*Table 7: Version 6.2.3 Time and Disk Space*

| Platform | Space on /Volume | Space on / | Space on FMC | Time |
|---|---|---|---|---|
| FMC | From 6.1.0: 7415 MB<br>From 6.2.0: 8863 MB<br>From 6.2.1: 8263 MB<br>From 6.2.2: 11860 MB | From 6.1.0: 17 MB<br>From 6.2.0: 24 MB<br>From 6.2.1: 23 MB<br>From 6.2.2: 24 MB | — | From 6.1.0: 38 min<br>From 6.2.0: 43 min<br>From 6.2.1: 37 min<br>From 6.2.2: 37 min |

| Platform | Space on /Volume | Space on / | Space on FMC | Time |
|---|---|---|---|---|
| FMCv | From 6.1.0: 7993 MB<br>From 6.2.0: 9320 MB<br>From 6.2.1: 11571 MB<br>From 6.2.2: 11487 MB | From 6.1.0: 23 MB<br>From 6.2.0: 28 MB<br>From 6.2.1: 24 MB<br>From 6.2.2: 24 MB | — | Hardware dependent |
| Firepower 2100 series | From 6.2.1: 7356 MB<br>From 6.2.2: 11356 MB | From 6.2.1: 7356 MB<br>From 6.2.2: 11356 MB | 1000 MB | From 6.2.1: 15 min<br>From 6.2.2: 15 min |
| Firepower 4100/9300 chassis | From 6.1.0: 5593 MB<br>From 6.2.0: 5122 MB<br>From 6.2.2: 7498 MB | From 6.1.0: 5593 MB<br>From 6.2.0: 5122 MB<br>From 6.2.2: 7498 MB | 795 MB | From 6.1.0: 10 min<br>From 6.2.0: 12 min<br>From 6.2.2: 15 min |
| ASA 5500-X series with FTD | From 6.1.0: 4322 MB<br>From 6.2.0: 6421 MB<br>From 6.2.2: 6450 MB | From 6.1.0: .088 MB<br>From 6.2.0: .092 MB<br>From 6.2.2: .088 MB | 1000 MB | From 6.1.0: 54 min<br>From 6.2.0: 53 min<br>From 6.2.2: 50 min |
| FTDv | From 6.1.0: 4225 MB<br>From 6.2.0: 5179 MB<br>From 6.2.2: 6450 MB | From 6.1.0: .076 MB<br>From 6.2.0: .092 MB<br>From 6.2.2: .092 MB | 1000 MB | Hardware dependent |
| Firepower 7000/8000 series | From 6.1.0: 5145 MB<br>From 6.2.0: 5732 MB<br>From 6.2.2: 6752 MB | From 6.1.0: 18 MB<br>From 6.2.0: 18 MB<br>From 6.2.2: 18 MB | 840 MB | From 6.1.0: 29 min<br>From 6.2.0: 31 min<br>From 6.2.2: 31 min |
| ASA FirePOWER | From 6.1.0: 7286 MB<br>From 6.2.0: 7286 MB<br>From 6.2.2: 10748 MB | From 6.1.0: 16 MB<br>From 6.2.0: 16 MB<br>From 6.2.2: 16 MB | From 6.1.0: 1200 MB<br>From 6.2.0: 1200 MB | From 6.1.0: 94 min<br>From 6.2.0: 104 min<br>From 6.2.2: 96 min |
| NGIPSv | From 6.1.0: 4115 MB<br>From 6.2.0: 5505 MB<br>From 6.2.2: 5871 MB | From 6.1.0: 18 MB<br>From 6.2.0: 19 MB<br>From 6.2.2: 19 MB | 741 MB | Hardware dependent |

# Traffic Flow, Inspection, and Device Behavior

You must identify potential interruptions in traffic flow and inspection during the upgrade. This can occur:

- When a device is rebooted.
- When you upgrade the operating system or virtual hosting environment on a device.
- When you upgrade the Firepower software on a device, or uninstall a patch.

- When you deploy configuration changes as part of the upgrade or uninstall process (Snort process restarts).

Device type, deployment type (standalone, high availability, clustered), and interface configurations (passive, IPS, firewall, and so on) determine the nature of the interruptions. We *strongly* recommend performing any upgrade or uninstall in a maintenance window or at a time when any interruption will have the least impact on your deployment.

# FTD Upgrade Behavior: Firepower 4100/9300 Chassis

This section describes device and traffic behavior when you upgrade a Firepower 4100/9300 chassis with FTD.

### Firepower 4100/9300 Chassis: FXOS Upgrade

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 8: Traffic Behavior During FXOS Upgrade*

| 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) | Fail-to-wire enabled: **Bypass: Standby** or **Bypass-Force**. (6.1+) | Passed without inspection |
| | Fail-to-wire disabled: **Bypass: Disabled**. (6.1+) | Dropped until at least one module is online |
| | No fail-to-wire module. | Dropped until at least one module is online |

### Standalone FTD Device: Firepower Software Upgrade

Interface configurations determine how a standalone device handles traffic during the upgrade.

*Table 9: Traffic Behavior During Firepower Software Upgrade: Standalone FTD Device*

| 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, fail-to-wire enabled: **Bypass: Standby** or **Bypass-Force** (6.1+) | Either:<br>• Dropped (6.1 through 6.2.2.x)<br>• Passed without inspection (6.2.3+) |
| | Inline set, fail-to-wire disabled: **Bypass: Disabled** (6.1+) | Dropped |
| | Inline set, no fail-to-wire module | Dropped |
| | Inline set, tap mode | Egress packet immediately, copy not inspected |
| | Passive, ERSPAN passive | Uninterrupted, not inspected |

### High Availability Pairs: Firepower Software Upgrade

You should not experience interruptions in traffic flow or inspection while upgrading the Firepower software on devices in high availability pairs. To ensure continuity of operations, they upgrade one at a time. Devices operate in maintenance mode while they upgrade.

The standby device 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.

### Clusters: Firepower Software Upgrade

You should not experience interruptions in traffic flow or inspection while upgrading the Firepower software on devices in Firepower Threat Defense clusters. To ensure continuity of operations, they upgrade one at a time. Devices operate in maintenance mode while they upgrade.

The slave security module or modules upgrade first, then the master. Security modules operate in maintenance mode while they upgrade.

During the master 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.

**Note** Upgrading an inter-chassis cluster from Version 6.2.0, Version 6.2.0.1, or Version 6.2.0.2 causes a 2-3 second traffic interruption in traffic inspection when each module is removed from the cluster. Whether traffic drops during this interruption or passes without further inspection depends on how the device handles traffic.

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

*Table 10: Traffic Behavior During FTD Deployment*

| 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 - 6.1.0.x) | 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 |

# FTD Upgrade Behavior: Other Devices

This section describes device and traffic behavior when you upgrade Firepower Threat Defense on Firepower 2100 series, ASA 5500-X series, ISA 3000, and FTDv.

### Standalone FTD Device: Firepower Software Upgrade

Interface configurations determine how a standalone device handles traffic during the upgrade.

*Table 11: Traffic Behavior During Firepower Software Upgrade: Standalone FTD Device*

| 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, fail-to-wire enabled: **Bypass: Standby** or **Bypass-Force** (6.1+) | Either:<br>• Dropped (6.1 through 6.2.2.x)<br>• Passed without inspection (6.2.3+) |
| | Inline set, fail-to-wire disabled: **Bypass: Disabled** (6.1+) | Dropped |
| | Inline set, no fail-to-wire module | Dropped |
| | Inline set, tap mode | Egress packet immediately, copy not inspected |
| | Passive, ERSPAN passive | Uninterrupted, not inspected |

### High Availability Pairs: Firepower Software Upgrade

You should not experience interruptions in traffic flow or inspection while upgrading the Firepower software on devices in high availability pairs. To ensure continuity of operations, they upgrade one at a time. Devices operate in maintenance mode while they upgrade.

The standby device 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.

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

*Table 12: Traffic Behavior During FTD Deployment*

| 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 - 6.1.0.x) | 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 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 13: 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:<br>• At the beginning of the upgrade process as link goes down and up (flaps) and the network card switches into hardware bypass.<br>• 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 Firepower devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

*Table 14: Traffic Behavior During Deployment: 7000/8000 Series*

| 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 |
| 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 15: 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 16: 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 17: 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 have read the upgrade warnings and guidelines in these release notes, see one of:

- Firepower Management Center Upgrade Guide—Upgrade Firepower Management Center deployments, including managed devices and companion operating systems.
- Cisco ASA Upgrade Guide—Upgrade ASA FirePOWER modules managed by ASDM.
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager—Upgrade a Firepower Threat Defense device with Firepower Device Manager.

# Upgrade Packages

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

- Firepower Management Center, including FMCv: 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 FTDv): 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

Upgrade packages from Version 6.2.1+ are signed tar archives (.tar). Do not untar.

*Table 18: Upgrade Packages from Version 6.2.1+*

| Platform | Package |
|---|---|
| FMC/FMCv | Sourcefire_3D_Defense_Center_S3_Upgrade-6.2.3-*build*.sh.REL.tar |
| Firepower 2100 series | Cisco_FTD_SSP_FP2K_Upgrade-6.2.3-*build*.sh.REL.tar |
| Firepower 4100/9300 chassis | Cisco_FTD_SSP_Upgrade-6.2.3-*build*.sh.REL.tar |
| ASA 5500-X series with FTD<br>Firepower Threat Defense Virtual | Cisco_FTD_Upgrade-6.2.3-*build*.sh.REL.tar |
| Firepower 7000/8000 series | Sourcefire_3D_Device_S3_Upgrade-6.2.3-*build*.sh.REL.tar |
| ASA FirePOWER | Cisco_Network_Sensor_Upgrade-6.2.3-*build*.sh.REL.tar |
| NGIPSv | Sourcefire_3D_Device_VMware_Upgrade-6.2.3-*build*.sh.REL.tar |

*Table 19: Upgrade Packages from Version 6.1.x or 6.2.0.x*

| Platform | Package |
|---|---|
| FMC/FMCv | Sourcefire_3D_Defense_Center_S3_Upgrade-6.2.3-*build*.sh |
| Firepower 4100/9300 chassis | Cisco_FTD_SSP_Upgrade-6.2.3-*buildbuild*.sh |
| ASA 5500-X series with FTD<br>FTDv | Cisco_FTD_Upgrade-6.2.3-*build*.sh |
| Firepower 7000/8000 series | Sourcefire_3D_Device_S3_Upgrade-6.2.3-*build*.sh |
| ASA FirePOWER | Cisco_Network_Sensor_Upgrade-6.2.3-*build*.sh |
| NGIPSv | Sourcefire_3D_Device_Virtual64_VMware_Upgrade-6.2.3-*build*.sh |