# Upgrade to Version 6.2.3

This chapter provides critical and release-specific information.

## About Upgrade Guidelines

Upgrading a Firepower deployment can be a complex process. Careful planning and preparation can help you avoid missteps. *Upgrade guidelines and warnings can appear in multiple places in this document.* Use this checklist to make sure you read them all.

*Table 1: Index to Upgrade Guidelines*

| ✓ | Resource | Details |
|---|---|---|
| | Guidelines and Warnings for Version 6.2.3, on page 2 | Read these for important upgrade guidelines and warnings that are new or specific to this release. |
| | Previously Published Guidelines and Warnings, on page 5 | Read these if your upgrade skips versions. |
| | General Guidelines and Warnings, on page 7 | Read these even if you are familiar with the upgrade process, as guidelines may have changed. |
| | Known Issues | Read these and be prepared to work around any bugs that affect upgrade.<br>If your upgrade skips versions, you should also read the known issues for the major versions you are skipping. See the appropriate Cisco Firepower Release Notes. |

| ✓ | Resource | Details |
|---|---|---|
| | Features and Functionality | Read these for additional items that may affect upgrade. Deprecated features especially can require pre-upgrade configuration changes.<br>If your upgrade skips versions, you should also read the new feature documentation for the versions you are skipping. See the appropriate Cisco Firepower Release Notes. |

# Guidelines and Warnings for Version 6.2.3

This checklist contains upgrade guidelines and warnings are new or specific to Version 6.2.3. Review these guidelines if you are currently running **Version 6.1.0 through 6.2.2**.

*Table 2: Version 6.2.3 New Guidelines*

| ✓ | Guideline | Platforms | Upgrading From | Directly To |
|---|---|---|---|---|
| | Sharing Data with Cisco, on page 2 | Any | Any | 6.2.3+ |
| | Upgrade Failure: Firepower 2100 Series from Version 6.2.2.5, on page 3 | Firepower 2100 series with FDM | 6.2.2.5 | 6.2.3 only |
| | Edit/Resave Realms After FTD/FDM Upgrade, on page 3 | FTD with FDM | 6.2.0 through 6.2.2.x | 6.2.3 only |
| | Upgrade Can Unregister FTD/FDM from CSSM, on page 4 | FTD with FDM | 6.2.0 through 6.2.2.x | 6.2.3 through 6.4.0 |
| | Edit/Resave Access Control Policies After Upgrade, on page 4 | Any | 6.1.0 through 6.2.2.x | 6.2.3 only |
| | Changes to Result Limits in Reports, on page 4 | FMC | 6.1.0 through 6.2.2.x | 6.2.3 through 6.4.0 |
| | Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade, on page 5 | FTD clusters | 6.1.0.x | 6.2.3 through 6.4.0 |

# Sharing Data with Cisco

**Deployments:** Any

**Upgrading from:** Version 6.1.0+

**Directly to:** Version 6.2.3+

Some features involve sharing data with Cisco.

### Cisco Success Network

In Version 6.2.3+, *Cisco Success Network* sends usage information and statistics to Cisco, which are essential to provide you with technical support.

During initial setup and upgrades, you may be asked to accept or decline participation. You can also opt in or out at any time.

### Web Analytics tracking

In Version 6.2.3+, *Web analytics tracking* sends non-personally-identifiable usage data to Cisco, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your FMCs.

Web analytics tracking is on by default (and by accepting the Version 6.5.0+ EULA you consent to web analytics tracking), but you can opt out at any time after you complete initial setup.

**Note** Upgrades to Version 6.2.3 through 6.6.x can enable (or reenable) web analytics tracking. This can occur *even if your current setting is to opt out*. If you do not want Cisco to collect this data, opt out after upgrading.

### Cisco Support Diagnostics

In Version 6.5.0+, *Cisco Support Diagnostics* (sometimes called *Cisco Proactive Support*) sends configuration and operational health data to Cisco, and processes that data through our automated problem detection system, allowing us to proactively notify you of issues. This feature also allows Cisco TAC to collect essential information from your devices during the course of a TAC case.

During initial setup and upgrades, you may be asked to accept or decline participation. You can also opt in or out at any time.

## Upgrade Failure: Firepower 2100 Series from Version 6.2.2.5

**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.

## 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.

# 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 through 6.4.0

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**.

# 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.

# Changes to Result Limits in Reports

**Deployments:** Firepower Management Center

**Upgrading from:** Version 6.1.0 through 6.2.2.x

**Directly to:** Version 6.2.3 through 6.4.0

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 3: 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.

## 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 through 6.4.0

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.

# Previously Published Guidelines and Warnings

These previously published guidelines and warnings apply to intermediate releases. Review this checklist if your upgrade path skips versions.

***Table 4: Version 6.2.3 Previously Published Guidelines***

| ✓ | Guideline | Platforms | Upgrading From | Directly To |
|---|---|---|---|---|
| | Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0, on page 5 | FTD with FDM | 6.2.0 only | 6.2.2 through 6.4.0 |
| | Access Control Can Get Latency-Based Performance Settings from SRUs, on page 6 | FMC | 6.1.0.x | 6.2.0 through 6.4.0 |
| | 'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 6 | FTD with FMC | 6.1.0.x | 6.2.0 through 6.4.0 |

## Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0

**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 through 6.4.0

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.

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

**Deployments:** FMC

**Upgrading from:** 6.1.x

**Directly to:** 6.2.0+

New access control policies in Version 6.2.0+ *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 6.2.0+, 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 5: 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.

# General Guidelines and Warnings

These general guidelines and warnings apply to all upgrades.

### Appliance Health and Communication

At all times during the upgrade process, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor. Resolve minor issues before they become major.

### 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.

### Preupgrade Checklist

This checklist highlights actions that can prevent common upgrade issues. However, this list is *not* comprehensive. Refer to the appropriate upgrade guide for full instructions: Upgrade Instructions, on page 22.

*Table 6: Firepower Software Preupgrade Checklist*

| ✓ | Action | Details |
|---|---|---|
| | Deployment assessment. | Before you upgrade any Firepower appliance, determine the current state of your deployment. Understanding where you are determines how you get to where you want to go.<br>You should be able to answer at least the following:<br>• What appliances do you have, and what Firepower version are they running? What version do you want them to run, and can they run that version? Is direct upgrade possible? In an FMC deployment, can you maintain FMC-device compatibility?<br>• Do any of your appliances require a separate operating system upgrade? Do you have virtual appliances that require a hosting environment upgrade?<br>• Are you configured for high availability/scalability? Are your devices deployed passively, as an IPS, as a firewall? |
| | Check management network bandwidth. | To upgrade a Firepower appliance (or perform a readiness check), the upgrade package must be on the appliance. Firepower upgrade package sizes vary. Make sure your management network has the bandwidth to perform large data transfers.<br>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. We recommend you manually push (copy) Firepower upgrade packages to managed devices before you upgrade.<br>See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote). |
| | Verify appliance access. | Firepower devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. 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 FMC deployments, you should also able to access the FMC management interface without traversing the device. |
| | Plan configuration changes. | Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. For example, deprecated FlexConfig commands can cause post-upgrade deployment issues.<br>Use the checklist in About Upgrade Guidelines, on page 1 to identify potential issues. |

| ✓ | Action | Details |
|---|---|---|
| | Perform backups. | Back up Firepower appliances both 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. 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.<br>**Caution** We *strongly* recommend you back up Firepower appliances to a secure remote location and verify transfer success. Backups left on an appliance may be deleted, either manually or by the upgrade process, which purges locally stored backups. And especially because backup files are unencrypted, do *not* allow unauthorized access. If backup files are modified, the restore process will fail.<br>Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. Careful planning and preparation can help you avoid missteps. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your Firepower product. |
| | Run readiness checks. | In FMC deployments, we recommend readiness checks. These checks assess an appliance's preparedness for a Firepower upgrade. They identify issues including database integrity, version inconsistencies, and device registration. |
| | Schedule upgrades. | We recommend you schedule upgrades for at a time when any interruption will have the least impact on your deployment.<br>When you schedule a maintenance window, consider the upgrade's effect on traffic flow and inspection, and how long the upgrade is likely to take. Also consider the tasks you *must* perform in the window, and those you can perform ahead of time. Minimize disruption with careful planning and preparation. Do not wait until the maintenance window to obtain and push upgrade packages, run readiness checks, create backups, and so on. |
| | Verify NTP synchronization. | Make sure Firepower 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 Time Synchronization Status health module does alert if clocks are out of sync by more than 10 seconds, but you should still check manually.<br>To check time:<br>• FMC: Choose **System** > **Configuration** > **Time**.<br>• Devices: Use the **show time** CLI command. |

| ✓ | Action | Details |
|---|---|---|
| | Disable ASA REST API on ASA FirePOWER devices. | Before you upgrade an ASA FirePOWER module, 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 uninstall: `rest-api agent`.<br>Note that ASA 5506-X series devices do not support the ASA REST API if you are also running ASA FirePOWER module (6.0+) |
| | Deploy configurations. | Deploying configurations to out-of-date devices before you upgrade reduces the chance of failure.<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. For more information, see Traffic Flow, Inspection, and Device Behavior, on page 13. |
| | Check running tasks. | Make sure essential tasks are complete before you upgrade. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed.<br>We also recommend you check for tasks that are scheduled to run during the upgrade, and cancel or postpone them. |
| | Check disk space. | Perform a final disk space check. Without enough free disk space, the upgrade fails. For more information, see Time Tests and Disk Space Requirements, on page 11. |

# Minimum Version to Upgrade

You can upgrade directly to Version 6.2.3 as follows. You do not need to be running any specific patch level.

*Table 7: Minimum Version to Upgrade Firepower Software to Version 6.2.3*

| Platform | Minimum Version |
|---|---|
| Firepower Management Center | 6.1.0 |
| Firepower devices with FMC | 6.1.0<br>FXOS 2.3.1.73+ required for Firepower 4100/9300. |
| Firepower devices with FDM | 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.

We provide reports of in-house time and disk space tests for reference purposes.

## About Time Tests

Time values given here are based on in-house tests.

**Note** 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.

### 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.
- 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: 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.

### Time Is For Upgrade Only

Values represent only the time it takes for the Firepower upgrade script to run on each platform. They do *not* include time for:

- Transferring upgrade packages to managed devices, whether before or during upgrade.
- Readiness checks.

- VDB and SRU updates.
- Deploying configurations.
- Reboots (values may be provided separately).

## About Disk Space Requirements

Space estimates are the *largest* reported for all 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).

## Version 6.2.3 Time and Disk Space

***Table 8: 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 |
| 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 |

| Platform | Space on /Volume | Space on / | Space on FMC | Time |
|---|---|---|---|---|
| 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 9300 Chassis

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

### Firepower 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 9: 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) | 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. |

### Standalone FTD Device: Firepower Software Upgrade

Firepower devices/security modules operate in maintenance mode while they upgrade. Entering maintenance mode at the beginning of the upgrade causes a 2-3 second interruption in traffic inspection. Interface configurations determine how a standalone device handles traffic both then and during the upgrade.

*Table 10: Traffic Behavior 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. |

| 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. |

### 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. The data security module or modules upgrade first, then the control module. Security modules operate in maintenance mode while they upgrade.

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.

**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.

### High Availability and Clustering Hitless Upgrade Requirements

Performing hitless upgrades have the following additional requirements.

**Flow Offload:** Due to bug fixes in the flow offload feature, some combinations of FXOS and FTD do not support flow offload; see the Cisco Firepower Compatibility Guide. To perform a hitless upgrade in a high availability or clustered deployment, you must make sure you are always running a compatible combination.

If your upgrade path includes upgrading FXOS to 2.2.2.91, 2.3.1.130, or later (including FXOS 2.4.1.x, 2.6.1.x, and so on) use this path:

1. Upgrade FTD to 6.2.2.2 or later.

2. Upgrade FXOS to 2.2.2.91, 2.3.1.130, or later.

3. Upgrade FTD to your final version.

For example, if you are running FXOS 2.2.2.17/FTD 6.2.2.0, and you want to upgrade to FXOS 2.6.1/FTD 6.4.0, then you can:

1. Upgrade FTD to 6.2.2.5.

2. Upgrade FXOS to 2.6.1.

3. Upgrade FTD to 6.4.0.

**Version 6.1.0 Upgrades:** Performing a hitless upgrade of an FTD high availability pair to Version 6.1.0 requires a preinstallation package. For more information, see Firepower System Release Notes Version 6.1.0 Preinstallation Package.

### 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 11: 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. |

| Interface Configuration | | Traffic Behavior |
|---|---|---|
| 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. |

# FTD Upgrade Behavior: Other Devices

This section describes device and traffic behavior when you upgrade Firepower Threat Defense on Firepower 1000/2100 series, ASA 5500-X series, ISA 3000, and FTDv.

### Standalone FTD Device: Firepower Software Upgrade

Firepower 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 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. |

| 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. |

### 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 13: 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. |

| Interface Configuration | | Traffic Behavior |
|---|---|---|
| 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 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 14: 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 |
| 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 15: 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 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 FMC deployments. | Cisco Firepower Management Center Upgrade Guide |
| Upgrade Firepower Threat Defense Software with FDM. | Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager<br>See the *System Management* chapter in the guide for the FTD 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 |
| Upgrade ASA FirePOWER modules with ASDM. | Cisco ASA Upgrade Guide |
| Upgrade the ROMMON image on the ISA 3000, ASA 5506-X, 5508-X, and 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 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

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

**Tip** An FMC with internet access can download Version 6.2.3.x–6.5.0.x Firepower patches directly from Cisco, about two weeks after they become available for manual download. Direct download from Cisco is *not* supported for:

- Major releases.
- Most patches to Version 6.6 or later.
- In FDM or ASDM deployments.

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

For example:

- Package: `Cisco_Firepower_Mgmt_Center_Upgrade-6.6.0-90.sh.REL.tar`
- Platform: Firepower Management Center
- Package type: Upgrade
- Version and build: 6.6.0-90
- File extension: sh.REL.tar

So that Firepower can verify that you are using the correct files, upgrade packages from 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. To speed up the display, remove signed packages after you no longer need them.

*Table 20: Firepower Software Upgrade Packages*

| Platform | Package |
|---|---|
| FMC/FMCv | Sourcefire_3D_Defense_Center_S3 |
| Firepower 2100 series | Cisco_FTD_SSP-FP2K |

| Platform | Package |
|---|---|
| Firepower 4100/9300 chassis | Cisco_FTD_SSP |
| ASA 5500-X series with FTD<br>ISA 3000 with FTD<br>FTDv | Cisco_FTD |
| Firepower 7000/8000 series<br>AMP models | Sourcefire_3D_Device_S3 |
| ASA FirePOWER | Cisco_Network_Sensor |
| NGIPSv | Sourcefire_3D_Device_VMware |

### Operating System Upgrade Packages

For information on operating system upgrade packages, see the *Planning Your Upgrade* chapters in the following guides:

- Cisco ASA Upgrade Guide, for ASA OS
- Cisco Firepower 4100/9300 Upgrade Guide, for FXOS