Upgrade to Version 6.4.0

This chapter provides critical and release-specific information for Version 6.4.0.
You should also read Features and Functionality for information on any new features and functionality, deprecated features and platforms, menu and terminology changes, blacklisted FlexConfig commands, and so on.

• Guidelines and Warnings for Version 6.4.0, on page 1
• Previously Published Guidelines and Warnings, on page 3
• General Guidelines and Warnings, on page 10
• Minimum Version to Upgrade, on page 12
• Time Tests and Disk Space Requirements, on page 13
• Traffic Flow, Inspection, and Device Behavior, on page 15
• Upgrade Instructions, on page 23
• Upgrade Packages, on page 23

Guidelines and Warnings for Version 6.4.0

This checklist contains important upgrade guidelines and warnings that are new for Version 6.4.0. You should also review Previously Published Guidelines and Warnings, on page 3 and General Guidelines and Warnings, on page 10.

Table 1: Version 6.4.0 New Guidelines

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic,</td>
<td>Firepower 1010</td>
<td>6.4.0</td>
<td>6.4.0.3 through 6.4.0.5</td>
</tr>
<tr>
<td></td>
<td>on page 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Upgrade Failure: Insufficient Disk Space on Container Instances, on page 2</td>
<td>Firepower 4100/9300</td>
<td>6.3.0 through</td>
<td>6.3.0.1 through 6.5.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6.4.0.x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Upgrade Failure: NGIPS Devices Previously at Version 6.2.3.12, on page</td>
<td>Firepower 7000/8000 series</td>
<td>6.2.3 through</td>
<td>6.4.0 only</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>ASA FirePOWER NGIPSv</td>
<td>6.3.0.x</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic

**Deployments:** Firepower 1010 with FTD

**Affected Versions:** Version 6.4.0 to 6.4.0.5

**Related Bug:** CSCvq81354

We strongly recommend you do not configure EtherChannels on Firepower 1010 devices running FTD Version 6.4.0 to Version 6.4.0.5. (Note that Versions 6.4.0.1 and 6.4.0.2 are not supported on this model.)

Due to an internal traffic hashing issue, some EtherChannels on Firepower 1010 devices may blackhole some egress traffic. The hashing is based on source/destination IP address so the behavior will be consistent for a given source/destination IP pair. That is, some traffic consistently works and some consistently fails.

We will fix this issue in an upcoming 6.4.0.x patch. It is also fixed in Version 6.5.0.

Upgrade Failure: Insufficient Disk Space on Container Instances

**Deployments:** Firepower 4100/9300 with FTD

**Upgrading from:** Version 6.3.0 through 6.4.0.x

**Directly to:** Version 6.3.0.1 through Version 6.5.0

Most often during major upgrades — but possible while patching — FTD devices configured with container instances can fail in the precheck stage with an erroneous insufficient-disk-space warning.

If this happens to you, you can try to free up more disk space. If that does not work, contact Cisco TAC.

Upgrade Failure: NGIPS Devices Previously at Version 6.2.3.12

**Deployments:** 7000/8000 series, ASA FirePOWER, NGIPSv

**Related bug:** CSCvp42398

**Upgrading from:** Version 6.2.3 through 6.3.0.x

**Directly to:** Version 6.4.0 only

You cannot upgrade an NGIPS device to Version 6.4.0 if:

- The device previously ran Version 6.2.3.12, and then
- You uninstalled the Version 6.2.3.12 patch, or upgraded to Version 6.3.0.x.
This also includes scenarios where you uninstalled the Version 6.2.3.12 patch and then upgraded to Version 6.3.0.x.

If this is your current situation, contact Cisco TAC.

**TLS Crypto Acceleration Enabled/Cannot Disable**

**Deployments:** Firepower 2100 series, Firepower 4100/9300 chassis

**Upgrading from:** Version 6.1.0 through 6.3.x

**Directly to:** Version 6.4.0+

SSL hardware acceleration has been renamed TLS crypto acceleration.

Depending on the device, TLS crypto acceleration might be performed in software or in hardware. The upgrade automatically enables acceleration on all eligible devices, even if you previously disabled the feature manually. In most cases you cannot configure this feature; it is automatically enabled and you cannot disable it.

**Upgrading to Version 6.4.0:** If you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can use the FXOS CLI to enable TLS crypto acceleration for one container instance per module/security engine. Acceleration is disabled for other container instances, but enabled for native instances.

**Upgrading to Version 6.5.0+:** If you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can use the FXOS CLI to enable TLS crypto acceleration for multiple container instances (up to 16) on a Firepower 4100/9300 chassis. New instances have this feature enabled by default. However, the upgrade does not enable acceleration on existing instances. Instead, use the `config hwCrypto enable` CLI command.

**Firepower 4100/9300 Requires Version 6.2.0 for Upgrade**

**Deployments:** Firepower 4100/9300 with FTD

**Upgrading from:** Version 6.1.x

**Directly to:** Version 6.4.0 only

Unlike other FMC-managed devices, you cannot upgrade the Firepower Threat Defense software directly from Version 6.1 → 6.4 on a Firepower 4100/9300 series device. This is because FXOS 2.6.1 is incompatible with FTD Version 6.1, but required for Version 6.4.

We recommend Version 6.2.3 on FXOS 2.3.1 as the intermediate version—and remember to upgrade FXOS first. Do not use Version 6.3 as an intermediate release; see the guidelines and warnings in the Firepower Release Notes, Version 6.3.0.

**Previously Published Guidelines and Warnings**

Review this checklist if your upgrade path skips major versions. You can upgrade to Version 6.4.0 from several previous major versions; see Minimum Version to Upgrade, on page 12.
## Table 2: Version 6.4.0 Previously Published Guidelines

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Timeouts for the URL Filtering Cache Can Change, on page 5</td>
<td>Any</td>
<td>6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv, on page 5</td>
<td>FMC Firepower 7000/8000 series NGIPSv</td>
<td>6.1.0 through 6.1.0.6 6.2.0 through 6.2.0.6 6.2.1 6.2.2 through 6.2.2.4 6.2.3 through 6.2.3.4</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>RA VPN Default Setting Change Can Block VPN Traffic, on page 5</td>
<td>FTD with FMC</td>
<td>6.2.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Updated Security for Appliance Access, on page 6</td>
<td>Any</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Security Intelligence Enables Application Identification, on page 6</td>
<td>FMC deployments</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Update VDB after Upgrade to Enable CIP Detection, on page 7</td>
<td>Any</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 7</td>
<td>Any</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Syslog Behavior Changes for Connection and Intrusion Events, on page 7</td>
<td>FMC</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Upgrade Can Unregister FTD/FDM from CSSM, on page 8</td>
<td>FTD with FDM</td>
<td>6.2.0 through 6.2.2.x</td>
<td>6.2.3 through 6.4.0</td>
</tr>
<tr>
<td></td>
<td>Changes to Result Limits in Reports, on page 8</td>
<td>FMC</td>
<td>6.1.0 through 6.2.2.x</td>
<td>6.2.3 through 6.4.0</td>
</tr>
<tr>
<td></td>
<td>Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade, on page 9</td>
<td>FTD clusters</td>
<td>6.1.0.x</td>
<td>6.2.3 through 6.4.0</td>
</tr>
<tr>
<td></td>
<td>Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0, on page 9</td>
<td>FTD with FDM</td>
<td>6.2.0 only</td>
<td>6.2.2 through 6.4.0</td>
</tr>
<tr>
<td></td>
<td>Access Control Can Get Latency-Based Performance Settings from SRUs, on page 9</td>
<td>FMC</td>
<td>6.1.0.x</td>
<td>6.2.0 through 6.4.0</td>
</tr>
</tbody>
</table>
Timeouts for the URL Filtering Cache Can Change

**Deployments:** Any

**Upgrading from:** Version 6.2.3.x

**Directly to:** Version 6.3.0+

New for Version 6.3.0, the GUI allows you configure a timeout value for the URL filtering cache. To minimize instances of URLs matching on stale data, you can set URLs in the cache to expire. If you worked with Cisco TAC to specify a timeout value for the URL filtering cache, the upgrade may change that value.

After the upgrade completes:

- FMC: Choose **System > Integration**, click the Cisco CSI tab, and evaluate the **Cached URLs Expire** setting.
- FDM: Choose **System Settings > Traffic Settings > URL Filtering Preferences** and evaluate the **URL Time to Live** setting.

Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv

**Deployments:** FMC, 7000/8000 series devices, NGIPSv

**Upgrading from:** Version 6.1.0 through 6.1.0.6, Version 6.2.0 through 6.2.0.6, Version 6.2.1, Version 6.2.2 through 6.2.2.4, and Version 6.2.3 through 6.2.3.4

**Directly to:** Version 6.3.0+

You cannot run the readiness check on the listed models when upgrading from one of the listed Firepower versions. This occurs because the readiness check process is incompatible with newer upgrade packages.

<table>
<thead>
<tr>
<th>Readiness Check Not Supported</th>
<th>First Patch with Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.0 through 6.1.0.6</td>
<td>6.1.0.7</td>
</tr>
<tr>
<td>6.2.0 through 6.2.0.6</td>
<td>6.2.0.7</td>
</tr>
<tr>
<td>6.2.1</td>
<td>None. Upgrade to Version 6.2.3.5+.</td>
</tr>
<tr>
<td>6.2.2 through 6.2.2.4</td>
<td>6.2.2.5</td>
</tr>
<tr>
<td>6.2.3 through 6.2.3.4</td>
<td>6.2.3.5</td>
</tr>
</tbody>
</table>

RA VPN Default Setting Change Can Block VPN Traffic

**Deployments:** Firepower Threat Defense configured for remote access VPN
Upgrading from: Version 6.2.x
Directly to: Version 6.3+

Version 6.3 changes the default setting for a hidden option, `sysopt connection permit-vpn`. Upgrading can cause your remote access VPN to stop passing traffic. If this happens, use either of these techniques:

- Create a FlexConfig object that configures the `sysopt connection permit-vpn` command. The new default for this command is `no sysopt connection permit-vpn`.
  
  This is the more secure method to allow traffic in the VPN, because external users cannot spoof IP addresses in the remote access VPN address pool. The downside is that the VPN traffic will not be inspected, which means that intrusion and file protection, URL filtering, or other advanced features will not be applied to the traffic.

- Create access control rules to allow connections from the remote access VPN address pool.

  This method ensures that VPN traffic is inspected and advanced services can be applied to the connections. The downside is that it opens the possibility for external users to spoof IP addresses and thus gain access to your internal network.

### Updated Security for Appliance Access

**Deployments:** Any

**Upgrading from:** Version 6.1 through 6.2.3.x

**Directly to:** Version 6.3+

To enhance security, in Version 6.3 we updated the list of supported ciphers and cryptographic algorithms for secure SSH access. If your SSH client fails to connect with a Firepower appliance due to a cipher error, update your client to the latest version.

### Security Intelligence Enables Application Identification

**Deployments:** Firepower Management Center

**Upgrading from:** Version 6.1 through 6.2.3.x

**Directly to:** Version 6.3+

In Version 6.3, Security Intelligence configurations enable application detection and identification. If you disabled discovery in your current deployment, the upgrade process may enable it again. Disabling discovery if you don't need it (for example, in an IPS-only deployment) can improve performance.

To disable discovery you must:

- Delete all rules from your network discovery policy.

- Use only simple network-based conditions to perform access control: zone, IP address, VLAN tag, and port. Do not perform any kind of application, user, URL, or geolocation control.

- (NEW) Disable network and URL-based Security Intelligence by deleting all whitelists and blacklists from your access control policy's Security Intelligence configuration, including the default Global lists.

- (NEW) Disable DNS-based Security Intelligence by deleting or disabling all rules in the associated DNS policy, including the default Global Whitelist for DNS and Global Blacklist for DNS rules.
Update VDB after Upgrade to Enable CIP Detection

Deployments: Any

Upgrading from: Version 6.1.0 through 6.2.3.x, with VDB 299+

Directly to: Version 6.3.0+

If you upgrade while using vulnerability database (VDB) 299 or later, an issue with the upgrade process prevents you from using CIP detection post-upgrade. This includes every VDB released from June 2018 to now, even the latest VDB.

Although we always recommend you update the vulnerability database (VDB) to the latest version after you upgrade, it is especially important in this case.

To check if you are affected by this issue, try to configure an access control rule with a CIP-based application condition. If you cannot find any CIP applications in the rule editor, manually update the VDB.

Invalid Intrusion Variable Sets Can Cause Deploy Failure

Deployments: Any

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3.0+

For network variables in an intrusion variable set, any IP addresses you exclude must be a subset of the IP addresses you include. This table shows you examples of valid and invalid configurations.

<table>
<thead>
<tr>
<th>Valid</th>
<th>Invalid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include: 10.0.0.0/8</td>
<td>Include: 10.1.0.0/16</td>
</tr>
<tr>
<td>Exclude: 10.1.0.0/16</td>
<td>Exclude: 172.16.0.0/12</td>
</tr>
<tr>
<td></td>
<td>Exclude: 10.0.0.0/8</td>
</tr>
</tbody>
</table>

Before Version 6.3.0, you could successfully save a network variable with this type of invalid configuration. Now, these configurations block deploy with the error: Variable set has invalid excluded values.

If this happens, identify and edit the incorrectly configured variable set, then redeploy. Note that you may have to edit network objects and groups referenced by your variable set.

Syslog Behavior Changes for Connection and Intrusion Events

Deployments: Firepower Management Center

Upgrading from: Version 6.1.0 through 6.2.3.x

Directly to: Version 6.3.0+

Version 6.3.0 changes and centralizes the way the system logs connection and intrusion events via syslog. You can access these settings on the new Logging tab in the access control policy.

The upgrade does not change your existing settings for connection event logging. However, you may suddenly start receiving intrusion events you did not "expect" via syslog. This is because after you upgrade to Version 6.3.0+, the intrusion policy sends syslog events to the destination on the new Logging tab. (Before Version
6.3.0, you could configure syslog alerting in an intrusion policy to send events to the syslog on the managed
device itself rather than to an external host.)

Also, messages sent from NGIPS devices (7000/8000 series, ASA FirePOWER, NGIPSv) now use the ISO
8601 timestamp format as specified in RFC 5425.

**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**.

---

**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 4: New Result Limits in Reports**

<table>
<thead>
<tr>
<th>Report Section Type</th>
<th>Max Records: HTML/CSV Report Section</th>
<th>Max Records: PDF Report Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bar chart</td>
<td>100 (top or bottom)</td>
<td>100 (top or bottom)</td>
</tr>
<tr>
<td>Pie chart</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Table view</td>
<td>400,000</td>
<td>100,000</td>
</tr>
<tr>
<td>Detail view</td>
<td>1,000</td>
<td>500</td>
</tr>
</tbody>
</table>

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.

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**

<table>
<thead>
<tr>
<th>Version 6.1 Failsafe</th>
<th>Version 6.2 Snort Fail Open</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled (default behavior)</td>
<td>Busy: Disabled</td>
<td>New and existing connections drop when the Snort process is busy and pass without inspection when the Snort process is down.</td>
</tr>
<tr>
<td></td>
<td>Down: Enabled</td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>Busy: Enabled</td>
<td>New and existing connections pass without inspection when the Snort process is busy or down.</td>
</tr>
<tr>
<td></td>
<td>Down: Enabled</td>
<td></td>
</tr>
</tbody>
</table>

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 important guidelines and warnings apply to every upgrade. However, this list is not comprehensive. For links to additional important information on the upgrade process, which can include planning upgrade paths, OS upgrades, readiness checks, backups, maintenance windows, and so on, see Upgrade Instructions, on page 23.

**Back Up Event and Configuration Data**

We strongly recommend you back up to an external location and verify transfer success. When you upgrade an appliance, it purges locally stored backups. In FMC deployments, we also recommend you back up the FMC after you upgrade your deployment. This is so you have a new FMC backup file that 'knows' that its devices have been upgraded.
As the first step in any backup, note the patch level and VDB version. This is important because if you need to restore the backup to a new or reimaged appliance, you must first update that new appliance to exactly those versions. You can restore a backup only from an appliance of the same model and Firepower version, with the same VDB.

**Verify NTP Synchronization**

Before you upgrade, 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.

To check time:

- **FMC**: Choose **System > Configuration > Time**.
- **Devices**: Use the **show time** CLI command.

**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 Firepower Management Center deployments, you should also be able to access the FMC management interface without traversing the device.

**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.

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.

**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`.

**Sharing Data with Cisco**

Some features involve sharing data with Cisco.

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

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. If you are upgrading from Version 6.1 through 6.2.2.x, the upgrade enables web analytics tracking. If you do not want Cisco to collect this data, you can opt out after the upgrade. (If you are upgrading from Version 6.2.3.x or Version 6.3.0.x, the upgrade process respects your current setting.)

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

**Upgrades Can Import and Auto-Enable Intrusion Rules**

If a newer intrusion rule uses keywords that are not supported in your current Firepower version, that rule is not imported when you update the intrusion rule database (SRU).

After you upgrade the Firepower software and those keywords become supported, the new intrusion rules are imported and, depending on your IPS configuration, can become auto-enabled and thus start generating events and affecting traffic flow.

Supported keywords depend on the Snort version included with your Firepower software:

- FMC: Choose Help > About.
- FTD with FDM: Use the show summary CLI command.
- ASA FirePOWER with ASDM: Choose ASA FirePOWER Configuration > System Information.

You can also find your Snort version on the Bundled Components section of the Cisco Firepower Compatibility Guide.

The Snort release notes contain details on new keywords. You can read the release notes on the Snort download page: https://www.snort.org/downloads.

**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 6.4.0 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 6.4.0**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Minimum Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower Management Center</td>
<td>6.1.0</td>
</tr>
<tr>
<td>All managed devices in FMC deployments except Firepower 4100/9300 series.</td>
<td>6.1.0</td>
</tr>
</tbody>
</table>
Minimum Version

Platform | Minimum Version
--- | ---
Firepower Threat Defense on Firepower 4100/9300 with FMC | 6.2.0 with FXOS 2.6.1.157+
You cannot upgrade FTD directly from Version 6.1 to 6.4 on an FMC-managed Firepower 4100/9300 series device. We recommend Version 6.2.3 on FXOS 2.3.1 as the intermediate version. See Firepower 4100/9300 Requires Version 6.2.0 for Upgrade, on page 3.

If you are upgrading a high availability or clustered deployment from Version 6.2.0.x, 6.2.2.0, or 6.2.2.1 and you require a hitless upgrade, see FTD Upgrade Behavior: Firepower 4100/9300 Chassis, on page 15.

Firepower Threat Defense (all platforms) 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. 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 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 6.4.0 Time and Disk Space

Table 7: Version 6.4.0 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>13.3 GB</td>
<td>26 MB</td>
<td>—</td>
<td>41 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>13.6 GB</td>
<td>29 MB</td>
<td>—</td>
<td>30 min</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>12 MB</td>
<td>8.9 GB</td>
<td>950 MB</td>
<td>20 min</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Deployment</th>
<th>Method</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standalone</td>
<td>—</td>
<td>Dropped</td>
</tr>
</tbody>
</table>
### 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**

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall interfaces</td>
<td>Route or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.</td>
</tr>
</tbody>
</table>
| IPS-only interfaces     | Inline set, fail-to-wire enabled: **Bypass: Standby or Bypass-Force** (6.1+) | Either:  
  • Dropped (6.1 through 6.2.2.x)  
  • 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, 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. Whether traffic drops during this interruption or passes without further inspection depends on how the device handles traffic.

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>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall interfaces</td>
<td>Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.</td>
</tr>
<tr>
<td>IPS-only interfaces</td>
<td>Inline set, Failsafe enabled or disabled (6.0.1 - 6.1.0.x)</td>
</tr>
<tr>
<td></td>
<td>Inline set, Snort Fail Open: Down enabled (6.2+)</td>
</tr>
<tr>
<td></td>
<td>Inline set, Snort Fail Open: Down enabled (6.2+)</td>
</tr>
<tr>
<td></td>
<td>Inline set, tap mode</td>
</tr>
<tr>
<td></td>
<td>Passive, ERSPAN passive</td>
</tr>
</tbody>
</table>

**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**

Interface configurations determine how a standalone device handles traffic during the upgrade.
### Table 11: Traffic Behavior During Firepower Software Upgrade: Standalone FTD Device

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall interfaces Routed or switched including EtherChannel, redundant, subinterfaces Switched interfaces are also known as bridge group or transparent interfaces.</td>
<td>Dropped</td>
</tr>
<tr>
<td>IPS-only interfaces Inline set, fail-to-wire enabled: <strong>Bypass:</strong> Standby or Bypass-Force (6.1+)</td>
<td>Either:</td>
</tr>
<tr>
<td></td>
<td>• Dropped (6.1 through 6.2.2.x)</td>
</tr>
<tr>
<td></td>
<td>• Passed without inspection (6.2.3+)</td>
</tr>
<tr>
<td>Inline set, fail-to-wire disabled: <strong>Bypass:</strong> Disabled (6.1+)</td>
<td>Dropped</td>
</tr>
<tr>
<td>Inline set, no fail-to-wire module</td>
<td>Dropped</td>
</tr>
<tr>
<td>Inline set, tap mode</td>
<td>Egress packet immediately, copy not inspected</td>
</tr>
<tr>
<td>Passive, ERSPAN passive</td>
<td>Uninterrupted, not inspected</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall interfaces</td>
<td>Dropped</td>
</tr>
<tr>
<td><strong>EtherChannel, redundant, subinterfaces</strong></td>
<td></td>
</tr>
<tr>
<td>Switched interfaces are also known as bridge group or</td>
<td></td>
</tr>
<tr>
<td>transparent interfaces.</td>
<td></td>
</tr>
<tr>
<td><strong>IPS-only interfaces</strong></td>
<td></td>
</tr>
<tr>
<td>Inline set, <strong>Failsafe</strong> enabled or disabled (6.0.1 -</td>
<td>Passed without inspection</td>
</tr>
<tr>
<td>6.1.0.x)</td>
<td></td>
</tr>
<tr>
<td>A few packets might drop if <strong>Failsafe</strong> is</td>
<td></td>
</tr>
<tr>
<td>disabled and Snort is busy but not down.</td>
<td></td>
</tr>
<tr>
<td>Inline set, <strong>Snort Fail Open: Down</strong> disabled (6.2+)</td>
<td>Dropped</td>
</tr>
<tr>
<td>Inline set, <strong>Snort Fail Open: Down</strong> enabled (6.2+)</td>
<td>Passed without inspection</td>
</tr>
<tr>
<td>Inline set, tap mode</td>
<td></td>
</tr>
<tr>
<td>Egress packet immediately, copy not inspected</td>
<td></td>
</tr>
<tr>
<td>Passive, ERSPAN passive</td>
<td>Uninterrupted, not inspected</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inline, hardware bypass enabled (<strong>Bypass Mode: Bypass</strong>)</td>
<td>Passed without inspection, although traffic is interrupted briefly at two points:</td>
</tr>
<tr>
<td></td>
<td>• At the beginning of the upgrade process as link goes down and up (flaps) and the network card switches into hardware bypass.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Inline, no hardware bypass module, or hardware bypass disabled (<strong>Bypass Mode: Non-Bypass</strong>)</td>
<td>Dropped</td>
</tr>
</tbody>
</table>
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

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

<table>
<thead>
<tr>
<th>Traffic Redirection Policy</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail open (sfr fail-open)</td>
<td>Passed without inspection</td>
</tr>
<tr>
<td>Fail closed (sfr fail-close)</td>
<td>Dropped</td>
</tr>
<tr>
<td>Monitor only (sfr {fail-close}</td>
<td>{monitor-only} fail-open)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inline</td>
<td>Dropped</td>
</tr>
<tr>
<td>Inline, tap mode</td>
<td>Egress packet immediately, copy not inspected</td>
</tr>
<tr>
<td>Passive</td>
<td>Uninterrupted, not inspected</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inline, <strong>Failsafe</strong> enabled or disabled</td>
<td>Passed without inspection</td>
</tr>
<tr>
<td></td>
<td>A few packets might drop if <strong>Failsafe</strong> is disabled and Snort is busy but not down.</td>
</tr>
<tr>
<td>Inline, tap mode</td>
<td>Egress packet immediately, copy bypasses Snort</td>
</tr>
<tr>
<td>Passive</td>
<td>Uninterrupted, not inspected</td>
</tr>
</tbody>
</table>

**Upgrade Instructions**

The release notes do not contain upgrade instructions. After you read the guidelines and warnings in these release notes, see one of:

- **Cisco Firepower Management Center Upgrade Guide**: Upgrade FMC deployments, including managed devices and companion operating systems.
- **Cisco ASA Upgrade Guide**: Upgrade ASA FirePOWER modules with ASDM.
- **Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager**: Upgrade FTD with FDM.

**Upgrade Packages**

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

- Firepower Management Center, including FMCv: [https://www.cisco.com/go/firepower-software](https://www.cisco.com/go/firepower-software)
- Firepower Threat Defense (all other models, including FTDv): [https://www.cisco.com/go/ftd-software](https://www.cisco.com/go/ftd-software)
- Firepower 7000 series: [https://www.cisco.com/go/7000series-software](https://www.cisco.com/go/7000series-software)
- Firepower 8000 series: [https://www.cisco.com/go/8000series-software](https://www.cisco.com/go/8000series-software)
- NGIPSv: [https://www.cisco.com/go/ngipsv-software](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+**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC/FMCv</td>
<td>Cisco_Firepower_Mgmt_Center_Upgrade-version-build.sh.REL.tar</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>Cisco_FTD_SSP_FP2K_Upgrade-version-build.sh.REL.tar</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>Cisco_FTD_SSP_Upgrade-version-build.sh.REL.tar</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD ISA 3000 with FTD</td>
<td>Cisco_FTD_Upgrade-version-build.sh.REL.tar</td>
</tr>
<tr>
<td>Firepower Threat Defense Virtual</td>
<td></td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>Cisco_Firepower_NGIPS_Appliance_Upgrade-version-build.sh.REL.tar</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>Cisco_Network_Sensor_Upgrade-version-build.sh.REL.tar</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>Cisco_Firepower_NGIPS_Virtual_Upgrade-version-build.sh.REL.tar</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Platform</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC/FMCv</td>
<td>Cisco_Firepower_Mgmt_Center_Upgrade-version-build.sh</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>Cisco_FTD_SSP_Upgrade-version-build.sh</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD Firepower Threat Defense Virtual</td>
<td>Cisco_FTD_Upgrade-version-build.sh</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>Cisco_Firepower_NGIPS_Appliance_Upgrade-version-build.sh</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>Cisco_Network_Sensor_Upgrade-version-build.sh</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>Cisco_Firepower_NGIPS_Virtual_Upgrade-version-build.sh</td>
</tr>
</tbody>
</table>