Important Update Notes

Before you begin the update process to Version 6.2.0, you should familiarize yourself with the behavior of the system during the update process, as well as with any compatibility issues or required pre- or post update configuration changes.

Caution Do *not* update to FXOS Version 2.3.1.56 if you are running an instance of Firepower Threat Defense that has been updated from Version 6.0.1.x of the Firepower System. Doing so may disable your Firepower Threat Defense application, which could interrupt traffic on your network. For more information, see CSCvh64138 in the Cisco Bug Search Tool.

Caution Do *not* reboot or shut down your appliance during the update until you see the login prompt. The system may appear inactive during the prechecks; this is expected behavior and does not require you to reboot or shut down your appliance.

Update Paths to Version 6.2.0

To update to Version 6.2.0, you must be running the following Firepower versions:

- Firepower Management Center—Version 6.1.0
- All other devices—Version 6.1.0

If you update from one major update to another, updating may cause or require significant configuration changes that you must address such as more memory or policy configuration. For example, the Version 6.2.0 update eliminates nested correlation rules, and you may need to take action related to this change.

Another example, updating a Firepower Management Center to Version 6.0 may cause traffic outages and system issues if you are are managing devices running X, Y, or earlier. Before you begin the update to Version 6.0, edit the access control policies deployed to those devices, disable the **Retry URL cache miss lookup** option on the Advanced Options section of the Access Control window, then redeploy. To review the release notes for each destination version on your update path, see the Release Notes page.

Firepower Management Center Update Paths

The following table describes update paths for Firepower Management Centers, including Firepower Management Center Virtual:

Firepower Management Center Platform	Update Path
MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500 Firepower Management Center Virtual: VMware	Version 5.4.1.1+ > Version 6.0.0 PreInstallation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 PreInstallation Package > Version 6.1.0 > Version 6.2.0
Firepower Management Center Virtual: AWS	Version 6.0.1 > Version 6.1.0 PreInstallation Package > Version 6.1.0 > Version 6.2.0
Firepower Management Center Virtual: KVM	Version 6.1.0 > Version 6.2.0

Firepower Threat Defense Update Paths—With Firepower Management Center

This table describes update paths for Firepower Threat Defense devices managed by a Firepower Management Center.

Firepower Threat Defense Platform	Update Path
ASA 5506-X, ASAS 5506H-X, ASA 5506W-X, ASA 5508-X, 16-X ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X Firepower Threat Defense Virtual: VMware Firepower Threat Defense Virtual: AWS Firepower 4110, 4120, 4140 Firepower 9300 with SM-24, SM-36, or SM-44 modules	Version 6.0.1 > Version 6.1.0 PreInstallation Package > Version 6.1.0 > Version 6.2.0
Firepower Threat Defense Virtual: KVM Firepower 4150	Version 6.1.0 > Version 6.2.0
Firepower Threat Defense Virtual: Azure	Version 6.2.0

Firepower Threat Defense Update Paths—With Firepower Device Manager

This table describes update paths for Firepower Threat Defense devices managed by Firepower Device Manager.

Firepower Threat Defense Platform	Update Path
ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X	Version 6.1.0 > Version 6.2.0

NGIPS Update Paths—With Firepower Management Center

This table describes update paths for NGIPS devices (including ASA FirePOWER modules) managed by a Firepower Management Center.

NGIPS Platform	Update Path
Firepower 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125 Firepower 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390 AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390 ASA FirePOWER: ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X ASA FirePOWER: ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60 NGIPSv: VMware	Version 5.4.0.2 > Version 6.0.0 PreInstallation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 PreInstallation Package > Version 6.1.0 > Version 6.2.0
ASA FirePOWER: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X	Version 5.4.1.1 > Version 6.0.0 PreInstallation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 Pre-nstallation Package > Version 6.1.0 > Version 6.2.0

NGIPS Update Paths—ASA FirePOWER with ASDM

This table describes update paths for ASA FirePOWER modules managed by ASDM.

ASA FirePOWER NGIPS Platform	Update Path
ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X	Version 5.4.1.1 > Version 6.0.0 PreInstallation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 PreInstallation Package > Version 6.1.0 > Version 6.2.0

ASA FirePOWER NGIPS Platform	Update Path
ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60	Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 PreInstallation Package > Version 6.1.0 > Version 6.2.0

Update Interface Options

If you are locally managing the ASA FirePOWER module with ASDM, use the ASDM to perform the update. To configure the ASA FirePOWER module through ASDM, see the Cisco ASA with FirePOWER Services Local Management Configuration Guide.

If you are locally managing a Firepower Threat Defense device with the Firepower Device Manager, use the Firepower Device Manager to update your Firepower Threat Defense device. To configure the Firepower Device Manager, see the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

Otherwise, use the Firepower Management Center to update first the Firepower Management Center and then the devices it manages. To configure the Firepower Management Center or its managed devices, see the Firepower Management Center Configuration Guide.

For more information about management, see Management Capability in Version 6.2.0.

Update Sequence Guidelines

Update your Firepower Management Center to at least Version 6.2.0 before updating the devices it manages. Then, use the Firepower Management Center to redeploy policies to all managed devices before updating those devices to Version 6.2.0 .

Note the following update sequence complications when you have high availability or device stacking configured:

Update Sequence for Firepower Management Centers in High Availability

This procedure explains how to upgrade the Firepower software on Firepower Management Centers in a high availability pair.

You upgrade peers one at a time. With synchronization paused, first upgrade the standby (or secondary), then the active (or primary). When the standby Firepower Management Center starts prechecks, its status switches from standby to active, so that both peers are active. This temporary state is called *split-brain* and is *not* supported except during upgrade. Do *not* make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you upgrade the Firepower Management Centers and restart synchronization.

Step 1 Pause the synchronization of the active Firepower Management Center of the high availability pair on the High Availability tab of the Integration page (**System** > **Integration**) as described in the Pausing Communication Between Paired Firepower Management Centers topic in the *Firepower Management Center Configuration Guide*, Version 6.2.0.

Step 2 Update the standby Firepower Management Center in the high availability pair.

After the update is completed, the Firepower Management Center switches from standby to active so both Firepower Management Centers in the high availability pair are active.

Step 3 Update the other Firepower Management Center within the pair.

The update is complete.

Step 4 Click **Make-Me-Active** on the High Availability tab of one of the Firepower Management Center web UIs.

The Firepower Management Center you do not make active automatically switches to standby mode. communication between the Firepower Management Center pairs automatically restarts.

Update Sequence for Firepower Threat Defense Devices in High Availability

Update the FXOS chassis of Firepower Threat Defense devices in a high availability pair to the most recent compatible FXOS version before installing the most recent Firepower version. For more information on FXOS versions, see the Firepower Compatibility Guide.

Caution You must *always* update the FXOS version on the standby device of a Firepower Threat Defense high availability pair. Do not update the FXOS version of the active device.

Note For Firepower Threat Defense high availability in Version 6.2.0, 169.254.0.0/16 and fd00:0:0:*::/64 are internally used subnets and cannot be used for the failover or state links. If you currently use IP addresses in this range, then you must change them to different IP addresses before you upgrade

Step 1 Update the FXOS version on the standby Firepower Threat Defense device within the high availability pair.

Step 2 Switch the active peer so the standby Firepower Threat Defense device is now the active device.

Step 3 Update the FXOS version on the standby Firepower Threat Defense device within the high availability pair.

What to do next

Update the Firepower Threat Defense high availabiltiy pair to the most recent Firepower version.

When you install a Firepower update on Firepower Threat Defense devices in a high availability pair, the devices are updated one at a time. When the update starts, Firepower first applies it to the standby device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. Once the standby Firepower Threat Defense update is complete, the active Firepower Threat Defense automatically fails over to standby mode and then is updated.

Update Sequence for Clustered FTD Devices

When you update clustered Firepower 9300 or Firepower 4100 series devices running Firepower Threat Defense, the system updates the security modules one at a time—first the secondary security modules, then the primary security module. Modules operate in maintenance mode while they are updated.

During the primary security module update, although traffic inspection and handling continues normally, the system stops logging events. Event logging resumes after the full update is completed.

Caution Updating FXOS reboots the device, which can affect traffic in a clustered environment until at least one module comes online. In an intra-chassis cluster, traffic drops if the cluster does not use an optional hardware bypass (fail-to-wire) module or if bypass is disabled. Traffic passes without inspection if bypass is enabled. In an inter-chassis cluster, traffic drops during the reboot if chassis reboots overlap before at least one module comes online; traffic is unaffected if there is no reboot overlap.

For more information, see the About Clustering on the Firepower 4100/9300 Chassis chapter of the *Firepower Management Center Configuration Guide* and the About Clustering on the Firepower 4100/9300 Chassis chapter of the *Cisco FXOS Firepower Chassis Manager Configuration Guide*.

Events for traffic processed during the logging downtime appear with out-of-sync timestamps after the update is complete. However, if the logging downtime was significant, the system may not log some of the oldest events because it may prune them before they can be logged.

Update Sequence for 7000 and 8000 Series Devices in High Availability

Note You cannot locally update 7000 and 8000 Series devices in a high availability pair. You *must* update from the managing Firepower Management Center.

When you install an update on 7000 and 8000 Series devices in a high availability pair, the system updates the devices one at a time. When the update starts, the system first applies it to the standby device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. The standby device then takes over the active role and the system updates the formerly active device, which follows the same process.

Update Sequence for High Availability 7000 and 8000 Series Devices in Inline Deployment

When you install an update on 7000 Series or 8000 Series devices in high availability configured for inline deployment, the system performs the update on the devices one at a time. The system first applies it to the primary device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. While the primary device is updated in maintenance mode, the secondary device temporarily becomes primary and does not drop traffic. When the primary device update is complete, the primary device moves from maintenance mode to primary mode and the system updates the secondary device.

Update Sequence for Stacked 8000 Series Devices

When you install an update on 8000 Series stacked devices, Firepower updates the stacked devices simultaneously. Each device resumes normal operation when the update is complete. Note the following scenarios:

- If the active device completes the update before all of the standby devices, the stack operates in a limited, mixed-version state until all devices have completed the update.
- If the active device completes the update after all of the standby devices, the stack resumes normal operation when the update is complete on the active device.

Preupdate Readiness Checks

Caution Do *not* reboot or shut down an appliance during the readiness check. If your appliance fails the readiness check, correct the issues and run the readiness check again. If the readiness check exposes issues that you cannot resolve, do not begin the upgrade. Instead, contact Cisco TAC.

- Checks Firepower software readiness only—The readiness check does not assess preparedness for intrusion rule, VDB, or GeoDB updates.
- Version 6.1+ required—The readiness check was introduced in Version 6.1. A readiness check on the upgrade *to* Version 6.1 may not return accurate results.
- Web interface vs shell—You can use the Firepower Management Center web interface to perform the readiness check on itself and its standalone managed devices only. For clustered devices, stacked devices, and devices in high availability pairs, run the readiness check from each device's shell.
- Time requirements—The time required to run the readiness check varies depending on your appliance model and database size. You may find it expedient to forgo readiness checks if your deployment is large (for example, if your Firepower Management Center manages more than 100 devices).

Run a Readiness Check through the Shell

For clustered devices, stacked devices, and devices in high availability pairs, you *must* use the shell.

Before you begin

- Download the upgrade package for the appliance whose readiness you want to check. Readiness checks are included in upgrade packages.
- Deploy configurations to managed devices whose configurations are out of date. Otherwise, the readiness check may fail.

Step 1 Log into the shell as a user with administrator privileges.

Step 2 Make sure the upgrade package is on the appliance in the correct place:

- Firepower Threat Defense devices: `/ngfw/var/sf/updates`
- All other Firepower appliances: `/var/sf/updates`

On Firepower Management Centers, you can use the web interface to upload the upgrade package.

If you cannot or do not want to use the Firepower Management Center web interface, use SCP to copy the upgrade package to the appliance. Initiate from the Firepower side.

Step 3 Run this command as the root user:

```
sudo install_update.pl --detach --readiness-check full_path_to_update_package
```

Unless you are running the readiness check from the console, use the `--detach` option to ensure the check does not stop if your user session times out. Otherwise, the readiness check runs as a child process of the user shell. If your connection is terminated, the process is killed, the check is disrupted, and the appliance may be left in an unstable state.

Step 4 (Optional) Monitor the readiness check.

If you use the `--detach` option (or begin another shell session), you can use the `tail` or `tailf` command to display logs, for example:

- Firepower Threat Defense devices: `tail /ngfw/var/log/sf/update_package_name/status.log`
- All other Firepower appliances: `tail /var/log/sf/update_package_name/status.log`

If you use `tailf` to display log entries as they occur, you must cancel (Ctrl+C) to return to the command prompt.

Step 5 When the readiness check completes, access the full readiness check report.

- Firepower Threat Defense devices: `/ngfw/var/log/sf/$rpm_name/upgrade_readiness`
- All other Firepower appliances: `/var/log/sf/$rpm_name/upgrade_readiness`

Run a Readiness Check through the Firepower Management Center Web Interface

You can use the Firepower Management Center web interface to perform readiness checks on itself and its standalone managed devices.

Before you begin

- Readiness checks are included in upgrade packages. Note that upgrade packages from Version 6.2.1+ are *signed*, and terminate in .sh.REL.tar instead of just .sh. Do *not* untar signed upgrade packages before performing either a readiness check or the upgrade itself.
- Redeploy configuration changes to any managed devices. Otherwise, the readiness check may fail.

Step 1 On the Firepower Management Center web interface, choose **System** > **Updates**.

Step 2 Click the Install icon next to the upgrade you want the readiness check to evaluate.

Step 3 Click **Launch Readiness Check**.

Step 4 Monitor the progress of the readiness check in the Message Center.
When the readiness check completes, the system reports success or failure on the Readiness Check Status page.

Step 5 Access the full readiness check report in `/var/log/sf/$rpm_name/upgrade_readiness`.

Preupdate Modifications to Correlation Policies

If you are updating a Firepower Management Center where you configured correlation policies, follow the rule modifications listed below. If you reimage the Firepower Management Center rather than update it, or if you have not configured correlation policies, the rule modifications listed below are not required.

Version 6.2.0 no longer supports nested correlation rules. In earlier releases, you can use a correlation rule as a trigger for another correlation rule if the rules share a base event type. For example, if you create Rule A and Rule B, which both trigger on an intrusion event, you can use the criteria "Rule A is true" as a constraint for Rule B. In this configuration, Rule A is considered "nested" within Rule B.

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

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

The update cannot flatten nested rules if the nested and nesting rule have specific types of conflict. In these cases, the update fails.

To avoid this failure, modify your correlation rules as follows before you run the update:

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

For information on correlation rules, see the Firepower Management Center Configuration Guide.

Preupdate Configuration and Event Backups

Before you begin the update, we *strongly* recommend that you back up current event and configuration data to an external location. If you back up to an external location, verify the external backup is successful before updating the system.

The Firepower Management Center purges locally stored backups from previous updates. To retain archived backups, store the backups externally. Use the Firepower Management Center to back up event and configuration data for itself and the devices it manages. For more information on the backup and restore feature, see the Firepower Management Center Configuration Guide.

Use the Firepower Device Manager to back up event and configuration data for the device it manages. For more information on the backup and restore feature, see the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

Traffic Flow and Inspection During the Update

When you update your sensing devices, traffic either drops throughout the update or traverses the network without inspection depending on how your devices are configured and deployed: routed or transparent, inline versus passive, bypass mode settings, and so on. We *strongly* recommend performing the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.

Note When you update devices in a high availability pair, the system performs the update one device at a time to avoid traffic interruption.

This section discusses traffic behavior during the followng update stages:

- The update itself, including related reboots
- FXOS updates on clustered Firepower Threat Defense devices
- Configuration deployments after the update

Traffic Behavior During the Update

The following table describes how updates, including related device reboots, affect traffic flow for different deployments. Note that switching, routing, NAT, and VPN are not performed during the update process, regardless of how you configure any inline sets.

Caution Do *not* update to FXOS Version 2.3.1.56 if you are running an instance of Firepower Threat Defense that has been updated from Version 6.0.1.x of the Firepower System. Doing so may disable your Firepower Threat Defense application, which could interrupt traffic on your network. For more information, see CSCvh64138 in the Cisco Bug Search Tool.

Table 1: Update Traffic Behavior

Device	Deployment	Traffic Behavior
Firepower Threat Defense	inline with optional hardware bypass module; bypass enabled: (**Bypass: Standby** or **Bypass-Force**) or, bypass disabled: (**Bypass: Disabled**)	dropped
Firepower Threat Defense Firepower Threat Defense Virtual	inline with no hardware bypass module; routed, transparent (including EtherChannel, redundant, subinterface)	
	inline in tap mode	egress packet immediately, copy not inspected
	passive	uninterrupted, not inspected
7000 and 8000 Series	inline with optional hardware bypass module, bypass enabled (**Bypass Mode: Bypass**)	passed without inspection Note that traffic is interrupted briefly at two points: • At the beginning of the update process as link goes down and up (flaps) and the network card switches into hardware bypass. • After the update 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. The hardware bypass option is *not* supported on nonbypass network modules on Firepower 8000 series devices, or SFP transceivers on Firepower 7000 series.
	inline with optional hardware bypass module, bypass disabled (**Bypass Mode: Non-Bypass**)	dropped

Device	Deployment	Traffic Behavior
7000 and 8000 Series NGIPSv	inline with no hardware bypass module	dropped
	inline in tap mode	egress packet immediately, copy not inspected
	passive	uninterrupted, not inspected
	routed, switched	dropped
ASA FirePOWER	routed or transparent, fail-open (**Permit Traffic**)	passed without inspection (requires the latest supported ASA OS version; otherwise, traffic dropped)
	routed or transparent, fail-close (**Close Traffic**)	dropped

Caution Rebooting the ASA FirePOWER module on an ASA 5585-X, including a reboot that occurs during a module upgrade, causes traffic to drop for up to thirty seconds on the interfaces on the ASA FirePOWER hardware module while the module reboots.

Traffic Behavior When Updating FXOS on Clustered Firepower Threat Defense Devices

Updating FXOS reboots the chassis, which can affect traffic in a clustered environment until at least one module comes online. Whether and how traffic is affected depends on the cluster type:

- **Intra-chassis cluster**—Traffic drops if the cluster does not use an optional hardware bypass (fail-to-wire) module or if bypass is disabled. Traffic passes without inspection if bypass is enabled.
- **Inter-chassis cluster**—Traffic drops during the overlap if multiple chassis reboots overlap before at least one module comes online. Traffic is unaffected if there is no reboot overlap.

  For example, there would be no reboot overlap, and no dropped traffic, if you complete the FXOS update first on one chassis and then on another. Depending on when each update is initiated, there could be reboot overlap (and dropped traffic) if you update multiple chassis simultaneously.

The following table summarizes this behavior.

Table 2: Traffic Behavior During an FXOS Update of Clustered Firepower Threat Defense Devices

Device Model	Deployment	Traffic Behavior
Firepower 9300	Intra-chassis cluster without optional hardware bypass module	Dropped
	Intra-chassis cluster with optional hardware bypass module, bypass disabled	Dropped
	Intra-chassis cluster with optional hardware bypass module, bypass enabled	Passed without inspection
Firepower 9300 Firepower 4100 Series	Inter-chassis cluster with no reboot overlap	Unaffected
	Inter-chassis cluster with reboot overlap before at least one module comes online	Dropped

Traffic Behavior During Configuration Deployment

During the upgrade process, you deploy configurations either twice (standalone devices) or three times (devices managed by the Firepower Management Center). When you deploy, resource demands may result in a small number of packets dropping without inspection. In most cases, the deployment immediately after the upgrade restarts the Snort process. During subsequent deployments, the Snort process restarts only if, before deploying, you modify specific policy or device configurations that always restart the process when deployed.

The following table describes how different devices handle traffic during Snort process restarts.

Table 3: Restart Traffic Effects by Managed Device Model

Device Model	Interface Configuration	Restart Traffic Behavior
Firepower Threat Defense, Firepower Threat Defense Virtual	Inline, **Snort Fail Open: Down**: disabled	Dropped
	Inline, **Snort Fail Open: Down**: enabled	Passed without inspection
	Routed, transparent (including EtherChannel, redundant, subinterface) CLI command: **configure snort preserve-connection enable** (default); this functionality requires Version 6.2.0.2 or a subsequent 6.2.0.x patch	Existing flows: passed without inspection New flows: dropped
	Routed, transparent (including EtherChannel, redundant, subinterface) CLI command, Version 6.2.0.2 or a subsequent 6.2.0.x patch: **configure snort preserve-connection disable**	Dropped
	Inline, tap mode	Egress packet immediately, copy bypasses Snort
	Passive	Uninterrupted, not inspected
7000 and 8000 Series, NGIPSv	Inline, **Failsafe** enabled or disabled	Passed without inspection A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
	Inline, tap mode	Egress packet immediately, copy bypasses Snort
	Passive	Uninterrupted, not inspected
7000 and 8000 Series	Routed, switched, transparent	Dropped
ASA FirePOWER	Routed or transparent with fail-open (**Permit Traffic**)	Passed without inspection
	Routed or transparent with fail-close (**Close Traffic**)	Dropped

Automatic Modifications to Failsafe Configuration during Update

In Version 6.2.0, the Snort Fail Open configuration replaces the Failsafe option on FTD physical and virtual devices managed by a Firepower Management Center. This new feature provides the same functionality as the Failsafe option, but it also lets you choose whether to drop traffic when the Snort process is down.

When you update a Firepower Management Center to Version 6.2.0, Failsafe is still supported for the following managed devices:

- FTD devices running Version 6.1.x
- 7000 Series, 8000 Series, and NGIPSv devices running Version 6.2.0

When you update a FTD device to Version 6.2.0, the update determines whether Failsafe is enabled and, if so, migrates the Failsafe option to a matching Snort Fail Open configuration. We **strongly** recommend that you consider whether to enable or disable Failsafe before updating your FTD device.

Table 4: Migrating Failsafe to Snort Fail Open

When Version 6.1 Failsafe is…	Snort Fail Open is set to...	
	Busy	**Down**
disabled (default behavior) New and existing connections drop when the Snort process is busy and pass without inspection when the Snort process is down	disabled New and existing connections drop when the Snort process is busy	enabled New and existing connections pass without inspection when the Snort process is down
enabled New and existing connections pass without inspection when the Snort process is busy or down	enabled New and existing connections pass without inspection when the Snort process is busy	enabled New and existing connections pass without inspection when the Snort process is down

For more information, see the Firepower Management Center Configuration Guide.

Additional Memory Requirements When Version 6.0 is in Your Update Path

If your update path to Verison 6.2.0 begins with Verison 5.4.x or earlier, you may need to update your Firepower Management Center memory before you update to Version 6.0. You must update the Firepower Management Center memory before you update to Verison 6.2.0. See Update Paths to Version 6.2.0, on page 1 for more information.

Firepower Version 6.0 requires more memory than the previous versions for some Firepower Management Center models (previously referred to as the FireSIGHT Management Center or the Defense Center). To be

specific, MC750 requires two 4GB dual in-line memory modules (DIMM). Similarly, MC1500 with 6GB of memory also requires additional memory.

Because the increase in memory was driven by Cisco product requirements, we make memory upgrade kits available for customers with these models. You can order these kits at no cost if you are entitled to run Version 6.0 or later on a qualifying MC750 or MC1500 Firepower Management Center model.

For more information on ordering memory kits, see http://www.cisco.com/c/en/us/support/docs/field-notices/640/fn64077.html. For instructions on replacing the memory after you receive the kit, see "Memory Upgrade Instructions for Firepower Management Centers" in the *Cisco Firepower Management Center 750, 1500, 2000, 3500, 4000, 4500 Hardware Installation Guide*.

Time and Disk Space Requirements for Updating to Version 6.2.0

The following table provides disk space and time guidelines for the Version 6.2.0 update. Note that when you use the Firepower Management Center to update a managed device, the Firepower Management Center requires additional disk space on its **/Volume** partition.

Caution Do *not* reboot or shut down your appliance during the update until you see the login prompt. The system may appear inactive during the prechecks; this is expected behavior and does not require you to reboot or shut down your appliance.

Note The following guidelines do not include the time required to complete the readiness check. For more information about the readiness check, see Preupdate Readiness Checks, on page 7.

If you encounter issues with the progress of your update, contact Cisco TAC.

Table 5: Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time
Firepower Management Center	17 MB	10207 MB	–	57 minutes
Firepower Management Center Virtual	17 MB	10207 MB	–	hardware dependent
7000 and 8000 Series managed device	16.5 MB	6129 MB	1.2 GB	27 minutes
NGIPSv device	18 MB	7028 MB	1.3 GB	hardware dependent

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time
ASA FirePOWER module	15.6 MB	6619 MB	1.1 GB	165 minutes
Cisco ASA with Firepower Threat Defense	96 KB	5213 MB	938 MB	83 minutes
Firepower 9300 appliance or Firepower 4100 series security appliance running Firepower Threat Defense	5234 MB	5234 MB	734 MB	21 minutes
Firepower Threat Defense Virtual device	1 MB	5663 MB	936 MB	hardware dependent

Post Update Tasks

After you perform the update on the Firepower Management Center or managed devices, you must deploy configuration changes to the devices.

Note You must deploy configuration changes first after updating the Firepower Management Center and then again after updating its managed devices.

When you deploy configuration changes, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations requires the Snort process to restart, which temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends how the managed device handles traffic. For more information, see the Firepower Management Center Configuration Guide.

There are several additional post update steps you should take to ensure that your deployment is performing properly, which include the following include:

- Verify that the update succeeded.
- Make sure that all appliances in your deployment are communicating successfully.
- Update your intrusion rules and vulnerability database (VDB) and deploy configuration changes. (See the Firepower Management Center Configuration Guide for details.)
- Make configuration changes based on new features and functionality.
- Redeploy policies and configuration.