Important Update Notes

Before you begin the update process to Version 6.2.0.*x*, 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.

Note After you update to Version 6.2.0.3, you *must* apply Hotfix BH. If you do not apply Hotfix BH, you cannot edit or deploy access control rules.

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.*x*

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 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.x.

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.*x*.

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.

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, the system stops logging events. Event logging resumes after the full update is completed.

Caution Upgrading an inter-chassis cluster to Version 6.2.0.1, Version 6.2.0.2, or Version 6.2.0.3 can cause a 2-3 second traffic interruption when each module is removed from the cluster.

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 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 Upgrading an inter-chassis cluster to Version 6.2.0.1, Version 6.2.0.2, or Version 6.2.0.3 can cause a 2-3 second traffic interruption when each module is removed from the cluster.

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

Patch or Hotfix for New Dynamic Analysis CA Certificate

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

Upgrading from: A patched/hotfixed system with new CA certificates

Directly to: Version 6.2 through 6.2.3

On June 15, 2018, some Firepower deployments stopped being able to submit files for dynamic analysis. This occurred due to an expired CA certificate that was required for communications with the AMP Threat Grid cloud. In Version 6.1+ deployments, you can obtain a new certificate with a patch or hotfix. For earlier versions, you must upgrade to at least Version 6.1, then patch or hotfix.

If you already patched or hotfixed your deployment, upgrading to a later major version (Version 6.2 through 6.2.3) reverts to the old certificate and disables dynamic analysis. You must patch or hotfix again.

Note If this is your first time installing the patch or hotfix, make sure your firewall allows outbound connections to `fmc.api.threatgrid.com` (replacing `panacea.threatgrid.com`) from both the FMC and its managed devices. Managed devices submit files to the cloud for dynamic analysis; the FMC queries for results.

The following table lists the patches and hotfixes that contain the new certificates, for each major version sequence and platform. Patches and hotfixes are available on the Cisco Support & Download site. For release notes, see Firepower Release Notes.

Table 4: Patches and Hotfixes with New CA Certificates

Versions with Old Cert	First Patch with New Cert	Hotfix with New Cert	
6.2.3 through 6.2.3.3	6.2.3.4	Hotfix G	FTD devices
		Hotfix H	FMC, NGIPS devices
6.2.2 through 6.2.2.3	6.2.2.4	Hotfix BN	All platforms
6.2.1	None. You must upgrade.	None. You must upgrade.	
6.2.0 through 6.2.0.5	6.2.0.6	Hotfix BX	FTD devices
		Hotfix BW	FMC, NGIPS devices
6.1.0 through 6.1.0.6	6.1.0.7	Hotfix EM	All platforms
6.0.x	None. You must upgrade.	None. You must upgrade.	

Version 6.2.0.6 Time and Disk Space

Platform	Space on /	Space on /Volume	Space on FMC	Time
FMC	104 MB	8547 MB	—	From 6.2.0: 97 min From 6.2.0.5: 36 min
FMCv	30 MB	8543 MB	—	Hardware dependent
Firepower 9300 chassis	4085 MB	4085 MB	789 MB	From 6.2.0: 23 min From 6.2.0.5: 13 min
FTDv	226 MB	4526 MB	918 MB	Hardware dependent
ASA 5500-X series with FTD	227 MB	4960 MB	918 MB	From 6.2.0: 56 min From 6.2.0.5:27 min
Firepower 7000/8000 series	29 MB	7464 MB	944 MB	From 6.2.0: 60 min From 6.2.0.5: 24 min
ASA FirePOWER	28 MB	7191 MB	878 MB	From 6.2.0: 75 min From 6.2.0.5: 49 min
NGIPSv	29 MB	1658 MB	284 MB	Hardware dependent

Version 6.2.0.5 Time and Disk Space

The following table provides disk space and time guidelines for the 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 to Update From Version 6.2.0	Time to Update from Version 6.2.0.4
Firepower Management Center	179.908 MB	6008.8 MB	–	1 hour 12 minutes	34 minutes
Firepower Management Center Virtual	19.648 MB	6942.728 MB	–	hardware dependent	
7000 and 8000 Series managed device	17.104 MB	5805.964 MB	693 MB	51 minutes	18 minutes
NGIPSv device	17.444 MB	1300.334 MB	211 MB	hardware dependent	
ASA FirePOWER module	15.628 MB	5944.352 MB	703 MB	1 hour 6 minutes	27 minutes
Cisco ASA with Firepower Threat Defense	134.228 MB	4315.904MB	548 MB	46 minutes	22 minutes
Firepower 9300 appliance running Firepower Threat Defense	3008.86 MB	3008.86 MB	441 MB	28 minutes	16 minutes
Firepower 4100 series security appliance running Firepower Threat Defense	3008.86 MB	3008.86 MB	441 MB	28 minutes	16 minutes
Firepower Threat Defense Virtual device	134.436 MB	2804.828 MB	548 MB	hardware dependent	

Version 6.2.0.4 Time and Disk Space

The following table provides disk space and time guidelines for the 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 6: Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time to Update From Version 6.2.0	Time to Update from Version 6.2.0.3
Firepower Management Center	166.884 MB	5270.372 MB	–	1 hour 24 minutes	50 minutes
Firepower Management Center Virtual	19.516 MB	5345.924 MB	–	hardware dependent	
7000 and 8000 Series managed device	17.104 MB	4613.548 MB	608 MB	45 minutes	17 minutes
NGIPSv device	17.516 MB	1066.92 MB	208 MB	hardware dependent	
ASA FirePOWER module	15.636 MB	4584.264 MB	597 MB	3 hours 34 minutes	1 hour 23 minutes
Cisco ASA with Firepower Threat Defense	133.776 MB	3592.632 MB	448 MB	2 hours 28 minutes	1 hour 9 minutes
Firepower 9300 appliance running Firepower Threat Defense	1827.372 MB	1827.372 MB	325 MB	23 minutes	12 minutes
Firepower 4100 series security appliance running Firepower Threat Defense	1827.372 MB	1827.372 MB	325 MB	23 minutes	12 minutes

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time to Update From Version 6.2.0	Time to Update from Version 6.2.0.3
Firepower Threat Defense Virtual device	135.212 MB	274.3712 MB	448 MB	hardware dependent	

Version 6.2.0.3 Time and Disk Space

The following table provides disk space and time guidelines for the 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 7: Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time to Update From Version 6.2.0	Time to Update from Version 6.2.0.2
Firepower Management Center	18 MB	3352 MB	–	75 minutes	37 minutes
Firepower Management Center Virtual	19 MB	3342 MB	–	hardware dependent	
7000 and 8000 Series managed device	17 MB	3526 MB	554 MB	38 minutes	19 minutes
NGIPSv device	17 MB	842 MB	202 MB	hardware dependent	
ASA FirePOWER module	3361 MB	15 MB	521 MB	3 hours	97 minutes

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time to Update From Version 6.2.0	Time to Update from Version 6.2.0.2
Cisco ASA with Firepower Threat Defense	2302 MB	131 MB	384 MB	118 minutes	76 minutes
Firepower 9300 appliance running Firepower Threat Defense	1355 MB	—	319 MB	18 minutes	12 minutes
Firepower 4100 series security appliance running Firepower Threat Defense	1361	—	319 MB	20 minutes	12 minutes
Firepower Threat Defense Virtual device	17 MB	842 MB	384 MB	hardware dependent	

Version 6.2.0.2 Time and Disk Space

The following table provides disk space and time guidelines for the 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 8: Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time to Update From Version 6.2.0	Time to Update from Version 6.2.0.1
Firepower Management Center	35 MB	1665 MB	–	36 minutes	30 minutes
Firepower Management Center Virtual	21 MB	2834 MB	–	hardware dependent	
7000 and 8000 Series managed device	17 MB	2110 MB	458 MB	54 minutes	35 minutes
NGIPSv device	19 MB	612 MB	195 MB	hardware dependent	
ASA FirePOWER module	17 MB	2014 MB	383 MB	40 minutes	80 minutes
Cisco ASA with Firepower Threat Defense	144 MB	1808 MB	295 MB	95 minutes	59 minutes
Firepower 9300 appliance or Firepower 4100 series security appliance running Firepower Threat Defense	1060 MB	1060 MB	274 MB	12 minutes	9 minutes
Firepower Threat Defense Virtual device	143 MB	998 MB	295 MB	hardware dependent	

Version 6.2.0.1 Time and Disk Space

The following table provides disk space and time guidelines for the 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 9: Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time to Update From Version 6.2.0
Firepower Management Center	49.5 MB	1236.9 MB	–	28 minutes
Firepower Management Center Virtual	22.8 MB	1488 MB	–	hardware dependent
7000 and 8000 Series managed device	17.32 MB	1134 MB	184.4 MB	22 minutes
NGIPSv device	18.80 MB	720.8 MB	97.6 MB	hardware dependent
ASA FirePOWER module	16.78 MB	96.17 MB	205.8 MB	69 minutes
Cisco ASA with Firepower Threat Defense	143.33 MB	944.8 MB	158.2 MB	62 minutes
Firepower 9300 appliance or Firepower 4100 series security appliance running Firepower Threat Defense	524 MB	524 MB	136.8 MB	12 minutes
Firepower Threat Defense Virtual device	9.6 MB	143.6 MB	158.2 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.