Upgrade Guidelines

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

Upgrade Warnings for All Releases

These important warnings apply to every upgrade.

Traffic Flow, Inspection, and Device Behavior

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

- When you upgrade the operating system or virtual hosting environment on a managed device.
- When you upgrade the Firepower software on a managed device.
- When you deploy configuration changes as part of the upgrade process.

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 in a maintenance window or at a time when any interruption will have the least impact on your deployment.

For details, see Traffic Flow, Inspection, and Device Behavior During Upgrade in the *Firepower Management Center Upgrade Guide*.

Appliance Access During Upgrade

Before you upgrade a Firepower device, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In Firepower Management Center deployments, you should also able to access the FMC management interface without traversing the device.

This is because Firepower devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails.

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.

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 1: 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

Versions with Old Cert	First Patch with New Cert	Hotfix with New Cert	
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.	

Cisco Smart Licensing: Check Status After Upgrade

Deployments: Firepower Device Manager

In some cases, upgrading a Firepower Threat Defense device managed by Firepower Device Manager unregisters the device from the Cisco Smart Software Manager. After the upgrade completes, check your license status.

1. Click **Device**, then click **View Configuration** in the Smart License summary.
2. If the device is not registered, click **Register Device**.

Upgrade Warnings for Previous Releases

These release notes provide warnings that are *new* to Version 6.2.3. Unless you are upgrading from the most recent major release or one of its patches, you *must* review the warnings and guidelines from intermediate releases. Even if your upgrade path skips a release, its guidelines may still apply.

Read This	If You Are Upgrading From			
	6.2.2.x	6.2.1	6.2.0.x	6.1.0.x
Version-Specific Guidelines for Firepower Software Upgrades in the *Firepower Management Center Upgrade Guide*	□	□	□	□
Version 6.2.3 Release Notes (this document)	□	□	□	□
Version 6.2.2 Release Notes	—	□	□	□
Version 6.2.0 Release Notes	—	—	—	□

Upgrade Warnings for Version 6.2.3

These important warnings apply to Version 6.2.3.

FTD Clusters (6.1.x): Remove Site IDs Before Upgrade

Deployments: Firepower Threat Defense clusters

Upgrading from: Version 6.1.x

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.

Sharing Data with Cisco During and After Upgrade

Deployments: Any

Upgrading from: Version 6.1+

Features in Version 6.2.3+ involve sharing data with Cisco.

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

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

Note You cannot opt out of web analytics participation during the upgrade process. You can either disable web analytics after the upgrade or not install the upgrade.

Edit/Resave Access Control Policies After Upgrade

Deployments: Any

Upgrading from: Version 6.1+

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

Firepower Device Manager Deployments: Edit/Resave Realms After Upgrade

Deployments: Firepower Device Manager

Upgrading from: Version 6.2.0, Version 6.2.1, or Version 6.2.2

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

Changes to Result Limits in Reports

Deployments: Firepower Management Center

Upgrading from: Version 6.1+

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.

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

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

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

Version Requirements to Upgrade

The following table lists the minimum version of the Firepower software you must be running to upgrade to Version 6.2.3.

Appliance	Manager	Minimum Version to Upgrade
Firepower Management Center	—	6.1.0+
7000 and 8000 series device NGIPSv ASA FirePOWER module	Firepower Management Center	6.1.0+
Firepower Threat Defense device	Firepower Management Center	6.1.0+
	Firepower Device Manager	6.2.0+
ASA FirePOWER module	ASDM	6.2.0+

Time Estimates 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 Firepower Management Center requires additional disk space in its /Volume partition.

You must also have enough time to perform the upgrade. We provide estimates of upgrade times for each release.

About Time Estimates

Upgrade time estimates are based on in-house tests.

Estimates for devices 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.

Because lower-memory appliances tend to take longer to upgrade, we try to test on those platforms. For virtual platforms, we use the default settings for memory and resources. However, upgrades may still take longer than the provided estimates for any of the following reasons.

Push and Reboot Not Included

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

In FMC deployments, insufficient bandwidth between the Firepower Management Center 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 Firepower Management Center to its devices. For more information, see Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).

Estimates also do not include reboots. We do not have estimates for readiness checks, separate operating system upgrades, or configuration deploys.

Time Is per Device

Estimates 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. 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 perform time tests 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.

Version 6.2.3 Time and Disk Space

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

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