

Cisco Firepower Release Notes, Version 6.6.0.1

First Published: 2020-07-22

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Welcome to Version 6.6.x.x** 1

About the Release Notes 1

Release Dates 1

CHAPTER 2 **Compatibility** 3

Firepower Management Centers 3

Firepower Devices 4

Manager-Device Compatibility 6

Web Browser Compatibility 6

Screen Resolution Requirements 8

Additional Compatibility Resources 8

CHAPTER 3 **Features and Functionality** 9

New Features 9

Deprecated Features 9

FMC How-To Walkthroughs 9

CHAPTER 4 **Upgrade to Version 6.6.x.x** 11

Guidelines and Warnings for Version 6.6.x.x 11

General Guidelines and Warnings 11

Minimum Version to Upgrade 14

Time Tests and Disk Space Requirements 14

About Time Tests 14

About Disk Space Requirements 15

Version 6.6.0.1 Time and Disk Space 15

Traffic Flow, Inspection, and Device Behavior 16

FTD Upgrade Behavior: Firepower 4100/9300 Chassis 16
FTD Upgrade Behavior: Other Devices 20
ASA FirePOWER Upgrade Behavior 21
NGIPSv Upgrade Behavior 22
Upgrade Instructions 23
Upgrade Packages 23

CHAPTER 5 **Uninstall an Update** 25
Guidelines and Limitations for Uninstalling 25
Uninstall Order for HA/Scalability Deployments 27
Uninstall Instructions 29
Uninstall from a Standalone FMC 29
Uninstall from High Availability FMCs 30
Uninstall from Any Device (FMC Managed) 31
Uninstall from ASA FirePOWER (ASDM Managed) 33
Uninstall Packages 34

CHAPTER 6 **Freshly Install the Software** 37
Deciding to Freshly Install 37
Guidelines and Limitations for Fresh Installs 39
Unregistering Smart Licenses 41
Unregister a Firepower Management Center 42
Unregister an FTD Device Using FDM 42
Installation Instructions 42

CHAPTER 7 **Documentation** 45
Documentation Roadmaps 45

CHAPTER 8 **Resolved Issues** 47
Searching for Resolved Issues 47
Version 6.6.0.1 Resolved Issues 48

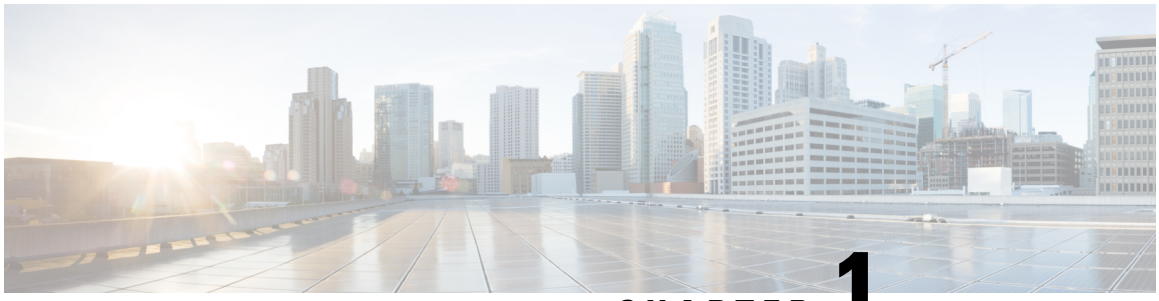
CHAPTER 9 **Known Issues** 49

Searching for Known Issues 49

CHAPTER 10 For Assistance 51

Online Resources 51

Contact Cisco 51



CHAPTER 1

Welcome to Version 6.6.x.x

Thank you for choosing Firepower.

- About the Release Notes, on page 1
- Release Dates, on page 1

About the Release Notes

The release notes provide critical and release-specific information, including upgrade warnings and behavior changes. Read this document even if you are familiar with Firepower releases and have previous experience upgrading Firepower deployments.

For links to upgrade and installation instructions, see:

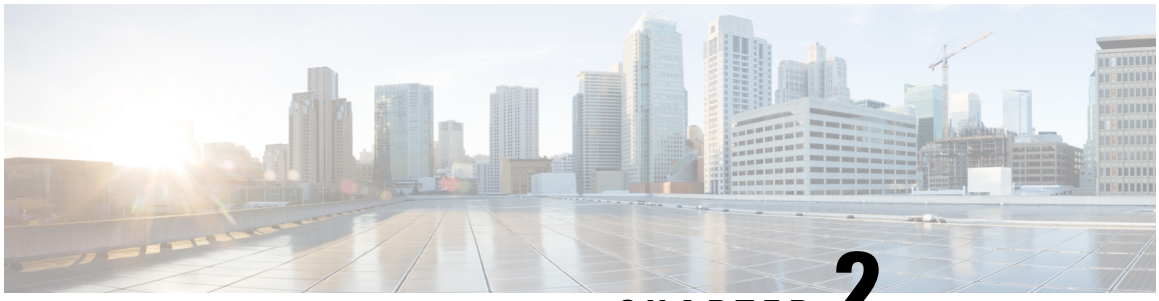
- Upgrade Instructions, on page 23
- Installation Instructions, on page 42

Release Dates

For a list of all platforms available with this version, see Compatibility, on page 3.

Table 1: Version 6.6.x.x Patch Dates

Version	Build	Date	Platforms
6.6.0.1	7	2020-07-22	All



CHAPTER 2

Compatibility

For detailed compatibility information for all supported Firepower versions, including links to end-of-sale and end-of-life announcements for deprecated platforms, see the Cisco Firepower Compatibility Guide.

For compatibility information for this Firepower version, see:

- Firepower Management Centers, on page 3
- Firepower Devices, on page 4
- Manager-Device Compatibility, on page 6
- Web Browser Compatibility, on page 6
- Screen Resolution Requirements, on page 8
- Additional Compatibility Resources, on page 8

Firepower Management Centers

Firepower Management Center Physical Platforms

Version 6.6.x.x FMC software is supported on these physical platforms:

- FMC 1600, 2600, 4600
- FMC 1000, 2500, 4500
- FMC 2000, 4000

We recommend you keep the BIOS and RAID controller firmware up to date. For more information, see the Cisco Firepower Compatibility Guide.

Firepower Management Center Virtual (FMCv) Platforms:

Version 6.6.x.x FMCv software is supported in both on-premises and cloud-based deployments:

- FMCv and FMCv 300 for VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7
- FMCv for Kernel-based virtual machine (KVM)
- FMCv for Amazon Web Services (AWS)
- FMCv for Microsoft Azure

For supported FMCv instances, see the Cisco Firepower Management Center Virtual Getting Started Guide.

Firepower Devices

Cisco Firepower devices monitor network traffic and decide whether to allow or block specific traffic based on a defined set of security rules.

About Firepower Devices

Depending on platform, Firepower devices can have different software, operating systems, and management methods:

- **Software:** Some Firepower devices run Firepower Threat Defense (FTD) software; some run NGIPS/ASA FirePOWER software. Some can run either—but not both at the same time.
- **OS/Hypervisor:** Some Firepower implementations bundle the operating system with the software. Others require that you upgrade the operating system yourself. For versions and builds of bundled operating systems, see the *Bundled Components* information in the Cisco Firepower Compatibility Guide.
- **Remote management:** All Firepower devices support remote management with a Firepower Management Center (FMC), which can manage multiple devices.
- **Local management:** Most Firepower devices—especially newer models and versions—support local, single-device management. Use Firepower Device Manager (FDM) to manage Firepower Threat Defense (FTD). Use Cisco Adaptive Security Device Manager (ASDM) to manage ASA FirePOWER.
- **Cloud management:** Firepower Threat Defense devices support Cisco Defense Orchestrator (CDO) concurrently with local FDM management. Although some configurations still require FDM, CDO allows you to establish and maintain consistent security policies across multiple FTD devices without using an FMC.

Supported Firepower Devices

These Firepower Threat Defense devices are supported in Version 6.6.x.x. You can manage these devices with FMC, FDM, and CDO.

Table 2: Firepower Threat Defense Devices in Version 6.6.x.x

FTD Device Platform	OS/Hypervisor
Firepower 1010, 1120, 1140, 1150	—
Firepower 2110, 2120, 2130, 2140	—
Firepower 4110, 4120, 4140, 4150 Firepower 4112, 4115, 4125, 4145	FXOS 2.8.1.105+ Upgrade FXOS first. To resolve issues, you may need to upgrade FXOS to the latest build. To help you decide, see the Cisco FXOS Release Notes, 2.8(1).

FTD Device Platform	OS/Hypervisor
Firepower 9300: SM-24, SM-36, SM-44 modules Firepower 9300: SM-40, SM-48, SM-56 modules	FXOS 2.8.1.105+ Upgrade FXOS first. To resolve issues, you may need to upgrade FXOS to the latest build. To help you decide, see the Cisco FXOS Release Notes, 2.8(1).
ASA 5508-X, 5516-X ASA 5525-X, 5545-X, 5555-X ISA 3000	—
Firepower Threat Defense Virtual (FTDv)	Any of: • VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7 • KVM: Kernel-based Virtual Machine • AWS: Amazon Web Services • Microsoft Azure For supported instances, see the appropriate FTDv Getting Started guide.

These NGIPS/ASA FirePOWER devices are supported in Version 6.6.x.x. You can manage these devices with FMC. ASA FirePOWER devices also support ASDM management.

Table 3: NGIPS/ASA FirePOWER Devices in Version 6.6.x.x

NGIPS Device Platform	OS/Hypervisor
ASA 5508-X, 5516-X ASA 5525-X, 5545-X, 5555-X ISA 3000	ASA 9.5(2) to 9.14(x) Except: ASA 5525-X, 5545-X, and 5555-X devices do not support ASA 9.15(x)+. There is wide compatibility between ASA and ASA FirePOWER versions. However, even if an ASA upgrade is not strictly required, resolving issues may require an upgrade to the latest supported version. See the Cisco ASA Upgrade Guide for order of operations. We recommend you upgrade the ASA 5508-X and 5516-X to the latest ROMMON image; see the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.
NGIPSv	VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7 For supported instances, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.

Manager-Device Compatibility

The FMC must run at least the same maintenance release (third-digit release) as the devices it manages. Although you can manage a patched device (fourth-digit release) with an unpatched FMC, new features and resolved issues often require the latest patch on *both* the FMC and its managed devices. We *strongly* recommend that you update your entire deployment.

Table 4: FMC-Device Compatibility

Version 6.6.0.x FMC	*can manage*	Version 6.2.3 through 6.6.0.x devices.
Version 6.6.0.x devices	*require*	Version 6.6.0 FMC.

Table 5: FDM-Device Compatibility

Version 6.6.0.x FDM	*can manage*	one FTD device.

Table 6: ASDM-Device Compatibility

Version 7.14.1 ASDM	*can manage*	Version 6.6.0.x and earlier ASA FirePOWER modules. Although there is wide compatibility between ASA, ASDM, and ASA FirePOWER versions, some newer versions of ASDM may not be able to manage ASA FirePOWER modules on older ASA devices. For details, see Cisco ASA Compatibility.
Version 6.6.0.x ASA FirePOWER modules	*require*	Version 7.14.1 ASDM.

Web Browser Compatibility

Browsers Tested with Firepower Web Interfaces

Firepower web interfaces are tested with the latest versions of the following popular browsers, running on currently supported versions of macOS and Microsoft Windows:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer 11 (Windows only)

If you encounter issues with any other browser, or are running an operating system that has reached end of life, we ask that you switch or upgrade. If you continue to encounter issues, contact Cisco TAC.

Note We do not perform extensive testing on this Firepower version with Apple Safari or Microsoft Edge, nor do we test Microsoft Internet Explorer with FMC walkthroughs. However, Cisco TAC welcomes feedback on issues you encounter.

Browser Settings and Extensions

Regardless of browser, you must make sure JavaScript, cookies, and TLS v1.2 remain enabled.

If you are using Microsoft Internet Explorer 11:

- For the **Check for newer versions of stored pages** browsing history option, choose **Automatically**.
- Disable the **Include local directory path when uploading files to server** custom security setting.
- Enable **Compatibility View** for the Firepower web interface IP address/URL.

Note that some browser extensions can prevent you from saving values in fields like the certificate and key in PKI objects. These extensions include, but are not limited to, Grammarly and Whatfix Editor. This happens because these extensions insert characters (such as HTML) in the fields, which causes the system to see them invalid. We recommend you disable these extensions while you're logged into Firepower appliances.

Securing Communications

When you first log in to a Firepower web interface, the system uses a self-signed digital certificate to secure web communications. Your browser should display an untrusted authority warning, but also should allow you to add the certificate to the trust store. Although this will allow you to continue to the Firepower web interface, we do recommend that you replace the self-signed certificate with a certificate signed by a globally known or internally trusted certificate authority (CA).

To begin replacing the self-signed certificate:

- FMC: Select **System** > **Configuration**, then click **HTTPS Certificates**.
- FDM: Click **Device**, then the **System Settings** > **Management Access** link, then the **Management Web Server** tab.

For detailed procedures, see the online help or the configuration guide for your Firepower product.

Note If you do not replace the self-signed certificate:

- Google Chrome does not cache static content, such as images, CSS, or JavaScript. Especially in low bandwidth environments, this can extend page load times.
- Mozilla Firefox can stop trusting the self-signed certificate when the browser updates. If this happens, you can refresh Firefox, keeping in mind that you will lose some settings; see Mozilla's Refresh Firefox support page.

Browsing from a Firepower-Monitored Network

Many browsers use Transport Layer Security (TLS) v1.3 by default. If you are using an SSL policy to handle encrypted traffic, and people in your monitored network use browsers with TLS v1.3 enabled, websites that support TLS v1.3 may fail to load.

For more information, see the software advisory titled: *Failures loading websites using TLS 1.3 with SSL inspection enabled*.

Screen Resolution Requirements

Table 7: Screen Resolution Requirements for Firepower User Interfaces

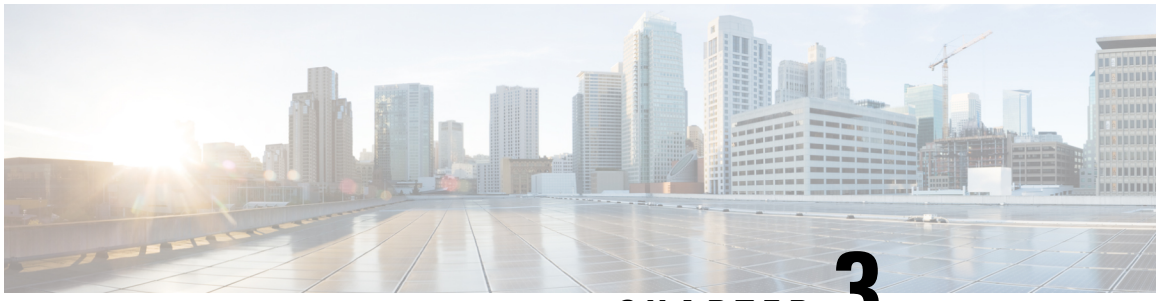
Interface	Resolution
Firepower Management Center	1280 x 720
Firepower Device Manager	1024 x 768
ASDM managing an ASA FirePOWER module	1024 x 768
Firepower Chassis Manager for Firepower 4100/9300 chassis	1024 x 768

Additional Compatibility Resources

This table provides links to release notes and additional compatibility information. For full documentation roadmaps, see Documentation Roadmaps, on page 45.

Table 8: Additional Compatibility Resources

Description	Resources
Compatibility guides provide detailed compatibility information for supported hardware models and software versions, including bundled components and integrated products.	Cisco Firepower Compatibility Guide Cisco ASA Compatibility Cisco Firepower 4100/9300 FXOS Compatibility
Release notes provide critical and release-specific information, including upgrade warnings and behavior changes.	Cisco Firepower Release Notes Cisco ASA Release Notes Cisco Firepower 4100/9300 FXOS Release Notes
Sustaining bulletins provide support timelines for the Cisco Next Generation Firewall product line, including management platforms and operating systems.	Cisco NGFW Product Line Software Release and Sustaining Bulletin



CHAPTER 3

Features and Functionality

Patches contain new features, functionality, and behavior changes related to urgent or resolved issues.

- New Features, on page 9
- Deprecated Features, on page 9
- FMC How-To Walkthroughs, on page 9

New Features

We have not introduced features or changed system behavior in Version 6.6.x.x patches.

Deprecated Features

Deprecated features can prevent upgrade or require pre- or post-upgrade configuration changes.

Note Version 6.6.0 is the last major release that will support the Cisco Firepower User Agent software as an identity source. You will not be able to further upgrade FMCs with user agent configurations. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC) now. This will also allow you to take advantage of features that are not available with the user agent. To convert your license, contact Sales.

For more information, see the appropriate *Cisco Firepower User Agent Configuration Guide* on the Cisco Firepower Management Center Configuration Guides page.

There are no features deprecated in Version 6.6.x.x patches.

FMC How-To Walkthroughs

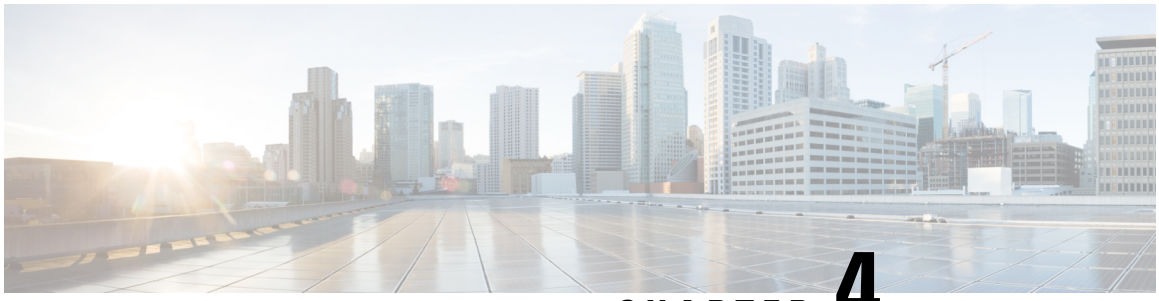
FMC walkthroughs (also called *how-tos*) guide you through a variety of basic tasks such as device setup and policy configuration. Just click **How To** at the bottom of the browser window, choose a walkthrough, and follow the step-by-step instructions.

Note FMC walkthroughs are tested on the Firefox and Chrome browsers. If you encounter issues with a different browser, we ask that you switch to Firefox or Chrome. If you continue to encounter issues, contact Cisco TAC.

The following table lists some common problems and solutions. To end a walkthrough at any time, click the **x** in the upper right corner.

Table 9: Troubleshooting Walkthroughs

Problem	Solution
Cannot find the **How To** link to start walkthroughs.	Make sure walkthroughs are enabled. From the drop-down list under your username, select **User Preferences** then click **How-To Settings**.
Walkthrough appears when you do not expect it.	If a walkthrough appears when you do not expect it, end the walkthrough.
Walkthrough disappears or quits suddenly.	If a walkthrough disappears: • Move your pointer. Sometimes the FMC stops displaying an in-progress walkthrough. For example, pointing to a different top-level menu can make this happen. • Navigate to a different page and try again. If moving your pointer does not work, the walkthrough may have quit.
Walkthrough is out of sync with the FMC: • Starts on the wrong step. • Advances prematurely. • Will not advance.	If a walkthrough is out of sync, you can: • Attempt to continue. For example, if you enter an invalid value in a field and the FMC displays an error, the walkthrough can prematurely move on. You may need to go back and resolve the error to complete the task. • End the walkthrough, navigate to a different page, and try again. Sometimes you cannot continue. For example, if you do not click **Next** after you complete a step, you may need to end the walkthrough.



CHAPTER 4

Upgrade to Version 6.6.x.x

This chapter provides critical and release-specific information.

- Guidelines and Warnings for Version 6.6.x.x, on page 11
- General Guidelines and Warnings, on page 11
- Minimum Version to Upgrade, on page 14
- Time Tests and Disk Space Requirements, on page 14
- Traffic Flow, Inspection, and Device Behavior, on page 16
- Upgrade Instructions, on page 23
- Upgrade Packages, on page 23

Guidelines and Warnings for Version 6.6.x.x

There are no important upgrade guidelines and warnings that apply specifically to Version 6.6.x.x patches.

To avoid upgrade failure, review these additional guidelines and warnings.

Table 10: Additional Upgrade Guidelines and Warnings

✓	Resource	Details
	General Guidelines and Warnings, on page 11	Read these even if you are familiar with the upgrade process, as guidelines may have changed.
	Known Issues, on page 49	Although we do not list known issues for patches, you can use the Cisco Bug Search Tool to obtain an up-to-date list of open bugs for Firepower products.
	Features and Functionality, on page 9	Although patches only contain functionality and behavior changes related to urgent or resolved issues, we still recommend you check this chapter. Deprecated features especially can require pre-upgrade configuration changes.

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

When supported, we strongly recommend you back up both before and after upgrade:

- Before upgrade: If an upgrade fails catastrophically, you may have to reimage and restore. Reimaging returns most settings to factory defaults, including the system password. If you have a recent backup, you can return to normal operations more quickly.
- After upgrade: This creates a snapshot of your freshly upgraded deployment. We recommend you back up the FMC after you upgrade its managed devices, so your new FMC backup file 'knows' that its devices have been upgraded.

You should back up to a secure remote location and verify transfer success. Upgrades purge locally stored backups. And especially because backup files are unencrypted, do not allow unauthorized access. If backup files are modified, the restore process will fail.

As the first step in any backup, note the appliance model and version, including patch level. For FMCs running Version 6.5.0.x and earlier, note the VDB version. For Firepower 4100/9300 chassis, note the FXOS version. This is important because if you need to restore the backup to a new or reimaged appliance, you may need to update the new appliance first.



Note Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. Careful planning and preparation can help you avoid missteps. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your Firepower product.

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.

Check Bandwidth

To upgrade a Firepower appliance (or perform a readiness check), the upgrade package must be on the appliance. Firepower upgrade package sizes vary. Make sure your management network has the bandwidth to perform large data transfers.

In FMC deployments, if you transfer an upgrade package to a managed device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. We recommend you manually push (copy) Firepower upgrade packages to managed devices before you upgrade, either from the

FMC or, for FTD devices, from your own internal web server. For more information, see Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).

Appliance Access

Firepower devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade a Firepower device, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also able to access the FMC management interface without traversing the device.

Signed Upgrade Packages

So that Firepower can verify that you are using the correct files, upgrade and hotfix packages are *signed* archives. Do not untar signed (.tar) packages.



Note After you upload a signed upgrade package, the GUI can take several minutes to load as the system verifies the package. To speed up the display, remove signed packages after you no longer need them.

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. Major upgrades enable web analytics tracking, even if your current setting is to opt out. If you do not want Cisco to collect this data, opt out after each major upgrade.

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

Patches can change the fourth digit *only*. You cannot upgrade directly to a patch from a previous major or maintenance release.

For example:

- 6.6.0 → 6.6.0.x **is** supported.

  Patches are cumulative. You can always install the latest patch to a major or maintenance release.

- 6.5.0 → 6.6.0.x **is not** supported.

  You must be running at least Version 6.6.0 to patch to 6.6.0.x.

Time Tests and Disk Space Requirements

To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. When you use the Firepower Management Center to upgrade a managed device, the FMC requires additional disk space in its /Volume partition, for the device upgrade package. You must also have enough time to perform the upgrade.

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

About Time Tests

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

Note Although we report the *slowest* time of all upgrades tested for a particular platform/series, your upgrade will likely take longer than the provided times for multiple reasons, provided below.

Test Conditions

- Deployment: Values are from tests in a Firepower Management Center deployment. This is because raw upgrade times for remotely and locally managed devices are similar, given similar conditions.
- Versions: For major upgrades, we test upgrades from all eligible previous major versions. For patches, we test upgrades from the base version.
- Models: In most cases, we test on the lowest-end models in each series, and sometimes on multiple models in a series.
- Virtual settings: We test with the default settings for memory and resources.
- High availability and scalability: We test on standalone devices.

  In a high availability or clustered configuration, devices upgrade one at a time to preserve continuity of operations, with each device operating in maintenance mode while it upgrades. Upgrading a device pair or entire cluster, therefore, takes longer than upgrading a standalone device.
- Configurations: We test on appliances with minimal configurations and traffic load.

  Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how those things are affected by the upgrade. For example, if you use a lot of access control rules and the upgrade needs to make a backend change to how those rules are stored, the upgrade can take longer.

Time Is For Upgrade Only

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

- Transferring upgrade packages to managed devices, whether before or during upgrade.
- Readiness checks.
- VDB and SRU updates.
- Deploying configurations.
- Reboots (values may be provided separately).

About Disk Space Requirements

Space estimates are the *largest* reported for all upgrades. For releases after early 2020, they are:

- Not rounded up (under 1 MB).
- Rounded up to the next 1 MB (1 MB - 100 MB).
- Rounded up to the next 10 MB (100 MB - 1GB).
- Rounded up to the next 100 MB (greater than 1 GB).

Version 6.6.0.1 Time and Disk Space

In this table, the upgrade time includes reboot.

Table 11: Version 6.6.0.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.6.0
FMCv: VMware 6.0	1.1 GB	23 MB	—	17 min
Firepower 1000 series	450 MB	450 MB	240 MB	21 min
Firepower 2100 series	260 MB	260 MB	270 MB	17 min
Firepower 4100 series	470 MB	470 MB	46 MB	11 min
Firepower 9300	460 MB	460 MB	46 MB	33 min
ASA 5500-X series with FTD	440 MB	120 MB	46 MB	17 min
ISA 3000 with FTD	440 MB	120 MB	46 MB	21 min
FTDv: VMware 6.0	430 MB	120 MB	46 MB	11 min
ASA FirePOWER	80 MB	20 MB	15 MB	18 min
NGIPSv: VMware 6.0	64 MB	28 MB	15 MB	9 min

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 12: Traffic Behavior During FXOS Upgrade

Deployment	Method	Traffic Behavior
Standalone	—	Dropped
High availability	**Best Practice:** Update FXOS on the standby, switch active peers, upgrade the new standby.	Unaffected
	Upgrade FXOS on the active peer before the standby is finished upgrading.	Dropped until one peer is online
Inter-chassis cluster (6.2+)	**Best Practice:** Upgrade one chassis at a time so at least one module is always online.	Unaffected
	Upgrade chassis at the same time, so all modules are down at some point.	Dropped until at least one module is online
Intra-chassis cluster (Firepower 9300 only)	Fail-to-wire enabled: **Bypass: Standby** or **Bypass-Force**. (6.1+)	Passed without inspection
	Fail-to-wire disabled: **Bypass: Disabled**. (6.1+)	Dropped until at least one module is online
	No fail-to-wire module.	Dropped until at least one module is online

Standalone FTD Device: Firepower Software Upgrade

Interface configurations determine how a standalone device handles traffic during the upgrade.

Table 13: Traffic Behavior During Firepower Software Upgrade: Standalone FTD Device

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces Switched interfaces are also known as bridge group or transparent interfaces.	Dropped

Interface Configuration		Traffic Behavior
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 data security module or modules upgrade first, then the control module. Security modules operate in maintenance mode while they upgrade.

During the control security module upgrade, although traffic inspection and handling continues normally, the system stops logging events. Events for traffic processed during the logging downtime appear with out-of-sync timestamps after the upgrade is completed. However, if the logging downtime is significant, the system may prune the oldest events before they can be logged.



Note Upgrading an inter-chassis cluster from Version 6.2.0, 6.2.0.1, or 6.2.0.2 causes a 2-3 second traffic interruption in traffic inspection when each module is removed from the cluster. 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 14: Traffic Behavior During FTD Deployment

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

FTD Upgrade Behavior: Other Devices

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

Standalone FTD Device: Firepower Software Upgrade

Interface configurations determine how a standalone device handles traffic during the upgrade.

Table 15: Traffic Behavior During Firepower Software Upgrade: Standalone FTD Device

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces Switched interfaces are also known as bridge group or transparent interfaces.	Dropped
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.

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 16: Traffic Behavior During FTD Deployment

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

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 17: Traffic Behavior During ASA FirePOWER Upgrade

Traffic Redirection Policy	Traffic Behavior
Fail open (**sfr fail-open**)	Passed without inspection
Fail closed (**sfr fail-close**)	Dropped
Monitor only (**sfr {fail-close}|{fail-open} monitor-only**)	Egress packet immediately, copy not inspected

Traffic Behavior During ASA FirePOWER Deployment

Traffic behavior while the Snort process restarts is the same as when you upgrade the ASA FirePOWER module.

You deploy configurations multiple times during the upgrade process. Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying,

you modify specific policy or device configurations. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection. Your service policies determine whether traffic drops or passes without inspection during the interruption.

NGIPSv Upgrade Behavior

This section describes device and traffic behavior when you upgrade NGIPSv.

Firepower Software Upgrade

Interface configurations determine how NGIPSv handles traffic during the upgrade.

Table 18: Traffic Behavior During NGIPSv Upgrade

Interface Configuration	Traffic Behavior
Inline	Dropped
Inline, tap mode	Egress packet immediately, copy not inspected
Passive	Uninterrupted, not inspected

Traffic Behavior During Deployment

You deploy configurations multiple times during the upgrade process. Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 19: Traffic Behavior During NGIPSv Deployment

Interface Configuration	Traffic Behavior
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

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
- Firepower Threat Defense (ISA 3000): https://www.cisco.com/go/isa3000-software
- Firepower Threat Defense (all other models, including FTDv): https://www.cisco.com/go/ftd-software
- ASA with FirePOWER Services (ASA 5500-X series): https://www.cisco.com/go/asa-firepower-sw
- ASA with FirePOWER Services (ISA 3000): https://www.cisco.com/go/isa3000-software
- NGIPSv: https://www.cisco.com/go/ngipsv-software

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

Tip An FMC with internet access can download Version 6.6.x maintenance releases (third-digit upgrades) directly from Cisco, about two weeks after they are available for manual download. Direct download from Cisco is not supported for major releases, most patches, or to managed devices—including to devices managed by FDM.

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

For example:

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

- File extension: sh.REL.tar

Upgrade packages from Version 6.2.1+ are signed tar archives (.tar). Do not untar. Do not transfer upgrade packages by email.

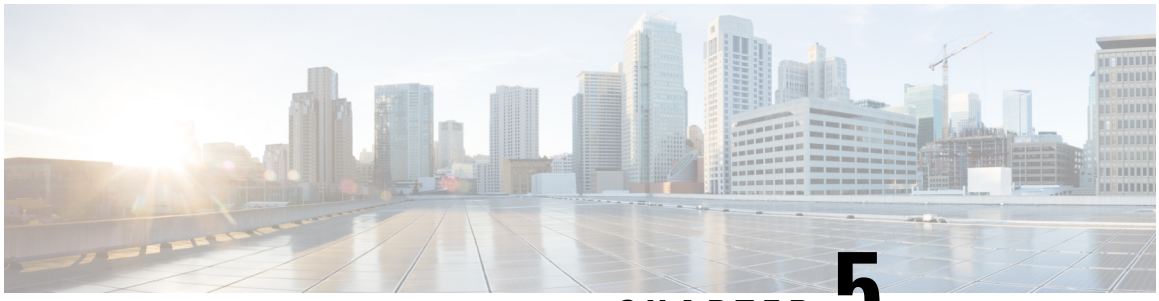
Table 20: Upgrade Package Naming Schemes for Firepower Software

Platform	Package
FMC/FMCv	Cisco_Firepower_Mgmt_Center
Firepower 1000 series	Cisco_FTD_SSP-FP1K
Firepower 2100 series	Cisco_FTD_SSP-FP2K
Firepower 4100/9300 chassis	Cisco_FTD_SSP
ASA 5500-X series with FTD ISA 3000 with FTD FTDv	Cisco_FTD
ASA FirePOWER	Cisco_Network_Sensor
NGIPSv	Cisco_Firepower_NGIPS_Virtual

Operating System Upgrade Packages

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

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



CHAPTER 5

Uninstall an Update

You can uninstall Firepower patches from:

- FMCs and their managed devices
- ASA FirePOWER modules managed by ASDM

Uninstalling a patch results in an appliance running the version you upgraded from.

Note You cannot uninstall a patch from an FTD device managed by FDM. You also cannot uninstall a major version of the Firepower software from any appliance. In those cases, you must reimage.

For more information, see:

- Guidelines and Limitations for Uninstalling, on page 25
- Uninstall Order for HA/Scalability Deployments, on page 27
- Uninstall Instructions, on page 29
- Uninstall Packages, on page 34

Guidelines and Limitations for Uninstalling

These important guidelines and limitations apply to uninstall.

Verify Uninstall is Supported for Your Patch

Uninstalling specific patches can cause issues on Firepower appliances, including:

- Inability to deploy configuration changes after uninstall.
- Incompatibilities between the operating system and the Firepower software.
- FSIC (file system integrity check) failure when the appliance reboots, if you patched with security certifications compliance enabled (CC/UCAPL mode).

Caution If security certifications compliance is enabled and the FSIC fails, Firepower software does not start, remote SSH access is disabled, and you can access the appliance only via local console. If this happens, contact Cisco TAC.

In these cases, if you need to revert to an earlier patch, we recommend you reimage and then upgrade.

Note Uninstall is currently supported for all 6.6.0.x patches.

Uninstall from Devices First, Using the Shell

In FMC deployments, uninstall patches from managed devices first. We recommend that FMCs run a higher version than their managed devices.

To uninstall a device patch, you must use the Linux shell, also called expert mode. This means that you uninstall from devices both *individually* and *locally*. In other words:

- You cannot batch-uninstall patches from clustered, stacked, or high availability (HA) Firepower devices, or from clustered or failover ASA with FirePOWER Services devices. To plan an uninstall order that minimizes disruption, see Uninstall Order for HA/Scalability Deployments, on page 27.
- You cannot use an FMC, ASDM, or FDM to uninstall a patch from a device, nor can you use the local web interface on a 7000/8000 series device.
- You cannot use an FMC user account to log into and uninstall the patch from one of its managed devices. Firepower appliances maintain their own user accounts.
- You must have access to the device shell as the `admin` user for the device, or as another local user with CLI configuration access. If you disabled shell access, you cannot uninstall device patches. Contact Cisco TAC to reverse the device lockdown.

Uninstall from FMCs After Devices

Uninstall patches from FMCs after you uninstall from their managed devices. As with upgrade, you must uninstall from high availability FMCs one at a time; see Uninstall Order for HA/Scalability Deployments, on page 27.

We recommend you use the FMC web interface to uninstall FMC patches. You must have Administrator access. If you cannot use the web interface, you can use the Linux shell as either the `admin` user for the shell, or as an external user with shell access. If you disabled shell access, contact Cisco TAC to reverse the FMC lockdown.

Verify NTP Synchronization

Before you uninstall, make sure Firepower appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause uninstall 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 uninstall (depending on interface configurations), or if the uninstall fails. Before you uninstall a patch from 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.

Disable ASA REST API on ASA FirePOWER Devices

Before you uninstall an ASA FirePOWER patch, make sure the ASA REST API is disabled. Otherwise, the uninstall could fail. From the ASA CLI: `no rest api agent`. You can reenable after the uninstall: `rest-api agent`.

Unresponsive Uninstalls

Do *not* deploy changes to or from, manually reboot, or shut down an uninstalling appliance. Do *not* restart an uninstall in progress. The uninstall process may appear inactive at times; this is expected. If you encounter issues with the uninstall, including a failed uninstall or unresponsive appliance, contact Cisco TAC.

A failed uninstall may require a reimage, which returns most settings to factory defaults. For this reason, we *strongly* recommend you back up event and configuration data to an external location before you reimage.

Traffic Flow, Inspection, and Device Behavior

Interruptions in traffic flow and inspection during an uninstall are the same as the interruptions that occur during an upgrade. We *strongly* recommend performing any uninstall in a maintenance window or at a time when any interruption will have the least impact on your deployment. For more information, see Traffic Flow, Inspection, and Device Behavior, on page 16.

Uninstall Order for HA/Scalability Deployments

You uninstall patches from Firepower appliances individually, even those that you upgraded as a unit. Especially in high availability (HA) and scalability deployments, you should plan an uninstall order that minimizes disruption. Unlike upgrade, the system does not do this for you. The tables below outline uninstall order for HA/scalability deployments.

Note that in most cases, you will:

- Uninstall from the secondary/standby/data units first, then the primary/active/control.
- Uninstall one at a time. Wait until the patch has fully uninstalled from one unit before you move on to the next unit.

Table 21: Uninstall Order for FMCs in HA

FMC Deployment	Uninstall Order
FMC high availability	With synchronization paused, which is a state called *split-brain*, uninstall from FMC peers one at a time. Do not make or deploy configuration changes while the pair is split-brain. **1.** Pause synchronization (enter split-brain). **2.** Uninstall from the standby. **3.** Uninstall from the active. **4.** Restart synchronization (exit split-brain).

Table 22: Uninstall Order for FTD devices in HA or Clusters

FTD Deployment	Uninstall Order
FTD high availability	You cannot uninstall a patch from FTD devices configured for high availability. You must break high availability first. **1.** Break high availability. **2.** Uninstall from the former standby. **3.** Uninstall from the former active. **4.** Reestablish high availability.
FTD cluster	Uninstall from one unit at a time, leaving the control unit for last. Clustered units operate in maintenance mode while the patch uninstalls. **1.** Uninstall from the data modules one at a time. **2.** Make one of the data modules the new control module. **3.** Uninstall from the former control.

Table 23: Uninstall Order for ASA with FirePOWER Services Devices in ASA Failover Pairs/Clusters

ASA Deployment	Uninstall Order
ASA active/standby failover pair, with ASA FirePOWER	Always uninstall from the standby. **1.** Uninstall from the ASA FirePOWER module on the standby ASA device. **2.** Fail over. **3.** Uninstall from the ASA FirePOWER module on the new standby ASA device.

ASA Deployment	Uninstall Order
ASA active/active failover pair, with ASA FirePOWER	Make both failover groups active on the unit you are not uninstalling. 1. Make both failover groups active on the primary ASA device. 2. Uninstall from the ASA FirePOWER module on the secondary ASA device. 3. Make both failover groups active on the secondary ASA device. 4. Uninstall from the ASA FirePOWER module on the primary ASA device.
ASA cluster, with ASA FirePOWER	Disable clustering on each unit before you uninstall. Uninstall from one unit at a time, leaving the control unit for last. 1. On a data unit, disable clustering. 2. Uninstall from the ASA FirePOWER module on that unit. 3. Reenable clustering. Wait for the unit to rejoin the cluster. 4. Repeat for each data unit. 5. On the control unit, disable clustering. Wait for a new control unit to take over. 6. Uninstall from the ASA FirePOWER module on the former control unit. 7. Reenable clustering.

Uninstall Instructions

The following sections explain how to uninstall Firepower patches from eligible appliances.

Uninstall from a Standalone FMC

Use this procedure to uninstall a patch from a standalone Firepower Management Center, including Firepower Management Center Virtual.

Before you begin

Uninstall patches from managed devices. We recommend that FMCs run a higher version than their managed devices.

Step 1 Deploy to managed devices whose configurations are out of date.

Deploying before you uninstall reduces the chance of failure.

Step 2 Perform prechecks.

- Check health: Use the Message Center on the FMC (click the System Status icon on the menu bar). Make sure the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

- Running tasks: Also in the Message Center, make sure essential tasks are complete. Tasks running when the uninstall begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

Step 3 Choose **System** > **Updates**.

Step 4 Click the Install icon next to the uninstall package for the FMC, then choose the FMC.

If you do not have the correct uninstall package, contact Cisco TAC.

Step 5 Click **Install** to begin the uninstall.

Confirm that you want to uninstall and reboot the FMC.

Step 6 Monitor progress in the Message Center until you are logged out.

Do not make configuration changes or deploy to any device while the patch is uninstalling. Even if the Message Center shows no progress for several minutes or indicates that the uninstall has failed, do *not* restart the uninstall or reboot the FMC. Instead, contact Cisco TAC.

Step 7 Log back into the FMC after the patch uninstalls and the FMC reboots.

Step 8 Verify success.

Choose **Help** > **About** to display current software version information.

Step 9 Use the Message Center to recheck deployment health.

Step 10 Redeploy configurations.

Uninstall from High Availability FMCs

Use this procedure to uninstall a patch from a Firepower Management Center in a high availability pair.

You uninstall from peers one at a time. With synchronization paused, first uninstall from the standby, then the active. When the standby FMC starts the uninstall, 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 and uninstall. Do *not* make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you restart synchronization.

Before you begin

Uninstall patches from managed devices. We recommend that FMCs run a higher version than their managed devices.

Step 1 On the active FMC, deploy to managed devices whose configurations are out of date.

Deploying before you uninstall reduces the chance of failure.

Step 2 Use the Message Center to check deployment health before you pause synchronization.

Click the System Status icon on the FMC menu bar to display the Message Center. Make sure the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 3 Pause synchronization.

a) Choose **System** > **Integration**.

b) On the **High Availability** tab, click **Pause Synchronization**.

Step 4 Uninstall the patch from the FMCs one at a time—first the standby, then the active.

Follow the instructions in Uninstall from a Standalone FMC, on page 29, but omit the initial deploy, and stop after you verify update success on each FMC. In summary, for each FMC:

a) Perform prechecks (health, running tasks).
b) On the **System** > **Updates** page, uninstall the patch.
c) Monitor progress until you are logged out, then log back in when you can.
d) Verify uninstall success.

Do *not* make or deploy configuration changes while the pair is split-brain.

Step 5 On the FMC you want to make the active peer, restart synchronization.

a) Choose **System** > **Integration**.
b) On the **High Availability** tab, click **Make-Me-Active**.
c) Wait until synchronization restarts and the other FMC switches to standby mode.

Step 6 Use the Message Center to recheck deployment health.

Step 7 Redeploy configurations.

Uninstall from Any Device (FMC Managed)

Use this procedure to uninstall a patch from a *single* managed device in a Firepower Management Center deployment. This includes physical and virtual devices, security modules, and ASA FirePOWER modules.

Before you begin

- Make sure you are uninstalling from the correct device, especially in HA/scalability deployments. See Uninstall Order for HA/Scalability Deployments, on page 27.
- For ASA FirePOWER modules, make sure the ASA REST API is disabled. From the ASA CLI: `no rest api agent`. You can reenable after the uninstall: `rest-api agent`.

Step 1 If the device's configurations are out of date, deploy now from the FMC.

Deploying before you uninstall reduces the chance of failure.

Exception: Do not deploy to mixed-version stacks, clusters, or HA pairs. In an HA/scalability deployment, deploy before you uninstall from the first device, but then not again until you have uninstalled the patch from all members.

Step 2 Perform prechecks.

- Check health: Use the Message Center on the FMC (click the System Status icon on the menu bar). Make sure the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.
- Running tasks: Also in the Message Center, make sure essential tasks are complete. Tasks running when the uninstall begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

Step 3 Access the Firepower CLI on the device. Log in as `admin` or another Firepower CLI user with configuration access.

You can either SSH to the device's management interface (hostname or IP address) or use the console.

If you use the console, some devices default to the operating system CLI, and require an extra step to access the Firepower CLI.

Firepower 1000/2100 series	`connect ftd`
Firepower 4100/9300 chassis	`connect module` *`slot_number`* `console`, then `connect ftd` (first login only)
ASA FirePOWER	`session sfr`

Step 4 At the Firepower CLI prompt, use the `expert` command to access the Linux shell.

Step 5 Run the uninstall command, entering your password when prompted.

```
sudo install_update.pl --detach /var/sf/updates/uninstall_package_name
```

The package name varies by platform; see Uninstall Packages, on page 34. Do not untar signed (.tar) packages.

Unless you are running the uninstall from the console, use the `--detach` option to ensure the uninstall does not stop if your user session times out. Otherwise, the uninstall 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.

Caution The system does *not* ask you to confirm that you want to uninstall. Entering this command starts the uninstall, which includes a device reboot. Interruptions in traffic flow and inspection during an uninstall are the same as the interruptions that occur during an upgrade. Make sure you are ready.

Step 6 Monitor the uninstall.

If you did not detach the uninstall, progress is displayed on the console or terminal. If you did detach, you can use `tail` or `tailf` to display logs:

- FTD devices: `tail /ngfw/var/log/sf/update.status`
- All other devices: `tail /var/log/sf/update.status`

Step 7 Verify success.

After the patch uninstalls and the device reboots, confirm that the device has the correct software version. On the FMC, choose **Devices** > **Device Management**.

Step 8 Use the Message Center to recheck deployment health.

Step 9 Redeploy configurations.

Exception: In a HA/scalability deployment, do *not* deploy to mixed-version stacks, clusters, or HA pairs. Deploy only after you repeat this procedure for all members.

What to do next

- For HA/scalability deployments, repeat this procedure for each device in your planned sequence. Then, make any final adjustments. For example, in an FTD HA deployment, reestablish HA after you uninstall from both peers.

- For ASA FirePOWER modules, reenable the ASA REST API if you disabled it earlier. From the ASA CLI: `rest-api agent`.

Uninstall from ASA FirePOWER (ASDM Managed)

Use this procedure to uninstall a patch from a locally managed ASA FirePOWER module. If you manage ASA FirePOWER with an FMC, see Uninstall from Any Device (FMC Managed), on page 31.

Before you begin

- Make sure you are uninstalling from the correct device, especially in ASA failover/cluster deployments. See Uninstall Order for HA/Scalability Deployments, on page 27.
- Make sure the ASA REST API is disabled. From the ASA CLI: `no rest api agent`. You can reenable after the uninstall: `rest-api agent`.

Step 1 If the device's configurations are out of date, deploy now from ASDM.

Deploying before you uninstall reduces the chance of failure.

Step 2 Perform prechecks.

- System status: Choose **Monitoring** > **ASA FirePOWER Monitoring** > **Statistics** and make sure everything is as expected.
- Running tasks: Choose **Monitoring** > **ASA FirePOWER Monitoring** > **Tasks** and make sure essential tasks are complete. Tasks running when the uninstall begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

Step 3 Access the Firepower CLI on the ASA FirePOWER module. Log in as `admin` or another Firepower CLI user with configuration access.

You can either SSH to the module's management interface (hostname or IP address) or use the console. If you use the console, note that ASA 5585-X series devices have a dedicated ASA FirePOWER console port. On other ASA models, the console port defaults to the ASA CLI and you must use the `session sfr` command to access the Firepower CLI.

Step 4 At the Firepower CLI prompt, use the `expert` command to access the Linux shell.

Step 5 Run the uninstall command, entering your password when prompted.

```
sudo install_update.pl --detach
/var/sf/updates/Cisco_Network_Sensor_Patch_Uninstaller-version-build.sh.REL.tar
```

Do not untar signed (.tar) packages.

Unless you are running the uninstall from the console, use the `--detach` option to ensure the uninstall does not stop if your user session times out. Otherwise, the uninstall 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.

Caution The system does *not* ask you to confirm that you want to uninstall. Entering this command starts the uninstall, which includes a device reboot. Interruptions in traffic flow and inspection during an uninstall are the same as the interruptions that occur during an upgrade. Make sure you are ready.

Step 6 Monitor the uninstall.

If you did not detach the uninstall, progress is displayed on the console or terminal. If you did detach, you can use `tail` or `tailf` to display logs:

```
tail /var/log/sf/update.status
```

Do not deploy configurations to the device while the patch is uninstalling. Even if the log shows no progress for several minutes or indicates that the uninstall has failed, do not restart the uninstall or reboot the device. Instead, contact Cisco TAC.

Step 7 Verify success.

After the patch uninstalls and the module reboots, confirm that the module has the correct software version. Choose **Configuration** > **ASA FirePOWER Configurations** > **Device Management** > **Device**.

Step 8 Redeploy configurations.

What to do next

- For ASA failover/cluster deployments, repeat this procedure for each device in your planned sequence.
- For ASA FirePOWER modules, reenable the ASA REST API if you disabled it earlier. From the ASA CLI: `rest-api agent`.

Uninstall Packages

When you patch a Firepower appliances, the uninstaller for that patch is automatically created in the upgrade directory:

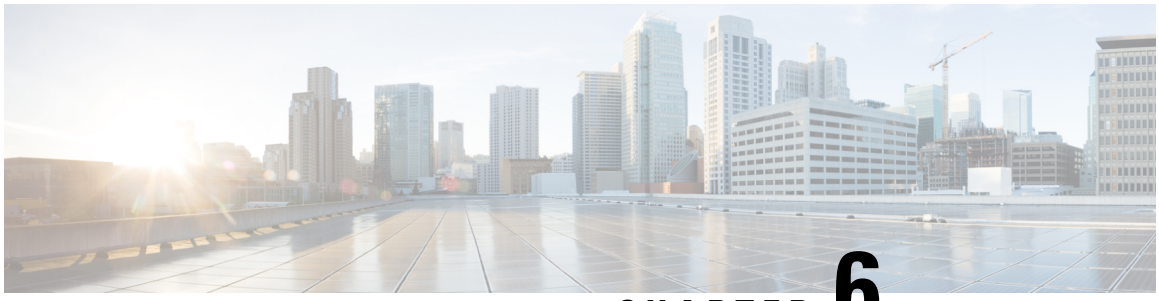
- `/ngfw/var/sf/updates` on FTD devices
- `/var/sf/updates` on the FMC and Classic devices (ASA FirePOWER, NGIPSv)

If the package is not in the upgrade directory (for example, if you manually deleted it) contact Cisco TAC. Do not untar signed (.tar) packages.

Table 24: Uninstall Packages for Firepower Patches

Platform	Package
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Patch_Uninstaller-*version-build*.sh.REL.tar
Firepower 1000 series	Cisco_FTD_SSP_FP1K_Patch_Uninstaller-*version-build*.sh.REL.tar
Firepower 2100 series	Cisco_FTD_SSP_FP2K_Patch_Uninstaller-*version-build*.sh.REL.tar
Firepower 4100/9300 chassis	Cisco_FTD_SSP_Patch_Uninstaller-*version-build*.sh.REL.tar
ASA 5500-X series with FTD ISA 3000 with FTD FTDv	Cisco_FTD_Patch_Uninstaller-*version-build*.sh.REL.tar

Platform	Package
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Patch_Uninstaller-*version-build*.sh.REL.tar
ASA FirePOWER	Cisco_Network_Sensor_Patch_Uninstaller-*version-build*.sh.REL.tar



CHAPTER 6

Freshly Install the Software

If you cannot or do not want to upgrade, you can freshly install major and maintenance releases.

We do not provide installation packages for patches. To run a particular patch, install the appropriate major or maintenance release, then apply the patch.

- Deciding to Freshly Install, on page 37
- Guidelines and Limitations for Fresh Installs, on page 39
- Unregistering Smart Licenses, on page 41
- Installation Instructions, on page 42

Deciding to Freshly Install

Use this table to identify scenarios where you need to freshly install (also called *reimaging*). Note that for Firepower devices, in all of these scenarios—including switching device management between local and remote—*you will lose device configurations*.

Note Address licensing concerns before you reimage or switch management. If you are using Cisco Smart Licensing, you may need to unregister from the Cisco Smart Software Manager (CSSM) to avoid accruing orphan entitlements. These can prevent you from reregistering.

Table 25: Scenarios: Do You Need a Fresh Install?

Scenario	Solution	Cisco Smart Licensing
Upgrade FMC-managed devices from a much older Firepower version.	The upgrade path from older versions can include intermediate versions. Especially in larger deployments where you must alternate FMC and device upgrade, this multi-step process can be time consuming. To save time, you can reimage older devices instead of upgrading: **1.** Remove the devices from the FMC. **2.** Upgrade the FMC only to its target version. **3.** Reimage the devices. **4.** Re-add the devices to the FMC.	Removing devices from the FMC unregisters them. Reassign licenses after you re-add the devices.
Change FTD management from FDM to FMC (local to remote).	Use the **configure manager** CLI command; see Cisco Firepower Threat Defense Command Reference.	Unregister the device before you switch management. Reassign its license after you add it to the FMC.
Change FTD management from FMC to FDM (remote to local).	Use the **configure manager** CLI command; see Cisco Firepower Threat Defense Command Reference. **Exception:** The device is running or was upgraded from Version 6.0.1. In this case, reimage.	Remove the device from the FMC to unregister it. Reregister using FDM.
Change ASA FirePOWER management between ASDM and FMC.	Start using the other management method.	Contact Sales for new Classic licenses. ASA FirePOWER licenses are associated with a specific manager.
Replace ASA FirePOWERwith FTD on the *same* physical device.	Reimage.	Convert Classic to Smart licenses; see the Firepower Management Center Configuration Guide.
Replace NGIPSv with FTDv.	Reimage.	Contact Sales for new Smart licenses.
Uninstall an FTD patch with FDM.	Reimage. You cannot uninstall patches in FDM deployments.	Unregister the device before you reimage. Reregister after.
Return to a previous major or maintenance release.	Reimage. You cannot uninstall major or maintenance upgrades. If possible, restore from backup.	Do not unregister before you reimage, and do not remove devices from the FMC. If you do, you must unregister again after you restore, then re-register. Instead, revert any licensing changes made since you took the backup. After the restore completes, reconfigure licensing. If you notice licensing conflicts or orphan entitlements, contact Cisco TAC.

Scenario	Solution	Cisco Smart Licensing
Restore a failed FMC or FTD device from backup.	In an RMA scenario, the replacement will arrive configured with factory defaults. However, if the replacement is already configured, we recommend you reimage before you restore.	Do not unregister before you reimage, and do not remove devices from the FMC. If you do, you must unregister again after you restore, then re-register. Instead, revert any licensing changes made since you took the backup. After the restore completes, reconfigure licensing. If you notice licensing conflicts or orphan entitlements, contact Cisco TAC.

Guidelines and Limitations for Fresh Installs

Careful planning and preparation can help you avoid missteps. Even if you are familiar with Firepower releases and have previous experience reimaging Firepower appliances, make sure you read these guidelines and limitations, as well as the instructions linked in Installation Instructions, on page 42.

Back Up Event and Configuration Data

When supported, we strongly recommend you back up before you reimage.

Note If you are reimaging so that you don't have to upgrade, due to version restrictions you cannot use a backup to import your old configurations. You must recreate your configurations manually.

You should back up to a secure remote location and verify transfer success. Reimaging returns most settings to factory defaults, including the system password. It deletes any backups left on the appliance. And especially because backup files are unencrypted, do not allow unauthorized access. If backup files are modified, the restore process will fail.

As the first step in any backup, note the appliance model and version, including patch level. For FMCs running Version 6.5.0 and earlier, note the VDB version. For Firepower 4100/9300 chassis, note the FXOS version. This is important because if you need to restore the backup to a new or reimaged appliance, you may need to update the new appliance first.

Note Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. Careful planning and preparation can help you avoid missteps. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your Firepower product.

Remove Devices from the Firepower Management Center

If you plan to manually configure the reimaged appliance, remove devices from remote management before you reimage:

- If you are reimaging the FMC, remove all its devices from management.

- If you are reimaging a single device or switching from remote to local management, remove that one device.

Note that if you plan to restore from backup after reimaging the FMC or FTD device, you do not need to remove devices from remote management.

Address Licensing Concerns

Before you reimage *any* Firepower appliance, address licensing concerns. You may need to unregister from the Cisco Smart Software Manager, or you may need to contact Sales for new licenses. See Deciding to Freshly Install to determine what you need to do, depending on your scenario.

For more information on licensing, see:

- Cisco Firepower System Feature Licenses Guide
- Frequently Asked Questions (FAQ) about Firepower Licensing
- The licensing chapter in your *Configuration Guide*.

Appliance Access

Reimaging returns most settings to factory defaults.

If you do not have physical access to an appliance, the reimage process lets you keep management network settings. This allows you to connect to the appliance after you reimage to perform the initial configuration. If you delete network settings, you *must* have physical access to the appliance. You cannot use Lights-Out Management (LOM).



Note Reimaging to an earlier major version automatically deletes network settings. In this rare case, you must have physical access.

For devices, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also able to access the FMC management interface without traversing the device.

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 initial setup, 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. Web analytics tracking is on by default (by accepting the EULA you consent to web analytics tracking), but you can opt out at any time after you complete initial setup. You may also have to opt out again after major upgrades, which can reenable this feature.

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

information from your devices during the course of a TAC case. During initial setup, you may be asked to accept or decline participation. You can also opt in or out at any time.

Reimaging Firepower 1000/2100 Series Devices to Earlier Major Versions

We recommend that you perform *complete* reimages of Firepower 1000/2100 series devices. If you use the erase configuration method, FXOS may not revert along with the Firepower Threat Defense software. This can cause failures, especially in high availability deployments.

For more information, see the reimage procedures in the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 Series Running Firepower Threat Defense.

Unregistering Smart Licenses

Firepower Threat Defense devices, whether locally (Firepower Device Manager) or remotely (Firepower Management Center) managed, use Cisco Smart Licensing. To use licensed features, you must register with Cisco Smart Software Manager (CSSM). If you later decide to reimage or switch management, you must unregister to avoid accruing orphan entitlements. These can prevent you from reregistering.



Note If you need to restore an FMC or FTD device from backup, do *not* unregister before you reimage, and do not remove devices from the FMC. Instead, revert any licensing changes made since you took the backup. After the restore completes, reconfigure licensing. If you notice licensing conflicts or orphan entitlements, contact Cisco TAC.

Unregistering removes an appliance from your virtual account, unregisters it from the cloud and cloud services, and releases associated licenses so they can be can be reassigned. When you unregister an appliance, it enters Enforcement mode. Its current configuration and policies continue to work as-is, but you cannot make or deploy any changes.

Manually unregister from CSSM before you:

- Reimage a Firepower Management Center that manages FTD devices.
- Shut down the source Firepower Management Center during model migration.
- Reimage a Firepower Threat Defense device that is locally managed by FDM.
- Switch a Firepower Threat Defense device from FDM to FMC management.

Automatically unregister from CSSM when you remove a device from the FMC so you can:

- Reimage an Firepower Threat Defense device that is managed by an FMC.
- Switch a Firepower Threat Defense device from FMC to FDM management.

Note that in these two cases, removing the device from the FMC is what automatically unregisters the device. You do not have to unregister manually as long as you remove the device from the FMC.

Tip Classic licenses for NGIPS devices are associated with a specific manager (ASDM/FMC), and are not controlled using CSSM. If you are switching management of a Classic device, or if you are migrating from an NGIPS deployment to an FTD deployment, contact Sales.

Unregister a Firepower Management Center

Unless you plan to restore from backup, unregister a Firepower Management Center from CSSM before you reimage. This also unregisters any managed Firepower Threat Defense devices.

If the FMC is configured for high availability, licensing changes are automatically synchronized. You do not need to unregister the other FMC.

Step 1 Log into the Firepower Management Center.

Step 2 Choose **System** > **Licenses** > **Smart Licenses**.

Step 3 Next to Smart License Status, click **Stop Sign** ().

Step 4 Read the warning and confirm that you want to unregister.

Unregister an FTD Device Using FDM

Unregister locally managed Firepower Threat Defense devices from the Cisco Smart Software Manager before you either reimage or switch to remote (FMC) management.

If the device is configured for high availability, you must log into the other unit in the high availability pair to unregister that unit.

Step 1 Log into the Firepower Device Manager.

Step 2 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 3 Select **Unregister Device** from the gear drop-down list.

Step 4 Read the warning and confirm that you want to unregister.

Installation Instructions

The release notes do not contain installation instructions. Instead, see one of the following documents. Installation packages are available on the Cisco Support & Download site.

Table 26: Firepower Management Center Installation Instructions

FMC Platform	Guide
FMC 1600, 2600, 4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide

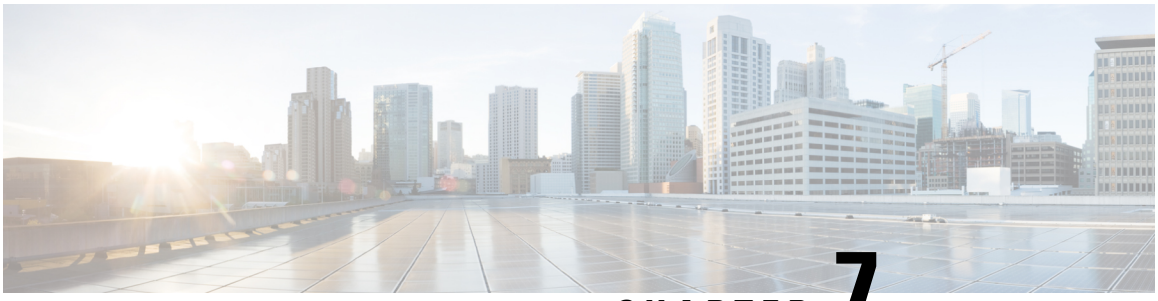
FMC Platform	Guide
FMC 1000, 2500, 4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
FMC 2000, 4000	Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide
FMCv and FMCv 300	Cisco Firepower Management Center Virtual Getting Started Guide

Table 27: Firepower Threat Defense Installation Instructions

FTD Platform	Guide
Firepower 1000/2100 series	Cisco ASA and Firepower Threat Defense Reimage Guide Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 Series Running Firepower Threat Defense
Firepower 4100/9300 chassis	Cisco Firepower 4100/9300 FXOS Configuration Guides: *Image Management* chapters Cisco Firepower 4100 Getting Started Guide Cisco Firepower 9300 Getting Started Guide
ASA 5500-X series	Cisco ASA and Firepower Threat Defense Reimage Guide
ISA 3000	Cisco ASA and Firepower Threat Defense Reimage Guide
FTDv: VMware	Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide
FTDv: KVM	Cisco Firepower Threat Defense Virtual for KVM Getting Started Guide
FTDv: AWS	Cisco Firepower Threat Defense Virtual for the AWS Cloud Getting Started Guide
FTDv: Azure	Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide

Table 28: NGIPSv and ASA FirePOWER Installation Instructions

NGIPS Platform	Guide
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware
ASA FirePOWER	Cisco ASA and Firepower Threat Defense Reimage Guide ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide: *Managing the ASA FirePOWER Module*



CHAPTER 7

Documentation

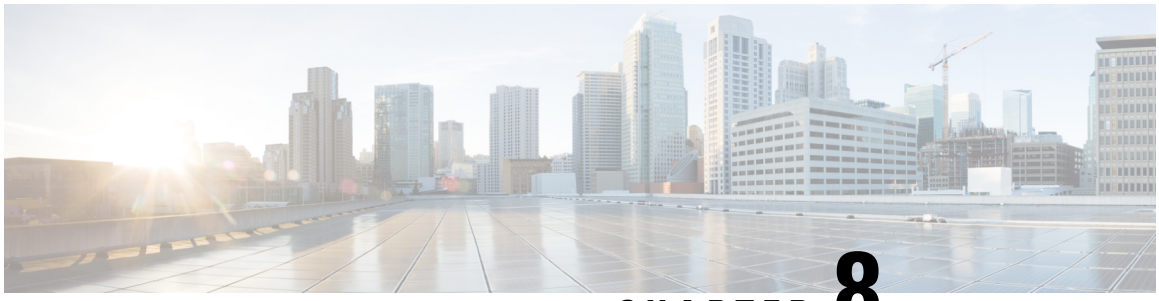
We update Firepower documentation if a patch requires it.

- Documentation Roadmaps, on page 45

Documentation Roadmaps

Documentation roadmaps provide links to currently available and legacy documentation:

- Navigating the Cisco Firepower Documentation
- Navigating the Cisco ASA Series Documentation
- Navigating the Cisco FXOS Documentation



CHAPTER 8

Resolved Issues

For your convenience, these release notes list the resolved bugs for each patch.

Note Each list is auto-generated *once* and is not subsequently updated. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes. You should regard the Cisco Bug Search Tool as the 'source of truth.'

For resolved issues, see:

- Searching for Resolved Issues, on page 47
- Version 6.6.0.1 Resolved Issues, on page 48

Searching for Resolved Issues

If you have a support contract, you can use the Cisco Bug Search Tool to obtain an up-to-date list of resolved bugs for Firepower products. You can constrain searches to bugs affecting specific Firepower platforms and versions. You can also search by bug ID, or for specific keywords.

These general queries display resolved bugs for Firepower products running Version 6.6.0:

- Firepower Management Center
- Firepower Management Center Virtual
- Firepower Threat Defense
- ASA with FirePOWER Services
- NGIPSv

These general queries display resolved bugs for Firepower products running Version 6.6.x.x patches:

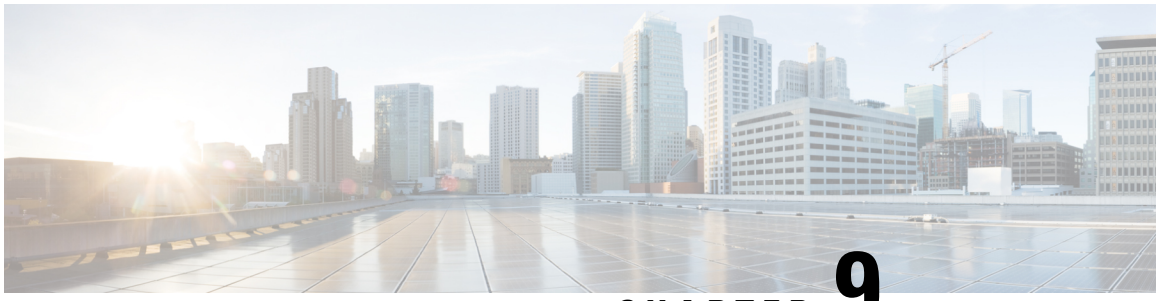
- Firepower Management Center
- Firepower Management Center Virtual
- Firepower Threat Defense
- ASA with FirePOWER Services

- NGIPSv

Version 6.6.0.1 Resolved Issues

Table 29: Version 6.6.0.1 Resolved Issues

Bug ID	Headline
CSCvt03598	Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability
CSCvu65843	FP2100: Fiber SFP Interfaces down due autonegotiation changes in 6.6.0



CHAPTER 9

Known Issues

We do not list known issues for patches.

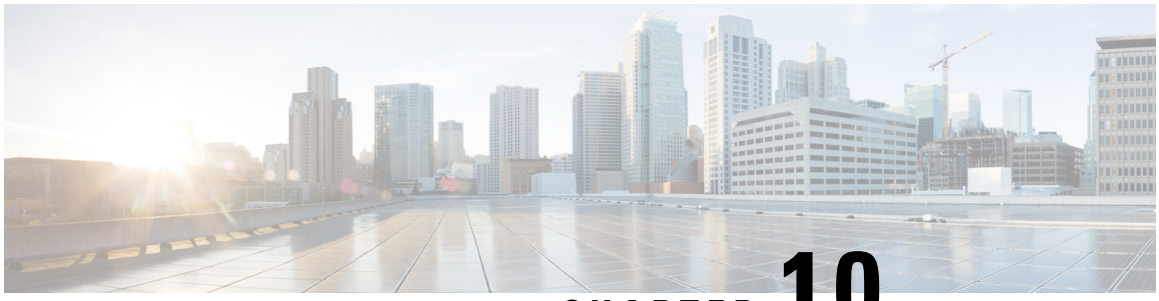
- Searching for Known Issues, on page 49

Searching for Known Issues

If you have a support contract, you can use the Cisco Bug Search Tool to obtain an up-to-date list of open bugs for Firepower products. You can constrain searches to bugs affecting specific Firepower platforms and versions. You can also search by bug ID, or for specific keywords.

These general queries display open bugs for Firepower products running Version 6.6.x.x patches:

- Firepower Management Center
- ASA with FirePOWER Services
- NGIPSv



CHAPTER 10

For Assistance

Thank you for choosing Firepower.

- Online Resources, on page 51
- Contact Cisco, on page 51

Online Resources

Cisco provides online resources to download documentation, software, and tools, to query bugs, and to open service requests. Use these resources to install and configure Firepower software and to troubleshoot and resolve technical issues.

- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.cisco.com/cisco/support/notifications.html

Access to most tools on the Cisco Support & Download site requires a Cisco.com user ID and password.

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts