Cisco Firepower Release Notes, Version 6.3.0 Patches

First Published: 2019-02-18

Last Modified: 2022-03-08

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.

CONTENTS

CHAPTER 9

CHAPTER 10

CHAPTER 1

Welcome

This document contains critical and release-specific information.

- Release Dates, on page 1
- Suggested Release, on page 2

Release Dates

Sometimes Cisco releases updated builds. In most cases, only the latest build for each platform is available on the Cisco Support & Download site. We *strongly* recommend you use the latest build. If you downloaded an earlier build, do not use it.

Table 1: Version 6.3.0 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.3.0	85	2019-01-22	Firepower 4100/9300	Firepower 4100/9300
6.3.0	84	2018-12-18	FMC/FMCv ASA FirePOWER	—
6.3.0	83	2019-06-27	—	FMC 1600, 2600, 4600
		2018-12-03	All FTD devices except Firepower 4100/9300 Firepower 7000/8000 NGIPSv	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices except Firepower 4100/9300

Table 2: Version 6.3.0 Patch Dates

Version	Build	Date	Platforms
6.3.0.5	35	2019-11-18	Firepower 7000/8000 series NGIPSv
	34	2019-11-18	FMC/FMCv All FTD devices ASA FirePOWER
6.3.0.4	44	2019-08-14	All
6.3.0.3	77	2019-06-27	FMC 1600, 2600, 4600
		2019-05-01	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices
6.3.0.2	67	2019-06-27	FMC 1600, 2600, 4600
		2019-03-20	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices
6.3.0.1	85	2019-06-27	FMC 1600, 2600, 4600
		2019-02-18	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices

Suggested Release

To take advantage of new features and resolved issues, we recommend you upgrade all eligible appliances to at least the suggested release. On the Cisco Support & Download site, the suggested release is marked with a gold star.

We also list the suggested release in the new feature guides:

- Cisco Firepower Management Center New Features by Release
- Cisco Firepower Device Manager New Features by Release

Suggested Releases for Older Appliances

If an appliance is too old to run the suggested release and you do not plan to refresh the hardware right now, choose a major version then patch as far as possible. Some major versions are designated *long-term* or *extra* *long-term*, so consider one of those. For an explanation of these terms, see Cisco NGFW Product Line Software Release and Sustaining Bulletin.

If you are interested in a hardware refresh, contact your Cisco representative or partner contact.

CHAPTER 2

Compatibility

For general compatibility information see:

- Cisco Firepower Compatibility Guide: Detailed compatibility information for all supported versions, including versions and builds of bundled operating systems and other components, as well as links to end-of-sale and end-of-life announcements for deprecated platforms.
- Cisco NGFW Product Line Software Release and Sustaining Bulletin: Support timelines for the Cisco Next Generation Firewall product line, including management platforms and operating systems.

For compatibility information for this version, see:

Firepower Management Center

The Firepower Management Center is a fault-tolerant, purpose-built network appliance that provides a centralized firewall management console. Firepower Management Center Virtual brings full firewall management functionality to virtualized environments.

Firepower Management Center

This release supports the following hardware FMC platforms:

- FMC 1600, 2600, 4600
- FMC 1000, 2500, 4500
- FMC 2000, 4000
- FMC 750, 1500, 3500

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

This release supports the following FMCv public cloud implementations:

- Firepower Management Center Virtual for Amazon Web Services (AWS)

This release supports the following FMCv on-prem/private cloud implementations:

- Firepower Management Center Virtual for Kernel-based virtual machine (KVM)
- Firepower Management Center Virtual for VMware vSphere/VMware ESXi 6.0 or 6.5

For supported 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. 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.

Note These release notes list the supported devices for *this* release. Even if an older device has reached EOL and you can no longer upgrade, you can still manage that device with a newer FMC, up to a few versions ahead. Similarly, newer versions of ASDM can manage older ASA FirePOWER modules. For supported management methods, including backwards compatibility, see Manager-Device Compatibility, on page 8.

Table 3: Firepower Threat Defense in Version 6.3.0

FTD Platform	OS/Hypervisor	Additional Details
Firepower 2110, 2120, 2130, 2140	—	—
Firepower 4110, 4120, 4140, 4150 Firepower 9300: SM-24, SM-36, SM-44 modules	FXOS 2.4.1.214 or later build.	Upgrade FXOS first. To resolve issues, you may need to upgrade FXOS to the latest build. To help you decide, see the Cisco Firepower 4100/9300 FXOS Release Notes, 2.4(1).
ASA 5508-X, 5516-X ASA 5515-X ASA 5525-X, 5545-X, 5555-X ISA 3000	—	Although you do not separately upgrade the operating system on these devices in FTD deployments, you should make sure you have the latest ROMMON image on the ISA 3000, ASA 5508-X and 5516-X. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.

FTD Platform	OS/Hypervisor	Additional Details
FTDv	Any of: • AWS: Amazon Web Services • Azure: Microsoft Azure • KVM: Kernel-based Virtual Machine • VMware vSphere/VMware ESXi 6.0 or 6.5	For supported instances, see the appropriate FTDv Getting Started guide.

Table 4: NGIPS/ASA FirePOWER in Version 6.3.0

NGIPS/ASA FirePOWER Platform	OS/Hypervisor	Additional Details
ASA 5508-X, 5516-X ISA 3000	ASA 9.5(2) to 9.16(x)	There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues. See the Cisco ASA Upgrade Guide for order of operations. You should also make sure you have the latest ROMMON image on the ISA 3000, ASA 5508-X and 5516-X. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.
ASA 5515-X	ASA 9.5(2) to 9.12(x)	
ASA 5525-X, 5545-X, 5555-X	ASA 9.5(2) to 9.14(x)	
ASA 5585-X-SSP-10, -20, -40, -60	ASA 9.5(2) to 9.12(x)	
NGIPSv	VMware vSphere/VMware ESXi 6.0 or 6.5	For supported instances, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.
Firepower 7010, 7020, 7030, 7050 Firepower 7110, 7115, 7120, 7125 Firepower 8120, 8130, 8140 Firepower 8250, 8260, 8270, 8290 Firepower 8350, 8360, 8370, 8390 AMP 7150, 8050, 8150 AMP 8350, 8360, 8370, 8390	—	—

Manager-Device Compatibility

Firepower Management Center

All devices support remote management with the Firepower Management Center, which can manage multiple devices. The FMC must run the *same or newer* version as its managed devices. You *cannot* upgrade a device past the FMC. Even for maintenance (third-digit) releases, you must upgrade the FMC first.

A newer FMC can manage older devices up to a few major versions back, as listed in the following table. However, we recommend you always update your entire deployment. New features and resolved issues often require the latest release on both the FMC and its managed devices.

Table 5: FMC-Device Compatibility

FMC Version	Oldest Device Version You Can Manage
6.7.x	6.3.0
6.6.x	6.2.3
6.5.0	6.2.3
6.4.0	6.1.0
6.3.0	6.1.0
6.2.3	6.1.0

Firepower Device Manager

Firepower Device Manager (FDM) is built into FTD and can manage a single device. FDM lets you configure the basic features of the software that are most commonly used for small or mid-size networks.

Table 6: FDM-FTD Compatibility

FTD Platform	FDM Compatibility
Firepower 2100 series	6.2.1+
Firepower 4100/9300	6.5.0+
ASA 5500-X series	6.1.0 to 7.0.x
ISA 3000	6.2.3+
FTDv for AWS	6.6.0+
FTDv for Azure	6.5.0+
FTDv for KVM	6.2.3+
FTDv for VMware	6.2.2+

Adaptive Security Device Manager

ASA with FirePOWER Services is an ASA firewall that runs Firepower NGIPS software as a separate application, also called the ASA FirePOWER module. You can use Cisco Adaptive Security Device Manager (ASDM) to manage both applications.

In most cases, newer ASDM versions are backwards compatible with all previous ASA versions. However, there are some exceptions. For example, ASDM 7.13(1) can manage an ASA 5516-X on ASA 9.10(1). ASDM 7.13(1) and ASDM 7.14(1) did not support ASA 5512-X, 5515-X, 5585-X, and ASASM; you must upgrade to ASDM 7.13(1.101) or 7.14(1.48) to restore ASDM support. For details, see Cisco ASA Compatibility.

A newer ASA FirePOWER module requires a newer version of ASDM, as listed in the following table.

Table 7: ASDM-ASA FirePOWER Compatibility

ASA FirePOWER Version	Minimum ASDM Version
6.7.x	7.15.1
6.6.x	7.14.1
6.5.0	7.13.1
6.4.0	7.12.1
6.3.0	7.10.1
6.2.3	7.9.2

Web Browser Compatibility

Browsers

We test 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 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 appliance 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 our products.

Securing Communications

When you first log in, 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, 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:

- Firepower Management Center or 7000/8000 series: Select **System** > **Configuration**, then click **HTTPS Certificates**.
- Firepower Device Manager: 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 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 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 8: Screen Resolution Requirements

Interface	Resolution
Firepower Management Center	1280 x 720
7000/8000 series device (limited local interface)	1280 x 720
Firepower Device Manager	1024 x 768
ASDM managing an ASA FirePOWER module	1024 x 768
Firepower Chassis Manager for the Firepower 4100/9300	1024 x 768

CHAPTER 3

Features and Functionality

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

Features for Firepower Management Center Deployments

Note Version 6.6.0/6.6.x is the last release to support the Cisco Firepower User Agent software as an identity source. You cannot upgrade a Firepower Management Center with user agent configurations to Version 6.7.0+. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC). This will also allow you to take advantage of features that are not available with the user agent. To convert your license, contact your Cisco representative or partner contact.

For more information, see the End-of-Life and End-of-Support for the Cisco Firepower User Agent announcement and the Firepower User Identity: Migrating from User Agent to Identity Services Engine TechNote.

New Features in FMC Version 6.3.0 Patches

Table 9:

Feature	Description
Version 6.3.0.4 Detection of rule conflicts in FTD NAT policies	**Upgrade impact.** After you upgrade to Version 6.3.0.4 or later patch, you can no longer create FTD NAT policies with conflicting rules (often referred to as *duplicate* or *overlapping* rules). This fixes an issue where conflicting NAT rules were applied out-of-order. If you currently have conflicting NAT rules, you will be able to deploy post-upgrade. However, your NAT rules will continue to be applied out-of-order. Therefore, we recommend that after the upgrade, you inspect your FTD NAT policies by editing (no changes are needed) then attempting to resave. If you have rule conflicts, the system will prevent you from saving. Correct the issues, save, and then deploy. Note that upgrading to Version 6.4.0 deprecates this fix. It is fixed again in Version 6.4.0.2.
Version 6.3.0.4 ISE Connection Status Monitor module	A new module, the *ISE Connection Status Monitor*, monitors the status of the server connections between the Cisco Identity Services Engine (ISE) and the FMC. Note that upgrading to Version 6.4.0 deprecates this module. Support returns in Version 6.4.0.2. New/modified screens: **System** > > **Policy** > create or edit policy > **ISE Connection Status Monitor**
Version 6.3.0.3 2048-bit certificate keys now required (security enhancement)	When making secure connections to external data sources, such as AMP for Endpoints or Cisco Threat Intelligence Detector (TID), the FMC now requires that the server certificate be generated with keys that are at least 2048 bits long. Certificates previously generated with 1024-bit keys will no longer work. If you cannot connect, regenerate the server certificate on your data source. If necessary, reconfigure the FMC connection to the data source.
Version 6.3.0.1 EMS extension support	**Upgrade impact.** Version 6.3.0.1 reintroduces EMS extension support, which was introduced in Version 6.2.3.8/6.2.3.9 but was not included in Version 6.3.0. Both the **Decrypt-Resign** and **Decrypt-Known Key** SSL policy actions again support the EMS extension during ClientHello negotiation, enabling more secure communications. The EMS extension is defined by RFC 7627. In FMC deployments, this feature depends on the *device* version. Although best practice is to upgrade your whole deployment, this feature is supported even if you patch only the device.

Features for Firepower Device Manager Deployments

New Features in FDM Version 6.3.0 Patches

Table 10:

Feature	Description
Version 6.3.0.1 EMS extension support	**Upgrade impact.** Version 6.3.0.1 reintroduces EMS extension support, which was introduced in Version 6.2.3.8/6.2.3.9 but was not included in Version 6.3.0. Both the **Decrypt-Resign** and **Decrypt-Known Key** SSL policy actions again support the EMS extension during ClientHello negotiation, enabling more secure communications. The EMS extension is defined by RFC 7627.

Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

Intrusion rule updates (SRUs) provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. If a newer intrusion rule uses keywords that are not supported in your current version, that rule is not imported when you update the SRU.

After you upgrade 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 your Snort version:

- 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 in 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.

How-To Walkthroughs for the FMC

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 11: 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.

Sharing Data with Cisco

Web Analytics tracking

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.

You are enrolled in web analytics tracking by default (by accepting the Version 6.5.0+ EULA you consent to web analytics tracking), but you can change your enrollment at any time after you complete initial setup.

Note Upgrades to Version 6.2.3 through 6.6.x can enroll you in web analytics tracking. This can occur even if you purposely unenrolled. If you do not want Cisco to collect this data, unenroll after upgrading.

Cisco Success Network

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 and upgrades, you may be asked to enroll. You can also change your enrollment at any time.

Cisco Support Diagnostics

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 and upgrades, you may be asked to enroll. You can also change your enrollment at any time.

Note This feature is supported on Firepower Management Centers and their managed Firepower Threat Defense devices. In Version 6.5.0 only, FTD support is restricted to the Firepower 4100/9300 with FTD and FTDv for Azure. This feature is not supported with Firepower Device Manager.

CHAPTER 4

Upgrade the Software

This chapter provides critical and release-specific information.

Planning Your Upgrade

Careful planning and preparation can help you avoid missteps. This table summarizes the upgrade planning process. For detailed checklists and procedures, see the the appropriate upgrade or configuration guide for full instructions: Upgrade Instructions, on page 33.

Table 12: Upgrade Planning Phases

Planning Phase	Includes
Planning and Feasibility	Assess your deployment. Plan your upgrade path. Read *all* upgrade guidelines and plan configuration changes. Check appliance access. Check bandwidth. Schedule maintenance windows.
Backups	Back up the software. Back up FXOS on the Firepower 4100/9300. Back up ASA for ASA FirePOWER.
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.

Planning Phase	Includes
Associated Upgrades	Upgrade virtual hosting in virtual deployments. Upgrade FXOS on the Firepower 4100/9300. Upgrade ASA for ASA FirePOWER.
Final Checks	Check configurations. Check NTP synchronization. Check disk space. Deploy configurations. Run readiness checks. Check running tasks. Check deployment health and communications.

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.

Upgrade Guidelines for Version 6.3.0.x Patches

This checklist contains upgrade guidelines for Version 6.3.0 patches.

Table 13: Version 6.3.0.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: Insufficient Disk Space on Container Instances, on page 20	Firepower 4100/9300	6.3.0 through 6.4.0.x	6.3.0.1 through 6.5.0

Upgrade Failure: Insufficient Disk Space on Container Instances

Deployments: Firepower 4100/9300 with FTD

Upgrading from: Version 6.3.0 through 6.4.0.x

Directly to: Version 6.3.0.1 through Version 6.5.0

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

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

Unresponsive Upgrades

Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot, shut down, or restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Traffic Flow and Inspection

Interruptions in traffic flow and inspection can occur when you:

- Reboot a device.
- Upgrade the device software, operating system, or virtual hosting environment.
- Uninstall the device software.
- Move a device between domains.
- Deploy configuration changes (Snort process restarts).

Device type, high availability/scalibility configurations, and interface configurations determine the nature of the interruptions. We *strongly* recommend performing these tasks in a maintenance window or at a time when any interruption will have the least impact on your deployment.

Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300

FXOS Upgrades

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 14: Traffic Behavior: FXOS Upgrades

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.

Deployment	Method	Traffic Behavior
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)	Hardware bypass enabled: **Bypass: Standby** or **Bypass-Force**. (6.1+)	Passed without inspection.
	Hardware bypass disabled: **Bypass: Disabled**. (6.1+)	Dropped until at least one module is online.
	No hardware bypass module.	Dropped until at least one module is online.

Software Upgrades for Standalone Devices

Devices operate in maintenance mode while they upgrade. Entering maintenance mode at the beginning of the upgrade causes a 2-3 second interruption in traffic inspection. Interface configurations determine how a standalone device handles traffic both then and during the upgrade.

Table 15: Traffic Behavior: Software Upgrades for Standalone Devices

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, hardware bypass force-enabled: **Bypass: Force** (6.1+).	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby** (6.1+).	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: **Bypass: Disabled** (6.1+).	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability/Scalability

You should not experience interruptions in traffic flow or inspection while upgrading high availability or clustered devices.

- FTD with FMC: For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.

  For clusters, the data security module or modules upgrade first, then the control module. 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.

- FTD with FDM: For high availability pairs, upgrade the standby, manually switch roles, then upgrade the new standby.

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. Upgrading high availability or clustered devices from Version 6.0.1 through 6.2.2.x may have additional upgrade path requirements; see the upgrade path information in the planning chapter of the Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.

Software Uninstall (Patches)

In Version 6.2.3 and later, uninstalling a patch returns you to the version you upgraded from, and does not change configurations.

- FTD with FMC: For standalone devices, interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In high availability/scalability deployments, you must explicitly plan an uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.

- FTD with FDM: Not supported.

Deploying Configuration Changes

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 devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 16: Traffic Behavior: Deploying Configuration Changes

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).	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.

Firepower Threat Defense Upgrade Behavior: Other Devices

Software Upgrades for Standalone Devices

Devices operate in maintenance mode while they upgrade. Entering maintenance mode at the beginning of the upgrade causes a 2-3 second interruption in traffic inspection. Interface configurations determine how a standalone device handles traffic both then and during the upgrade.

Table 17: Traffic Behavior: Software Upgrades for Standalone Devices

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, hardware bypass force-enabled: **Bypass: Force** (Firepower 2100 series, 6.3+).	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby** (Firepower 2100 series, 6.3+).	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: **Bypass: Disabled** (Firepower 2100 series, 6.3+).	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability/Scalability

You should not experience interruptions in traffic flow or inspection while upgrading high availability devices.

- Firepower Threat Defense with FMC: For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.
- Firepower Threat Defense with FDM: For high availability pairs, upgrade the standby, manually switch roles, then upgrade the new standby.

Software Uninstall (Patches)

In Version 6.2.3 and later, uninstalling a patch returns you to the version you upgraded from, and does not change configurations.

- FTD with FMC: For standalone devices, interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In high availability/scalability deployments, you must explicitly plan an uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.
- FTD with FDM: Not supported.

Deploying Configuration Changes

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 devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 18: Traffic Behavior: Deploying Configuration Changes

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).	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.

Firepower 7000/8000 Series Upgrade Behavior

The following sections describe device and traffic behavior when you upgrade Firepower 7000/8000 series devices.

Standalone 7000/8000 Series: Firepower Software Upgrade

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

Table 19: Traffic Behavior During Upgrade: Standalone 7000/8000 Series

Interface Configuration	Traffic Behavior
Inline, hardware bypass enabled (**Bypass Mode: Bypass**)	Passed without inspection, although traffic is interrupted briefly at two points: • At the beginning of the upgrade process as link goes down and up (flaps) and the network card switches into hardware bypass. • After the upgrade finishes as link flaps and the network card switches out of bypass. Inspection resumes after the endpoints reconnect and reestablish link with the device interfaces.

Interface Configuration	Traffic Behavior
Inline, no hardware bypass module,or hardware bypass disabled (**Bypass Mode: Non-Bypass**)	Dropped
Inline, tap mode	Egress packet immediately, copy not inspected
Passive	Uninterrupted, not inspected
Routed, switched	Dropped

7000/8000 Series High Availability Pairs: Firepower Software Upgrade

You should not experience interruptions in traffic flow or inspection while upgrading devices (or device stacks) in high availability pairs. To ensure continuity of operations, they upgrade one at a time. Devices operate in maintenance mode while they upgrade.

Which peer upgrades first depends on your deployment:

- Routed or switched: Standby upgrades first. The devices switch roles, then the new standby upgrades. When the upgrade completes, the devices' roles remain switched. If you want to preserve the active/standby roles, manually switch the roles before you upgrade. That way, the upgrade process switches them back.
- Access control only: Active upgrades first. When the upgrade completes, the active and standby maintain their old roles.

8000 Series Stacks: Firepower Software Upgrade

In an 8000 series stack, devices upgrade simultaneously. Until the primary device completes its upgrade and the stack resumes operation, traffic is affected as if the stack were a standalone device. Until all devices complete the upgrade, the stack operates in a limited, mixed-version state.

Traffic Behavior During Deployment

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

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection on all devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 20: Traffic Behavior During Deployment: 7000/8000 Series

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.

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

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 21: 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 22: Traffic Behavior During NGIPSv Upgrade

Interface Configuration	Traffic Behavior
Inline	Dropped

Interface Configuration	Traffic Behavior
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 23: 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

Time and Disk Space Tests

For reference purposes, we provide reports of in-house time and disk space tests for the FTD and FMC software.

Time Tests

We report the *slowest* tested time of all software upgrades tested on a particular platform/series. Your upgrade will likely take longer than the provided times for multiple reasons, as explained in the following table. We recommend you track and record your own upgrade times so you can use them as future benchmarks.

⚠ **Caution** Even if the system appears inactive, do not manually reboot, shut down, or restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Table 24: Time Test Conditions for Software Upgrades

Condition	Details
Deployment	Times for FTD upgrades are from tests in a FMC deployments. Raw upgrade times for remotely and locally managed devices are similar, given similar conditions.
Versions	For major and maintenance releases, we test upgrades from all eligible previous major versions. For patches, we test upgrades from the base version. Upgrade time usually increases if your upgrade skips versions.
Models	In most cases, we test on the lowest-end models in each series, and sometimes on multiple models in a series.
Virtual appliances	We test with the default settings for memory and resources. However, note that upgrade time in virtual deployments is highly hardware dependent.
High availability/scalability	Unless otherwise noted, 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.
Components	We report times for the software upgrade itself and the subsequent reboot *only*. This does not include time for operating system upgrades, transferring upgrade packages, readiness checks, VDB and intrusion rule (SRU/LSP) updates, or deploying configurations.

Disk Space Tests

We report the *most* disk space used of all software upgrades tested on a particular platform/series. This includes the space needed to copy the upgrade package to the device.

We also report the space needed on the FMC (in /var) for the device upgrade package. If you are using FDM, ignore those values.

When we report disk space estimates for a particular location (for example, /var or /ngfw), we are reporting the disk space estimate for the partition mounted in that location. On some platforms, these locations may be on the same partition.

Table 25: Checking Disk Space

Platform	Command
FMC	Choose **System** > **Monitoring** > **Statistics** and select the FMC. Under Disk Usage, expand the By Partition details.

Platform	Command
FTD with FMC	Choose **System** > **Monitoring** > **Statistics** and select the device you want to check. Under Disk Usage, expand the By Partition details.
FTD with FDM	Use the **show disk** CLI command.

Version 6.3.0.5 Time and Disk Space

Table 26: Version 6.3.0.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	4.9 GB	200 MB	—	46 min
FMCv: VMware	4.5 GB	180 MB	—	41 min
Firepower 2100 series	2.3 GB	2.3 GB	480 MB	21 min
Firepower 4100 series	1.6 GB	1.6 GB	280 MB	13 min
Firepower 9300	1.6 GB	1.6 GB	280 MB	17 min
ASA 5500-X series with FTD	1.7 GB	110 MB	270 MB	26 min
FTDv: VMware	1.7 GB	110 MB	270 MB	17 min
Firepower 7000/8000 series	2.6 GB	210 MB	600 MB	23 min
ASA FirePOWER	3.6 GB	47 MB	540 MB	74 min
NGIPSv	2.1 GB	160 MB	440 MB	17 min

Version 6.3.0.4 Time and Disk Space

Table 27: Version 6.3.0.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	3.4 GB	180 MB	—	34 min
FMCv: VMware	4.4 GB	180 MB	—	38 min
Firepower 2100 series	2.3 GB	2.3 GB	480 MB	17 min
Firepower 4100 series	1.6 GB	1.6 GB	280 MB	12 min
Firepower 9300	1.8 GB	1.8 GB	280 MB	12 min
ASA 5500-X series with FTD	1.7 GB	110 MB	270 MB	23 min
FTDv: VMware	1.7 GB	110 MB	270 MB	18 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
Firepower 7000/8000 series	3.3 GB	170 MB	600 MB	21 min
ASA FirePOWER	3.5 GB	31 MB	530 MB	48 min
NGIPSv	2.1 GB	160 MB	430 MB	16 min

Version 6.3.0.3 Time and Disk Space

Table 28: Version 6.3.0.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	3.7 GB	180 MB	—	33 min
FMCv: VMware	3.2 GB	180 MB	—	24 min
Firepower 2100 series	1.2 GB	1.2 GB	290 MB	18 min
Firepower 4100 series	990 MB	990 MB	99 MB	11 min
Firepower 9300	990 MB	990 MB	99 MB	12 min
ASA 5500-X series with FTD	620 MB	110 MB	79 MB	18 min
FTDv: VMware	240 MB	110 MB	79 MB	7 min
Firepower 7000/8000 series	2.6 GB	170 MB	400 MB	20 min
ASA FirePOWER	2.9 GB	30 MB	340 MB	45 min
NGIPSv	1.5 GB	160 MB	250 MB	4 min

Version 6.3.0.2 Time and Disk Space

Table 29: Version 6.3.0.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	3.5 GB	180 MB	—	53 min
FMCv: VMware	3.2 GB	180 MB	—	28 min
Firepower 2100 series	1.2 GB	1.2 GB	100 MB	17 min
Firepower 4100 series	970 MB	970 MB	100 MB	12 min
Firepower 9300	970 MB	970 MB	100 MB	11 min
ASA 5500-X series with FTD	570 MB	110 MB	80 MB	12 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FTDv: VMware	600 MB	110 MB	80 MV	10 min
Firepower 7000/8000 series	2.5 GB	170 MB	400 MB	20 min
ASA FirePOWER	3.0 GB	30 MB	340 MB	45 min
NGIPSv	1.5 GB	160 MB	250 MB	10 min

Version 6.3.0.1 Time and Disk Space

Table 30: Version 6.3.0.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	3.0 GB	170 MB	—	31 min
FMCv: VMware	2.4 GB	170 MB	—	25 min
Firepower 2100 series	1.2 GB	1.2 GB	290 MB	18 min
Firepower 4100 series	740 MB	740 MB	100 MB	12 min
Firepower 9300	740 MB	740 MB	100 MB	12 min
ASA 5500-X series with FTD	400 MB	150 MB	72 MB	17 min
FTDv: VMware	400 MB	150 MB	72 MB	10 min
Firepower 7000/8000 series	2.1 GB	170 MB	350 MB	20 min
ASA FirePOWER	2.4 GB	28 MB	270 MB	44 min
NGIPSv	1.5 GB	150 MB	350 MB	10 min

Upgrade Instructions

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

Table 31: Firepower Upgrade Instructions

Task	Guide
Upgrade in Firepower Management Center deployments.	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0

Task	Guide
Upgrade Firepower Threat Defense with Firepower Device Manager.	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager See the *System Management* chapter in the guide for the Firepower Threat Defense version you are currently running—not the version you are upgrading to.
Upgrade FXOS on a Firepower 4100/9300 chassis.	Cisco Firepower 4100/9300 Upgrade Guide, Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1
Upgrade ASA FirePOWER modules with ASDM.	Cisco ASA Upgrade Guide
Upgrade the ROMMON image on the ISA 3000, ASA 5508-X, and ASA 5516-X.	Cisco ASA and Firepower Threat Defense Reimage Guide See the *Upgrade the ROMMON Image* section. You should always make sure you have the latest image.

CHAPTER 5

Uninstall a Patch

In Firepower Management Center and ASDM deployments, you can uninstall most patches. Uninstalling returns you to the version you upgraded from, and does not change configurations.

Uninstall is not supported for Firepower Device Manager. Do not attempt to uninstall a hotfix. Instead, contact Cisco TAC.

Patches That Support Uninstall

Uninstalling specific patches can cause issues, *even when the uninstall itself succeeds*. These issues include:

- Inability to deploy configuration changes after uninstall.
- Incompatibilities between the operating system and the 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, the 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.

Version 6.3.0 Patches That Support Uninstall

This table lists supported uninstall scenarios for Version 6.3.0 patches. Remember that uninstalling returns you to the patch level you upgraded from. If uninstall will take you farther back than what is supported, we recommend you reimage and then upgrade to your desired patch level.

Table 32: Version 6.3.0 Patches That Support Uninstall

Current Version	Farthest Back You Should Uninstall
6.3.0.5	—
6.3.0.1 through 6.3.0.4	6.3.0

Guidelines for Uninstalling Patches

Uninstall from Devices First, Using the Shell

The Firepower Management Center must run the *same or newer* version as its managed devices. This means that in FMC deployments, uninstall patches from managed devices first.

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 devices in high availability/scalability deployments. To plan an uninstall order that minimizes disruption, see Uninstall Order for HA/Scalability Deployments, on page 36.
- You cannot use the FMC or ASDM to uninstall a patch from a device, nor can you use the local web interface on a 7000/8000 series device.
- You cannot use FMC user accounts to log into and uninstall the patch from one of its managed devices. Devices 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 the FMC After Devices

Uninstall patches from the FMC after you uninstall from 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 36.

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.

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 33: Uninstall Order for FMCs in HA

Deployment	Uninstall Order
FMC high availability	With synchronization paused, which is a state called *split-brain*, uninstall from 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 34: Uninstall Order for FTD devices in HA or Clusters

Deployment	Uninstall Order
Device high availability	You cannot uninstall a patch from 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.
Device 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 35: Uninstall Order for 7000/8000 Series Devices in HA or Stacks

7000/8000 Series Deployment	Uninstall Order
7000/8000 series high availability	Always uninstall from the standby. An 7000/8000 series device in an HA pair operates in maintenance mode while the patch uninstalls. 1. Uninstall from the standby. 2. Switch roles. 3. Uninstall from the new standby.
8000 series stack	Uninstall from all devices in the stack at the same time. Until you uninstall the patch from all devices in a stack, the stack operates in a limited, mixed-version state.

Table 36: 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 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

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 39, 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 36.
- 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 clusters, stacks, 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. Note that ASA 5585-X series devices have a dedicated ASA FirePOWER console port.

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

Firepower 2100 series	`connect ftd`
Firepower 4100/9300	`connect module` *`slot_number`* `console`, then `connect ftd` (first login only)
ASA FirePOWER, except ASA 5585-X series	`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/uninstaller_name
```

When you patch a Firepower appliance, an easily identifiable uninstaller for that patch is automatically created in the upgrade directory; see Uninstall Packages, on page 44.

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 clusters, stacks, 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 41.

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 36.
- 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

Patch uninstallers are named like upgrade packages, but have 'Patch_Uninstaller' instead of 'Patch' in the file name. When you patch a Firepower appliance, the uninstaller for that patch is automatically created in the upgrade directory:

- `/ngfw/var/sf/updates` on Firepower Threat Defense devices
- `/var/sf/updates` on the Firepower Management Center and NGIPS devices (7000/8000 series, ASA FirePOWER, NGIPSv)

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

CHAPTER 6

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.

Installation Checklist and Guidelines

Reimaging returns most settings to factory defaults, including the system password. This checklist highlights actions that can prevent common reimage issues. However, this checklist is *not* comprehensive. See the appropriate installation guide for full instructions: Installation Instructions, on page 48.

Table 37:

✓	Action/Check
	Check appliance access. 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 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.

✓	Action/Check
	Perform backups. Back up before reimaging, when supported. Note that 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. **Caution** We *strongly* recommend you 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. Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your deployment.
	Determine if you must remove devices from FMC management. 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. If you plan to restore from backup after reimaging, you do not need to remove devices from remote management.
	Address licensing concerns. Before you reimage *any* appliance, address licensing concerns. You may need to unregister from the Cisco Smart Software Manager (CSSM) to avoid accruing orphan entitlements, which can prevent you from reregistering. Or, you may need to contact Sales for new licenses. For more information, see: • The configuration guide for your product. • Unregistering Smart Licenses, on page 47 • Cisco Firepower System Feature Licenses Guide • Frequently Asked Questions (FAQ) about Firepower Licensing

Reimaging Firepower 2100 Series Devices to Earlier Major Versions

We recommend that you perform complete reimages of Firepower2100 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.

Reimaging Version 5.x Hardware to Version 6.3.0+

The renamed installation packages in Version 6.3+ cause issues with reimaging older *physical* appliances: FMC 750, 1500, 2000, 3500, and 4000, as well as 7000/8000 series devices and AMP models. If you are currently running Version 5.x and need to freshly install Version 6.3.0, rename the installation package to the "old" name after you download it; see the *Renamed Upgrade and Installation Packages* information in the Cisco Firepower Release Notes, Version 6.3.0.

After you reimage an FMC (Defense Center) from Version 5.x to a more recent version, it cannot manage its older devices. You should also reimage those devices, then re-add them to the FMC. Note that Series 2 devices are EOL and cannot run Firepower software past Version 5.4.0.x. You must replace them.

Unregistering Smart Licenses

Firepower Threat Defense uses Cisco Smart Licensing. To use licensed features, 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 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.
- 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.

Installation Instructions

Table 38: Firepower Management Center Installation Instructions

FMC	Guide
FMC 1600, 2600, 4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
FMC 1000, 2500, 4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
FMC 750, 1500, 3500 FMC 2000, 4000	Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide
FMCv	Cisco Firepower Management Center Virtual Getting Started Guide

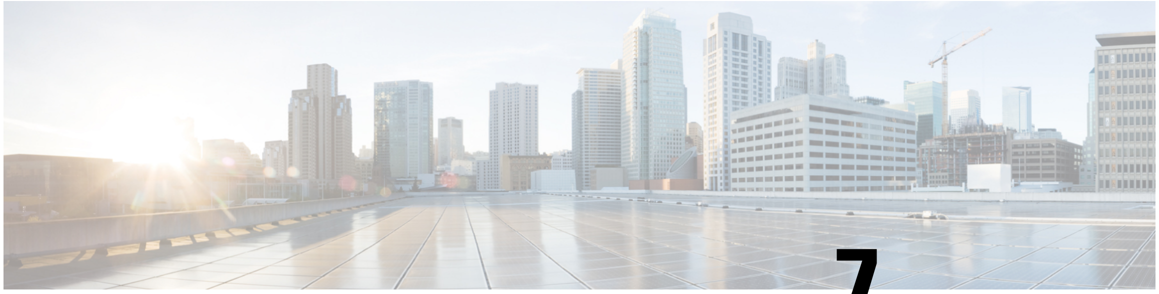
Table 39: Firepower Threat Defense Installation Instructions

FTD Platform	Guide
Firepower 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	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: 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
FTDv: KVM	Cisco Firepower Threat Defense Virtual for KVM Getting Started Guide
FTDv: VMware	Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide

Table 40: Firepower 7000/8000 Series, NGIPSv, and ASA FirePOWER Installation Instructions

NGIPS Platform	Guide
Firepower 7000 series	Cisco Firepower 7000 Series Getting Started Guide: *Restoring a Device to Factory Defaults*

NGIPS Platform	Guide
Firepower 8000 series	Cisco Firepower 8000 Series Getting Started Guide: *Restoring a Device to Factory Defaults*
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 51

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, the release notes list the resolved issues for each patch.

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

Important Bug lists are auto-generated *once* and are 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.

Version 6.3.0.5 Resolved Issues

Table 41: Version 6.3.0.5 Resolved Issues

Bug ID	Headline
CSCve24102	GUI should allow max 256 addresses per DHCP pool
CSCvh73096	Read sAMAccountUserName from ISE when it is available
CSCvk26612	"default Keyring's certificate is invalid, reason: expired" health alert
CSCvk43854	Cisco Firepower Threat Defense Detection Engine Policy Bypass Vulnerability
CSCvm40288	Port-Channel issues on HA link
CSCvm48451	Intrusion Event Performance Graphs load blank on 4100 and 9300
CSCvm68648	review of CVE-2016-8858 (OpenSSH) on Firepower software

Bug ID	Headline
CSCvm76266	Lina traceback in Thread Name: cli_xml_server
CSCvm82966	Linux Kernel 4.14 Vulnerabilities
CSCvn24594	add NTPDATE update of blade sysclock from the supervisor before starting NTPD
CSCvn77388	SDI - SUSPENDED servers cause 15sec delay in the completion of a authentication with a good server
CSCvn81898	Device name doesn't exist in a syslog message if syslog alerting for connection events is configured
CSCvn83385	Cisco FTD, FMC, and FXOS Software PAM Denial of Service Vulnerability
CSCvo11280	ASA Enhancement: Generate syslog message once member of the SDI cluster changes state
CSCvo14961	ASA may traceback and reload while waiting for "dns_cache_timer" process to finish.
CSCvo28118	Traceback in VPN Clustering HA timer thread when member tries to join the cluster
CSCvo29989	Cisco FirePower Threat Defense Information Disclosure Vulnerability
CSCvo43795	OSPF Process ID doesnot change even after clearing OSPF process
CSCvo66546	Firepower frequent traceback and restart on SFDataCorrelator process
CSCvo68448	ASA report SFR module as 'Unresponsive' after reloading ASA module on 5585 platform
CSCvo73250	ENH: ACE details for warning "found duplicate element"
CSCvo74397	ENH: Add process information to "Command Ignored, configuration in progress..."
CSCvo83169	Cisco ASA Software and FTD Software FTP Inspection Denial of Service Vulnerability
CSCvo86038	Simultaneous FINs on flow-offloaded flows lead to stale conns
CSCvo86940	PROMPTING FOR PASSWORD WHEN TRYING TO CONFIGURE enic, vfio-pci , igb_uio ON BLADE
CSCvo90998	LACPDUs should not be sent to snort for inline-set interfaces
CSCvp04186	cts import-pac tftp: syntax does not work
CSCvp12582	Option to display port number on access-list instead of well known port name on ASA
CSCvp19910	Unable to process gtpv1 identification req message for header TEID : 0
CSCvp19998	ASA drops GTPV1 SGSN Context Req message with header TEID:0
CSCvp23579	Network FIle Trajectory page takes 90 seconds to load each time

Bug ID	Headline
CSCvp33052	Firepower 8000 interfaces might flap due to unhandled resource temporarily unavailable issue
CSCvp33341	Cisco ASA and Firepower Threat Defense Software WebVPN Cross-Site Scripting Vulnerability
CSCvp46173	Changes in interface-group or interface-zone in subdomain overwrites Global domain.
CSCvp49576	FTD traceback due to watchdog on xlate_detach
CSCvp54261	Audit syslog for SFR module/7000/8000 devices uses TCP instead of UDP for syslog communication
CSCvp55901	LINA traceback on ASA in HA Active Unit repeatedly
CSCvp55941	FILE RESUME BLOCK being randomly thrown causing access issues on files from SMB share.
CSCvp58028	natd thread of nfm_exceptiond uses about 90% to 100% CPU time
CSCvp67257	USGv6 Failures From Kernel Upgrade [3.10 to 4.14]
CSCvp67626	2100 upgrade failure in 000_start/125_verify_bundle.sh when gateway IP improperly set
CSCvp72244	Evaluate Cisco 8000 series for CVE-2019-11815
CSCvp76944	Cisco ASA and FTD Software WebVPN CPU Denial of Service Vulnerability
CSCvp84546	ASA 9.9.2 Clientless WebVPN - HTML entities are incorrectly decoded when processing HTML
CSCvp87623	Upload an update gives "update request entity too large" error when using CAC(HTTPS Client Certs)
CSCvp97061	URL Filtering Shows All URLs as Uncategorized
CSCvp97799	Policy deploy failure 6.5.0-1148 post upgrade with CC mode with openSSL call during SSL pol Export
CSCvp98066	On reset CD not clearing its flags[parseFailoverReqIssued] which prevents further node join attempts
CSCvp99137	ASA on Firepower 2100: Excessive amount of DNS queries on Management Interface
CSCvq00675	Linux Kernel sas_expander.c Race Condition Arbitrary Code Execution ...
CSCvq01459	LINA Traceback after upgrade to 9.12.2.1
CSCvq05113	ASA failover LANTEST messages are sent on first 10 interfaces in the configuration.
CSCvq06790	Snort processes dump core with memory corruption on Series 3 devices
CSCvq08684	Policy Deployment Failure due to Special Characters & encoding

Bug ID	Headline
CSCvq09093	VPN Pre-deploy validations takes around 20 seconds for each device
CSCvq11513	Traceback: "saml identity-provider" command will crash multi-context ASAs
CSCvq12411	ASA may traceback due to SCTP traffic despite fix CSCvj98964
CSCvq13442	When deleting context the ssh key-exchange goes to Default GLOBALLY!
CSCvq16123	Firepower Dynamic Snort Rules are Disabled After a Deployment Involving a Snort Reload
CSCvq17263	FTD LINA traceback at DATAPATH-8-15821
CSCvq19525	Evaluation of sfims for TCP_SACK
CSCvq21607	"ssl trust-point" command will be removed when restoring backup via CLI
CSCvq24134	ASA IKEv2 - ASA sends additional delete message after initiating a phase 2 rekey
CSCvq25626	Watchdog on ASAv when logging to buffer
CSCvq25775	FTD Firepower 2100: external authentication fails if bind user password contains special characters
CSCvq26794	GTP response messages with non existent cause are getting dropped with error message TID is 0
CSCvq27010	Memory leak observed when ASA-SFR dataplane communication flaps
CSCvq28250	ENH: ASA Cluster debug for syn cookie issues
CSCvq32681	Fail to Wire configuration disabled for multiple interface-pair inline-sets during FTD upgrades
CSCvq36042	lost heartbeat causing reload
CSCvq39083	Security Intelligence does not drop HTTPS connections to blacklisted URLs when SSL policy is enabled
CSCvq39317	ASA is unable to verify the file integrity
CSCvq40943	FTD 4150 VPN s2s deployment failure with 6K spokes
CSCvq44665	FTD/ASA : Traceback in Datapath with assert snp_tcp_intercept_assert_disabled
CSCvq46918	SNMPv3 User(s) deleted after upgrade
CSCvq50314	Failed SSH Login attempts not being exported via syslog
CSCvq54242	Warning "There is an empty group in the source networks" in SSL policy
CSCvq54667	SSL VPN may not be able to establish due to SSL negotiation issue

Bug ID	Headline
CSCvq56138	User login fails into FMC GUI for LDAP user if the password contains SPACE in the string
CSCvq56462	File policy not inspecting some malware document (.doc) and Adobe flash (.swf) files.
CSCvq60131	ASA traceback observed when moving EZVPN spokes to the device.
CSCvq63024	Dual stacked ASAv manual failover issues
CSCvq64742	ASA5515-K9 standby traceback in Thread Name ssh
CSCvq65092	Slow device related REST API calls
CSCvq65241	ASA Traceback on Saleen in Thread Name: IPv6 IDB
CSCvq65542	Disable asp load-balance per-packet functionality from fp2100 until all bugs fixed
CSCvq69111	Traceback: Cluster unit lina assertion in thread name:Cluster controller
CSCvq70468	ASA cluster does not flush OSPF routes
CSCvq70485	Slow "securityzones" REST API
CSCvq75743	ASA:BGP recursive route lookup for destination 3 hop away is failing.
CSCvq76533	F_RNA_EVENT_LIMIT for MC4000 should be 20 million
CSCvq77547	Connections fail to replicate in failover due to failover descriptor mis-match on port-channels
CSCvq80318	ASA generates incorrect error message about PCI cfg space when enumerating Internal-Data0/1
CSCvq80735	Cannot add neighbor in BGP when the neighbor is on the same subnet as one interface
CSCvq81516	VPN events between 12 and 1 PM UTC are not displayed on the FMC
CSCvq91645	Flow Offload Hashing Change of Behavior

Version 6.3.0.4 Resolved Issues

Table 42: Version 6.3.0.4 Resolved Issues

Bug ID	Headline
CSCvf83160	Traceback on Thread Name: DATAPATH-2-1785
CSCvg01007	https pdf attachment issues
CSCvg74603	eStreamer archive events are not pruned correctly by diskmanager
CSCvi63474	Unable to edit the system policy of a SFR module via ASDM after upgrading to 6.2.2

Bug ID	Headline
CSCvk14242	sfstunnel process in FTD is holding large cloud db files that are already deleted
CSCvm27111	FTD Lina traceback while removing OSPF configuration.
CSCvm36362	Route tracking failure
CSCvm50421	ASA traceback on slave/standby during sync config due to OSPF/EIGRP and IPv6 used together in ACE
CSCvm70274	tcp proxy: ASA traceback on DATAPATH
CSCvm88294	High Disk utilization due to partition force drain not occurring
CSCvn25605	FTW: Bypass LED stays on solid amber even after total recovery of sensor
CSCvn34246	Loading AC policy editor takes too long, needs loading indicator
CSCvn45750	FMC Audit Logs will only display Admin and System as owners when deploying to 3D devices -GUI/SYSLOG
CSCvn57284	Unsupported EC curve x25519 on FTD
CSCvn66248	Configuring "boot config" has no effect if file was modified off-box and copied back on
CSCvn76875	Graceful Restart BGP does not work intermittently
CSCvn78597	Firepower block page not displayed on MS IE11 and Edge for HTTPS blocked sites when proxy is enabled
CSCvo03700	ASA may traceback in thread logger when cluster is enabled on slave unit
CSCvo24145	ids_event_alerter high memory usage due to large firewall_rule_cache table
CSCvo31695	Traceback in threadname DATAPATH-0-1668 while freeing memory block
CSCvo33348	Mysql traffic on non standard port is not correctly classified
CSCvo33851	ngfwManager doesn't start if ngfw.properties is empty
CSCvo43679	FTD Lina traceback, due to packet looping in the system by normaliser
CSCvo48838	Lina does not properly report the error for configuration line that is too long
CSCvo50168	Audit Log Settings Failing Leading to being unable to edit System Settings
CSCvo51265	SCP large file transfer to the box result in a traceback
CSCvo54799	ssh to device fails due to corrupted devpts entry in fstab
CSCvo56836	SCALE: with 500+ devices, UMS causes the UI to hang, especially during deploy
CSCvo60862	Internal Error when editing an Access Control Policy
CSCvo62060	Telemetry not sent when FMC managing lots of devices

Bug ID	Headline
CSCvo65464	FPR2100: EIGRP routes with learned over port channel interface become Infinite FD
CSCvo66534	Traceback and reload citing Datapath as affected thread
CSCvo70866	SGT tag shows untagged in server packet for every client packet with SGT tag with some value
CSCvo72179	For SMB, remote storage configuration should allow configuring version string with dot(.)
CSCvo72232	ERR_SSL_BAD_RECORD_MAC_ALERT or SSL_ERROR_BAD_MAC_ALERT in the browser
CSCvo74350	ASA may traceback and reload. Potentially related to WebVPN traffic
CSCvo74625	6.4.0 - IPv6 routing doesn't work for WM and KP when mgmt gateway configure as data-interfaces
CSCvo74745	cloud agent core after generating a large number of continuous URL lookups (>30M)
CSCvo78789	Cisco Adaptive Security Appliance Smart Tunnel Vulnerabilities
CSCvo80501	Standby Firewall reloads with a traceback upon doing a manual failover
CSCvo81073	Unable to load Device Management page or upgrade FMC due to missing NGFWHA EO
CSCvo81260	FMC "FQDN" via API causes all objects within a network attribute to be "ANY"
CSCvo83574	Device goes into a bad state when switching the inline set from TAP mode
CSCvo87930	HTTP with ipv6 using w3m is failing
CSCvo88188	SSL rules with App-ID conditions can limit decryption capability
CSCvo88306	NAT rules can get applied in the wrong order when you have duplicate rules
CSCvo89224	FMC times out after 10 mins to fetch device list for deployment
CSCvo90153	ASA unable to authenticate users with special characters via https
CSCvo90550	Firepower Recommendations does not enable IPS rules that are GID 3
CSCvo90805	Cisco Firepower Management Center RSS Cross-Site Scripting Vulnerabilities
CSCvo93872	Memory leak while inspecting GTP traffic
CSCvo94486	Snort process exits while processing Security Intelligence.
CSCvp03498	Health monitoring options for user identity functionality on FMC.
CSCvp07143	DTLS 1.2 and AnyConnect oMTU

Bug ID	Headline
CSCvp09150	Cisco ASA Software Web-Based Management Interface Privilege Escalation Vulnerability
CSCvp12052	ASA may traceback and reload. suspecting webvpn related
CSCvp16979	ssl and daq debug logs can't be enabled/disabled dynamically
CSCvp18878	ASA: Watchdog traceback in Datapath
CSCvp21837	Allow FTDs to perform URL lookups directly without having to go through the FMC Pre 6.5.0
CSCvp23137	ASA/FTD generates syslog for missing SSD 2: /dev/sdb is present. Status: Inoperable.
CSCvp24787	(snort)File is not getting detected when going over HTTPS (SSL Resign)
CSCvp25581	in FMC-HA user_group_map entries are wiped out in split-brain
CSCvp25583	FTD sets automatically metric 0 when we redistribute OSPF into BGP via FMC GUI.
CSCvp25782	EventHandler core while pruning metadata cache
CSCvp27263	Multiple ClamAV Vulnerabilities For Cisco Firepower Management Center for pre 6.5.0
CSCvp29245	FTD and FDM operations fail due to depleted disk space from excessive eventing logs
CSCvp32617	"established tcp" does not work post 9.6.2
CSCvp35359	FMC-ISE integration doesn't work if explicit UPN doesn't match implicit UPN
CSCvp36425	Cisco ASA & FTD Software Cryptographic TLS and SSL Driver Denial of Service Vulnerability
CSCvp37779	FTD show tech from troubleshooting files incomplete
CSCvp38808	FP2100: Removal of fault "The password encryption key has not been set."
CSCvp43474	REST API query /api/fmc_config/v1/domain/UUID/devices/devicerecords fails
CSCvp43536	On upgraded FMC Device FXOS devices are shown dirty even after successful deployment.
CSCvp46341	Fail-to-Wire (FTW) Ports fail to recover on 2100 Firepower platforms.
CSCvp54634	Wrong rule matched when using ambiguous DND
CSCvp58310	integrate pxgrid capability, connection hang, curl hang issues
CSCvp72488	Firepower: AMP for network connectivity failure after upgrading to 6.3.0.2+
CSCvp72601	FMC UI: VPN Hub and Spoke topology slow loading

Bug ID	Headline
CSCvp72770	BCDB file copy from FMC on to vFTD getting truncated, vFTD running on Azure platform.
CSCvp78197	Policy deployment remove and add back ospf neighbor
CSCvp81967	Slowness in loading Device Management page on FMC when there are over 500 managed devices
CSCvp82945	NAT policy apply failing with error duplicate
CSCvp96934	Ensure Error Message with Dup NATs Is Clear and Actionable
CSCvq08684	Policy Deployment Failure due to Special Characters & encoding
CSCvq34224	Firepower Primary Detection Engine process terminated after Manager upgrade
CSCvq61651	URL DB download failure alerts on FMC; new URL DB updates not taking effect on FMC/FDM

Version 6.3.0.3 Resolved Issues

Table 43: Version 6.3.0.3 Resolved Issues

Bug ID	Headline
CSCvi16224	snmp-server host command for SNMPv3 doesn't apply properly when deploy ASAv VM on NFVIS (KVM) system
CSCvi62112	Blocking BPDU via FlexConfig on FTD Transparent causes deployment and registration issues
CSCvj06993	ASA HA with NSF: NSF is not triggered properly when there is an Interface failure in ASA HA
CSCvj82652	Deployment changes are not pushed to the device due to disk0 mounted on read-only
CSCvk06386	FTD Files are Allowed Through Multiple Pre-existing Connections Despite the File Policy Verdict
CSCvm00066	ASA is stuck on "reading from flash" for several hours
CSCvm16724	FXOS ASA/FTD needs means to poll Internal-data interface counters
CSCvm35373	Pruner process fails to start due to configuration
CSCvm62846	restore of TID | Config only backup failed:
CSCvm86008	Policy Deployment: Delta config doesn't get copied to running config, LINA config remains unchanged
CSCvn07452	712x devices become unstable when switching inline set from TAP to inline

Bug ID	Headline
CSCvn09383	Manual URL lookup returns Uncategorized if same URL is entered second time without "www." part
CSCvn25949	Digitial Signature Verification Failed during upload of Rest-Api image to ASA
CSCvn30108	The 'show memory' CLI output is incorrect on ASAv
CSCvn31347	ACL Unable to configure an ACL after access-group configuration error
CSCvn38453	ASA: Not able to load Quovadis Root Certificate as trustpoint when FIPS is enabled
CSCvn44222	6.3.0-79: HA upgrade/deployment fails from from missing RAVPN diskfiles on secondary
CSCvn49854	Subsequent HTTP requests not retrieving URL and XFF
CSCvn67137	ASA5506 may slowly leak memory when using NetFlow
CSCvn67570	amp-stunnel.conf does not point to correct amp cloud server post FMC upgrade
CSCvn68527	KP:AnyConnect used IP from pool shows as available
CSCvn71592	After FMC reboot, intrusion events generated by Snort are not sent to FMC and show up in webGUI
CSCvn74112	FTDv does not have configuration on initial bringup with mix of vmxnet3 and ixgbevf interfaces
CSCvn75368	FPR platform IPsec VPN goes down intermittently
CSCvn78593	Control-plane ACL doesn't work correctly on FTD
CSCvn78870	ASA Multicontext traceback and reload due to allocate-interface out of range command
CSCvn82895	Diskmanager may not track all event files
CSCvn87965	While associating FMC with TG account, FMC should not redirect users to TG console
CSCvn95711	Traceback on Thread Name: Unicorn Admin Handler after adding protocol to IKEV2 ipsec-proposal
CSCvn96898	Memory Leak in DMA_Pool in binsize 1024 with SCP download
CSCvn99712	Cisco Firepower Management Center Persistent Cross-Site Scripting Vulnerability
CSCvo02097	Upgrading ASA cluster to 9.10.1.7 cause traceback
CSCvo04444	Ikev2 tunnel creation fails
CSCvo06216	Support more than 255 chars for Split DNS-commit issue in hanover for CSCuz22961
CSCvo09046	Upgrading ASA cluster to 9.10.1.7 cause low memory
CSCvo13497	Unable to remove access-list with 'log default' keyword

Bug ID	Headline
CSCvo19247	Traceback while processing an outbound SSL packet
CSCvo21210	PDTS has incorrect numa node info resulting in incorrect load balancing
CSCvo23222	AnyConnect session rejected due to resource issue in multi context deployments
CSCvo23366	Deploy failed because adaptive profiling config file corrupt
CSCvo27109	Standby may enter reboot loop upon upgrading to 9.6(4)20 from 9.6(4)6
CSCvo29973	ssl rules with cipher suite conditions can cause unneeded tls 1.3 downgrade
CSCvo31353	SSL connections may fail when URL categories are used and certificate common name doesn't match
CSCvo39094	Delay/Longer processing time to insert policy deploy task after selecting the device for deploy
CSCvo40210	Update Talos RSS feed in dashboard widget
CSCvo42174	ASA IPSec VPN EAP Fails to Load Valid Certificate in PKI
CSCvo42884	Cannot make Site-to-site VPN changes on FTD after upgrading to 6.3
CSCvo43693	FTD HA creation fails due to multiple files modules*.tgz and vdb*.tgz being transferred from FMC
CSCvo44064	aggressive downgrade action is taken when url look up is pending due to no sni
CSCvo45209	FTD-CLUSTER:Adding new unit in cluster can cause traffic drop
CSCvo45675	FMC upgrade process should check configuration that would be invalid after upgrade
CSCvo50230	SSL Connections to uncategorized URLs may fail repeatedly
CSCvo55151	crypto ipsec inner-routing-lookup should not be allowed to be configured with VTI present
CSCvo55282	Policy deploy fails when user is able to enter invalid inline port range in AC Rule accidentally
CSCvo56675	ASA or FTD traceback and reload due to failover state change or xlates cleared
CSCvo56895	Some donut charts on the Context Explorer failing to load
CSCvo61091	eStreamer memory and CPU grow when sending NAP policy metadata
CSCvo63168	temp_id leak if Sybase connection fails
CSCvo63232	UIMP not updating users from a realm that resides in a child domain.
CSCvo63240	Smart Tunnel bookmarks don't work after upgrade giving certificate error
CSCvo67454	Invalid port range object causes AC policy deploy to fail

Bug ID	Headline
CSCvo72238	FMC backup fails when FTD cluster is managed in domain and sub-domain AC Policy is assigned to it
CSCvo74743	FMC-HA changes to child domain on primary, not getting to ADI.conf on secondary

Version 6.3.0.2 Resolved Issues

Table 44: Version 6.3.0.2 Resolved Issues

Bug ID	Headline
CSCuz28594	Diskmanager - critical alert on /var/storage due to disk manager not pruning till 99%
CSCvh26064	Unable to use "Change Reconciliation" on 7000/8000 sensors
CSCvi28763	FTD Platform Settings: change default DH-group in SSL custom settings to 2
CSCvi34533	Cannot save modification in Access List if there's no SNMPv3 user defined
CSCvi55841	errors saving blacklist config file are not detected
CSCvk16876	Traffic matches incorrect Access Control Rule
CSCvk31472	Smart License logging is polluting syslog AND causing fast log rotation
CSCvk40964	Deployment of empty interface config to device lead to traffic outage
CSCvm14875	Large number of stale cloudconfig EO causing performance issues
CSCvm24210	One of the two schedule tasks running on same timestamp fails if they both access the same file
CSCvm40545	downgrading FTD twice in a row without updating in between results in wrong lina version
CSCvm58799	During deploy, if multiple Snorts are not responding, recovery takes too long
CSCvm60039	Custom DNS security intelligence feed fail to download intermittently
CSCvm60548	Security Intelligence synchronization tasks fail
CSCvm66743	Domain page takes long time to load on scale setup
CSCvm87892	sftls crash in snort found when traffic is soaked overnight
CSCvn10634	Files are not detected in HTTP flows when there's an Out of Order (ACK before actual data)
CSCvn16102	Diskmanager file capture data not increasing for hours at a time
CSCvn17347	Traceback and reload when displaying CPU profiling results

Bug ID	Headline
CSCvn19074	MSP -Access Control Rule to Block with Reset for CIP Write application is not blocking
CSCvn38010	Let remove_peers.pl scripts bailout when it is run in FTD HA setup
CSCvn38082	FMC should identify and recover from mongo corruption
CSCvn38189	SFDataCorrelator is not restarted after backup scripts died
CSCvn41903	Snort reload fails and causes restart due to dce2-mem-reloader memory adjustments taking too long
CSCvn43798	Deleting a domain fails to delete some objects if a Realm is in that domain
CSCvn46474	FP2120 FTD went unresponsive after power outage
CSCvn47788	UI validation fails on a valid hostname IP for Audit Log Host in Firepower platform setting policy
CSCvn48739	FTD show tech taken from CLISH mode and in troubleshoot may be truncated
CSCvn48790	Slave node kicked out of cluster if SI task running during policy apply
CSCvn49561	update FireAMP curl calls to use CA path
CSCvn53145	Policy deploy throws "Variable set has invalid execulded values"
CSCvn65575	Snort termination can occur when active authentication is enabled and an SSL policy is not enabled
CSCvn67888	Object added using REST API result in policy deploy failure
CSCvn68145	Snort Unexpectedly Exiting when using SSL decryption
CSCvn69019	usernames with single quotes are not written into user_ip_map file
CSCvn72650	FTD Address not mapped traceback on 6.3.0.x release
CSCvn72683	FMC webGUI device management page loading time is too long around 45s with 25s fetching license
CSCvn73244	After upgrading to 6.3, unable to deploy RA VPN policy due to anyconnect-custom-attr
CSCvn76046	Preshared key with " character will not deploy after upgrading to 6.3
CSCvn76783	Monitor rule with enabled logging to syslog server does not report connection events to the server.
CSCvn77285	After upgrading to 6.3, SI Health Alert is no longer accurate
CSCvn93499	Snort/Data Correlator can crash while exiting on Firepower 4100/9300 devices.
CSCvo00887	ssl client hello should not be modified if "Do Not Decrypt" rule will be the only possible verdict

Bug ID	Headline
CSCvo03186	Domain page in Firepower Management Center takes long time to load
CSCvo03808	Deploy from FMC fails due to OOM with no indication of why
CSCvo11077	Memory leak found in IPsec when we establish and terminate a new IKEv1 tunnel.
CSCvo15484	Unable to delete User IOC if user info is inconsistent between mysql & sybase - part fix
CSCvo23150	excessive DB queries for user identities causes slowness in user session processing.
CSCvo27164	SFDataCorrelator logs inappropriate "Resuming storage of old events" messages
CSCvo32329	Deleted realm is causing many user_id's loaded into user_identities cache
CSCvo56616	Deployment times out in some cases resulting in non-terminated AQ

Version 6.3.0.1 Resolved Issues

Bug ID	Headline
CSCuy90400	Enhancement to support extended master secret in SSL
CSCva62256	Appliance status widget taking too long with 500 sensors
CSCvd03903	Firepower is affected by TCP Dump Vulnerability
CSCvd12834	FP Audit Logs do not log passed and failed SSH authentication attempts
CSCve29930	Cannot configure LOM on secondary FMC from HA pair
CSCvf20266	Firepower Management Center System Configuration Email Notification Password Length Too Short
CSCvh13022	SSL decryption is bypassed when client hello payload is < 6 bytes
CSCvi97028	fmc GUI too slow when configuring unreachable syslog server
CSCvi97500	AMP Cloud event on Firepower Management Center are seen with different file types
CSCvj65154	FMC failing to communicate with SSM when proxy password contains @ character
CSCvj74643	Enabling Use CAC authentication and authorization on AD breaks RADIUS when changed.
CSCvj87287	simultaneous flood of REST-API requests to FMC results in inaccessibility
CSCvj97229	'User Name Template' should be required filed for external authentication object for CAC in FMC
CSCvk19946	Sftunnel service broken due to cache archive data flooding

Bug ID	Headline
CSCvk39339	Unable to run the scheduling report generation on Japanese FMC
CSCvk55634	Random policy deployment failure due to stuck notification for policy deployment
CSCvk56988	Cisco ClamAV MEW unpacker Denial of Service Vulnerability
CSCvm46014	Copy config should not fail if standby device is corrupted on FTD HA
CSCvm47713	SSL policy disallows viewing of PDF on *.lightning.force.com when Chrome browser is used
CSCvm59983	The file-size directive returns invalid input error and breaks the captures from clish
CSCvm64230	verify_firmwareRunning() return code not checked
CSCvm76760	FMC - External RADIUS authentication - Text in the "Shell Access Filter" field is not validated
CSCvm80933	ssl policy can match incorrect rule when server uses a cert with wildcard common name
CSCvm87315	FTD registration can fail because of TID in RegistrationTR::addToLamplighter
CSCvm91280	Intrusion Events Report Date, Hour Of Day, Day Of Week comes in UTC and Time comes in local timezone
CSCvm96339	/dev/root partition will fill to 100% due to archive_cache_seed.sensor file
CSCvn03507	"set ip next-hop verify-availability" is applied incorrectly with subsequent deployments
CSCvn05797	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCvn06618	On LINA config rollback the startup-config is being merged with the default running
CSCvn08146	Missing audit detail for changes to x509 certificates and keys
CSCvn14650	Linux Kernel Use-After-Free Race Condition Vulnerability
CSCvn16489	AMP Dynamic Analysis's clouds should be tracked separately for submission rates.
CSCvn19289	Multiple Vulnerabilities in curl
CSCvn20411	Device management page never loads and times out after an error message
CSCvn21899	Firepower: Disable TLS 1.0 permanently for SFTunnel communication
CSCvn23701	Deployment failed with - ftp_telnet.conf(4) => Invalid keyword 'memcap' for 'global' configuration.
CSCvn30118	mysql-server.err file is not fully deleted and keeps consuming Firepower disk space
CSCvn31753	ssl inspection policy may cause SEC_ERROR_REUSED_ISSUER_AND_SERIAL browser error

Bug ID	Headline
CSCvn31793	TLS 1.3 connections reported as 1.2 in FMC connection events
CSCvn36393	exclude tls1.0 and tls1.1 in stunnel config file
CSCvn46121	Security Intelligence IP monitor Events are not sent to syslog if default action logs to syslog
CSCvn53131	snort validation error during policy apply after FMC upgrade
CSCvn53732	Modified SSL connections that are not decrypted should be closed
CSCvo02577	Buffer exhaustion with SSL HW decryption
CSCvo11743	fpreplication snapshot streaming loops when last batch is 100% full.

CHAPTER 9

Known Issues

For your convenience, the release notes list the known issues for major releases. We do not list known issues for maintenance releases or patches.

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

Important Bug lists are auto-generated *once* and are 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.

Version 6.3.0 Known Issues

Table 45: Version 6.3.0 Known Issues

Bug ID	Headline
CSCvk74150	After FDM HA switch the deploy takes longer than 25 minutes on 6.3.0-1376
CSCvm14296	Cisco Firepower Threat Defense Software Multi-Instance Container Escape Vulnerabilities
CSCvm29525	After creating MAX number of LOM users you cannot login remotely using ipmitool
CSCvm32307	Need option to do packet capture on a Port channel Sub-interface
CSCvm37935	Sometimes rule evaluation is aborted on virtual devices due to lower default PPM threshold value
CSCvn07587	Network IPv6 range doesn't deploy correctly to lina
CSCvn12381	4140 Multi-Instance Not Load-Balancing Correctly with 4 Instances
CSCvn19074	MSP -Access Control Rule to Block with Reset for CIP Write application is not blocking

Bug ID	Headline
CSCvn19289	Multiple Vulnerabilities in curl
CSCvn32308	Restoring self backup on secondary requires license re-registrations
CSCvn44222	6.3.0-79: HA upgrade/deployment fails from from missing RAVPN diskfiles on secondary
CSCvn46121	Security Intelligence IP monitor Events are not sent to syslog if default action logs to syslog
CSCvn52181	FMC4500 : Noticed failures related to IPv6 configuration and NTP on console during baseline
CSCvn53145	Policy deploy throws "Variable set has invalid execulded values"
CSCvn67630	Govt UCAPL - Maximum Login Sessions through CLI - test case fails on 6.4.0-1088
CSCvn81898	Device name doesn't exist in a syslog message if syslog alerting for connection events is configured
CSCvo06696	FTD may drop conns through GRE tunnels if firewall receives GRE packet before inner packet
CSCvo15627	Maxfailedlogin for non ucapl user's set to 5 in ucapl mode
CSCvo17612	Return error messages when failing to retrieve objects from database
CSCvo19666	28 Core instance is achieving 20% lower performance than expected
CSCvo31831	Deleting a base policy does not delete the EOs of child policies
CSCvo37273	Adding a validation check in FMC UI to validate the object network configured in static route
CSCvo48771	FMC should check for configuration line length prior to deployment
CSCvo49295	RabbitMQ constantly fails to start with error "case_clause,undefined"
CSCvo49344	RabbitMQ malfunctions and does not recover after SFRemediateD is killed
CSCvo74233	FTD 6.3.0 traceback seen with tftp traffic
CSCvo77796	Slow deployment due to slower IntrusionPolicy step in global snapshot population
CSCvo81219	FP 2100: Reset should be direction aware similar to other platforms
CSCvo87456	Unable to mount SMBv1 share in 6.3.0
CSCvo90413	FTD-REST-API: HTML returned when wrong version passed in URL
CSCvp00236	Upgrading FMC to 6.3.0 fails with error UNABLE TO LOAD stricts.pm and FlyLoader.pm
CSCvp01515	ASA SFR: preprocessors won't be enabled, if enable dependency rules

Bug ID	Headline
CSCvp01542	FMC 6.3 Multitenancy/Domain LDAPS User/Group Download Failure Due to Certificate Location
CSCvp09972	connection event page is not displaying table on UI - max rows user preference is empty
CSCvp11760	Search-Index update fails due to missing Activity Event publish
CSCvp20985	Internet Download Manager detector doesn't match all flows
CSCvp24480	fmc-ha uip snapshot processing stuck in a loop.
CSCvp25581	in FMC-HA user_group_map entries are wiped out in split-brain
CSCvp25782	EventHandler core while pruning metadata cache
CSCvp26548	FDM upgrade fails due to objects validation failure
CSCvp30447	Syslog alerts are not sent to server when Global Rule Thresholding is disabled on Intrusion Policy
CSCvp45786	Not able to upload the STIX or Flat File Manually under Threat Intelligence Director
CSCvp55941	FILE RESUME BLOCK being randomly thrown causing access issues on files from SMB share.
CSCvp95663	InlineResult for IPS event missing metadata "Would have blocked"
CSCvq53902	Cisco Firepower Management Center Multiple Cross-Site Scripting Vulnerabilities
CSCvq65542	Disable asp load-balance per-packet functionality from fp2100 until all bugs fixed
CSCvq89794	FDM - user downloads not working with LDAPS
CSCvq93768	Lodash lodash Object.prototype Denial of Service Vulnerability
CSCvq93769	Bootstrap collapse Plugin Data-Parent Attribute Cross-Site Scripting V
CSCvq93770	Bootstrap tooltip Plugin Data-Container Property Cross-Site Scripting
CSCvq93771	Bootstrap scrollspy Data-Target Property Cross-Site Scripting Vulnerab
CSCvr06515	Access-control-config hit counter not incrementing
CSCvr33428	FMC generates Connection Events from a SYN flood attack
CSCvr52077	Variable set is not validated at deploy if it is not a part of AC rule
CSCvr72665	FMC upgrading to 6.3/6.4 shouldn't remove existing deprecated flexconfig
CSCvs33392	Known Key SSL decryption and connections can fail when servers are using unsupported TLS options
CSCvs55937	Deployment fails for FDM due to neo4j error

Bug ID	Headline
CSCvt00140	Series 3 sensors fail system restore to 6.3 and 6.4
CSCvt49334	On the 4120 sensor, the task delete is not removing the "task_xx" files from the cron.d directory
CSCvt55927	Unable to break HA in 6.4.0.9-34 FDM
CSCvt86650	Terracotta Quartz Scheduler initDocumentParser XML External Entity Vul
CSCvt86666	Apache Commons Compress ZipArchiveInputStream Denial of Service Vulner
CSCvt87127	Memcached lru Commands NULL Pointer Dereference Vulnerablity
CSCvt87141	GNU Wget set_file_metadata Information Disclosure Vulnerability
CSCvu69541	Query FMC using Ext. DB & unable to extract the 'url_category' from connection_log table as expected
CSCvu86734	FTD Backup and Restore does not restore the hostname of the device locally
CSCvu91792	SNMP IfDiscards OIDs for Internal-Data 0/0 and 0/1 wrong Values
CSCvv03258	FTD/LINA traceback and reload on process name lina
CSCvv54860	backup file can be extremely large when rabbitmq queue backed up

CHAPTER 10

For Assistance

Online Resources

Cisco provides the following online resources to download documentation, software, and tools; to query bugs; and to open service requests. Use these resources to install and configure Cisco 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