Cisco Firepower Release Notes, Version 6.7.x Patches

First Published: 2021-03-24

Last Modified: 2022-02-17

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

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 1

Welcome

This document contains critical and release-specific information.

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

Release Dates

Table 1: Version 6.7.0 Dates

Version	Build	Date	Platforms
6.7.0	65	2020-11-02	All

Table 2: Version 6.7.0 Patch Dates

Version	Build	Date	Platforms
6.7.0.3	105	2022-02-17	All
6.7.0.2	24	2021-05-11	All
6.7.0.1	13	2021-03-24	All

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

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)

- Firepower Management Center Virtual for Microsoft Azure
- Firepower Management Center Virtual for Google Cloud Platform (GCP)
- Firepower Management Center Virtual for Oracle Cloud Infrastructure (OCI)

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, 6.5, or 6.7

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 5.

Table 3: Firepower Threat Defense in Version 6.7.0/6.7.x

FTD Platform	OS/Hypervisor	Additional Details
Firepower 1010, 1120, 1140, 1150 Firepower 2110, 2120, 2130, 2140	—	—
Firepower 4110, 4120, 4140, 4150 Firepower 4112, 4115, 4125, 4145 Firepower 9300: SM-24, SM-36, SM-44 modules Firepower 9300: SM-40, SM-48, SM-56 modules	FXOS 2.9.1.131 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 FXOS Release Notes, 2.9(1).
ASA 5508-X, 5516-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. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.

FTD Platform	OS/Hypervisor	Additional Details
Firepower Threat Defense Virtual (FTDv)	Any of: • AWS: Amazon Web Services • Azure: Microsoft Azure • GCP: Google Cloud Platform • OCI: Oracle Cloud Infrastructure • KVM: Kernel-based Virtual Machine • VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7	For supported instances, see the appropriate FTDv Getting Started guide.

Table 4: NGIPS/ASA FirePOWER in Version 6.7.0/6.7.x

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. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.
NGIPSv	VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7	For supported instances, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.

Manager-Device Compatibility

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
6.7.0/6.7.x	6.3.0
6.6.0/6.6.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 and Cisco Defense Orchestrator

As an alternative to the FMC, many FTD devices support Firepower Device Manager and Cisco Defense Orchestrator management:

- Firepower Device Manager is built into FTD and can manage a single device.

  This lets you configure the basic features of the software that are most commonly used for small or mid-size networks.

- Cisco Defense Orchestrator (CDO) is cloud-based and can manage multiple FTD devices.

  This allows you to establish and maintain consistent security policies across your deployment without using the FMC. Although some configurations still require FDM, CDO allows you to establish and maintain consistent security policies across multiple FTD devices.

All FTD devices that support local management with the FDM also support CDO concurrently.

Table 6: FDM/CDO Compatibility with FTD

FTD Platform	FDM Compatibility	CDO Compatibility
Firepower 1000 series	6.4.0+	6.4.0+
Firepower 2100 series	6.2.1+	6.4.0+
Firepower 4100/9300	6.5.0+	6.5.0+
ASA 5500-X series	6.1.0+	6.4.0+
ISA 3000	6.2.3+	6.4.0+
FTDv for AWS	6.6.0+	6.6.0+
FTDv for Azure	6.5.0+	6.5.0+

FTD Platform	FDM Compatibility	CDO Compatibility
FTDv for GCP	—	—
FTDv for KVM	6.2.3+	6.4.0+
FTDv for OCI	—	—
FTDv for VMware	6.2.2+	6.4.0+

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
6.7.0/6.7.x	7.15.1
6.6.0/6.6.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 Edge (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, nor do we extensively test Microsoft Edge 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 Edge, do not enable IE mode.

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: 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
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

There are no new or deprecated features for Firepower Management Center deployments in Version 6.7.x patches.

Features for Firepower Device Manager Deployments

There are no new or deprecated features for Firepower Device Manager deployments in Version 6.7.x patches.

Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

Intrusion rule updates (SRUs/LSPs) 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/LSP.

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 9: Troubleshooting Walkthroughs

Problem	Solution
Cannot find the How To link to start walkthroughs.	Make sure walkthroughs are enabled. From the drop-down list under your username, select User Preferences then click How-To Settings. Version 6.7.0 discontinues walkthroughs for the Classic theme. You can switch themes in your user preferences.
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.

Problem	Solution
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.

Upgrade Checklist

This pre-upgrade checklist highlights actions that can prevent common issues. However, we still recommend you refer to the appropriate upgrade or configuration guide for full instructions: Upgrade Instructions, on page 32.

Important At all times during the process, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported. Do not deploy changes to or from, manually reboot, or shut down an upgrading appliance. In most cases, do not restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, there may be something you can do — see the Note on Unresponsive Upgrades.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 10:

✓	Action/Check
	Assess your deployment. Determine the current state of your deployment. Understanding where you are determines how you get to where you want to go. In addition to current version and model information, determine if your devices are configured for high availability/scalability, and if they are deployed passively, as an IPS, as a firewall, and so on.
	Plan your upgrade path. This is especially important for multi-appliance deployments, multi-hop upgrades, or situations where you need to upgrade operating systems or hosting environments, all while maintaining deployment compatibility. Always know which upgrade you just performed and which you are performing next. **Note** In FMC deployments, you usually upgrade the FMC, then its managed devices. However, in some cases you may need to upgrade devices first.
	Read ***all*** upgrade guidelines and plan configuration changes. Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. Upgrade guidelines can appear in multiple places. Make sure you read them all. They include: • Upgrade Guidelines for Version 6.7.x.x Patches, on page 20: Important upgrade guidelines that are new or specific to this release. • Known Issues, on page 67: Be prepared to work around any bugs that affect upgrade. • Features and Functionality, on page 11: New and deprecated features can require pre- or post-upgrade configuration changes, or even prevent upgrade.
	Check appliance access. Devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade, 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.
	Check bandwidth. Make sure your management network has the bandwidth to perform large data transfers. In FMC deployments, if you transfer an upgrade package to a managed device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. Whenever possible, copy upgrade packages to managed devices before you initiate the device upgrade. See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).
	Schedule maintenance windows. Schedule maintenance windows when they will have the least impact, considering any effect on traffic flow and inspection and the time the upgrade is likely to take. Also consider the tasks you must perform in the window, and those you can perform ahead of time. For example, do not wait until the maintenance window to copy upgrade packages to appliances, run readiness checks, perform backups, and so on.

Upgrade Packages

Upgrade packages are available on the Cisco Support & Download site.

Table 11:

✓	Action/Check
	Upload upgrade packages. In FMC deployments, upload FMC and all Classic device (ASA FirePOWER, NGIPSv) upgrade packages to the FMC. For FTD, you can either upload upgrade packages to the FMC, or configure your own internal web server as the source for upgrade packages. In FMC high availability deployments, you must upload the FMC upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to HA synchronization, you can transfer the package to the active peer during the preparation stage of the upgrade, and to the standby peer as part of the actual upgrade process, after you pause synchronization.
	Copy upgrade packages to managed devices. In FMC deployments, we recommend you copy (push) upgrade packages to managed devices before you initiate the device upgrade. **Note** For the Firepower 4100/9300, we recommend (and sometimes require) you copy the upgrade package before you begin the required companion FXOS upgrade.

Backups

The ability to recover from a disaster is an essential part of any system maintenance plan.

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.

Caution We strongly recommend you back up to a secure remote location and verify transfer success, both before and after upgrade.

Table 12:

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

✓	Action/Check
	Back up FXOS on the Firepower 4100/9300. Use the Firepower Chassis Manager or the FXOS CLI to export chassis configurations before and after upgrade, including logical device and platform configuration settings.
	Back up ASA for ASA with FirePOWER Services. Use ASDM or the ASA CLI to back up configurations and other critical files before and after upgrade, especially if there is an ASA configuration migration.

Associated Upgrades

Because operating system and hosting environment upgrades can affect traffic flow and inspection, perform them in a maintenance window.

Table 13:

✓	Action/Check
	Upgrade virtual hosting. If needed, upgrade the hosting environment for any virtual appliances. If this is required, it is usually because you are running an older version of VMware and are performing a major device upgrade.
	Upgrade FXOS on the Firepower 4100/9300. If needed, upgrade FXOS before you upgrade FTD. This is usually a requirement for major upgrades, but very rarely for maintenance releases and patches. To avoid interruptions in traffic flow and inspection, upgrade FXOS in FTD high availability pairs and inter-chassis clusters one chassis at a time. **Note** Before you upgrade FXOS, make sure you read all upgrade guidelines and plan configuration changes. Start with the FXOS release notes: Cisco Firepower 4100/9300 FXOS Release Notes.
	Upgrade ASA on ASA with FirePOWER Services. If desired, upgrade ASA. There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues. For standalone ASA devices, upgrade the ASA FirePOWER module just after you upgrade ASA and reload. For ASA clusters and failover pairs, to avoid interruptions in traffic flow and inspection, fully upgrade these devices one at a time. Upgrade the ASA FirePOWER module just before you reload each unit to upgrade ASA. **Note** Before you upgrade ASA, make sure you read all upgrade guidelines and plan configuration changes. Start with the ASA release notes: Cisco ASA Release Notes.

Final Checks

A set of final checks ensures you are ready to upgrade.

Table 14:

✓	Action/Check
	Check configurations. Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes.
	Check NTP synchronization. Make sure all appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In FMC deployments, the health monitor does alert if clocks are out of sync by more than 10 seconds, but you should still check manually. To check time: • FMC: Choose System > Configuration > Time. • Devices: Use the show time CLI command.
	Check disk space. Run a disk space check for the software upgrade. Without enough free disk space, the upgrade fails. See the Upgrade the Software chapter in the Cisco Firepower Release Notes for your target version.
	Deploy configurations. Deploying configurations before you upgrade reduces the chance of failure. In some deployments, you may be blocked from upgrade if you have out-of-date configurations. In FMC high availability deployments, you only need to deploy from the active peer. When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device handles traffic, may interrupt traffic until the restart completes. See the Upgrade the Software chapter in the Cisco Firepower Release Notes for your target version.
	Check running tasks. Make sure essential tasks are complete before you upgrade, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. We also recommend you check for tasks that are scheduled to run during the upgrade, and cancel or postpone them. **Note** In some deployments, upgrades automatically postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. This feature is currently supported for FMCs running Version 6.4.0.10 and later patches, Version 6.6.3 and later maintenance releases, and Version 6.7.0+. Note that this feature is supported for all upgrades from a supported version. This feature is not supported for upgrades to a supported version from an unsupported version.
	Run readiness checks. We recommend compatibility and readiness checks. These checks assess your preparedness for a software upgrade.

Note on Unresponsive Upgrades

Starting with major and maintenance FTD upgrades from Version 6.7.0, you can manually cancel failed or in-progress upgrades, and retry failed upgrades:

- FMC deployments: Use the Upgrade Status pop-up, accessible from the Device Management page and the Message Center.
- FDM deployments: Use the System Upgrade panel.

You can also use the FTD CLI.

Note By default, FTD automatically reverts to its pre-upgrade state upon upgrade failure ("auto-cancel"). To be able to manually cancel or retry a failed upgrade, disable the auto-cancel option when you initiate the upgrade. Note that auto-cancel is not supported for patches. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

If you have exhausted all options, or if your deployment does not support cancel/retry, contact Cisco TAC.

Upgrade Guidelines for Version 6.7.x.x Patches

This checklist contains upgrade guidelines for Version 6.7.x patches.

Table 15: Version 6.7.x.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: FMC with Email Alerting for Intrusion Events, on page 20	FMC	6.2.3 through 6.7.0.x	6.7.0 6.6.0, 6.6.1, or 6.6.3 All patches to these releases

Upgrade Failure: FMC with Email Alerting for Intrusion Events

Deployments: Firepower Management Center

Upgrading from: Version 6.2.3 through 6.7.0.x

Directly to: Version 6.6.0, 6.6.1, 6.6.3, or 6.7.0, as well as any patches to these releases

Related bugs: CSCvw38870, CSCvx86231

If you configured email alerting for individual intrusion events, fully disable it before you upgrade a Firepower Management Center to any of the versions listed above. Otherwise, the upgrade will fail.

You can reenable this feature after the upgrade. If you already experienced an upgrade failure due to this issue, contact Cisco TAC.

To fully disable intrusion email alerting:

1. On the Firepower Management Center, choose Policies > Actions > Alerts, then click Intrusion Email.
2. Set the State to off.
3. Next to Rules, click Email Alerting per Rule Configuration and deselect any rules.

   Note which rules you deselected so you can reselect them after the upgrade.

   Tip If reselecting rules would be too time consuming, contact Cisco TAC before you upgrade. They can guide you through saving your selections, so you can quickly reimplement them post-upgrade.

4. Save your configurations.

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.

Time and Disk Space Tests

You must have enough free disk space or the upgrade fails. You must also have enough time to perform the upgrade. We provide reports of in-house time and disk space tests for reference purposes.

About Time Tests

Time values are based on in-house tests.

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

Table 16: Time Test Conditions

Condition	Details
Deployment	Values are from tests in a Firepower Management Center deployment. 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.
Models	In most cases, we test on the lowest-end models in each series, and sometimes on multiple models in a series.
Virtual settings	We test with the default settings for memory and resources.

Condition	Details
High availability and 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	Values represent only the time it takes for the software upgrade script to run. This does not include: • Operating system upgrades. • Transferring upgrade packages. • Readiness checks. • VDB and intrusion rule (SRU/LSP) updates. • Deploying configurations. • Reboots, although reboot time may be provided separately.

About Disk Space Requirements

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

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

Values represent only the space needed to upload and run the software upgrade script. They do not include values for operating system upgrades, VDB or intrusion rule (SRU/LSP) updates, and so on.

Note When you use the Firepower Management Center to upgrade a managed device, the Firepower Management Center requires additional disk space in /Volume for the device upgrade package (unless you configure an internal web server where your devices can get the package; requires Firepower Threat Defense Version 6.6.0+) .

Checking Disk Space

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.

To check disk space:

- Firepower Management Center and its managed devices: Use the System > Monitoring > Statistics page on the FMC. After you select the appliance you want to check, under Disk Usage, expand the By Partition details.
- Firepower Threat Defense with Firepower Device Manager: Use the show disk CLI command.
- ASA FirePOWER with ASDM: Use the Monitoring > ASA FirePOWER Monitoring > Statistics page. Under Disk Usage, expand the By Partition details.

Version 6.7.0.3 Time and Disk Space

Table 17: Version 6.7.0.3 Time and Disk Space

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time from 6.7.0	Reboot Time
FMC	2.9 GB in /var	34 MB in /	—	38 min	7 min
FMCv: VMware	2.6 GB in /var	39 MB in /	—	30 min	5 min
Firepower 1000 series	—	3.3 GB in /ngfw	650 MB	9 min	13 min
Firepower 2100 series	—	3.2 GB in /ngfw	700 MB	7 min	14 min
Firepower 4100 series	—	2.5 GBin /ngfw	450 MB	5 min	7 min
Firepower 4100 series container instance	—	2.4 GB in /ngfw	450 MB	6 min	4 min
Firepower 9300	—	3.1 GB in /ngfw	450 MB	4 min	8 min
ASA 5500-X series with FTD	2.3 GB in /ngfw/Volume	110 MB in /ngfw	380 MB	13 min	9 min
ISA 3000 with FTD	2.2 GB in /ngfw/Volume	110 MB in /ngfw	380 MB	19 min	8 min
FTDv: VMware	2.3 GB in /ngfw/Volume	110 MBin /ngfw	380 MB	6 min	5 min
FTDv: KVM	2.3 GB in /ngfw/Volume	110 MB in /ngfw	380 MB	8 min	5 min
ASA FirePOWER	3.1 GB in /var	36 MB in /	450 MB	64 min	6 min
NGIPSv	970 MB in /var	34 MB in /	300 MB	5 min	4 min

Version 6.7.0.2 Time and Disk Space

Table 18: Version 6.7.0.2 Time and Disk Space

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time from 6.7.0	Reboot Time
FMC	2.3 GB in /var	20 MB in /	—	35 min	7 min
FMCv: VMware	2.4 GB in /var	23 MB in /	—	28 min	2 min
Firepower 1000 series	—	3.0 GB in /ngfw	610 MB	8 min	13 min
Firepower 2100 series	—	3.0 GB in /ngfw	660 MB	6 min	14 min
Firepower 9300	—	2.6 GB in /ngfw	410 MB	5 min	7 min
Firepower 4100 series	—	2.4 GB in /ngfw	410 MB	4 min	7 min
Firepower 4100 series container instance	—	2.3 GB in /ngfw	410 MB	5 min	4 min
ASA 5500-X series with FTD	2.2 GB in /ngfw/Volume	110 MB in /ngfw	370 MB	10 min	7 min
ISA 3000 with FTD	2.3 GB in /ngfw/Volume	110 MB in /ngfw	370 MB	17 min	9 min
FTDv: VMware	2.2 GB in /ngfw/Volume	110 MB in /ngfw	370 MB	6 min	4 min
FTDv: KVM	2.2 GB in /ngfw/Volume	110 MB in /ngfw	370 MB	6 min	8 min
ASA FirePOWER	3.0 GB in /var	21 MB in /	430 MB	73 min	4 min
NGIPSv	930 MB in /var	19 MB in /	290 MB	5 min	3 min

Version 6.7.0.1 Time and Disk Space

Table 19: Version 6.7.0.1 Time and Disk Space

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time from 6.7.0	Reboot Time
FMC	1.8 GB in /var	20 MB in /	—	32 min	7 min
FMCv: VMware	1.4 GB in /var	23 MB in /	—	28 min	5 min
Firepower 1000 series	—	1.4 GB in /ngfw	340 MB	7 min	12 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time from 6.7.0	Reboot Time
Firepower 2100 series	—	1.4 GB in /ngfw	400 MB	7 min	12 min
Firepower 9300	—	710 MB in /ngfw	130 MB	5 min	7 min
Firepower 4100 series	—	700 MB in /ngfw	130 MB	4 min	5 min
Firepower 4100 series container instance	—	480 MB in /ngfw	130 MB	5 min	2 min
ASA 5500-X series with FTD	540 MB in /ngfw/Volume	110 MB in /ngfw	88 MB	10 min	12 min
ISA 3000 with FTD	540 MB in /ngfw/Volume	110 MB in /ngfw	88 MB	13 min	7 min
FTDv: VMware	530 MB in /ngfw/Volume	110 MB in /ngfw	88 MB	6 min	4 min
FTDv: KVM	550 MB in /ngfw/Volume	110 MB in /ngfw	88 MB	7 min	3 min
ASA FirePOWER	1.2 GB in /var	21 MB in /	41 MB	66 min	2 min
NGIPSv	82 MB in /var	18 MB in /	9 MB	6 min	3 min

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 or revert 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 20: 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.
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 21: 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 (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.

- Firepower Threat Defense 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.

- 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.

- Firepower Threat Defense 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.

- Firepower Threat Defense with FDM: Not supported.

Software Revert (Major/Maintenance Releases)

Reverting returns FTD to its state just before the last major or maintenance upgrade. Regardless of deployment — even for high availability/scalability — you should expect interruptions to traffic flow and inspection. This is because revert is more successful when all units are reverted simultaneously. Simultaneous revert means that interruptions to traffic flow and inspection depend on interface configurations only, as if every device were standalone.

Support for revert begins in Version 6.7.0 for Firepower Device Manager deployments, and in Version 7.1.0 for Firepower Management Center deployments.

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 22: 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 23: 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 (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.

- Firepower Threat Defense 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.
- Firepower Threat Defense with FDM: Not supported.

Software Revert (Major/Maintenance Releases)

Reverting returns FTD to its state just before the last major or maintenance upgrade. Regardless of deployment — even for high availability/scalability — you should expect interruptions to traffic flow and inspection. This is because revert is more successful when all units are reverted simultaneously. Simultaneous revert means that interruptions to traffic flow and inspection depend on interface configurations only, as if every device were standalone.

Support for revert begins in Version 6.7.0 for Firepower Device Manager deployments, and in Version 7.1.0 for Firepower Management Center deployments.

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 24: 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.

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 25: 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 26: Traffic Behavior During NGIPSv Upgrade

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

Traffic Behavior During Deployment

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

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

Table 27: Traffic Behavior During NGIPSv Deployment

Interface Configuration	Traffic Behavior
Inline, Failsafe enabled or disabled	Passed without inspection A few packets might drop if Failsafe is disabled and Snort is busy but not down.
Inline, tap mode	Egress packet immediately, copy bypasses Snort
Passive	Uninterrupted, not inspected

Upgrade Instructions

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

Table 28: Firepower Upgrade Instructions

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

Upgrade Packages

Upgrade packages are available on the Cisco Support & Download site.

- Firepower Management Center, including Firepower Management Center Virtual: https://www.cisco.com/go/firepower-software

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

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

Tip A Firepower Management Center with internet access can download select releases directly from Cisco, some time after the release is available for manual download. The length of the delay depends on release type, release adoption, and other factors.

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

For example:

- Package: `Cisco_Firepower_Mgmt_Center_Patch-6.7.0.1-999.sh.REL.tar`
- Platform: Firepower Management Center
- Package type: Patch
- Version and build: 6.7.0.1-999
- File extension: sh.REL.tar

So that the system can verify that you are using the correct files, upgrade packages from Version 6.2.1+ are signed tar archives (.tar). Do not untar signed (.tar) packages. And, do not transfer upgrade packages by email.

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

Software Upgrade Packages

Table 29:

Platform	Package
FMC/FMCv	Cisco_Firepower_Mgmt_Center
Firepower 1000 series	Cisco_FTD_SSP-FP1K

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

ASA and FXOS Upgrade Packages

For information on operating system upgrade packages, see the planning topics in the following guides:

- Cisco ASA Upgrade Guide, for ASA OS
- 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, for FXOS

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 6.7.0/6.7.x Patches That Support Uninstall

Uninstall is currently supported for all 6.7.0/6.7.x patches.

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.
- 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 30: 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 31: 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 32: Uninstall Order for ASA with FirePOWER Services Devices in ASA Failover Pairs/Clusters

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

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

Uninstall Instructions

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 38, 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.

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 or HA pairs. In an HA/scalability deployment, deploy before you uninstall from the first device, but then not again until you have uninstalled the patch from all members.

Step 2 Perform prechecks.

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

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

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

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

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

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

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

```
sudo install_update.pl --detach /var/sf/updates/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 43.

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 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.

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 40.

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.

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. Note that 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.

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 (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 47.

Table 33:

✓	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 1000/2100 Series Devices to Earlier Major Versions

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

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

Unregistering Smart Licenses

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

Manually unregister from CSSM before you:

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

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

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

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

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

Installation Instructions

Table 34: Firepower Management Center Installation Instructions

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

FMC	Guide
FMC 1000, 2500, 4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
FMCv	Cisco Firepower Management Center Virtual Getting Started Guide

Table 35: Firepower Threat Defense Installation Instructions

FTD Platform	Guide
Firepower 1000/2100 series	Cisco ASA and Firepower Threat Defense Reimage Guide Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 Series Running Firepower Threat Defense
Firepower 4100/9300	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: GCP	Cisco Firepower Threat Defense Virtual for the Google Cloud Platform Getting Started Guide
FTDv: KVM	Cisco Firepower Threat Defense Virtual for KVM Getting Started Guide
FTDv: OCI	Cisco Firepower Threat Defense Virtual for the Oracle Cloud Infrastructure Getting Started Guide
FTDv: VMware	Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide

Table 36: NGIPSv and ASA FirePOWER Installation Instructions

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

CHAPTER 7

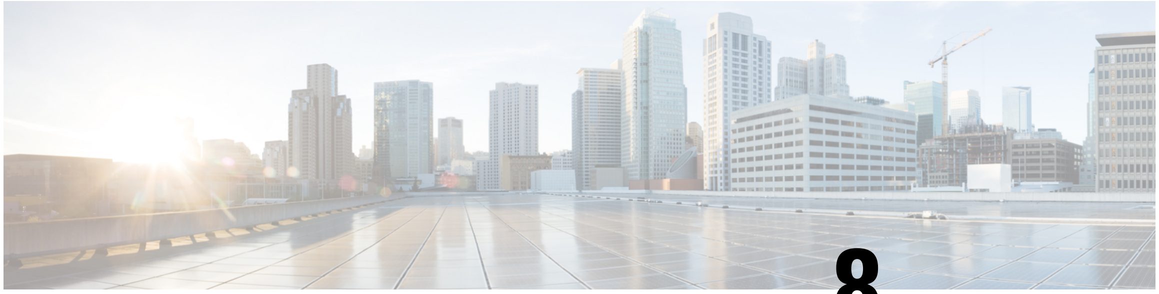
Documentation

We update Firepower documentation if a patch requires it.

Documentation Roadmaps

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 6.7.0.3 Resolved Issues

Table 37: Version 6.7.0.3 Resolved Issues

Bug ID	Headline
CSCvr11958	AWS FTD: Deployment failure with ERROR: failed to set interface to promiscuous mode
CSCvr94911	FXOS: some interface transition logs have no reason
CSCvt62869	SPLIT-BRAIN: Pre allocation of blocks for failover control messages
CSCvt68055	snmpd is respawning frequently on fxos for FP21xx device
CSCvu44472	FMC System processes are starting
CSCvu53810	TD2 does not load balance MPLS across backplane interfaces and sends it all to first interface
CSCvu84127	Firepower may reboot for no apparent reason

Bug ID	Headline
CSCvv21602	cfprApSmMonitorTable is missing in the FP2K MIB
CSCvv24647	FTD 2100 - SNMP: incorrect values returned for Ethernet statistics polling
CSCvv36788	MsgLayer[PID]: Error : Msglyr::ZMQWrapper::registerSender() : Failed to bind ZeroMQ Socket
CSCvv41811	CIAM: net-snmp 5.1 CVE-2019-20892
CSCvv43771	Unable to select multiple devices for scheduled backups
CSCvv46490	Policy Deployment Failure on FMC due to ERROR in SnortAttribConfig
CSCvv59036	Static routes deleted from the FMC without user deleting it.
CSCvv67196	FTD does not try all the crl urls for getting crl file
CSCvv89715	Fastpath rules for Firepower 8000 series stack disappear randomly from the FMC
CSCvv90079	No router BGP pushed after making chnages on 9300 intra chassis cluster
CSCvv90753	Syncd process hangs due to SLA
CSCvv92897	System might hit previously missing memcap limits on upgrade to version 6.6.0
CSCvw05392	Message appearing constantly on diagnostic-cli
CSCvw15359	KP fxos snmp has uninit strings for entPhysicalSerialNum,entPhysicalAssetID on EPM index
CSCvw33536	4100/9300: Cannot associate port channel / interface to App
CSCvw38870	FMC upgrade failure to 6.6.0, 6.6.1, 6.6.3, or 6.7.0 at 800_post/1027_ldap_external_auth_fix.pl
CSCvw51436	Cisco ASA Software and FTD Software SNMP Access Vulnerability
CSCvw55788	Traffic from VTI interface hitting wrong rule
CSCvw62255	"Link not connected" error when using WSP-Q40GLR4L transceiver and Arista switch with Firepower 4100
CSCvw67974	SSH access with public key authentication fails after FXOS upgrade
CSCvw72260	ASA upgrade failed with: "CSP directory does not exist - STOP_FAILED Application_Not_Found"
CSCvw72608	Failed event for standby received on Active causes future deployments to be skipped on standby
CSCvw74231	CIAM: linux-kernel 3.14.39 CVE-2020-14305 and others
CSCvw74660	Syslog-ng not starting up while CC mode due to possble bad syslog-ng patch

Bug ID	Headline
CSCvw77924	Radius Key with the ASCII character " configured on FXOS does not work after chassis reload.
CSCvw79465	FXOS upgrade does not do proper compatibility check for FTD image
CSCvw81322	FTD running multi-instance mode gets snort GID 3 rules disabled after SRU install and deploy
CSCvw81976	ENH: Rename status BYPASS-FAIL for fail-to-wire inline pairs
CSCvw83498	FTD-API: LDAP Attribute map not handling ldapValue including a space
CSCvw83810	CIAM: curl 7.66.0 CVE-2020-8286 and others
CSCvw85377	URL is not updated in the access policy URL filtering rule
CSCvw90634	FP2100 ASA - 1 Gbps SFP in network module down/down after upgrade to 9.15.1.1
CSCvw90923	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 101, seq 4)
CSCvw93159	Firepower 2100: ASA/FTD generates message "Local disk 2 missing on server 1/1"
CSCvw95181	FXOS upgrade fails with error "does not support application instances of deployment type container"
CSCvw97201	SFDataCorrelator exits after FTD upgrade to 6.7 caused by ClamAV
CSCvw97256	Need handling of rmu read failure to ignore link state update when link state API read fails
CSCvw98315	FXOS reporting old FTD version after FTD upgrade to 6.7.0
CSCvx05956	High snort cpu usage while copying navl attribute
CSCvx06920	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 103, seq 5)
CSCvx14602	Firepower memory leak in svc_sam_dcosAG
CSCvx16700	FXOS clock sync issue during blade boot up due to "MIO DID NOT RESPOND TO FORCED TIME SYNC"
CSCvx19563	FDM: Need to update various items to use STO Certificate Trust Bundle (QuoVadis Root CA Issue)
CSCvx19934	Deployment gets failed for snmp settings while deleting snmpv1 and adding snmpv3 at a time in 6.6.3
CSCvx23907	Evaluate the impact of NGFW for CVE-2021-1405
CSCvx25336	ENH: add a way to disable the FQDN check
CSCvx27992	CIAM: open-ldap 2.4.48 CVE-2020-36230 and others
CSCvx28070	Update QuoVadis root CA for Smart license as it is getting decommissioned

Bug ID	Headline
CSCvx29429	ma_ctx*.log consuming high diskspace on FPR4100/FPR9300 despite the fix for CSCvx07389
CSCvx29448	FTD: SNMP host configured with diagnostic int able to poll management int
CSCvx32283	Cisco Firepower Management Center Open Redirect Vulnerability
CSCvx33904	Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privilege escalation
CSCvx38047	FXOS show fault warning code F4526902
CSCvx45976	ASA/FTD Watchdog forced traceback and reload in Threadname: vnet-proxy (rip: socks_proxy_datarelay)
CSCvx47550	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 105, seq 6)
CSCvx47634	The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and
CSCvx47895	Cisco ASA Software and FTD Software Identity-Based Rule Bypass Vulnerability
CSCvx49005	CIAM: openssl 1.1.1g
CSCvx50636	Snort process may traceback and restart due TLS1.3 flow
CSCvx50980	ASA CP CPU wrong calculation leads to high percentage (100% CP CPU)
CSCvx52541	Update SSEConnector config to use the CA bundle /etc/ssl/certs.pem
CSCvx55664	Cisco Firepower Management Center Cross-site Scripting Vulnerability
CSCvx66329	FTD Hotfix Cisco_FTD_SSP_FP2K_Hotfix_O installation fails on script 000_start/125_verify_bundle.sh
CSCvx66494	Handle CIMC Watchdog reset in MIO
CSCvx67468	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 107, seq 7)
CSCvx67996	FMC RAVPN: Deployment is failing when IPv6 DNS is configured under Group Policy
CSCvx71156	access list is not working on 6.7
CSCvx79526	Cisco ASA and FTD Software Resource Exhaustion Denial of Service Vulnerability
CSCvx79793	Slow file transfer or file upload with SSL policy is applied with Decrypt resign action
CSCvx82705	Evaluation of ssp for OpenSSL March 2021 vulnerabilities
CSCvx86231	FMC upgrade failure to 6.6.3 on 999_finish/935_change_reconciliation_baseline.pl
CSCvx86283	Cisco Firepower Threat Defense Software Command Injection Vulnerabilities
CSCvx89827	Not able to set Bangkok time zone in FPR 2110

Bug ID	Headline
CSCvx95255	Supportive change in ASA to differentiate, new ASDM connections from existing ASDM context switch
CSCvx95652	ASAv Azure: Some or all interfaces might stop passing traffic after a certain period of run time
CSCvx98041	FTD-API: ruleId duplicate sequence number causes invalid snort ngfw.rules to be deployed
CSCvx98807	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 109, seq 9)
CSCvy02240	Cisco Firepower Threat Defense Ethernet Industrial Protocol Policy Bypass Vulnerabilities
CSCvy02247	Cisco Firepower System Software Rule Editor Non-impactful Buffer Overflow Vulnerability
CSCvy03045	Failure accessing FXOS with connect fxos admin from Multi-Context ASA if admin context is changed
CSCvy04959	FXOS : 'Memory leak' may casue appAG process traceback and reload
CSCvy04965	WM Standby fails to re-join HA with msg "CD App Sync error is Failed to apply SSP config on standby"
CSCvy05966	Snort 2.9.16.3-3033 traceback (FTD 6.6.3)
CSCvy08798	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 110, seq 10)
CSCvy09217	HA goes to active-active state due to cipher mismatch
CSCvy09252	Syncd exits repeatedly on secondary FMC part of FMC HA
CSCvy10789	FTD 2110 ascii characters are disallowed in LDAP password
CSCvy13229	FDM - GUI Inaccessible - tomcat is opening too many file descriptors
CSCvy13543	Cisco Firepower Threat Defense Software SSH Connections Denial of Service Vulnerability
CSCvy16559	Cisco Firepower Threat Defense Software Command Injection Vulnerabilities
CSCvy16573	Cisco Firepower Threat Defense Command Injection Vulnerability
CSCvy19136	Web portal persistent redirects when certificate authentication is used.
CSCvy19225	Cisco Firepower Threat Defense Command Injection Vulnerability
CSCvy20504	Cisco ASA and FTD Software Web Services Interface Cross-Site Scripting Vulnerability
CSCvy23349	FTD unnecessarily ACKing TCP flows on inline-pair deployment
CSCvy31400	FPR1K: Fiber SFP Interfaces down due to speed autonegotiation disabled

Bug ID	Headline
CSCvy31424	QP FTD application fails to start due to outdated affinity.conf following FXOS/FTD upgrade
CSCvy34333	When ASA upgrade fails, version status is desynched between platform and application
CSCvy35948	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 111, seq 11)
CSCvy36910	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS
CSCvy39791	Lina traceback and core file size is beyond 40G and compression fails.
CSCvy40482	9.14MR3: snmpwalk got failed with [Errno 146] Connection refused error.
CSCvy41757	Cisco Firepower Threat Defense Software CLI Arbitrary File Write Vulnerability
CSCvy41771	Cisco Firepower Management Center Software Authenticated Directory Traversal Vulnerability
CSCvy43187	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS
CSCvy51814	Firepower flow-offload stops offloading all existing and new flows
CSCvy55054	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS
CSCvy58278	Denial of Service vulnerability handling the config-request request
CSCvy61008	Time out of sync between Lina and FXOS
CSCvy64145	WR6 and WR8 commit id update in CCM layer(sprint 113, seq 12)
CSCvy65802	AppAgent Heartbeat enhancement
CSCvy66942	FPR4100/9300 IPv6 config cannot be applied using Rest API LTP on 9300/4100 Supervisor
CSCvy69730	Cisco FMC Software Configuration Information Disclosure Vulnerability
CSCvy72118	High snort cpu usage while copying navl attribute - (Fragmented metadata)
CSCvy72194	Cisco FMC Software Configuration Information Disclosure Vulnerability
CSCvy73585	FMC should not allow to configure port-channel ID higher than 8 on FPR1010
CSCvy80325	Include the ios pem files into the patch upgrade package for vFTD
CSCvy83116	FTD 1000 standby fails to re-join HA with msg "CD App Sync error is SSP Config Generation Failure"
CSCvy83657	FXOS process core pruned/deleted from system files (no validation)
CSCvy89144	Cisco ASA and FTD Web Services Denial of Service Vulnerability

Bug ID	Headline
CSCvy89440	s2sCryptoMap Configuration Loss
CSCvy93480	Cisco ASA and FTD Software IKEv2 Site-to-Site VPN Denial of Service Vulnerability
CSCvy95329	Incorrect Access rule matching because of ac rule entry missing
CSCvy96625	Roll back changes introduced by CSCvr33428 and CSCvy39659
CSCvy96698	Resolve spurious status actions checking speed values twice in FXOS portmgr
CSCvz05767	FP-1010 HA link goes down or New hosts unable to connect to the device
CSCvz14616	No connection events due to SFDataCor process stuck
CSCvz15676	In Firepower 1010 device, after upgrading ASA app, device going for fail safe mode
CSCvz27235	Multiple Cisco Products Snort Modbus Denial of Service Vulnerability
CSCvz32386	FTD Deployment error when FMC pushes PFS21 and IKEv1 settings on same crypto map entry
CSCvz38811	Deleted files holding disk space under Java process
CSCvz53993	Random packet block by Snort in SSL flow
CSCvz59464	IPReputation Feed Error Message-Method Not Allowed
CSCwa46963	Security: CVE-2021-44228 -> Log4j 2 Vulnerability
CSCwa70008	Expired certs cause Security Intel. and malware file preclassification signature updates to fail
CSCwa87714	6.7.0.3:Peer certificate cannot be authenticated with known CA certificates upon doing SRU update
CSCwa88571	Unable to register FMC with the Smart Portal

Version 6.7.0.2 Resolved Issues

Table 38: Version 6.7.0.2 Resolved Issues

Bug ID	Headline
CSCvh19737	HTTPS access on FTD data interface (off-box management) is failing
CSCvm82290	ASA core blocks depleted when host unreachable in IRB/TFW configuration
CSCvp69936	ASA : Traceback on tcp_intercept Thread name : Threat detection
CSCvs72450	FXOS - Recover hwclock of service module from corruption due to simultaneous write collision

Bug ID	Headline
CSCvs82926	Critical RPM alert on FPR2100 Series with ASA 'Chassis 0 Cooling Fan OK' SCH message
CSCvu91097	Cisco Firepower Management Center Software Policy Vulnerability
CSCvv19230	ASAv Anyconnect users unexpectedly disconnect with reason: Idle Timeout
CSCvv70984	ASA traceback while modifying the bookmark SSL Ciphers configuration
CSCvv85029	ASA5555 traceback and reload on Thread Name: ace_work
CSCvv86861	Traceback in KP in timer while running VPN, EMIX and SNMP traffic for overnight.
CSCvv89708	ASA/FTD may traceback in thread name fover_FSM_thread and reload
CSCvv97877	Secondary unit not able to join the cluster
CSCvw16165	Firepower 1000 Series stops passing traffic when a member of the port-channel is down
CSCvw16619	Offloaded traffic not failed over to secondary route in ECMP setup
CSCvw18614	ASA traceback in the LINA process
CSCvw19272	Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability
CSCvw23199	ASA/FTD Traceback and reload in Thread Name: Logger
CSCvw24084	FTD might crash in SNMP with rip Netsnmp_config_req_dequeue_and_send+269 at snmp/snmp_config_utils.c
CSCvw26544	Cisco ASA and FTD Software SIP Denial of Service Vulnerability
CSCvw38614	AZURE ASA/FTD NIC MAC address might get re-ordered upon a reboot
CSCvw43486	ASA/FTD Traceback and reload during PBR configuration change
CSCvw46630	FTD: NLP path dropping return ICMP destination unreachable messages
CSCvw51307	ASA/FTD traceback and reload in process name "Lina"
CSCvw51950	FPR 4K: SSL trust-point removed from new active ASA after manual Failover
CSCvw51985	ASA: AnyConnect sessions cannot be resumed due to ipv6 DACL failure
CSCvw53596	FPR4120 - Lina watchdog traceback in cli_xmlserver_thread
CSCvw53796	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerability
CSCvw59035	Connection issues to directly connected IP from FTD BVI address
CSCvw71766	ASA traceback and reload in Thread: Ikev2 Daemon

Bug ID	Headline
CSCvw76572	After FMC upgrade to 6.7 deployment fails if a policy map table has more than 1000 entries
CSCvw79542	Policy Deployment failure due to: "certificate eo not defined".
CSCvw81897	ASA: OpenSSL Vulnerability CVE-2020-1971
CSCvw82629	ASA Tracebacks when making "configuration session" changes regarding an ACL.
CSCvw83572	BVI HTTP/SSH access is not working in versions 9.14.1.30 or above
CSCvw84339	Managed device backup fails, for FTD, if hostname exceeds 30 characters
CSCvw87788	ASA traceback and reload webvpn thread
CSCvw89365	ASA/FTD may traceback and reload during certificate changes.
CSCvw93139	Cisco ASA and FTD Software for FP 1000/2100 Series Command Injection Vulnerability
CSCvw93272	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCvw93276	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCvw93282	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCvw93513	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCvw95301	ASA traceback and reload with Thread name: ssh when capture was removed
CSCvw95368	ASA: Traceback at emweb/https and reload when Remote Access VPN is enabled
CSCvw96488	Traceback in inspect_h323_ras+1810
CSCvw97256	Need handling of rmu read failure to ignore link state update when link state API read fails
CSCvw97821	ASA: VPN traffic does not pass if no dACL is provided in CoA
CSCvw98840	ASA: dACL with no IPv6 entries is not applied to v6 traffic after CoA
CSCvw99916	ASAv: SNMP result for used memory value incorrect after upgrade to 9.14
CSCvx01381	FMC GUI year drop-down list for Manual Time set up only listing until 2020
CSCvx01786	Pre-login-banner not showing on FCM WebUI
CSCvx02869	Traceback in Thread Name: Lic TMR
CSCvx03764	Offload rewrite data needs to be fixed for identity nat traffic and clustering environment
CSCvx04057	When SGT name is unresolved and used in ACE, line is not being ignored/inactive
CSCvx04643	ASA reload is removing 'content-security-policy' config

Bug ID	Headline
CSCvx05381	Cisco ASA and FTD Software Command Injection Vulnerability
CSCvx05385	ASA may generate a traceback in Logger thread during configuration sync in HA
CSCvx06385	Fail-to-wire ports in FPR 2100 flapping after upgrade to 6.6.1
CSCvx08734	ASA: default IPv6/IPv4 route tunneled does not work
CSCvx09164	FDM v6.6 -> v6.7 upgrade causing snort3 invocation failure
CSCvx09535	ASA Traceback: CRL check for an Anyconnect client with a revoked certificate triggers reload
CSCvx11295	ASA may traceback and reload on thread Crypto CA
CSCvx11460	Firepower 2110 silently dropping traffic with TFC enabled on the remote end
CSCvx13694	ASA/FTD traceback in Thread Name: PTHREAD-4432
CSCvx14564	1000 Series FTD in Disabled state with CD App Sync Error - Failed to apply SSP config on standby
CSCvx15040	DHCP Proxy Offer is getting drop on the ASA/FTD
CSCvx17664	ASA may traceback and reload in Thread Name 'webvpn_task'
CSCvx17780	FPR-2100-ASA : SNMP Walk for ifType is showing "other" for ASA interfaces in the latest versions
CSCvx17785	Crash seen consistently by adding/removing acl & entering into route-map command
CSCvx17842	Prevent lina from traceback due to object loop sent by FMC. Fail the deployment instead.
CSCvx20303	ASA/FTD may traceback in after changing snmp host-group object
CSCvx22695	ASA traceback and reload during OCSP response data cleanup
CSCvx25719	X-Frame-Options header is not set in webvpn response pages
CSCvx25836	ASA traceback & reload due to "show crashinfo" adding a new output log
CSCvx26221	Traceback into snmp at handle_agentx_packet / snmp takes long time to come up on FP1k and 5508
CSCvx26808	FTD traceback and reload on process lina on FPR2100 series
CSCvx27430	ASA: Unable to import PAC file if FIPS is enabled.
CSCvx29771	Firewall CPU can increase after a bulk routing update with flow offload
CSCvx29814	IP address in DHCP GIADDR field is reversed after sending DHCP DECLINE to DHCP server

Bug ID	Headline
CSCvx30735	Cisco Firepower Device Manager Software Filesystem Space Exhaustion Denial of Service Vuln
CSCvx34237	ASA reload with FIPS failure
CSCvx41171	Concurrent modification of ACL configuration breaks output of "show running-config" completely
CSCvx42081	FPR4150 ASA Standby Ready unit Loops to failed and remove config to install it again
CSCvx42197	ASA EIGRP route stuck after neighbour disconnected
CSCvx44401	FTD/ASA traceback in Thread Name : Unicorn Proxy Thread
CSCvx47230	X-Frame-Options header support for older versions of IE and windows platforms
CSCvx50366	Traceback in Thread Name: fover_health_monitoring_thread
CSCvx52122	ASA traceback and reload in SNMP Notify Thread while deleting transparent context
CSCvx54235	ASP capture dispatch-queue-limit shows no packets
CSCvx54396	Deployment failures on FTD when multicast is enabled.
CSCvx54606	FTD 6.6.1/6.7.0 is sending SNMP Ifspeed OID (1.3.6.1.2.1.2.2.1.5) response value = 0
CSCvx57417	Smart Tunnel Code signing certifcate renewal
CSCvx59120	COA Received before data tunnel comes up results in tear down of parent session
CSCvx63647	ASA traceback and reload on Thread Name: CTM Daemon
CSCvx68128	ASA internal deadlock leads to loss of feature functionality (syslogs, reload, ASDM, anyconnect)
CSCvx68785	FTD-API: deployment API unable to serialize record
CSCvx69405	ASA Traceback and reload in Thread Name: SNMP ContextThread
CSCvx71434	ASA/FTD Traceback and reload in Thread Name: pix_startup_thread due to asa_run_ttyS0 script
CSCvx72904	Optimise ifmib polls
CSCvx74035	ASA traceback and reload after run "clear configure all" with multiple ACLs and objects configured
CSCvx76233	ASA traceback and reload in thread ci/console when copying a system image to flash

Version 6.7.0.1 Resolved Issues

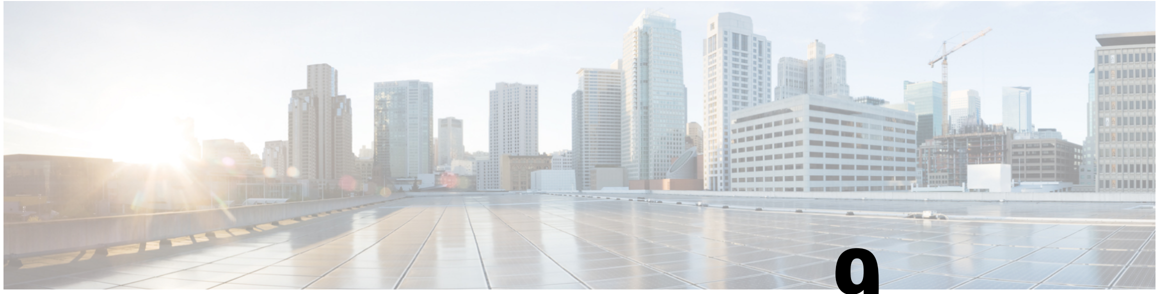
Table 39: Version 6.7.0.1 Resolved Issues

Bug ID	Headline
CSCvg69380	ASA - rare cp processing corruption causes console lock
CSCvo34210	ASA running 9.6.4.20 Traceback in threadname Unicorn Proxy Thread
CSCvr33428	FMC generates Connection Events from a SYN flood attack
CSCvr85295	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote
CSCvs13204	ASAv failover traffic on SR-IOV interfaces might be dropped due to interface-down
CSCvs84542	ASA traceback with thread: idfw_proc
CSCvt71529	ASA traceback and reload during SSL handshake
CSCvt75760	Traceback/Page-fault in Clientless WebVPN due to HTTP cleanup
CSCvt77665	[ciam] GNU readline _rl_tropen Function Insecure Temporary File Creation Vulnerability
CSCvu64784	CIAM: linux-kernel 3.14.39 need to investigate vulnerabilities (2015 and older)
CSCvu64884	CIAM: linux-kernel 3.14.39 vulnerabilities (2017-2020, SIR - Medium))
CSCvu70493	FXOS - AAA/RADIUS - NAS-IP Field set to 127.0.01
CSCvu96592	CIAM: pcre 8.35 and 8.38
CSCvu98222	FTD Lina engine may traceback in datapath after enabling SSL decryption policy
CSCvv15572	ASA traceback observed when "config-url" is entered while creating new context
CSCvv17585	Netflow template not sent under certain circumstances
CSCvv36393	statsAG memory leak
CSCvv52349	No utility to handle XFS corruption on 2100/1000 series Firepower devices
CSCvv58480	FXOS: Voltage on DC PSU displayed with wrong values from the 'show stats'
CSCvv66005	ASA traceback and reload on inspect esmtp
CSCvv67500	ASA 9.12 random traceback and reload in DATAPATH
CSCvv72466	OSPF network commands go missing in the startup-config after upgrading the ASA
CSCvv73017	Traceback due to fover and ssh thread

Bug ID	Headline
CSCvv80782	Traceback leads to the purg_process
CSCvv84358	VIC adapter kernel crash at boot
CSCvv85742	Upgrade : FSM status can show incorrect value after upgrade
CSCvv86926	Unexpected traceback and reload on FTD creating a Core file
CSCvv87232	ASA: High number of CPU hog in igb_saleen_io_sfp_mod_poll_thread process
CSCvv88017	ASA: EasyVPN HW Client triggers duplicate phase 2 rekey causing disconnections across the tunnel
CSCvv90720	ASA/FTD: Mac address-table flap seen on connected switch after a HA switchover
CSCvv94165	FTD 6.6 : High CPU spikes on snmpd process
CSCvv94701	ASA keeps reloading with "octnic_hm_thread". After the reload, it takes very long time to recover.
CSCvv95277	FPR2100 High disk usage in partition /opt/cisco/platform/logs due to growth of httpd log files
CSCvv96092	Cisco FXOS and NX-OS Software UDLD DoS and Arbitrary Code Execution Vulnerability
CSCvv98751	CIAM: linux-kernel 3.14.39 CVE-2020-14386 and others
CSCvv98764	CIAM: libproxy 0.4.11 CVE-2020-25219
CSCvv98773	CIAM: gnutls 3.3.5 CVE-2020-24659
CSCvv98959	[ciam] GNOME project libxml2 v2.9.10 and earlier have a global Buffer Overflow in at The
CSCvw00161	ASA traceback and reload due to VPN thread on firepower 2140
CSCvw07000	Snort busy drops with PDTS Tx queue stuck
CSCvw12008	ASA traceback and reload while executing "show tech-support" command
CSCvw12100	ASA stale VPN Context seen for site to site and AnyConnect sessions
CSCvw13348	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 98, seq 2)
CSCvw19401	Memory leak : DME process may traceback generating core on Firepower 4100/9300 (M5 series only)
CSCvw19907	restart of snmpd for agx communication fail to snmp-sa
CSCvw21844	FTD traceback and reload on DATAPATH thread when processing encapsulated flows
CSCvw22435	Error "No such file or directory" happended when using "copy ftp: wrokspace:" in FXOS 2.8.1

Bug ID	Headline
CSCvw22881	radius_rcv_auth can shoot up control plane CPU to 100%.
CSCvw22986	Secondary unit stuck in Bulk sync infinitely due to interface of Primary stuck in init state
CSCvw24556	TCP File transfer (Big File) not properly closed when Flow offload is enabled
CSCvw24642	CIAM: linux-kernel 3.14.39 CVE-2020-25645 and others
CSCvw26171	ASA syslog traceback while strncpy NULL string passed from SSL library
CSCvw26331	ASA traceback and reload on Thread Name: ci/console
CSCvw27072	SNMP V3 walk fails on Secondary nodes with Authorization Error
CSCvw27301	IKEv2 with EAP, MOBIKE status fails to be processed.
CSCvw28814	SNMP process crashed, while upgrading the QP to v9.14.1.109
CSCvw30252	ASA/FTD may traceback and reload due to memory corruption in SNMP
CSCvw31569	Director/Backup flows are left behind and traffic related to this flow is blackholed
CSCvw32518	ASASM traceback and reload after upgrade up to 9.12(4)4 and higher
CSCvw36662	TACACS+ ASCII password change request not handled properly
CSCvw37259	VPN syslogs are generated at a rate of 600/s until device goes into a hang state
CSCvw38984	Cisco FXOS and NX-OS Software UDLD DoS and Arbitrary Code Execution Vulnerability
CSCvw42999	9.10.1.11 ASA on FPR2110 traceback and reloads randomly
CSCvw44122	ASA: "class-default" class-map redirecting non-DNS traffic to DNS inspection engine
CSCvw44182	CIAM: tcp-dump 4.9.3 CVE-2020-8037
CSCvw45863	ASAv snmp traceback on reload
CSCvw46885	ASA/FTD traceback and reload related to SNMP and management-access configuration
CSCvw47321	IPSec transport mode traffic corruption for inbound traffic for some FPR platforms
CSCvw48517	DAP stopped working after upgrading the ASA to 9.13(1)13
CSCvw48829	Timezone in "show clock" is different from which in "show run clock"
CSCvw51462	IPv4 Default Tunneled Route Rejected
CSCvw53427	ASA Fails to process HTTP POST with SAML assertion containing multiple query parameters
CSCvw53494	CRUZ paloview is not accessible on release build

Bug ID	Headline
CSCvw53884	M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service
CSCvw54640	FPR-4150 - ASA traceback and reload with thread name DATAPATH
CSCvw58414	Name of anyconnect custom attribute of type dynamic-split-exclude-domains is changed after reload
CSCvw63862	ASA: Random L2TP users cannot access resources due to stale ACL filter entries
CSCvw74940	ASA traceback in IKE Daemon and reload
CSCvw83780	Standby FTD 6.6.1 core at Process Name: lina
CSCvw84786	ASA traceback and reload on Thread name snmp_alarm_thread
CSCvx09123	M500IT Model Solid State Drives on ISA3000 may go unresponsive after 3.2 Years in service
CSCvx09248	SNMP walk for v2 and v3 fails with No Such Object available on this agent at this OID is seen
CSCvx30314	ASA 9.15.1.7 traceback and reload in Thread Name: DATAPATH



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 6.7.0 Known Issues

Table 40: Version 6.7.0 Known Issues

Bug ID	Headline
CSCvv59527	Unresponsive pxGridv2 endpoint download hangs ADI, SFDataCorrelator
CSCvv95130	FTD device (ASA 5500-X & Firepower 1000/2100 series) does not respond after restore from backup
CSCvv99419	[6.7.0] FDM Snort 3 SSL Policy addition/removal causing Snort to restart w/o UI warning
CSCvw20092	File Policy not set in eStreamer event for malware event created by a retrospective event
CSCvw41726	FMC Monitoring Syslog setting manually the Page works erratically
CSCvw46630	FTD: NLP path dropping return ICMP destination unreachable messages
CSCvw48743	Performance Degradation observed with connection based debugging

Bug ID	Headline
CSCvw51105	6.7.0 FMC pxGrid connection to ISE 3.0 does not work when ipv6 is configured
CSCvx71029	Speed autonegotiation may need to be disabled on switch connected to FPR device with SFP link

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.

- Documentation: http://www.cisco.com/go/threatdefense-67-docs
- 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