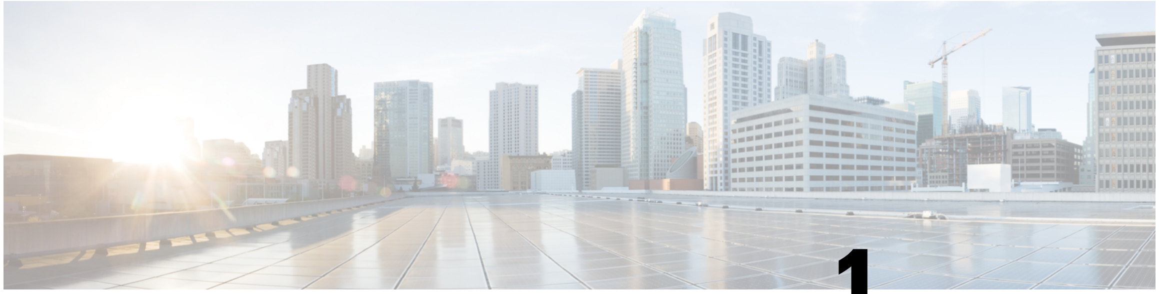
Cisco Firepower Release Notes, Version 6.2.3 Patches

First Published: 2018-05-02

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

CONTENTS



CHAPTER 1

Welcome

This document contains critical and release-specific information.

Release Dates

Sometimes Cisco releases updated builds. In most cases, only the latest build for each platform is available on the Cisco Support & Download site. We strongly recommend you use the latest build. If you downloaded an earlier build, do not use it. For more information, see Resolved Issues in New Builds, on page 66.

Table 1: Version 6.2.3 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.2.3	113	2020-06-01	FMC/FMCv	FMC/FMCv
6.2.3	111	2019-11-25	—	FTDv: AWS, Azure
6.2.3	110	2019-06-14	—	—
6.2.3	99	2018-09-07	—	—
6.2.3	96	2018-07-26	—	—
6.2.3	92	2018-07-05	—	—
6.2.3	88	2018-06-11	—	—
6.2.3	85	2018-04-09	—	—
6.2.3	84	2018-04-09	Firepower 7000/8000 series NGIPSv	—

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.2.3	83	2018-04-02	FTD/FTDv ASA FirePOWER	FTD: Physical platforms FTDv: VMware, KVM Firepower 7000/8000 ASA FirePOWER NGIPSv
6.2.3	79	2018-03-29	—	—

Table 2: Version 6.2.3 Patch Dates

Version	Build	Date	Platforms
6.2.3.18	50	2022-02-16	All
6.2.3.17	30	2021-06-21	All
6.2.3.16	59	2020-07-13	All
6.2.3.15	39	2020-02-05	FTD/FTDv
	38	2019-09-18	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
6.2.3.14	41	2019-07-03	All
	36	2019-06-12	All
6.2.3.13	53	2019-05-16	All
6.2.3.12	80	2019-04-17	All
6.2.3.11	55	2019-03-17	All
	53	2019-03-13	—
6.2.3.10	59	2019-02-07	All
6.2.3.9	54	2019-01-10	All
6.2.3.8	51	2019-01-02	No longer available.
6.2.3.7	51	2018-11-15	All
6.2.3.6	37	2018-10-10	All

Version	Build	Date	Platforms
6.2.3.5	53	2018-11-06	FTD/FTDv
	52	2018-12-09	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
6.2.3.4	42	2018-08-13	All
6.2.3.3	76	2018-07-11	All
6.2.3.2	46	2018-06-27	All
	42	2018-06-06	—
6.2.3.1	47	2018-06-28	All
	45	2018-06-21	—
	43	2018-05-02	—

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 1000, 2500, 4500
- FMC 2000, 4000
- FMC 750, 1500, 3500

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

Firepower Management Center Virtual

This release supports the following FMCv public cloud implementations:

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

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

- Firepower Management Center Virtual for Kernel-based virtual machine (KVM)
- Firepower Management Center Virtual for VMware vSphere/VMware ESXi 5.5, 6.0, or 6.5

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

Firepower Devices

Cisco Firepower devices monitor network traffic and decide whether to allow or block specific traffic based on a defined set of security rules. Some Firepower devices run Firepower Threat Defense (FTD) software; some run NGIPS/ASA FirePOWER software. Some can run either—but not both at the same time.

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

Table 3: Firepower Threat Defense in Version 6.2.3

FTD Platform	OS/Hypervisor	Additional Details
Firepower 2110, 2120, 2130, 2140	—	—
Firepower 4110, 4120, 4140, 4150 Firepower 9300: SM-24, SM-36, SM-44 modules	FXOS 2.3.1.73 or later build. **Note** Firepower 6.2.3.16+ requires FXOS 2.3.1.157+.	Upgrade FXOS first. To resolve issues, you may need to upgrade FXOS to the latest build. To help you decide, see the Cisco Firepower 4100/9300 FXOS Release Notes, 2.3(1).
ASA 5506-X, 5506H-X, 5506W-X ASA 5508-X, 5516-X ASA 5512-X ASA 5515-X ASA 5525-X, 5545-X, 5555-X ISA 3000	—	Although you do not separately upgrade the operating system on these devices in FTD deployments, you should make sure you have the latest ROMMON image on the ISA 3000, ASA 5506-X, 5508-X, and 5516-X. 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 • KVM: Kernel-based Virtual Machine • VMware vSphere/VMware ESXi 5.5, 6.0, or 6.5	For supported instances, see the appropriate FTDv Getting Started guide.

Table 4: NGIPS/ASA FirePOWER in Version 6.2.3

NGIPS/ASA FirePOWER Platform	OS/Hypervisor	Additional Details
ASA 5506-X, 5506H-X, 5506W-X	ASA 9.6(x) to 9.9(x)	There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues. See the Cisco ASA Upgrade Guide for order of operations. You should also make sure you have the latest ROMMON image on the ISA 3000, ASA 5506-X, 5508-X, and 5516-X. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.
ASA 5508-X, 5516-X	ASA 9.5(2) to 9.16(x)	
ASA 5512-X	ASA 9.5(2) to 9.9(x)	
ASA 5515-X	ASA 9.5(2) to 9.12(x)	
ASA 5525-X, 5545-X, 5555-X	ASA 9.5(2) to 9.14(x)	
ASA 5585-X-SSP-10, -20, -40, -60	ASA 9.5(2) to 9.12(x)	
NGIPSv	VMware vSphere/VMware ESXi 5.5, 6.0, or 6.5	For supported instances, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.
Firepower 7010, 7020, 7030, 7050 Firepower 7110, 7115, 7120, 7125 Firepower 8120, 8130, 8140 Firepower 8250, 8260, 8270, 8290 Firepower 8350, 8360, 8370, 8390 AMP 7150, 8050, 8150 AMP 8350, 8360, 8370, 8390	—	—

Manager-Device Compatibility

Firepower Management Center

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

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

Table 5: FMC-Device Compatibility

FMC Version	Oldest Device Version You Can Manage
6.7.0/6.7.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

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

Table 6: FDM-FTD Compatibility

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

Adaptive Security Device Manager

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

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

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

Table 7: ASDM-ASA FirePOWER Compatibility

ASA FirePOWER Version	Minimum ASDM Version
6.7.0/6.7.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 Internet Explorer 10 and 11 (Windows only)

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

Note We do not perform extensive testing with Apple Safari or Microsoft Edge. However, Cisco TAC welcomes feedback on issues you encounter.

Browser Settings and Extensions

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

If you are using Microsoft Internet Explorer 10 or 11:

- For the Check for newer versions of stored pages browsing history option, choose Automatically.
- Disable the Include local directory path when uploading files to server custom security setting (Internet Explorer 11 only).
- Enable Compatibility View for the appliance IP address/URL.

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

Securing Communications

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

To begin replacing the self-signed certificate:

- Firepower Management Center or 7000/8000 series: Select System > Configuration, then click HTTPS Certificates.
- Firepower Device Manager: Click Device, then the System Settings > Management Access link, then the Management Web Server tab.

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

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

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

Browsing from a Monitored Network

Many browsers use Transport Layer Security (TLS) v1.3 by default. If you are using an SSL policy to handle encrypted traffic, and people in your monitored network use browsers with TLS v1.3 enabled, websites that support TLS v1.3 fail to load. As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation. In Version 6.2.3.7+, a new CLI command allows you to specify when to downgrade; see Features and Functionality, on page 13.

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

Screen Resolution Requirements

Table 8: Screen Resolution Requirements

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

CHAPTER 3

Features and Functionality

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

Features for Firepower Management Center Deployments

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

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

New Features in FMC Version 6.2.3 Patches

Table 9:

Feature	Description
Version 6.2.3.13 Detection of rule conflicts in FTD NAT policies	After you upgrade to Version 6.2.3.13+, you can no longer create FTD NAT policies with conflicting rules (often referred to as duplicate or overlapping rules). This fixes an issue where conflicting NAT rules were applied out-of-order. If you currently have conflicting NAT rules, you will be able to deploy post-upgrade. However, your NAT rules will continue to be applied out-of-order. Therefore, we recommend that after the upgrade, you inspect your FTD NAT policies by editing (no changes are needed) then attempting to resave. If you have rule conflicts, the system will prevent you from saving. Correct the issues, save, and then deploy. **Note** Upgrading to Version 6.3.0 or 6.4.0 deprecates this fix. The issue is addressed in Version 6.3.0.4 and 6.4.0.2. Supported platforms: Firepower Threat Defense
Version 6.2.3.8 EMS extension support	Both the Decrypt-Resign and Decrypt-Known Key SSL policy actions now support the EMS extension during ClientHello negotiation, enabling more secure communications. The EMS extension is defined by RFC 7627. **Note** Version 6.2.3.8 was removed from the Cisco Support & Download site on 2019-01-07. Upgrading to Version 6.2.3.9 also enables EMS extension support. Version 6.3.0 discontinues EMS extension support. In FMC deployments, this feature depends on the device version. Upgrading the FMC to Version 6.3.0 does not discontinue support, but upgrading the device does. Support is reintroduced in Version 6.3.0.1. Supported platforms: Any
Version 6.2.3.7 TLS v1.3 downgrade CLI command for FTD	A new CLI command allows you to specify when to downgrade TLS v1.3 connections to TLS v1.2. Many browsers use 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 fail to load. For more information, see the system support commands in the Cisco Firepower Threat Defense Command Reference. We recommend you use these commands only after consulting with Cisco TAC. Supported platforms: Firepower Threat Defense
Version 6.2.3.3 Site-to-site VPN with clustering	You can now configure site-to-site VPN with clustering. Site-to-site VPN is a centralized feature; only the control unit supports VPN connections. Supported platforms: Firepower 4100/9300

Deprecated Features in FMC Version 6.2.3 Patches

Table 10:

Feature	Upgrade Impact	Description
Versions 6.2.3.1–6.2.3.3 Expired CA certificates for dynamic analysis	None, but you should patch.	On June 15, 2018, some AMP for Networks deployments stopped being able to submit files for dynamic analysis. See Expired CA Certificates for Dynamic Analysis, on page 25.

Features for Firepower Device Manager Deployments

New Features in FDM Version 6.2.3 Patches

Table 11:

Feature	Description
Version 6.2.3.8 EMS extension support	Both the Decrypt-Resign and Decrypt-Known Key SSL policy actions now support the EMS extension during ClientHello negotiation, enabling more secure communications. The EMS extension is defined by RFC 7627. **Note** Version 6.2.3.8 was removed from the Cisco Support & Download site on 2019-01-07. Upgrading to Version 6.2.3.9 also enables EMS extension support. Version 6.3.0 discontinues EMS extension support. Support is reintroduced in Version 6.3.0.1.
Version 6.2.3.7 TLS v1.3 downgrade CLI command for FTD	A new CLI command allows you to specify when to downgrade TLS v1.3 connections to TLS v1.2. Many browsers use 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 fail to load. For more information, see the system support commands in the Cisco Firepower Threat Defense Command Reference. We recommend you use these commands only after consulting with Cisco TAC.

Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

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

After you upgrade and those keywords become supported, the new intrusion rules are imported and, depending on your IPS configuration, can become auto-enabled and thus start generating events and affecting traffic flow.

Supported keywords depend on your Snort version:

- FMC: Choose Help > About.
- FTD with FDM: Use the show summary CLI command.
- ASA FirePOWER with ASDM: Choose ASA FirePOWER Configuration > System Information.

You can also find your Snort version in the Bundled Components section of the Cisco Firepower Compatibility Guide.

The Snort release notes contain details on new keywords. You can read the release notes on the Snort download page: https://www.snort.org/downloads.

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 46.

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. Do not restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 12:

✓	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 6.2.3.x Patches, on page 24: Important upgrade guidelines that are new or specific to this release. • Known Issues, on page 109: Be prepared to work around any bugs that affect upgrade. • Features and Functionality, on page 13: 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 13:

✓	Action/Check
	Upload upgrade packages. In FMC deployments, upload all upgrade packages—including for managed devices—to the FMC. 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 14:

✓	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 15:

✓	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 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 16:

✓	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 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.
	Disable ASA REST API on ASA with FirePOWER Services. Before you upgrade an ASA FirePOWER module currently running Version 6.3.0 or earlier, make sure the ASA REST API is disabled. Otherwise, the upgrade could fail. From the ASA CLI: `no rest api agent`. You can reenable after the upgrade: `rest-api agent`.
	Run readiness checks. We recommend compatibility and readiness checks. These checks assess your preparedness for a software upgrade.

Upgrade Guidelines for Version 6.2.3.x Patches

This checklist contains upgrade guidelines for Version 6.2.3 patches.

Table 17: Version 6.2.3.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure, on page 24	FTD	6.2.3 through 6.2.3.9	6.2.3.10 only
	Version 6.2.3.3 FTD Device Cannot Switch to Local Management, on page 24	FTD with FMC	6.2.3 through 6.2.3.2	6.2.3.3
	Expired CA Certificates for Dynamic Analysis, on page 25	Any	6.2.3 through 6.2.3.2	6.2.3.1 through 6.2.3.3
	Upgrade Can Unregister FTD/FDM from CSSM, on page 26	FTD with FDM	6.2.3 through 6.2.3.1	6.2.3.2 through 6.2.3.5
	Hotfix Before Upgrading Version 6.2.3-88 FMCs, on page 26	FMC	6.2.3-88	6.2.3.1 through 6.2.3.3

Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure

Deployments: Firepower Threat Defense

Upgrading from: Version 6.2.3 through 6.2.3.9

Directly to: Version 6.2.3.10 only

Known issue: CSCvo39052

Upgrading an FTD device to Version 6.2.3.10 with CC mode enabled causes a FSIC (file system integrity check) failure when the device reboots.

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.

If your FTD deployment requires security certifications compliance (CC mode), we recommend you upgrade directly to Version 6.2.3.13+. For Firepower 4100/9300 devices, we also recommend that you upgrade to FXOS 2.3.1.130+.

Version 6.2.3.3 FTD Device Cannot Switch to Local Management

Deployments: FTD wth FMC

Upgrading from: Version 6.2.3 through Version 6.2.3.2

Directly to: Version 6.2.3.3 only

In Version 6.2.3.3, you cannot switch Firepower Threat Defense device management from FMC to FDM. This happens even if you uninstall the Version 6.2.3.3 patch. If you want to switch to local management at that point, either freshly install Version 6.2.3, or contact Cisco TAC.

As a workaround, switch management before you upgrade to Version 6.2.3.3. Or, upgrade to the latest patch. Keep in mind that you lose device configurations when you switch management.

Note that you can switch management from FDM to FMC in Version 6.2.3.3.

Expired CA Certificates for Dynamic Analysis

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

Affected Versions: Version 6.0.0+

Resolves: CSCvj07038

On June 15, 2018, some Firepower deployments stopped being able to submit files for dynamic analysis. This occurred due to an expired CA certificate that was required for communications with the AMP Threat Grid cloud. Version 6.3.0 is the first major version with the new certificate.

Note If you do not want to upgrade to Version 6.3.0+, you must patch or hotfix to obtain the new certificate and reenable dynamic analysis. However, subsequently upgrading a patched or hotfixed deployment to either Version 6.2.0 or Version 6.2.3 reverts to the old certificate and you must patch or hotfix again.

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

This table lists the versions with the old certificates, as well as the patches and hotfixes that contain the new certificates, for each major version sequence and platform. Patches and hotfixes are available on the Cisco Support & Download site.

Table 18: Patches and Hotfixes with New CA Certificates

Versions with Old Cert	First Patch with New Cert	Hotfix with New Cert	
6.2.3 through 6.2.3.3	6.2.3.4	Hotfix G	FTD devices
		Hotfix H	FMC, NGIPS devices
6.2.2 through 6.2.2.3	6.2.2.4	Hotfix BN	All platforms
6.2.1	None. You must upgrade.	None. You must upgrade.	

Versions with Old Cert	First Patch with New Cert	Hotfix with New Cert	
6.2.0 through 6.2.0.5	6.2.0.6	Hotfix BX	FTD devices
		Hotfix BW	FMC, NGIPS devices
6.1.0 through 6.1.0.6	6.1.0.7	Hotfix EM	All platforms
6.0.x	None. You must upgrade.	None. You must upgrade.	

Upgrade Can Unregister FTD/FDM from CSSM

Deployments: FTD with FDM

Upgrading from: Version 6.2.3 or 6.2.3.1

Directly to: 6.2.3.2 through 6.2.3.5

Upgrading a Firepower Threat Defense device managed by Firepower Device Manager may unregister the device from the Cisco Smart Software Manager. After the upgrade completes, check your license status.

Step 1 Click Device, then click View Configuration in the Smart License summary.

Step 2 If the device is not registered, click Register Device.

Hotfix Before Upgrading Version 6.2.3-88 FMCs

Deployments: FMC

Upgrading from: Version 6.2.3-88

Directly to: Version 6.2.3.1, Version 6.2.3.2, or Version 6.2.3.3

Sometimes Cisco releases updated builds of Firepower upgrade packages. Version 6.2.3-88 has been replaced by a later build. If you upgrade an FMC running Version 6.2.3-88 to Version 6.2.3.1, Version 6.2.3.2, or Version 6.2.3.3, the SSE cloud connection continuously drops and generates errors. Uninstalling the patch does not resolve the issue.

If you are running Version 6.2.3-88, install Hotfix T before you upgrade.

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.

Note For the Firepower 4100/9300 with FTD, Firepower 6.2.3.16+ requires FXOS 2.3.1.157 or later build. Upgrade FXOS first.

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 19: 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.
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. Note that stacked 8000 series devices upgrade simultaneously, with the stack operating in limited, mixed-version state until all devices complete the upgrade. This should not take significantly longer than upgrading a standalone device.
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.

Condition	Details
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) 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) 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 .

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 6.2.3.18 Time and Disk Space

Table 20: Version 6.2.3.18 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3	Reboot Time
FMC	3.4 GB	290 MB	—	40 min	9 min
FMCv: VMware 6.0	3.5 GB	250 MB	—	24 min	4 min
Firepower 2100 series	—	2.7 GB	600 MB	13 min	12 min
Firepower 4100 series	—	1.8 GB	400 MB	6 min	6 min
Firepower 9300	—	1.7 GB	400 MB	5 min	9 min
ASA 5500-X series with FTD	2.1 GB	200 MB	420 MB	15 min	53 min
FTDv: VMware 6.0	2.0 GB	200 MB	420 MB	8 min	5 min
Firepower 7000/8000 series	3.5 GB	200 MB	650 MB	10 min	83 min
ASA FirePOWER	3.8 GB	59 MB	580 MB	74 min	59 min
NGIPSv: VMware 6.0	2.3 GB	180 MB	480 MB	6 min	4 min

Version 6.2.3.17 Time and Disk Space

Table 21: Version 6.2.3.17 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3	Reboot Time
FMC	3.4 GB	300 MB	—	32 min	7 min
FMCv: VMware 6.0	4.1 GB	230 MB	—	23 min	5 min
Firepower 2100 series	—	2.7 GB	600 MB	12 min	12 min
Firepower 4100 series	—	1.7 GB	390 MB	5 min	6 min
Firepower 9300	—	1.7 GB	390 MB	5 min	7 min
ASA 5500-X series with FTD	2.1 GB	200 MB	420 MB	18 min	37 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3	Reboot Time
FTDv: VMware 6.0	2.1 GB	190 MB	420 MB	7 min	5 min
Firepower 7000/8000 series	3.5 GB	200 MB	640 MB	10 min	15 min
ASA FirePOWER	3.8 GB	58 MB	580 MB	72 min	61 min
NGIPSv: VMware 6.0	2.5 GB	180 MB	480 MB	5 min	4 min

Version 6.2.3.16 Time and Disk Space

Table 22: Version 6.2.3.16 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3	Reboot Time
FMC	3.6 GB	250 MB	—	40 min	9 min
FMCv: VMware 6.0	3.3 GB	220 MB	—	25 min	4 min
Firepower 2100 series	—	2.6 GB	620 MB	11 min	12 min
Firepower 4100 series	—	1.7 GB	410 MB	5 min	5 min
Firepower 9300	—	1.8 GB	410 MB	5 min	9 min
ASA 5500-X series with FTD	2.0 GB	200 MB	430 MB	18 min	33 min
FTDv: VMware 6.0	2.0 GB	190 MB	430 MB	8 min	5 min
Firepower 7000/8000 series	3.5 GB	200 MB	670 MB	31 min	14 min
ASA FirePOWER	3.8 GB	58 MB	600 MB	74 min	77 min
NGIPSv: VMware 6.0	2.3 GB	180 MB	500 MB	6 min	4 min

Version 6.2.3.15 Time and Disk Space

Table 23: Version 6.2.3.15 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.7 GB	260 MB	—	50 min
FMCv: VMware 6.0	4.7 GB	210 MB	—	Hardware dependent

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
Firepower 2100 series	—	2.3 GB	590 MB	27 min
Firepower 4100 series	—	1.7 GB	390 MB	10 min
Firepower 9300	—	2.4 GB	390 MB	11 min
ASA 5500-X series with FTD	2.0 GB	190 MB	410 MB	38 min
FTDv: VMware 6.0	2.4 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.5 GB	210 MB	640 MB	19 min
ASA FirePOWER	3.9 GB	56 MB	580 MB	100 min
NGIPSv: VMware 6.0	2.7 GB	180 MB	470 MB	Hardware dependent

Version 6.2.3.14 Time and Disk Space

Table 24: Version 6.2.3.14 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.5 GB	260 MB	—	58 min
FMCv: VMware 6.0	4.7 GB	190 MB	—	Hardware dependent
Firepower 2100 series	—	1.9 GB	590 MB	23 min
Firepower 4100 series	—	1.7 GB	390 MB	11 min
Firepower 9300	—	1.7 GB	390 MB	10 min
ASA 5500-X series with FTD	2.0 GB	200 MB	410 MB	32 min
FTDv: VMware 6.0	2.4 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.4 GB	200 MB	630 MB	19 min
ASA FirePOWER	3.7 GB	53 MB	560 MB	106 min
NGIPSv: VMware 6.0	2.6 GB	190 MB	470 MB	Hardware dependent

Version 6.2.3.13 Time and Disk Space

Table 25: Version 6.2.3.13 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.7 GB	290 MB	—	50 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMCv: VMware 6.0	4.6 GB	190 MB	—	Hardware dependent
Firepower 2100 series	—	2.6 GB	590 MB	25 min
Firepower 4100 series	—	1.7 GB	390 MB	11 min
Firepower 9300	—	1.8 GB	390 MB	11 min
ASA 5500-X series with FTD	2.4 GB	190 MB	410 MB	32 min
FTDv: VMware 6.0	2.3 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.8 GB	190 MB	620 MB	18 min
ASA FirePOWER	3.7 GB	51 MB	560 MB	105 min
NGIPSv: VMware 6.0	2.6 GB	180 MB	470 MB	Hardware dependent

Version 6.2.3.12 Time and Disk Space

Table 26: Version 6.2.3.12 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	3.9 GB	220 MB	—	49 min
FMCv: VMware 6.0	4.6 GB	160 MB	—	Hardware dependent
Firepower 2100 series	—	1.9 GB	390 MB	21 min
Firepower 4100 series	—	970 MB	190 MB	14 min
Firepower 9300	—	1.7 GB	190 MB	11 min
ASA 5500-X series with FTD	1.4 GB	96 MB	210 MB	30 min
FTDv: VMware 6.0	2.4 GB	200 MB	210 MB	Hardware dependent
Firepower 7000/8000 series	3.6 GB	160 MB	540 MB	19 min
ASA FirePOWER	3.5 GB	31 MB	480 MB	104 min
NGIPSv: VMware 6.0	2.6 GB	130 MB	400 MB	Hardware dependent

Version 6.2.3.11 Time and Disk Space

Table 27: Version 6.2.3.11 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.5 GB	250 MB	—	39 min
FMCv: VMware 6.0	4.6 GB	35 MB	—	Hardware dependent
Firepower 2100 series	—	2.8 GB	590 MB	40 min
Firepower 4100 series	—	2.0 GB	380 MB	10 min
Firepower 9300	—	1.6 GB	380 MB	11 min
ASA 5500-X series with FTD	1.8 GB	230 MB	410 MB	33 min
FTDv: VMware 6.0	2.2 GB	230 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.3 GB	170 MB	600 MB	23 min
ASA FirePOWER	3.6 GB	50 MB	530 MB	110 min
NGIPSv: VMware 6.0	2.6 GB	130 MB	450 MB	Hardware dependent

Version 6.2.3.10 Time and Disk Space

Table 28: Version 6.2.3.10 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.2 GB	200 MB	—	40 min
FMCv	4.5 GB	230 MB	—	Hardware dependent
Firepower 2100 series	—	1.8 GB	390 MB	21 min
Firepower 4100/9300	—	1.3 GB	190 MB	11 min
ASA 5500-X series with FTD	1.3 GB	140 MB	210 MB	25 min
FTDv	1.6 GB	140 MB	210 MB	Hardware dependent
Firepower 7000/8000 series	3.2 GB	190 MB	560 MB	25 min
ASA FirePOWER	3.4 GB	31 MB	480 MB	100 min
NGIPSv	2.1 GB	160 MB	400 MB	Hardware dependent

Version 6.2.3.9 Time and Disk Space

Table 29: Version 6.2.3.9 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	3630 MB	190 MB	—	35 min
FMCv	3596 MB	172 MB	—	Hardware dependent
Firepower 2100 series	—	1677 MB	385 MB	21 min
Firepower 4100/9300	—	779 MB	184 MB	9 min
ASA 5500-X series with FTD	1105 MB	130 MB	206 MB	12 min
ISA 3000 with FTD	1071 MB	130 MB	206 MB	25 min
FTDv	1094 MB	130 MB	206 MB	Hardware dependent
Firepower 7000/8000 series	2975 MB	161 MB	538 MB	30 min
ASA FirePOWER	3211 MB	27 MB	462 MB	38 min
NGIPSv	1883 MB	146 MB	378 MB	Hardware dependent

Version 6.2.3.8 Time and Disk Space

Version 6.2.3.8 was removed from the Cisco Support & Download site on 2019-01-07. If you are running this version, we recommend you upgrade.

Version 6.2.3.7 Time and Disk Space

Table 30: Version 6.2.3.7 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	2909 MB	137 MB	—	25 min
FMCv	3972 MB	211 MB	—	Hardware dependent
Firepower 2100 series	—	1668 MB	384 MB	19 min
Firepower 4100/9300	—	795 MB	183 MB	8 min
ASA 5500-X series with FTD	1067 MB	130 MB	205 MB	9 min
ISA 3000 with FTD	1080 MB	130 MB	205 MB	20 min
FTDv	1146 MB	130 MB	205 MB	Hardware dependent
Firepower 7000/8000 series	3300 MB	136 MB	477 MB	20 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
ASA FirePOWER	2291 MB	26 MB	411 MB	80 min
NGIPSv	1588 MB	121 MB	327 MB	Hardware dependent

Version 6.2.3.6 Time and Disk Space

Table 31: Version 6.2.3.6 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	2524 MB	47 MB	—	30 min
FMCv	2315 MB	101 MB	—	Hardware dependent
Firepower 2100 series	—	1673 MB	383 MB	10 min
Firepower 4100/9300	—	790 MB	182 MB	17 min
ASA 5500-X series with FTD	1220 MB	130 MB	205 MB	21 min
ISA 3000 with FTD	1087 MB	130 MB	205 MB	21 min
FTDv	1133 MB	130 MB	205 MB	Hardware dependent
Firepower 7000/8000 series	1196 MB	17 MB	204 MB	30 min
ASA FirePOWER	1844 MB	16 MB	226 MB	106 min
NGIPSv	364 MB	17 MB	142 MB	Hardware dependent

Version 6.2.3.5 Time and Disk Space

Table 32: Version 6.2.3.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1566 MB	24 MB	—	28 min
FMCv	2266 MB	80 MB	—	Hardware dependent
Firepower 2100 series	—	1001MB	257 MB	20 min
Firepower 4100/9300	—	370 MB	56 MB	7 min
ASA 5500-X series with FTD	587 MB	130 MB	78 MB	20 min
ISA 3000 with FTD	379 MB	130 MB	78 MB	20 min
Firepower 7000/8000 series	806 MB	17 MB	78 MB	22 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
ASA FirePOWER	1465 MB	15 MB	100 MB	70 min
NGIPSv	120 MB	17 MB	16 MB	Hardware dependent

Version 6.2.3.4 Time and Disk Space

Table 33: Version 6.2.3.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	2191 MB	107 MB	—	80 min
FMCv	1760 MB	35 MB	—	Hardware dependent
Firepower 2100 series	—	1014 MB	261 MB	17 min
Firepower 4100/9300	—	334 MB	59 MB	7 min
ASA 5500-X series with FTD	411 MB	128 MB	82 MB	20 min
ISA 3000 with FTD	393 MB	128 MB	82 MB	20 min
FTDv	411 MB	128 MB	82 MB	Hardware dependent
Firepower 7000/8000 series	800 MB	17 MB	82 MB	23 min
ASA FirePOWER	1385 MB	15 MB	103 MB	25 min
NGIPSv	191 MB	17 MB	20 MB	Hardware dependent

Version 6.2.3.3 Time and Disk Space

Table 34: Version 6.2.3.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1879 MB	88 MB	—	26 min
FMCv	2093 MB	90 MB	—	Hardware dependent
Firepower 2100 series	—	987 MB	255 MB	15 min
Firepower 4100/9300	—	313 MB	54 MB	5 min
ASA 5500-X series with FTD	553 MB	128 MB	77 MB	16 min
ISA 3000 with FTD	307 MB	90 MB	77 MB	15 min
FTDv	307 MB	90 MB	77 MB	Hardware dependent

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
Firepower 7000/8000 series	825 MB	17 MB	77 MB	15 min
ASA FirePOWER	634 MB	16 MB	98 MB	40 min
NGIPSv	102 MB	17 MB	77 MB	Hardware dependent

Version 6.2.3.2 Time and Disk Space

Table 35: Version 6.2.3.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1743 MB	27 MB	—	24 min
FMCv	1976 MB	70 MB	—	Hardware dependent
Firepower 2100 series	—	977 MB	252 MB	17 min
Firepower 4100/9300	—	374 MB	51 MB	4 min
ASA 5500-X series with FTD	585 MB	126 MB	73 MB	16 min
ISA 3000 with FTD	676 MB	126 MB	73 MB	17 min
FTDv	585 MB	126 MB	73 MB	Hardware dependent
Firepower 7000/8000 series	688 MB	11 MB	76 MB	13 min
ASA FirePOWER	1440 MB	15 MB	98 MB	40 min
NGIPSv	96 MB	17 MB	14 MB	Hardware dependent

Version 6.2.3.1 Time and Disk Space

Table 36: Version 6.2.3.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1361.8 MB	59.67 MB	—	25 min
FMCv	1240.8 MB	40.8 MB	—	Hardware dependent
Firepower 2100 series	—	948.3 MB	246 MB	81 min
Firepower 4100/9300	—	278 MB	45 MB	8 min
ASA 5500-X series with FTD	275.5 MB	89.9 MB	68 MB	16 min
ISA 3000 with FTD	343.4 MB	127.5 MB	68 MB	15 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FTDv	275.5 MB	89.9 MB	67 MB	Hardware dependent
Firepower 7000/8000 series	99.8 MB	36 MB	10 MB	19 min
ASA FirePOWER	867.9 MB	15.45 MB	32 MB	60 min
NGIPSv	101.9 MB	17.18 MB	9 MB	Hardware dependent

Traffic Flow and Inspection

Interruptions in traffic flow and inspection can occur when you:

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

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

Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300

FXOS Upgrades

Upgrade FXOS on each chassis independently, even if you have inter-chassis clustering or high availability pairs configured. How you perform the upgrade determines how your devices handle traffic during the FXOS upgrade.

Table 37: Traffic Behavior: FXOS Upgrades

Deployment	Method	Traffic Behavior
Standalone	—	Dropped.
High availability	Best Practice: Update FXOS on the standby, switch active peers, upgrade the new standby.	Unaffected.
	Upgrade FXOS on the active peer before the standby is finished upgrading.	Dropped until one peer is online.

Deployment	Method	Traffic Behavior
Inter-chassis cluster (6.2+)	Best Practice: Upgrade one chassis at a time so at least one module is always online.	Unaffected.
	Upgrade chassis at the same time, so all modules are down at some point.	Dropped until at least one module is online.
Intra-chassis cluster (Firepower 9300 only)	Hardware bypass enabled: Bypass: Standby or Bypass-Force. (6.1+)	Passed without inspection.
	Hardware bypass disabled: Bypass: Disabled. (6.1+)	Dropped until at least one module is online.
	No hardware bypass module.	Dropped until at least one module is online.

Software Upgrades for Standalone Devices

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

Table 38: Traffic Behavior: Software Upgrades for Standalone Devices

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.
IPS-only interfaces	Inline set, hardware bypass force-enabled: Bypass: Force (6.1+).	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: Bypass: Standby (6.1+).	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: Bypass: Disabled (6.1+).	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability/Scalability

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

- 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: Not supported.

Note Upgrading an inter-chassis cluster from Version 6.2.0, 6.2.0.1, or 6.2.0.2 causes a 2-3 second traffic interruption in traffic inspection when each module is removed from the cluster. Upgrading high availability or clustered devices from Version 6.0.1 through 6.2.2.x may have additional upgrade path requirements; see the upgrade path information in the planning chapter of the Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.

Software Uninstall (Patches)

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

- 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.

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 39: 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 40: Traffic Behavior: Software Upgrades for Standalone Devices

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

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

Software Upgrades for High Availability/Scalability

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

- Firepower Threat Defense with FMC: For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.
- Firepower Threat Defense with FDM: Not supported.

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.

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 41: Traffic Behavior: Deploying Configuration Changes

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.
IPS-only interfaces	Inline set, Failsafe enabled or disabled (6.0.1–6.1).	Passed without inspection. A few packets might drop if Failsafe is disabled and Snort is busy but not down.
	Inline set, Snort Fail Open: Down: disabled (6.2+).	Dropped.
	Inline set, Snort Fail Open: Down: enabled (6.2+).	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Firepower 7000/8000 Series Upgrade Behavior

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

Standalone 7000/8000 Series: Firepower Software Upgrade

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

Table 42: Traffic Behavior During Upgrade: Standalone 7000/8000 Series

Interface Configuration	Traffic Behavior
Inline, hardware bypass enabled (Bypass Mode: Bypass)	Passed without inspection, although traffic is interrupted briefly at two points: • At the beginning of the upgrade process as link goes down and up (flaps) and the network card switches into hardware bypass. • After the upgrade finishes as link flaps and the network card switches out of bypass. Inspection resumes after the endpoints reconnect and reestablish link with the device interfaces.
Inline, no hardware bypass module,or hardware bypass disabled (Bypass Mode: Non-Bypass)	Dropped

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

7000/8000 Series High Availability Pairs: Firepower Software Upgrade

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

Which peer upgrades first depends on your deployment:

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

8000 Series Stacks: Firepower Software Upgrade

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

Traffic Behavior During Deployment

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

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

Table 43: Traffic Behavior During Deployment: 7000/8000 Series

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

ASA FirePOWER Upgrade Behavior

Your ASA service policies for redirecting traffic to the ASA FirePOWER module determine how the module handles traffic during the Firepower software upgrade, including when you deploy certain configurations that restart the Snort process.

Table 44: 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 45: 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 46: 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 47: 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 5506-X, 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
- Firepower 7000 series: https://www.cisco.com/go/7000series-software
- Firepower 8000 series: https://www.cisco.com/go/8000series-software
- ASA with FirePOWER Services (ASA 5500-X series): https://www.cisco.com/go/asa-firepower-sw
- 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.

For example:

- Package: `Cisco_Firepower_Mgmt_Center_Patch-6.2.3.1-999.sh.REL.tar`
- Platform: Firepower Management Center
- Package type: Patch
- Version and build: 6.2.3.1-999
- 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 48:

Platform	Package
FMC/FMCv	Sourcefire_3D_Defense_Center_S3
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
Firepower 7000/8000 series AMP models	Sourcefire_3D_Device_S3
ASA FirePOWER	Cisco_Network_Sensor
NGIPSv	Sourcefire_3D_Device_VMware

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 6.2.3 Patches That Support Uninstall

This table lists supported uninstall scenarios for Version 6.2.3 patches. Remember that uninstalling returns you to the patch level you upgraded from. If uninstall will take you farther back than what is supported, we recommend you reimage and then upgrade to your desired patch level.

Table 49: Version 6.2.3 Patches That Support Uninstall

Current Version	Farthest Back You Should Uninstall		
	FTD/FTDv	Firepower 7000/8000 ASA FirePOWER NGIPSv	FMC/FMCv
6.2.3.16+	6.2.3.15	6.2.3.15	6.2.3.15
6.2.3.15	—	—	—
6.2.3.12 through 6.2.3.14	6.2.3	6.2.3.11	6.2.3.11
6.2.3.11	6.2.3	—	—
6.2.3.8 through 6.2.3.10	6.2.3	6.2.3.7	6.2.3.7
6.2.3.7	6.2.3	—	—
6.2.3.1 through 6.2.3.6	6.2.3	6.2.3	6.2.3

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 51.
- You cannot use the FMC or ASDM to uninstall a patch from a device, nor can you use the local web interface on a 7000/8000 series device.
- You cannot use FMC user accounts to log into and uninstall the patch from one of its managed devices. Devices maintain their own user accounts.
- You must have access to the device shell as the `admin` user for the device, or as another local user with CLI configuration access. If you disabled shell access, you cannot uninstall device patches. Contact Cisco TAC to reverse the device lockdown.

Uninstall from the FMC After Devices

Uninstall patches from the FMC after you uninstall from managed devices. As with upgrade, you must uninstall from high availability FMCs one at a time; see Uninstall Order for HA/Scalability Deployments, on page 51.

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.

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 50: 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 51: 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.

Deployment	Uninstall Order
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 52: Uninstall Order for 7000/8000 Series Devices in HA or Stacks

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

Table 53: Uninstall Order for ASA with FirePOWER Services Devices in ASA Failover Pairs/Clusters

ASA Deployment	Uninstall Order
ASA active/standby failover pair, with ASA FirePOWER	Always uninstall from the standby. 1. Uninstall from the ASA FirePOWER module on the standby ASA device. 2. Fail over. 3. Uninstall from the ASA FirePOWER module on the new standby ASA device.
ASA active/active failover pair, with ASA FirePOWER	Make both failover groups active on the unit you are not uninstalling. 1. Make both failover groups active on the primary ASA device. 2. Uninstall from the ASA FirePOWER module on the secondary ASA device. 3. Make both failover groups active on the secondary ASA device. 4. Uninstall from the ASA FirePOWER module on the primary ASA device.

ASA Deployment	Uninstall Order
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 53, 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 51.
- For ASA FirePOWER modules, make sure the ASA REST API is disabled. From the ASA CLI: `no rest api agent`. You can reenable after the uninstall: `rest-api agent`.

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

Deploying before you uninstall reduces the chance of failure.

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

Step 2 Perform prechecks.

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

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

You can either SSH to the device's management interface (hostname or IP address) or use the console. Note that ASA 5585-X series devices have a dedicated ASA FirePOWER console port.

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

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

ASA FirePOWER, except ASA 5585-X series	`session sfr`

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

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

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

When you patch a Firepower appliance, an easily identifiable uninstaller for that patch is automatically created in the upgrade directory; see Uninstall Packages, on page 58.

Unless you are running the uninstall from the console, use the `--detach` option to ensure the uninstall does not stop if your user session times out. Otherwise, the uninstall runs as a child process of the user shell. If your connection is terminated, the process is killed, the check is disrupted, and the appliance may be left in an unstable state.

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

Step 6 Monitor the uninstall.

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

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

Step 7 Verify success.

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

Step 8 Use the Message Center to recheck deployment health.

Step 9 Redeploy configurations.

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

What to do next

- For HA/scalability deployments, repeat this procedure for each device in your planned sequence. Then, make any final adjustments. For example, in an FTD HA deployment, reestablish HA after you uninstall from both peers.
- For ASA FirePOWER modules, reenable the ASA REST API if you disabled it earlier. From the ASA CLI: `rest-api agent`.

Uninstall from ASA FirePOWER (ASDM Managed)

Use this procedure to uninstall a patch from a locally managed ASA FirePOWER module. If you manage ASA FirePOWER with an FMC, see Uninstall from Any Device (FMC Managed), on page 55.

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 51.
- Make sure the ASA REST API is disabled. From the ASA CLI: `no rest api agent`. You can reenable after the uninstall: `rest-api agent`.

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

Deploying before you uninstall reduces the chance of failure.

Step 2 Perform prechecks.

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

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

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

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

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

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

Do not untar signed (.tar) packages.

Unless you are running the uninstall from the console, use the `--detach` option to ensure the uninstall does not stop if your user session times out. Otherwise, the uninstall runs as a child process of the user shell. If your connection is terminated, the process is killed, the check is disrupted, and the appliance may be left in an unstable state.

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

Step 6 Monitor the uninstall.

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

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

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

Step 7 Verify success.

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

Step 8 Redeploy configurations.

What to do next

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

Uninstall Packages

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

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

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

CHAPTER 6

Install the Software

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

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

Installation Checklist and Guidelines

Reimaging returns most settings to factory defaults, including the system password. This checklist highlights actions that can prevent common reimage issues. However, this checklist is not comprehensive. See the appropriate installation guide for full instructions: Installation Instructions, on page 61.

Table 54:

✓	**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 or Lights-Out Management (LOM) access to the appliance. Note that LOM is only supported on select appliances and must be already configured. **Note** Reimaging to an earlier version automatically deletes network settings. In this rare case, you must have physical or LOM 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 61 • Cisco Firepower System Feature Licenses Guide • Frequently Asked Questions (FAQ) about Firepower Licensing

Reimaging Firepower 2100 Series Devices to Earlier Major Versions

We recommend that you perform complete reimages of Firepower2100 series devices. If you use the erase configuration method, FXOS may not revert along with the Firepower Threat Defense software. This can cause failures, especially in high availability deployments.

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

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

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

Manually unregister from CSSM before you:

- Reimage a Firepower Management Center that manages FTD devices.
- Reimage a Firepower Threat Defense device that is locally managed by FDM.
- Switch a Firepower Threat Defense device from FDM to FMC management.

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

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

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

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

Installation Instructions

Table 55: Firepower Management Center Installation Instructions

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

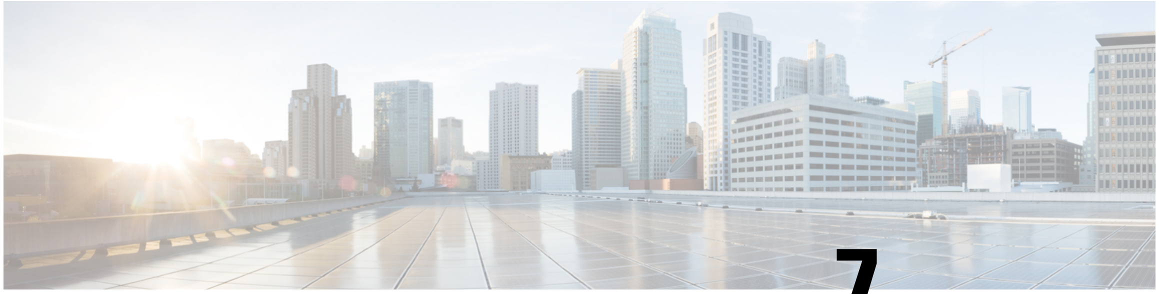
FMC	Guide
FMCv	Cisco Firepower Management Center Virtual Getting Started Guide

Table 56: Firepower Threat Defense Installation Instructions

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

Table 57: Firepower 7000/8000 Series, NGIPSv, and ASA FirePOWER Installation Instructions

NGIPS Platform	Guide
Firepower 7000 series	Cisco Firepower 7000 Series Getting Started Guide: Restoring a Device to Factory Defaults
Firepower 8000 series	Cisco Firepower 8000 Series Getting Started Guide: Restoring a Device to Factory Defaults
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware
ASA FirePOWER	Cisco ASA and Firepower Threat Defense Reimage Guide ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide: Managing the ASA FirePOWER Module



CHAPTER 7

Documentation

We update Firepower documentation if a patch requires it.

- Documentation Roadmaps, on page 63

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.

Resolved Issues in New Builds

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

You cannot upgrade from one build to another for the same Firepower version. If a new build would fix your issue, determine if an upgrade or hotfix would work instead. If not, contact Cisco TAC. See the Cisco Firepower Hotfix Release Notes for quicklinks to publicly available Firepower hotfixes.

Use this table to determine if a new build is available for your platform.

Table 58: Version 6.2.3.x Patches with New Builds

Version	New Build	Released	Platforms	Resolves
6.2.3.15	39	2020-01-05	FTD/FTDv	CSCvs84578: Upgrading FTD on 4100/9300 Platform to 6.2.3.15 break SSHD, preventing FTD instance from booting up CSCvs84713: After upgrading FTD on ASA55XX to 6.2.3.15, cannot SSH to the device CSCvs95725: Virtual FTD Running on 6.2.3.15 blocks SSH request and loses connection with the FMC If you already upgraded your FTD device to Version 6.2.3.15-38, apply Hotfix DW to the device. For more information, see the Software Advisory for CSCvs84578 and CSCvs84713.
6.2.3.14	41	2019-07-03	All	CSCvq34224: Firepower Primary Detection Engine process terminated after Manager upgrade If you already upgraded to Version 6.2.3.14-36 and have FTD devices configured for high availability, apply Hotfix CY to the FMC.
6.2.3.11	55	2019-03-17	All	Cisco Firepower System User Agent issues. If you already downloaded and installed Version 6.2.3.11-53, contact Cisco TAC for a hotfix.
6.2.3.5	53	2018-11-06	FTD/FTDv	CSCvk67239: ASA Firewalls and Firepower Threat Defense devices may traceback and reload when the state of the unit in a Failover pair or multi-unit cluster changes. This also occurred when upgrading from Version 6.2.3.5 to Version 6.2.3.6. For more information, see the Software Advisory for CSCck67239.

Version	New Build	Released	Platforms	Resolves
6.2.3.2	46	2017-06-27	All	CSCvj25386: In some cases, if a device ever ran Version 6.0, upgrading to any version earlier than Version 6.2.2.3 failed. CSCvk06176: Even with this new build, if an FMC ever ran Version 6.2.3-88, the SSE cloud connection drops and telemetry cannot send data after you upgrade. If your FMC is affected, apply Hotfix T.
6.2.3.1	47	2017-06-28	All	CSCvj25386: In some cases, if a device ever ran Version 6.0, upgrading to any version earlier than Version 6.2.2.3 failed. CSCvk06176: Even with this new build, if an FMC ever ran Version 6.2.3-88, the SSE cloud connection drops and telemetry cannot send data after you upgrade. If your FMC is affected, apply Hotfix T.
	45 and 46	2017-06-21	All	Component issues.

Version 6.2.3.18 Resolved Issues

Table 59: Version 6.2.3.18 Resolved Issues

Bug ID	Headline
CSCvm05464	CVE-2018-5391 Remote denial of service via improper IP fragment handling
CSCvp16933	Cisco Firepower Threat Defense Software Shell Access Vulnerability
CSCvq41939	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DHCP DoS
CSCvx00496	QuoVadis root CA decommission on pix-asa
CSCvx19563	FDM: Need to update various items to use STO Certificate Trust Bundle (QuoVadis Root CA Issue)
CSCvx28070	Update QuoVadis root CA for Smart license as it is getting decommissioned
CSCvx30107	Default trustpoint _SmartCallHome_ServerCA using SHA1 which is not supported
CSCvx32283	Cisco Firepower Management Center Open Redirect Vulnerability
CSCvx46296	Cisco ASA and FTD Software Transparent Mode Denial of Service Vulnerability
CSCvx47895	Cisco ASA Software and FTD Software Identity-Based Rule Bypass Vulnerability
CSCvx52541	Update SSEConnector config to use the CA bundle /etc/ssl/certs.pem
CSCvx55664	Cisco Firepower Management Center Cross-site Scripting Vulnerability

Bug ID	Headline
CSCvx57417	Smart Tunnel Code signing certifcate renewal
CSCvy16573	Cisco Firepower Threat Defense Command Injection Vulnerability
CSCvy20504	Cisco ASA and FTD Software Web Services Interface Cross-Site Scripting Vulnerability
CSCvy36910	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS
CSCvy41771	Cisco Firepower Management Center Software Authenticated Directory Traversal Vulnerability
CSCvy58278	Denial of Service vulnerability handling the config-request request
CSCvy80325	Include the ios pem files into the patch upgrade package for vFTD
CSCvy93480	Cisco ASA and FTD Software IKEv2 Site-to-Site VPN Denial of Service Vulnerability
CSCwa46963	Security: CVE-2021-44228 -> Log4j 2 Vulnerability
CSCwa70008	Expired certs cause Security Intel. and malware file preclassification signature updates to fail
CSCwa88571	Unable to register FMC with the Smart Portal

Version 6.2.3.17 Resolved Issues

Table 60: Version 6.2.3.17 Resolved Issues

Bug ID	Headline
CSCvh64138	FXOS upgrade to 2.3.1.X causes FTD logical device to not come up
CSCvk08565	App-instance in start-failed with "Application Failing to Start by ProcMgr" error on container app
CSCvn82441	[SXP] Issue with establishing SXP connection between ASA on FPR-2110 and switches
CSCvn95731	ASA traceback and reload on Thread Name SSH
CSCvo60166	KP: Can't login to fxos due to disk full error
CSCvo86940	PROMPTING FOR PASSWORD WHEN TRYING TO CONFIGURE enic, vfio-pci , igb_uio ON BLADE
CSCvp16482	ASA reloads when establishing simultaneous ASDM sessions
CSCvp49481	Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability

Bug ID	Headline
CSCvp57643	FTD/ASA - Cluster/HA - Master/Active unit does not update all the route changes to Slaves/Standby
CSCvp93468	Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability
CSCvq43920	Cisco Firepower Threat Defense Software Hidden Commands Vulnerability
CSCvr35872	ASA traceback Thread Name: DATAPATH with PBR configured
CSCvr55973	Unable to ping out of management 1/1 interface on a KP
CSCvr80164	WR6 and WR8 commit id update in CCM layer(sprint 72)
CSCvs45111	WR6 and WR8 commit id update in CCM layer(sprint 75)
CSCvs56888	Cisco Firepower Threat Defense Software TCP Flood Denial of Service Vulnerability
CSCvs81504	WR6 and WR8 commit id update in CCM layer(sprint 77)
CSCvt01282	WR6 and WR8 commit id update in CCM layer(sprint 79)
CSCvt02409	Cisco Firepower Threat Defense Software Inline Pair/Passive Mode DoS Vulnerability
CSCvt13445	Cisco ASA and FTD Software FTP Inspection Bypass Vulnerability
CSCvt18028	Cisco ASA and FTD WebVPN CRLF Injection Vulnerability
CSCvt30731	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 80)
CSCvt31177	Cisco ASA and FTD Software for FP 1000/2100 Series Appliances Secure Boot Bypass Vulns
CSCvt31178	Cisco ASA and FTD Software for FP 1000/2100 Series Appliances Secure Boot Bypass Vulns
CSCvt60190	Cisco ASA and FTD Web Services File Upload Denial of Service Vulnerability
CSCvt70322	Cisco ASA Software and FTD Software Web Services Denial of Service Vulnerability
CSCvt74037	Cisco FXOS Software Command Injection Vulnerability
CSCvt83121	Cisco ASA and FTD Software OSPFv2 Link-Local Signaling Denial of Service Vulnerability
CSCvu15801	Cisco ASA and FTD Software SIP Denial of Service Vulnerability
CSCvu20257	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 85)
CSCvu40531	FXOS LACP packet logging to pktmgr.out and lacp.out fills up /opt/cisco/platform/logs to 100%
CSCvu44910	Cisco ASA Software and FTD Software Web Services Cross-Site Scripting Vulnerability

Bug ID	Headline
CSCvu46685	Cisco ASA and FTD Software SSL/TLS Session Denial of Service Vulnerability
CSCvu59817	Cisco ASA and FTD Software SSL VPN Direct Memory Access Denial of Service Vulnerability
CSCvu61919	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 87)
CSCvu75581	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities
CSCvu75615	Cisco ASA Software and FTD Software WebVPN Portal Access Rule Bypass Vulnerability
CSCvu83309	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities
CSCvu91097	Cisco Firepower Management Center Software Policy Vulnerability
CSCvv13835	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities
CSCvv33712	Cisco ASA Software Web-Based Management Interface Reflected Cross-Site Scripting Vulnerabi
CSCvv56644	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web DoS
CSCvv65184	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web DoS
CSCvv79459	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 94, seq 1)
CSCvv95277	FPR2100 High disk usage in partition /opt/cisco/platform/logs due to growth of httpd log files
CSCvw13348	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 98, seq 2)
CSCvw26544	Cisco ASA and FTD Software SIP Denial of Service Vulnerability
CSCvw52609	Cisco ASA and FTD Software Web Services Buffer Overflow Denial of Service Vulnerability
CSCvw53796	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerability
CSCvw53884	M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service
CSCvw90923	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 101, seq 4)
CSCvx06920	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 103, seq 5)
CSCvx16700	FXOS clock sync issue during blade boot up due to "MIO DID NOT RESPOND TO FORCED TIME SYNC"

Version 6.2.3.16 Resolved Issues

Table 61: Version 6.2.3.16 Resolved Issues

Bug ID	Headline
CSCvg84794	All Interfaces does not come up after booting KP ASA image
CSCvj49994	Failed to download FXOS package during upgrade due to no IPv6 address
CSCvm48451	Intrusion Event Performance Graphs load blank on 4100 and 9300
CSCvm84994	SSH idle timeout not working on FTD on Firepower 4100 and Firepower 9300
CSCvm85823	Not able to ssh, ssh_exec: open(pager) error on console
CSCvn93683	ASA: cluster exec show commands not show all output
CSCvo62077	Cisco Firepower Threat Defense Software VPN System Logging Denial of Service Vulnerability
CSCvo78789	Cisco Adaptive Security Appliance Smart Tunnel Vulnerabilities
CSCvo80853	Cisco Firepower Threat Defense Software Packet Flood Denial of Service Vulnerability
CSCvp04134	Traceback in HTTP Cli Exec when upgrading to 9.12.1
CSCvp16945	Cisco ASA Software and FTD Software MGCP Denial of Service Vulnerabilities
CSCvp16949	Cisco ASA Software and FTD Software MGCP Denial of Service Vulnerabilities
CSCvp45149	Traceback while Reverting the primary system as active
CSCvp49481	Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability
CSCvp55941	FILE RESUME BLOCK being randomly thrown causing access issues on files from SMB share.
CSCvp87623	Upload an update gives "update request entity too large" error when using CAC(HTTPS Client Certs)
CSCvp90847	Refresh Root CAs that SSL uses for resigning in FTD/FMC
CSCvp93468	Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability
CSCvq12070	Not able to establish more than 2 simultaneous ASDM sessions
CSCvq13442	When deleting context the ssh key-exchange goes to Default GLOBALLY!
CSCvq20910	Cisco Firepower 2100 Series Security Appliances ARP Denial of Service Vulnerability
CSCvq35440	Upgrade Enhancements to STRAP verification for anyconnect - Cisco VPN session replay vulnerability

Bug ID	Headline
CSCvq36042	lost heartbeat causing reload
CSCvq54034	WRL6 and WRL8 commit-id update in CCM Layer (sprint 65)
CSCvq56257	Cached malware disposition does not always expire as expected
CSCvq66092	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software BGP DoS
CSCvq70485	Slow "securityzones" REST API
CSCvq70775	FPR2100 FTD Standby unit leaking 9K blocks
CSCvq71217	High Disk Utilization due to mysql-server.err failing to rotate after CSCvn30118
CSCvq73534	Cisco ASA Software Kerberos Authentication Bypass Vulnerability
CSCvq73599	Cisco VPN session replay vulnerability : STRAP fix on ASA for SSL(OpenSSL 1.0.2) and SCEP proxy
CSCvq93640	WRL6 and WRL8 commit id update in CCM layer (sprint 67)
CSCvr07419	Cisco ASA and FTD Software IPv6 DNS Denial of Service Vulnerability
CSCvr09748	Cisco FXOS and FTD Software Command Line Interface Arbitrary File Read and Write Vuln
CSCvr11395	Only a subset of devices where deployed from a device group during scheduled deploy
CSCvr17735	SFDataCorrelator high CPU during SI update
CSCvr37502	libexpat Improper Parsing Denial of Service Vulnerability
CSCvr39556	Segfault in libclamav.so (in the context of SFDataCorrelator)
CSCvr49734	Cisco FXOS and UCS Manager Software CLI Command Injection Vulnerability
CSCvr55825	Cisco ASA and FTD Software Path Traversal Vulnerability
CSCvr63941	KP ASA diagnostic-cli channel stops functioning
CSCvr85295	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote
CSCvr86213	CD is required to ignore Cluster-Msg-Delivery-Confirmation in Cluster Node Release Lina State
CSCvr90768	FTD: Deployment through slow links may fail
CSCvr92327	ASA/FTD may traceback and reload in Thread Name 'PTHREAD-1533'
CSCvs12288	Snort unexpectedly exits with SSL policy enabled and debug_policy_all
CSCvs19968	Fix consoled from getting stuck and causing HA FTD policy deployment errors.

Bug ID	Headline
CSCvs33416	Upgrade Kernel to 4.14.158
CSCvs34844	pm process becomes randomly deadlocked when communicating with hardware.
CSCvs50459	Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability
CSCvs59487	Observed crash in KP device while upgrading to 99.14.1.64 image.
CSCvs60254	libxml2 xmlParseBalancedChunkMemoryRecover Memory Leak Vulnerability
CSCvs61701	DME process crash due to memory leak on Firepower 2100
CSCvs77334	FTD failover due to error "Inspection engine in other unit has failed due to snort and disk failure"
CSCvs84578	Upgrading FTD on 4100/9300 Platform to 6.2.3.15 prevents the FTD instance from booting up
CSCvs84713	Cannot SSH to the device after upgrading FTD on ASA55XX/ISA 3000/FTDv to 6.2.3.15 build 38
CSCvs87168	SNORT Fatal Error due to out of range interface ID
CSCvs94486	CSCvs59487 requires additional fix for resolution
CSCvs98311	FSIC Failure after upgrade from 6.2.3.15-38 > 6.2.3.16-29 in CC Mode
CSCvt03598	Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability
CSCvt15163	Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability
CSCvt39135	snort instances CPU spikes to >90% at low non-SSL traffic with SSL policy applied
CSCvt39299	6.2.3.15 to 6.4.0 upgrade broken for Series-3 Sensors
CSCvt80172	Supervisor software needs to be upgraded to address CVE-2017-11610
CSCvu30830	NGIPS sensor SSH broken due to bad CiscoSSH keywork in sshd_config file

Version 6.2.3.15 Resolved Issues

Table 62: Version 6.2.3.15 Resolved Issues

Bug ID	Headline
CSCve24102	GUI should allow max 256 addresses per DHCP pool
CSCvg49225	Canceling scheduled FXOS upgrade does not clear the event
CSCvg85687	Error messages seen on console when FXOS boots up

Bug ID	Headline
CSCvk43854	Cisco Firepower Threat Defense Detection Engine Policy Bypass Vulnerability
CSCvm64400	IKEv2: IKEv2-PROTO-2: Failed to allocate PSH from platform
CSCvm68648	review of CVE-2016-8858 (OpenSSH) on Firepower software
CSCvm82966	Linux Kernel 4.14 Vulnerabilities
CSCvn46390	Lina msglayer performance improvements: port Hotfix BO
CSCvn77125	FXOS: copy command should allow for wildcards to transfer multiple files
CSCvo29989	Cisco FirePower Threat Defense Information Disclosure Vulnerability
CSCvo47390	ASA traceback in thread SSH
CSCvo48838	Lina does not properly report the error for configuration line that is too long
CSCvo68184	management-only of diagnostic I/F on secondary FTD get disappeared
CSCvo68448	ASA report SFR module as 'Unresponsive' after reloading ASA module on 5585 platform
CSCvo85861	Propagate link-state not shown in FTD CLI
CSCvo86485	incorrect HTML <base> tag handling by Grammar Based Parser
CSCvo88762	FTD inline/transparent sends packets back through the ingress interface
CSCvo89224	FMC times out after 10 mins to fetch device list for deployment
CSCvo90998	LACPDUs should not be sent to snort for inline-set interfaces
CSCvp07616	[ciam] Python urllib Security Bypass Vulnerablity
CSCvp15176	FTD/ASA installed on firepower devices may report comm failure and assume itself as active/master.
CSCvp16536	ASA traceback and reload observed in Datapath due to SIP inspection.
CSCvp16618	URL inside HTML base tag is not rewritten after it is handled by GBP
CSCvp27263	Multiple ClamAV Vulnerabilities For Cisco Firepower Management Center for pre 6.5.0
CSCvp35141	ASA sends invalid redirect response for POST request
CSCvp35769	[ciam] Apache HTTP Server URL Normalization Denial of Service Vulnerability
CSCvp37779	FTD show tech from troubleshooting files incomplete
CSCvp46150	[ciam] GNU Wget Buffer Overflow Vulnerability
CSCvp48273	[ciam] Linux Kernel cipso_v4_validate Denial of Service Vulnerability

Bug ID	Headline
CSCvp49576	FTD Cluster traceback experienced when other unit leaves the Cluster
CSCvp53637	Flows are getting offloaded on inline-sets
CSCvp54261	Audit syslog for SFR module/7000/8000 devices uses TCP instead of UDP for syslog communication
CSCvp55880	Fail-Closed FTD passes packets through on Snort processes down
CSCvp55901	LINA traceback on ASA in HA Active Unit repeatedly
CSCvp58028	natd thread of nfm_exceptiond uses about 90% to 100% CPU time
CSCvp66559	Deploy fails on FTD HA due to exception when parsing big xml response
CSCvp67257	USGv6 Failures From Kernel Upgrade [3.10 to 4.14]
CSCvp67392	ASA/FTD HA Data Interface Heartbeat dropped due to Reverse Path Check
CSCvp70699	ASA Failover split brain (both units active) after rebooting a Firepower chassis
CSCvp72244	Evaluate Cisco 8000 series for CVE-2019-11815
CSCvp72488	Firepower: AMP for network connectivity failure after upgrading to 6.3.0.2+
CSCvp83437	serial console/SSH login using local account succeeds but immediately returns to login prompt
CSCvp97061	URL Filtering Shows All URLs as Uncategorized
CSCvp97799	Policy deploy failure 6.5.0-1148 post upgrade with CC mode with openSSL call during SSL pol Export
CSCvp97916	Executing 'failover' twice on active unit, clears interface configuration on standby unit
CSCvp98066	On reset CD not clearing its flags[parseFailoverReqIssued] which prevents further node join attempts
CSCvq00675	Linux Kernel sas_expander.c Race Condition Arbitrary Code Execution ...
CSCvq06790	Snort processes dump core with memory corruption on Series 3 devices
CSCvq13917	ADI does not learn VPN user logins anymore
CSCvq19525	Evaluation of sfims for TCP_SACK
CSCvq19641	Evaluation of Firepower 4k/9k Supervisor for TCP_SACK
CSCvq27010	Memory leak observed when ASA-SFR dataplane communication flaps
CSCvq32681	Fail to Wire configuration disabled for multiple interface-pair inline-sets during FTD upgrades
CSCvq33916	Linkdown between FP 4100 and switch when using 40gb bidi to 40/100 bidi

Bug ID	Headline
CSCvq39083	Security Intelligence does not drop HTTPS connections to blacklisted URLs when SSL policy is enabled
CSCvq44665	FTD/ASA : Traceback in Datapath with assert snp_tcp_intercept_assert_disabled
CSCvq54242	Warrning "There is an empty group in the source networks" in SSL policy
CSCvq56462	File policy not inspecting some malware document (.doc) and Adobe flash (.swf) files.
CSCvq57710	Firepower Primary Detection Engine process might terminated after Manager upgrade
CSCvq61651	URL DB download failure alerts on FMC; new URL DB updates not taking effect on FMC/FDM
CSCvq65092	Slow device related REST API calls
CSCvq98171	Unable to do Recovery using latest r241 images

Version 6.2.3.14 Resolved Issues

Table 63: Version 6.2.3.14 Resolved Issues

Bug ID	Headline
CSCvb15074	FMC health notifications for interfaces removed or added out-of-band get stuck
CSCvi63474	Unable to edit the system policy of a SFR module via ASDM after upgrading to 6.2.2
CSCvk69823	FlexConfig objects pushed to device in spite of no changes being made to that on either FMC or FTD
CSCvm70274	tcp proxy: ASA traceback on DATAPATH
CSCvn86777	Deployment on FTD with low memory results on interface nameif to be removed
CSCvo24145	ids_event_alerter high memory usage due to large firewall_rule_cache table
CSCvo33348	Mysql traffic on non standard port is not correctly classified
CSCvo33851	ngfwManager doesn't start if ngfw.properties is empty
CSCvo43679	FTD Lina traceback, due to packet looping in the system by normaliser
CSCvo50168	Audit Log Settings Failing Leading to being unable to edit System Settings
CSCvo60580	ASA traceback and reloads when issuing "show inventory" command
CSCvo60862	Internal Error when editing an Access Control Policy
CSCvo74745	cloud agent core after generating a large number of continuous URL lookups (>30M)
CSCvo90805	Cisco Firepower Management Center RSS Cross-Site Scripting Vulnerabilities

Bug ID	Headline
CSCvp16979	ssl and daq debug logs can't be enabled/disabled dynamically
CSCvp18878	ASA: Watchdog traceback in Datapath
CSCvp19549	FTD lina cored with Thread name: cli_xml_server
CSCvp24728	Random SGT tags added by FTD
CSCvp24787	(snort)File is not getting detected when going over HTTPS (SSL Resign)
CSCvp25583	FTD sets automatically metric 0 when we redistribute OSPF into BGP via FMC GUI.
CSCvp29692	FIPS mode gets disabled after rollback from a failed policy deploy
CSCvp33052	Firepower 8000 interfaces might flap due to unhandled resource temporarily unavailable issue
CSCvp43536	On upgraded FMC Device FXOS devices are shown dirty even after successful deployment.
CSCvp54634	Wrong rule matched when using ambiguous DND
CSCvp78197	Policy deployment remove and add back ospf neighbor
CSCvp81967	Slowness in loading Device Management page on FMC when there are over 500 managed devices
CSCvp82945	NAT policy apply failing with error duplicate
CSCvp96934	Ensure Error Message with Dup NATs Is Clear and Actionable
CSCvq13917	6.2.3.13 ADI does not learn VPN user logins anymore
CSCvq34224	Firepower Primary Detection Engine process terminated after Manager upgrade

Version 6.2.3.13 Resolved Issues

Table 64: Version 6.2.3.13 Resolved Issues

Bug ID	Headline
CSCve13816	MEMCACHED software needs to be upgraded to address several security vulnerabilities
CSCvf83160	Traceback on Thread Name: DATAPATH-2-1785
CSCvg01007	https pdf attachment issues
CSCvg74603	eStreamer archive events are not pruned correctly by diskmanager
CSCvi16224	snmp-server host command for SNMPv3 doesn't apply properly when deploy ASAv VM on NFVIS (KVM) system

Bug ID	Headline
CSCvi32569	Excessive logging in mysql-server.err log causes huge log files in FTD
CSCvi59887	OSPF Route may become stale and stuck in the routing table after failover events
CSCvj49623	Memory Leak In Smart Licensing
CSCvk14242	sfstunnel process in FTD is holding large cloud db files that are already deleted
CSCvk26612	"default Keyring's certificate is invalid, reason: expired" health alert
CSCvk29263	SSH session stuck after committing changes within a Configure Session.
CSCvk30739	ASA CP core pinning leads to exhaustion of core-local blocks
CSCvk44166	Cisco ASA and FTD TCP Proxy Denial of Service Vulnerability
CSCvk72958	Qos applied on interfaces doesn't work.
CSCvm00066	ASA is stuck on "reading from flash" for several hours
CSCvm08769	Standby unit sending BFD packets with active unit IP, causing BGP neighborship to fail.
CSCvm17985	Initiating write net command with management access for BVI interfaces does not succeed
CSCvm27111	FTD Lina traceback while removing OSPF configuration.
CSCvm36362	Route tracking failure
CSCvm80779	ASA not inspecting H323 H225
CSCvm82290	ASA core blocks depleted when host unreachable in IRB configuration
CSCvm85257	Spin lock traceback when changing vpn-mode with traffic
CSCvm86008	Policy Deployment: Delta config doesn't get copied to running config, LINA config remains unchanged
CSCvm88294	High Disk utilization due to partition force drain not occurring
CSCvn22833	ADI process fails to start on ASA on Firepower 4100
CSCvn30108	The 'show memory' CLI output is incorrect on ASAv
CSCvn30393	ASA Traceback in emweb/https during Anyconnect Auth/DAP assessment
CSCvn31347	ACL Unable to configure an ACL after access-group configuration error
CSCvn32620	IKEv2 Failed to obtain an Other VPN license
CSCvn34246	Loading AC policy editor takes too long, needs loading indicator
CSCvn38453	ASA: Not able to load Quovadis Root Certificate as trustpoint when FIPS is enabled

Bug ID	Headline
CSCvn45750	FMC Audit Logs will only display Admin and System as owners when deploying to 3D devices -GUI/SYSLOG
CSCvn50320	Firepower MySQL Server : Oracle MySQL October 2018 Critical Patch Update
CSCvn55007	DTLS fails after rekey
CSCvn57284	Unsupported EC curve x25519 on FTD
CSCvn66248	Configuring "boot config" has no effect if file was modified off-box and copied back on
CSCvn67137	ASA5506 may slowly leak memory when using NetFlow
CSCvn68527	FPR21xx: AnyConnect assigned addresses not marked allocated on Standby
CSCvn71592	After FMC reboot, intrusion events generated by Snort are not sent to FMC and show up in webGUI
CSCvn73962	ASA 5585 9.8.3.14 traceback in Datapath with ipsec
CSCvn76829	ASA as an SSL Client Memory Leak in Handshake Error path
CSCvn77248	Cisco Secure Boot Hardware Tampering Vulnerability
CSCvn78597	Firepower block page not displayed on MS IE11 and Edge for HTTPS blocked sites when proxy is enabled
CSCvn78674	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvn78870	ASA Multicontext traceback and reload due to allocate-interface out of range command
CSCvn94100	"Process Name: lina" | ASA traceback caused by Netflow
CSCvn95711	Traceback on Thread Name: Unicorn Admin Handler after adding protocol to IKEV2 ipsec-proposal
CSCvn96898	Memory Leak in DMA_Pool in binsize 1024 with SCP download
CSCvn97591	Packet Tracer fails with "ERROR: TRACER: NP failed tracing packet", with circular asp drop captures
CSCvo04444	Ikev2 tunnel creation fails
CSCvo06216	Support more than 255 chars for Split DNS-commit issue in hanover for CSCuz22961
CSCvo11406	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvo11416	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvo13497	Unable to remove access-list with 'log default' keyword

Bug ID	Headline
CSCvo15484	Unable to delete User IOC if user info is inconsistent between mysql & sybase - part fix
CSCvo17033	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvo23222	AnyConnect session rejected due to resource issue in multi context deployments
CSCvo27109	Standby may enter reboot loop upon upgrading to 9.6(4)20 from 9.6(4)6
CSCvo42174	ASA IPSec VPN EAP Fails to Load Valid Certificate in PKI
CSCvo45093	Validation Check when two objects with different name but same network is used in route without ECMP
CSCvo45209	FTD-CLUSTER:Adding new unit in cluster can cause traffic drop
CSCvo51265	SCP large file transfer to the box result in a traceback
CSCvo55151	crypto ipsec inner-routing-lookup should not be allowed to be configured with VTI present
CSCvo56616	Deployment times out in some cases resulting in non-terminated AQ
CSCvo56836	SCALE: with 500+ devices, UMS causes the UI to hang, especially during deploy
CSCvo58847	Enhancement to address high IKE CPU seen due to tunnel replace scenario
CSCvo60627	Policy failing to deploy after adding new cluster unit to setup
CSCvo62060	Telemetry not sent when FMC managing lots of devices
CSCvo66534	Traceback and reload citing Datapath as affected thread
CSCvo70866	SGT tag shows untagged in server packet for every client packet with SGT tag with some value
CSCvo72179	For SMB, remote storage configuration should allow configuring version string with dot(.)
CSCvo72232	ERR_SSL_BAD_RECORD_MAC_ALERT or SSL_ERROR_BAD_MAC_ALERT in the browser
CSCvo74350	ASA may traceback and reload. Potentially related to WebVPN traffic
CSCvo76727	No warning about possible policy deployment failure when in route is more than one object
CSCvo81073	Unable to load Device Management page or upgrade FMC due to missing NGFWHA EO
CSCvo83574	Device goes into a bad state when switching the inline set from TAP mode
CSCvo87930	HTTP with ipv6 using w3m is failing

Bug ID	Headline
CSCvo88188	SSL rules with App-ID conditions can limit decryption capability
CSCvo88306	NAT rules can get applied in the wrong order when you have duplicate rules
CSCvo93872	Memory leak while inspecting GTP traffic
CSCvo94486	Snort process exits while processing Security Intelligence.
CSCvp21837	Allow FTDs to perform URL lookups directly without having to go through the FMC
CSCvp42398	Series 3 8250: Upgrade 6.4.0-87 failed at 999_finish/989_flip_mbr.sh
CSCvp54634	Wrong rule matched when using ambiguous DND

Version 6.2.3.12 Resolved Issues

Table 65: Version 6.2.3.12 Resolved Issues

Bug ID	Headline
CSCvh26064	Unable to use "Change Reconciliation" on 7000/8000 sensors
CSCvj82652	Deployment changes are not pushed to the device due to disk0 mounted on read-only
CSCvk56988	Cisco ClamAV MEW unpacker Denial of Service Vulnerability
CSCvm16724	FXOS ASA/FTD needs means to poll Internal-data interface counters
CSCvm24210	One of the two schedule tasks running on same timestamp fails if they both access the same file
CSCvm35373	Pruner process fails to start due to configuration
CSCvm40545	downgrading FTD twice in a row without updating in between results in wrong lina version
CSCvn07452	712x devices become unstable when switching inline set from TAP to inline
CSCvn09383	Manual URL lookup returns Uncategorized if same URL is entered second time without "www." part
CSCvn38189	SFDataCorrelator is not restarted after backup scripts died
CSCvn46358	overloading of the lina msglyr infra due to the sending of VPN status messages
CSCvn49854	Subsequent HTTP requests not retrieving URL and XFF
CSCvn67570	amp-stunnel.conf does not point to correct amp cloud server post FMC upgrade
CSCvn67888	Object added using REST API result in policy deploy failure

Bug ID	Headline
CSCvn72570	Cisco ASA Software and FTD Software VPN SAML Authentication Bypass Vulnerability
CSCvn73848	Snort sessions are timing out earlier than configured idle timeouts.
CSCvn74112	FTDv does not have configuration on initial bringup with mix of vmxnet3 and ixgbevf interfaces
CSCvn75368	FPR platform IPsec VPN goes down intermittently
CSCvn78593	Control-plane ACL doesn't work correctly on FTD
CSCvn82895	Diskmanager may not track all event files
CSCvn87965	While associating FMC with TG account, FMC should not redirect users to TG console
CSCvn99712	Cisco Firepower Management Center Persistent Cross-Site Scripting Vulnerability
CSCvo02097	Upgrading ASA cluster to 9.10.1.7 cause traceback
CSCvo12057	DHCPRelay does not consume DHCP Offer packet with Unicast flag
CSCvo15545	nfm-burnin.sh system validation test fails for latest NFM release
CSCvo17775	EIGRP breaks when new sub-interface is added and "mac-address auto" is enabled
CSCvo20847	Active FTP fails through Cluster due to xlate allocation corruption upon sync
CSCvo23150	excessive DB queries for user identities causes slowness in user session processing.
CSCvo27164	SFDataCorrelator logs inappropriate "Resuming storage of old events" messages
CSCvo29973	ssl rules with cipher suite conditions can cause unneeded tls 1.3 downgrade
CSCvo31353	SSL connections may fail when URL categories are used and certificate common name doesn't match
CSCvo31953	Memory leak in SFDataCorelator process
CSCvo32329	Deleted realm is causing many user_id's loaded into user_identities cache
CSCvo38051	segfault in ctm_ipsec_pfkey_parse_msg at ctm_ipsec_pfkey.c:602
CSCvo39052	FSIC error after enable the CC mode
CSCvo39094	Delay/Longer processing time to insert policy deploy task after selecting the device for deploy
CSCvo40210	Update Talos RSS feed in dashboard widget
CSCvo43693	FTD HA creation fails due to multiple files modules*.tgz and vdb*.tgz being transferred from FMC
CSCvo44064	aggressive downgrade action is taken when url look up is pending due to no sni

Bug ID	Headline
CSCvo47562	VPN sessions failing due to PKI handles not freed during rekeys
CSCvo50230	SSL Connections to uncategorized URLs may fail repeatedly
CSCvo54799	ssh to device fails due to corrupted devpts entry in fstab
CSCvo55203	Registered devices do not appear in the Device Management page
CSCvo55282	Policy deploy fails when user is able to enter invalid inline port range in AC Rule accidentally
CSCvo56675	ASA or FTD traceback and reload due to failover state change or xlates cleared
CSCvo56895	Some donut charts on the Context Explorer failing to load
CSCvo61091	eStreamer memory and CPU grow when sending NAP policy metadata
CSCvo62031	ASA Traceback and reload while running IKE Debug
CSCvo63240	Smart Tunnel bookmarks don't work after upgrade giving certificate error
CSCvo66920	Enhancement: add counter for Duplicate remote proxy
CSCvo67454	Invalid port range object causes AC policy deploy to fail
CSCvo72462	Do not decrypt rule causes traffic interruptions.

Version 6.2.3.11 Resolved Issues

Table 66: Version 6.2.3.11 Resolved Issues

Bug ID	Headline
CSCuz28594	Diskmanager - critical alert on /var/storage due to disk manager not pruning till 99%
CSCvi54162	"ha-replace" action not working when peer not present
CSCvi55841	errors saving blacklist config file are not detected
CSCvi62112	Blocking BPDU via FlexConfig on FTD Transparent causes deployment and registration issues
CSCvk06386	FTD Files are Allowed Through Multiple Pre-existing Connections Despite the File Policy Verdict
CSCvm14875	Large number of stale cloudconfig EO causing performance issues
CSCvm58799	During deploy, if multiple Snorts are not responding, recovery takes too long
CSCvm60039	Custom DNS security intelligence feed fail to download intermittently
CSCvm96339	/dev/root partition will fill to 100% due to archive_cache_seed.sensor file

Bug ID	Headline
CSCvn10634	Files are not detected in HTTP flows when there's an Out of Order (ACK before actual data)
CSCvn16102	Diskmanager file capture data not increasing for hours at a time
CSCvn17347	Traceback and reload when displaying CPU profiling results
CSCvn38082	FMC should identify and recover from mongo corruption
CSCvn41903	Snort reload fails and causes restart due to dce2-mem-reloader memory adjustments taking too long
CSCvn47788	UI validation fails on a valid hostname IP for Audit Log Host in Firepower platform setting policy
CSCvn48739	FTD show tech taken from CLISH mode and in troubleshoot may be truncated
CSCvn53145	Policy deploy throws "Variable set has invalid execulded values"
CSCvn69019	usernames with single quotes are not written into user_ip_map file
CSCvn72683	FMC webGUI device management page loading time is too long around 45s with 25s fetching license
CSCvn73848	Snort sessions are timing out earlier than configured idle timeouts.
CSCvo00887	ssl client hello should not be modified if "Do Not Decrypt" rule will be the only possible verdict
CSCvo03186	Domain page in Firepower Management Center takes long time to load
CSCvo03808	Deploy from FMC fails due to OOM with no indication of why
CSCvo11077	Memory leak found in IPsec when we establish and terminate a new IKEv1 tunnel.
CSCvo39052	FSIC error after enable the CC mode

Version 6.2.3.10 Resolved Issues

Table 67: Version 6.2.3.10 Resolved Issues

Bug ID	Headline
CSCuu67159	ASA: traceback in DATAPATH-2-1157
CSCva62256	Appliance status widget taking too long with 500 sensors
CSCvf81672	ASA Routes flushed after failover when etherchannel fails
CSCvg40735	GTP inspection may spike cpu usage

Bug ID	Headline
CSCvg56122	SSL handshake fails with large certificate chain size
CSCvi09811	Traceback in DATAPATH, assertion "0" failed: file "./snp_cluster_transport.h", line 480
CSCvi28763	FTD Platform Settings: change default DH-group in SSL custom settings to 2
CSCvi34533	Cannot save modification in Access List if there's no SNMPv3 user defined
CSCvi71622	Traceback in DATAPATH on standby FTD
CSCvi97028	fmc GUI too slow when configuring unreachable syslog server
CSCvj01704	ASA is getting traceback with reboot only on ASA 5585-X after shutdown SFR module
CSCvj65154	FMC failing to communicate with SSM when proxy password contains @ character
CSCvj74643	Enabling Use CAC authentication and authorization on AD breaks RADIUS when changed.
CSCvj87287	simultaneous flood of REST-API requests to FMC results in inaccessibility
CSCvj89445	Inconsistent deployment status on GUI
CSCvj97229	'User Name Template' should be required filed for external authentication object for CAC in FMC
CSCvk18330	Active FTP Data transfers fail with FTP inspection and NAT
CSCvk19946	Sftunnel service broken due to cache archive data flooding
CSCvk39339	Unable to run the scheduling report generation on Japanese FMC
CSCvk40964	Deployment of empty interface config to device lead to traffic outage
CSCvk46038	ERROR: The entitlement is already acquired while the configuration is cached.
CSCvk50815	GTP inspection should not process TCP packets
CSCvk55634	Random policy deployment failure due to stuck notification for policy deployment
CSCvm24706	GTP delete bearer request is being dropped
CSCvm28730	ASA/FTD-LINA Tracebacks observed while getting CPU Profiling information
CSCvm33553	Clock drift causes Heartbeat misses from ndclientd
CSCvm46014	Copy config should not fail if standby device is corrupted on FTD HA
CSCvm55091	HA failed primary unit shows active while "No Switchover" status on FP platforms
CSCvm59983	The file-size directive returns invalid input error and breaks the captures from clish
CSCvm67273	ASA: Memory leak due to PC alloc_fo_ipsec_info_buffer_ver_1+136

Bug ID	Headline
CSCvm87315	FTD registration can fail because of TID in RegistrationTR::addToLamplighter
CSCvm88004	SSH Service on ASA echoes back each typed/pasted character in its own packet
CSCvn05797	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCvn06618	On LINA config rollback the startup-config is being merged with the default running
CSCvn09322	FTD device rebooted after taking Active State for less than 5 minutes
CSCvn09367	Prevent administrators from installing CXSC module on ASA 5500-X
CSCvn15757	ASA may traceback due to SCTP traffic inspection without NULL check
CSCvn16489	AMP Dynamic Analysis's clouds should be tracked separately for submission rates.
CSCvn19823	ASA : Failed SSL connection not getting deleted and depleting DMA memory
CSCvn20411	Device management page never loads and times out after an error message
CSCvn21899	Firepower: Disable TLS 1.0 permanently for SFTunnel communication
CSCvn23224	FTD-HA forming failed with SNMP configured
CSCvn23254	SNMPv2 pulls empty ifHCInOctets value if Nameif is configured on the interface
CSCvn23701	Deployment failed with - ftp_telnet.conf(4) => Invalid keyword 'memcap' for 'global' configuration.
CSCvn24756	Security intelligence feature can falsely block IP addresses (URL block)
CSCvn30118	mysql-server.err file is not fully deleted and keeps consuming Firepower disk space
CSCvn32657	ASA traceback when removing interface configuration used in call-home
CSCvn33943	Standby node traceback in wccp_int_statechange() with HA configuration sync
CSCvn36393	exclude tls1.0 and tls1.1 in stunnel config file
CSCvn37829	ASA should allow GCM(SSL) connections to use DMA_ALT1 when primary DMA pool is exhausted
CSCvn38010	Let remove_peers.pl scripts bailout when it is run in FTD HA setup
CSCvn43798	Deleting a domain fails to delete some objects if a Realm is in that domain
CSCvn44201	ASA discards OSPF hello packets with LLS TLVs sent from a neighbor running on IOS XE 16.5.1 or later
CSCvn46474	FP2120 FTD went unresponsive after power outage
CSCvn47599	RA VPN + SAML authentication causes 2 authorization requests against the RADIUS server

Bug ID	Headline
CSCvn47800	ASA stops authenticating new AnyConnect connections due to fiber exhaustion
CSCvn48790	Slave node kicked out of cluster if SI task running during policy apply
CSCvn49561	update FireAMP curl calls to use CA path
CSCvn53732	Modified SSL connections that are not decrypted should be closed
CSCvn54347	Entitlement release error in Failover switchover or disband on fp2100/1000 KP/WM
CSCvn56095	selective acking not happening with SSL crypto hardware offload
CSCvn61662	ASA 5500-X may reload without crashinfo written due to CXSC module continuously reloading
CSCvn62787	To support multiple retry on devcmd failure to CRUZ during flow table configuration update.
CSCvn63549	Python pop3lib apop() Method Denial of Service Vulnerability
CSCvn64418	ISA3000 interop issue with Nokia 7705 router
CSCvn65575	Snort termination can occur when active authentication is enabled and an SSL policy is not enabled
CSCvn68145	Snort Unexpectedly Exiting when using SSL decryption
CSCvn69213	ASA traceback and reload due to multiple threads waiting for the same lock - watchdog
CSCvn76763	Two versions of messages-X-SNAPSHOT.jar in FTD causes deployment failure
CSCvn77636	ASA/webvpn: FF and Chrome: Bookmark is not rendered with Grammar Based Parser
CSCvn93499	Snort/Data Correlator can crash while exiting on Firepower 4100/9300 devices.

Version 6.2.3.9 Resolved Issues

Note Version 6.2.3.9 replaces Version 6.2.3.8, which was removed from the Cisco Support & Download site on 2019-01-07. The issues listed in Version 6.2.3.8 Resolved Issues, on page 88 are also fixed in Version 6.2.3.9.

Table 68: Version 6.2.3.9 Resolved Issues

Bug ID	Headline
CSCvn82378	Traffic through ASA/FTD might stop passing upon upgrading FMC to 6.2.3.8-51

Version 6.2.3.8 Resolved Issues

Note Version 6.2.3.8 was removed from the Cisco Support & Download site on 2019-01-07. This version is replaced by Version 6.2.3.9. The issues listed here are also fixed in Version 6.2.3.9.

Table 69: Version 6.2.3.8 Resolved Issues

Bug ID	Headline
CSCuy90400	Enhancement to support extended master secret in SSL
CSCvd03903	Firepower is affected by TCP Dump Vulnerability
CSCvd12834	FP Audit Logs do not log passed and failed SSH authentication attempts
CSCve29930	Cannot configure LOM on secondary FMC from HA pair
CSCvf20266	Firepower Management Center System Configuration Email Notification Password Length Too Short
CSCvf57596	After policy deploy has failed, ActionQueueScrape process did not exit
CSCvg10718	Correlation Policy With Traffic Profiles Doesn't Work
CSCvg36254	FTD Diagnostic Interface does Proxy ARP for br1 management subnet
CSCvh13022	SSL decryption is bypassed when client hello payload is < 6 bytes
CSCvh14743	IKEv2 MOBIKE session with Strongswan/3rd party client fails due to DPD with NAT detection payload.
CSCvi82404	Updating device can fail in 800_post/755_reapply_sensor_policy.pl
CSCvj67258	Change 2-tuple and 4-tuple hash table to lockless
CSCvj97213	ASA IKEv2 capture type isakmp is saving corrupted packets or is missing packets
CSCvk20292	FMC in HA mode, Health Policy is missing from Standby FMC when Active FMC failed
CSCvk30775	ENH: Addition of 'show fragment' to 'show tech' output
CSCvk30779	ENH: Addition of 'show ipv6 interface' to 'show tech' output
CSCvk30783	ENH: Addition of 'show aaa-server' to 'show tech' output
CSCvk33923	High disk usage after deleting managed FTD device from FMC
CSCvk51181	FTD IPV6 traffic outage after interface edit and deployment part 1/2

Bug ID	Headline
CSCvk62871	Firepower 2100 FTP Client in passive mode is not able to establish data channel with the Server
CSCvk72192	"Free memory" in "show memory" output is wrong as it includes memory utilisation due to overhead
CSCvm10968	CVE-2018-5391 Remote denial of service via improper IP fragment handling
CSCvm43975	Cisco ASA and FTD Denial of Service or High CPU due to SIP inspection Vulnerability
CSCvm47713	SSL policy disallows viewing of PDF on *.lightning.force.com when Chrome browser is used
CSCvm49283	Make Object Group Search Threshold disabled by default, and configurable. Causes outages.
CSCvm53531	Cisco Adaptive Security Appliance Software Privilege Escalation Vulnerability
CSCvm56371	ASA wrongly removes dACL for all Anyconnect clients which has the same dACL attached
CSCvm56719	Traceback high availability standby unit Thread Name: vpnfol_thread_msg
CSCvm60361	SSH public key auth not working on FTD on 5500
CSCvm62708	SSL connections negotiating NPN can fail with Do Not Decrypt SSL policy
CSCvm64230	verify_firmwareRunning() return code not checked
CSCvm65725	ASA kerberos auth fails switch to TCP if server has response too big (ERR_RESPONSE_TOO_BIG)
CSCvm67704	Memory Leak when handling KRB_ERR_RESPONSE_TOO_BIG (leak in krb5_extract_ticket)
CSCvm76760	FMC - External RADIUS authentication - Text in the "Shell Access Filter" field is not validated
CSCvm78449	Unable to modify access control license entry with log default command
CSCvm80933	ssl policy can match incorrect rule when server uses a cert with wildcard common name
CSCvm81052	local malware detection updates not downloading to FMC due to invalid certificate chain
CSCvm82966	Linux Kernel 3.10.107 Vulnerabilities
CSCvm91280	Intrusion Events Report Date, Hour Of Day, Day Of Week comes in UTC and Time comes in local timezone
CSCvm95669	ASA 5506 %Error copying http://x.x.x.x/asasfr-5500x-boot-6.2.3-4.img(No space left on device)

Bug ID	Headline
CSCvn03507	"set ip next-hop verify-availability" is removed from route-maps configuration with next deployment
CSCvn03966	FTD - When "object-group-search" is pushed through flexconfig, all ACLs get deleted causing outage.
CSCvn08146	Missing audit detail for changes to x509 certificates and keys
CSCvn09640	FTD: Need ability to trust ethertype ACLs from the parser. Need to allow BPDU to pass through
CSCvn09808	Captive portal bltd process fails on startup due to socket permission error
CSCvn11219	Policy deployment failed with error message "Not a directory"
CSCvn31753	ssl inspection policy may cause SEC_ERROR_REUSED_ISSUER_AND_SERIAL browser error

Version 6.2.3.7 Resolved Issues

Table 70: Version 6.2.3.7 Resolved Issues

Bug ID	Headline
CSCve34221	Internal server error seen on the UI when we enable CC mode
CSCvf54682	sudo : CVE-2017-1000368 : Sudo Parsed tty Information Privilege Escalation Vulnerability
CSCvh14743	IKEv2 MOBIKE session with Strongswan/3rd party client fails due to DPD with NAT detection payload.
CSCvi97500	AMP Cloud event on Firepower Management Center are seen with different file types
CSCvj14631	Appliance Information Widget shows IPv4 Address disabled if mgmt interface is not eth0
CSCvj58342	Multicast dropped after deleting a security context
CSCvj65064	Firepower 2100: Port-Channel down notification delayed
CSCvj67258	Change 2-tuple and 4-tuple hash table to lockless
CSCvj76858	Policy deployment take long time ~4 hours
CSCvj91795	SSL default policy action is taken when URL category lookup is pending
CSCvj97213	ASA IKEv2 capture type isakmp is saving corrupted packets or is missing packets
CSCvj98662	linux hotfix layer directory reorganisation

Bug ID	Headline
CSCvk18330	Active FTP Data transfers fail with FTP inspection and NAT
CSCvk30779	ENH: Addition of `show ipv6 interface` to `show tech` output
CSCvk31035	KVM (FTD): Mapping web server through outside not working consistent with other platforms
CSCvk33023	Policy deployment failure on Firepower module in cluster or failover
CSCvk48389	`[Error: Timed out communicating with DME]` when attempting to upgrade
CSCvk56513	Tor not blocked when traffic is passed through proxy.
CSCvk59260	On slower networks deployement may fail with Resource temporarily unavailable exception
CSCvk66529	FTD on FPR 9300 corrupts TCP headers with pre-filter enabled
CSCvk66771	The CPU profiler stops running without having hit the threshold and without collecting any samples.
CSCvk72192	show memory output shows wrong memory
CSCvk76146	Few devices /ngfw partition on 41xx shows 39GB whereas other shows 100 GB
CSCvm03931	software update downloads by Firepower failing due to newer CA certificates not being present
CSCvm04237	BusyBox `huft_build` Function Denial of Service Vulnerability
CSCvm05464	CVE-2018-5391 Remote denial of service via improper IP fragment handling
CSCvm08500	ASA cmd validation fails when deletion of NAT rule description includes Czech/Slovak characters
CSCvm09040	Resumption attempts for sessions using tickets and known-key action use full handshake
CSCvm19948	ssl connections without SNI could hit incorrect ssl rule
CSCvm32256	Slave unit fails to join FTD cluster when it is in disabled state
CSCvm32613	Format of syslog messages have changed after an update FMC 6.2.3.3 to 6.2.3.4
CSCvm43975	Cisco ASA and FTD Denial of Service or High CPU due to SIP inspection Vulnerability
CSCvm47595	FMC displays connections matching incorrect access control policy when not using SSL Policy
CSCvm49283	Make Object Group Search Threshold disabled by default, and configurable. Causes outages.
CSCvm51395	access control policy deploy fails in fwrulechecker due to memory limit

Bug ID	Headline
CSCvm56371	ASA wrongly removes dACL for all Anyconnect clients which has the same dACL attached
CSCvm56719	Traceback high availability standby unit Thread Name: `vpnfol_thread_msg`
CSCvm56851	eStreamer repeatedly exits after error deserializing File event or FireAMP event
CSCvm58672	Unable to deploy SSL policy while SSL Hardware offload feature is enabled
CSCvm60468	Linux Kernel `yurex_read` Privilege Escalation Vulnerability
CSCvm60548	Security Intelligence synchronization tasks fail
CSCvm60791	Linux Kernel `alarm_timer_nsleep()` Function Integer Overflow Vulnerab ...
CSCvm64255	SFNotificationd fails to stop
CSCvm65725	ASA kerberos auth fails switch to TCP if server has response too big `(ERR_RESPONSE_TOO_BIG)`
CSCvm67184	Audit Syslog messages are sent without User information
CSCvm67316	ASA: Add additional IKEv2/IPSec debugging for CSCvm70848
CSCvm67704	Memory Leak when handling `KRB_ERR_RESPONSE_TOO_BIG (leak in krb5_extract_ticket )`
CSCvm68467	Event alerting process CPU usage delays deployment on busy Firepower 2100
CSCvm71378	Policy Deployment failing due to NAT Rule
CSCvm78449	Unable to modify access control license entry with log default command
CSCvm80874	ASAv/FP2100 Smart Licensing - Unable to register/renew license
CSCvm82492	Snort process taking a long time to exit impacting traffic.
CSCvm82930	FTD: SSH to ASA Data interface fails if overlapping NAT statement is configured
CSCvm96634	Final stage of policy deployment is audit-logged under admin instead of current user
CSCvm96916	FMC is randomly sending strong-encryption-disable to ASA

Version 6.2.3.6 Resolved Issues

Table 71: Version 6.2.3.6 Resolved Issues

Bug ID	Headline
CSCux69220	WebVPN 'enable intf' with DHCP , CLI missing when ASA boot

Bug ID	Headline
CSCve95403	ASA boot loop caused by logs sent after FIPS boot test
CSCvf85831	asdm displays error uploading image
CSCvh16414	Health Monitoring can incorrectly show CPU on FTD as 100% or 150%
CSCvh69117	SFDataCorrelator log spam "Received an unknown event type"
CSCvh98781	ASA/FTD Deployment ERROR 'Management interface is not allowed as Data is in use by this instance'
CSCvi13054	scheduled rule recommendations update fails with "Attempted to store stale object"
CSCvi48170	ASA 9.4.4.8, SNMP causing slow memory leak
CSCvi71761	FTD cli prompt is stuck on Firepower 9300
CSCvi77340	race condition results in user id REST API not functioning
CSCvi90633	Edit GUI language on ASDM AC downloads but ignores the change FPR-21XX
CSCvi98909	RTP packets not matching the rule in AC policy
CSCvj42269	ASA 9.8.2 Receiving syslog 321006 reporting System Memory as 101%
CSCvj44032	snort premature connection closure during TCP 4-way teardown
CSCvj47256	ASA SIP and Skinny sessions drop, when two subsequent failovers take place
CSCvj67776	clear crypto ipsec ikev2 commands not replicated to standby
CSCvj72309	FTD does not send Marker for End-of-RIB after a BGP Graceful Restart
CSCvk04592	Flows get stuck in lina conn table in half-closed state
CSCvk12076	AnyConnect client profile doesn't show under group-policy not assigned under a connection profile.
CSCvk14768	ASA traceback with Thread Name: DATAPATH-1-2325
CSCvk23483	Elastic timeout not taking effect and enforcing 600 sec timeout
CSCvk24297	IKEv2 RA with EAP fails due to Windows 10 version 1803 IKEv2 fragmentation feature enabled.
CSCvk34648	Firepower 2100 tunnel flap at data rekey with high throughput Lan-to-Lan VPN traffic
CSCvk36087	When logging into the ASA via ASDM, syslog 611101 shows IP as 0.0.0.0 as remote IP
CSCvk36733	mac address is flapping on huasan switch when asa etherchannel is configued with active mode
CSCvk38176	Traceback and reload due to GTP inspection and Failover

Bug ID	Headline
CSCvk42473	QoS rule evaluation does not re-evaluate flows when applications change
CSCvk43865	Traceback: ASA 9.8.2.28 while doing mutex lock
CSCvk52667	FDM - Deployment is failing after latest SRU update in 6.2.3-83 build.
CSCvk62896	ASA IKEv2 crash while deleting SAs
CSCvk66722	Configuring DHCP option 'false' causes DHCP configuration to be not visible from GUI
CSCvk67239	ASA traceback and reload in "Thread Name: Logger Page fault: Address not mapped"
CSCvk68772	FMC UI not accessible if you enable client certificate and then upgrade
CSCvk68809	No soft link for ca-cert.pem file if you upgrade FMC from 5.4.0
CSCvk70676	Clientless webvpn fails when ASA sends HTTP as a message-body
CSCvk72652	FMC does not deploy 'crypto ikev1 am-disable' when aggressive mode is to be disabled
CSCvk74461	LDAP groups download but are not available in GUI
CSCvk76160	Unable to restore on KP 6.2.2.2 using FDM
CSCvk76547	IPS rule with flow established not blocking when retransmitted TCP handshake packets
CSCvm01396	Firepower block page not displayed on browser with proxy settings
CSCvm05821	Sensitive Data Detection being enabled automatically during SRU update
CSCvm07458	Using EEM to track VPN connection events may cause traceback and reload
CSCvm07643	FTD 6.2-Intrusion Events not displaying src and dst port
CSCvm09624	Protocol not updated based on AppID when enforcing IPS rules
CSCvm11389	Small percentage of ECDHE connections fail
CSCvm11714	EIGRP authentication key issue when using special character "&"
CSCvm15880	FPR 9k ASA cluster multicon mode/vpn-mode distribute causes a reboot-loop if transparent mode conf
CSCvm19585	Smart License getting deregistered after upgrade to 6.2.3.5.
CSCvm23370	ASA: Memory leak due to PC cssls_get_crypto_ctxt
CSCvm25972	ASA Traceback: Thread Name NIC Status Poll.
CSCvm26004	Incorrect calculation of AAB in ASA causes random AAB invocations.
CSCvm29973	False positive for DNS SI events!
CSCvm44905	ssl inspection may continue processing a flow without flow information

Bug ID	Headline
CSCvm56019	Cisco Adaptive Security Appliance WebVPN - VPN not connecting through Browser

Version 6.2.3.5 Resolved Issues

Table 72: Version 6.2.3.5 Resolved Issues

Bug ID	Headline
CSCvb19750	Cisco Firepower Management Center Cross-Site Request Forgery Vulnerability
CSCve39071	Option to disable attempts to connect to the ThreatGRID cloud
CSCve85565	Traceback when syslog sent over VPN tunnel
CSCvg33300	Unable to modify Integer Host Attributes after creating them
CSCvg51412	Unable to establish a estreamer sftunnel between managed device and estreamer client
CSCvg54724	Firepower Dynamic Analysis Association Only Redirects to US address
CSCvg75144	All apps matching the filter deletes all objects
CSCvg91631	URL Reputation shows high risk or Unknown in Encore
CSCvg94363	Prefix List "le 32" does not work on Firepower Threat Defense
CSCvh21219	"set ip next-hop verify-availability" is removed from PBR configuration with next deployment
CSCvh89017	Configure user add command does not accept numeric user
CSCvi01312	webvpn: multiple rendering issues on Confluence and Jira applications
CSCvi31540	Traceback and reload with 'show tech' on ASA with No Payload Encryption (NPE)
CSCvi34164	ASA does not send 104001 and 104002 messages to TCP/UDP syslog
CSCvi37644	PKI:- ASA fails to process CRL's with error "Add CA req to pool failed. Pool full."
CSCvi45989	Query Cisco CSI for Unknown URLs option being reset by ASA managed by ASDM (Regression)
CSCvi51370	race condition can result in syslog alerts without rule messages
CSCvi53708	ASA NAT position discrepancy between CLI and REST-API causing REST to delete wrong config
CSCvi69343	ids_event_processor leaks memory when resetting communications
CSCvi69356	SFDataCorrelator reports "Invalid column value name" error-eStreamer does not work on managed device

Bug ID	Headline
CSCvi76808	File detection failing for encrypted SMTP TLS with Decrypt - Known Key SSL rule action
CSCvi79691	LDAP over SSL crypto engine error
CSCvi79999	256 Byte block leak observed due to ARP traffic when using VTI
CSCvi85382	ASA5515 Low DMA memory when ASA-IC-6GE-SFP-A module is installed
CSCvi93500	snort's handling of x-forward-for-like headers is incorrect when there are multiple proxies
CSCvi94239	IDSEventAlerter log spam "Unable to get SSL certificate fingerprint"
CSCvi96442	Slave unit drops UDP/500 and IPSec packets for S2S instead of redirecting to Master
CSCvi97894	Several hardware rules are truncated when running capture traffic.
CSCvi98424	IDSEventAlerter and IDSEventProcessor stop working and spam logs after file read error
CSCvi99743	Standby traceback in Thread "Logger" after executing "failover active" with telnet access
CSCvj07038	Firepower devices need to trust Threat Grid certificate
CSCvj11442	Firepower Threat Defense: BGP order of deployment operation of neighbor causes failure
CSCvj19835	Decrypted connections using ECDHE-RSA-RC4-SHA cipher fail in the application data phase
CSCvj38002	SNMPv3 user engineID mismatch with Active engineID causes 'user not found' error on SNMP request
CSCvj44517	List of trusted CAs in SSL policy duplicates
CSCvj49452	sftunnel using weak SSL/TLS versions and ciphers
CSCvj54840	create/delete context stress test causes traceback in nameif_install_arp_punt_service
CSCvj65581	Excessive logging from ftdrpcd process on 2100 series appliances
CSCvj67504	Deploy of policy fails when adding users/groups to the ssl policy
CSCvj67740	Static IPv6 route prefix will be removed from the ASA configuration
CSCvj75793	2100/4100/9300: stopping/pausing capture from Management Center doesn't lower the CPU usage
CSCvj85516	Packet capture fails for interface named "management" on Firepower Threat Defense
CSCvj88514	IP Local pools configured with the same name.

Bug ID	Headline
CSCvj91449	ASA traceback when logging host command is enable for IPv6 after each reboot
CSCvj92040	TLS client offers some ciphersuites in CC mode that are not allowed by CC
CSCvj95451	webvpn-l7-rewriter: Bookmark logout fails on IE
CSCvj96173	After upgrading to 6.2.3, FMC still generates sha1 certificate for eStreamer clients
CSCvj97326	Unable to create SSL policy on Firepower Services
CSCvj98964	ASA may traceback due to SCTP traffic
CSCvk01577	Pigtail from CLISH mode in FTD 6.2.3 not allowed
CSCvk01981	users shows up as unknown after user purge
CSCvk06249	SFDataCorrelator alerting can cause deadlock restart when si_uuid not in firewall_rule_cache
CSCvk06336	FMC displays connections matching incorrect access control policy rules packet count is zero
CSCvk06368	Evaluation of FMC kernel vulnerabilities
CSCvk08377	ASA 5525 running 9.8.2.20 memory exhaustion.
CSCvk10252	SI Category may be incorrect for alerts or eStreamer; also performance and memory problems
CSCvk11898	GTP soft traceback seen while processing v2 handoff
CSCvk14910	SFDataCorrelator keeps exiting when processing FireAMP event without agent uuid
CSCvk16568	AppID stop processing traffic if Application ID has been detected
CSCvk17382	Snort exiting unexpectedly while processing rule evaluation.
CSCvk18378	ASA Traceback and reload when executing show process (rip: inet_ntop6)
CSCvk18578	Enabling compression necessary to load ASA SSLVPN login page customization
CSCvk18846	Firepower Management Center WebUI performance degraded due to sfdccsm logging level.
CSCvk19435	Unwanted IE present error when parsing GTP APN Restriction
CSCvk26887	Certificate import from Local CA fails due to invalid Content-Encoding
CSCvk27686	ASA may traceback and reload when acessing qos metrics via ASDM/Telnet/SSH
CSCvk28023	WebVPN: Grammar Based Parser fails to handle META tags
CSCvk30212	FMC negates BGPv6 commands and generates again if neighbor IPv6 address contains leading 0 in group

Bug ID	Headline
CSCvk30665	ASA "snmp-server enable traps memory-threshold" hogs CPU resulting in "no buffer" drops
CSCvk33947	Sensitive Data Threshold Configuration is incorrect
CSCvk35323	With Objects having override configured, copy config was not happening
CSCvk35761	Sensitive Data is not working as expected when processing multiple patterns in a single session.
CSCvk37890	Firepower 2110, Webvpn conditional debugging causes Threat Defense to traceback
CSCvk40332	UDP traffic without zone information will match incorrect AC rule
CSCvk49527	Add application level timeout for switchprimarynode API call
CSCvk50364	NGIPSV "system support capture-traffic" not working for inline-sets
CSCvk50732	AnyConnect 4.6 Web-deploy fails on MAC using Safari 11.1.x browsers
CSCvk52305	Snort process terminated with segfault in daq
CSCvk54078	Firepower Threat Defense high availability Creation with VPN configuration fails
CSCvk54491	Race condition processing Reputation causes Snort process to exit.
CSCvk54779	Async queue issues with fragmented packets leading to block depletion 9344
CSCvk55355	User/group download fails is at least one user belongs to two groups with same common name
CSCvk57516	Firepower Threat Defense: Low DMA memory leading to VPN failures due to incorrect crypto maps
CSCvk58188	Snort configuration validation failed due to Value specified for max_sessions is out of bounds
CSCvk66012	Policy deployment fails if a member of a cluster is shutdown/Disabled on the FMC
CSCvk71511	SFDataCorrelator event backlog grows when event storage is large and device count is high
CSCvk72602	Incorrect TCP checksum causes snort retries
CSCvk73990	Change Reconciliation report: simplify the rule deletion event
CSCvm01497	Scheduled reports not stored in correct domain when using another domain's report template
CSCvm06114	RDP bookmark plugin won't launch
CSCvm16686	Threat Defense interfaces goes down during high availability creation using redundant interface

Version 6.2.3.4 Resolved Issues

Table 73: Version 6.2.3.4 Resolved Issues

Bug ID	Headline
CSCuy01269	If last entry in `rna_client_app_map` is a dupe, SFDataCorrelator fails
CSCvd28906	ASA traceback at first boot in 5506 due to unable to allocate enough LCMB memory
CSCvd92210	IPV6 addresses not accepted in syslog
CSCvf61852	Threat Intelligence Director (TID) startup causes delay and stalls Tomcat startup
CSCvg28901	Unable to install certificate message when importing certificate to the Firepower Management Center
CSCvg96103	Including a very large HTML page for the Block response causes all Decrypted sites to fail to load.
CSCvh25088	MySQL table `secondary_login` grows unbounded forever
CSCvh91483	CloudAgent restarts once every minute when URL filtering license is expired or deleted
CSCvi03103	BGP ASN cause policy deployment failures.
CSCvi30280	`UserIdentity [ERROR]` Error while handling UserLoginInfo message: `[1] Invalid Argument`
CSCvi34210	Snort match the same connection for U-Turned traffic for different BVI in Transparent Threat Defense
CSCvi44713	show memory binsize and show memory top-usage do not show correct information, all show PC 0x0
CSCvi45807	ASA: dns expire-entry-timer configuration disappears after reboot
CSCvi59968	Firepower 2100 Incorrect reply for SNMP get request `1.3.6.1.2.1.1.2.0`
CSCvi65512	FTD: AAB might force a snort restart with relatively low load on the system
CSCvi97729	To-the-box traffic being routing out a data interface when failover is transitioning on a New Active
CSCvj15572	Flow-offload rewrite rules not updated when MAC address of interface changes
CSCvj25386	Missing default Identity realm EOs causing upgrade failure
CSCvj44531	Phantom SSL objects and empty deployments to sensors
CSCvj49502	Need client hello transmit info at lower debug level
CSCvj74210	Traceback at ssh when executing `show service-policy inspect gtp pdp-context detail`

Bug ID	Headline
CSCvj75655	External Database is unable to query Connection Events from the Firepower Management Center
CSCvj76748	Need to transition to `cloud-sa.amp.sourcefire.com` to `cloud-sa.amp.cisco.com`
CSCvj79729	(2 of 2) high memory usage of `user_id/user_group` broadcast in SFDataCorrelator(on sensor)
CSCvj91418	Snort uses large amounts of memory when appid is processing NetBIOS traffic.
CSCvj91965	Change Reconciliation reports in Firepower Management Center have certain fields blank
CSCvj93913	SSL Inspection TLS 1.3 downgrade needs to modify client/server random values to be RFC compliant
CSCvj94024	Firepower devices go into full recovery is busy is returned from network cards periodically
CSCvk02250	show memory binsize and show memory top-usage do not show correct information (Complete fix)
CSCvk06160	SFDC repeatedly exits while Initializing OS Vuln Map
CSCvk06176	SSEConnector is not coming up because of Wrong Executable
CSCvk06677	HTTPS sessions sometimes timeout without loading on HW SSL
CSCvk12841	SSL pages not loading when using Internet Explorer or Edge
CSCvk17163	force high availability break to 6.2.2 Firepower Threat Defense device, deployment fails with error
CSCvk17813	Policy deploy may fail with failed to retrieve device running configuration in pair environment
CSCvk19750	Import of `.sfo` file with large number of local rules taking more than 170+ hours
CSCvk21405	shell application not pin holing new connection from server
CSCvk25729	Large ACL taking long time to compile on boot causing outage
CSCvk27787	Management Center pair: `Manage_procs.pl` corrupting the cluster.conf file on the Managed Device
CSCvk30228	ASAv and FTDv deployment fails in Microsoft Azure and/or slow console response
CSCvk30778	Client hello digest for for layer `3` and `4` processed twice causing memory leak
CSCvk30865	SSL alert with TLS version other than differing from negotiated version report as corrupt record

Bug ID	Headline
CSCvk32718	Event processing slows during file malware attack involving many file events
CSCvk45443	ASA cluster: Traffic loop on CCL with NAT and high traffic
CSCvk59795	Remote access VPN using an OpenLDAP realm/server doesn't use the correct naming attribute

Version 6.2.3.3 Resolved Issues

Table 74: Version 6.2.3.3 Resolved Issues

Bug ID	Headline
CSCuz96856	New client hello flag for blocked session due to cache inconsistency
CSCvd13180	AVT : Missing Content-Security-Policy Header in ASA 9.5.2
CSCvd76939	ASA policy-map configuration is not replicated to cluster slave
CSCve17484	Intelligent Application Bypass drop percentage does not work on Firepower Threat Defense
CSCve53415	ASA traceback in DATAPATH thread while running captures
CSCvg42033	prune to cleanup unused data in eoattributes table at vms.db to reduce backup file size
CSCvg76652	Default DLY value of port-channel sub interface mismatch
CSCvg90365	icmp/telnet traffic fail by ipv6 address on transparent ASA
CSCvh53276	IPv6 protocol 112 packets passing through L2FW are dropping with Invalid IP length message
CSCvh55035	Firepower Threat Defense device unable to stablish ERSPAN with Nexus 9000
CSCvh55340	ASA Running config through REST-API Full Backup does not contain the specified context configuration
CSCvh71738	FQDN object are getting resolved after removing access-group configuration
CSCvh75060	Rest-API gives empty response for certain queries
CSCvh83849	DHCP Relay With Dual ISP and Backup IPSEC Tunnels Causes Flapping
CSCvh95960	Using the match keyword in capture command causes IPv6 traffic to be ignored in capture
CSCvi07974	Layer 2 traffic should not be hardcoded to be sent to Snort for inspection
CSCvi15830	wrong configurations on Threat Defense device when network group object is used on identity policy

Bug ID	Headline
CSCvi16024	SSL errors on session resume when server IP address changes
CSCvi19220	ASA fails to encrypt after performing IPv6 to IPv4 NAT translation
CSCvi36434	Cisco Firepower System Software SSL Denial of Service Vulnerability
CSCvi37374	SSL connections fail to complete when passing through a single inline set multiple times
CSCvi38151	ASA pair: IPv6 static/connected routes are not sync/replicated between Active/Standby pairs.
CSCvi42008	Stuck uauth entry rejects AnyConnect user connections
CSCvi51515	REST-API:`500 Internal Server Error`
CSCvi53420	User/Group Download fails when same user is part of multiple groups with comma (,) in common name
CSCvi58032	Management Center Internal Error creates an Auto-NAT rule which causes a policy deployment failure
CSCvi58183	Custom SI feed update in Firepower Management Center is not propagated to managed devices
CSCvi59000	SecGW - Data Loss during ASR
CSCvi59148	Sessions can remain active on managed device if they are from same IP address but different realms
CSCvi62671	users/groups download takes long time in 6.2.2.1 with high number of user/group mappings
CSCvi63968	`Internal Error is preventing Policy Validation` Cannot save access control policy.
CSCvi70606	ASA 9.6(4): WebVPN page not loading correctly
CSCvi73414	Unable to delete User Indication of Compromise if user info is inconsistent between mysql and sybase
CSCvi80928	HW Mode - SSL errors may occur when resumed sessions are not decrypted
CSCvi89194	pki handles: increase and fail to decrement
CSCvi97479	Snort restart while deploying access control policy changes
CSCvi97721	The memcap for Security Intelligence URL feeds needs to be increased for devices 4GB total memory
CSCvi98251	SMTP: Could not allocate SMTP mempool causing Policy Apply Failure and Snort Outage

Bug ID	Headline
CSCvj00918	(1 of 2) high memory usage of `user_id/user_group` broadcast in SFDataCorrelator(on sensor)
CSCvj06418	Custom SI DNS feed not synced to secondary Firepower Management Center
CSCvj09571	Firepower Management Center UI slow when managing large number of device with classic licenses
CSCvj10011	Management Center: IGMP gets enabled on interfaces which it has been configured but not enabled
CSCvj17609	synchronization failed (Cannot open file) entries in action queue when file is empty
CSCvj22491	Cluster: Enhance ifc monitor debounce-time for interface down->up scenario
CSCvj24036	Messaging on Firepower Management Center UI informing of ports required by RAVPN
CSCvj25386	Missing default Identity realm EOs causing upgrade failure
CSCvj25817	ASA responds to MOBIKE but clears SA due to DPD.
CSCvj26819	modifying `ssl_debug` settings requires a detection engine restart
CSCvj32264	ASA - zonelabs-integrity : Traceback and High CPU due to `Process Integrity FW task`
CSCvj33202	Cannot save Intrusion Policy with Firepower recommendations and shared policy layers
CSCvj37448	ASA : Device sends only ID certificate in SSL server certificate packet after reload
CSCvj37858	performance impact from `action_queue` queries
CSCvj37924	CWE-20: Improper Input Validation
CSCvj39858	Traceback: Thread Name: IPsec message handler
CSCvj40636	S2S VPN support for Firepower Threat Defense Cluster for the classic centralized VPN clustering
CSCvj42450	ASA traceback in Thread Name: DATAPATH-14-17303
CSCvj42680	Slowness due to frequent device registration queries on Firepower Management Center pair
CSCvj44262	portal-access-rule changing from deny to permit
CSCvj45594	SFDataCorrelator core when timing-out old host info on a slow Firepower Management Center
CSCvj46777	Firepower Threat Defense 2100 asa traceback for unknown reason
CSCvj48168	The `show memory` command returns low used memory numbers

Bug ID	Headline
CSCvj48340	ASA memory Leak - snp_svc_insert_dtls_session
CSCvj48931	Firepower recommendation updates task never runs
CSCvj49883	ASA traceback on Firepower Threat Defense 2130-ASA-K9
CSCvj50024	ASA portchannel lacp max-bundle 1 hot-sby port not coming up after link failure
CSCvj56008	Scansafe feature doesn't work at all for HTTPS traffic
CSCvj56909	ASA does not unrandomize the SLE and SRE values for SACK packet generated by ASA module
CSCvj56963	Management Center error about `Only 8 equal cost routes are allowed` when adding the fifth route
CSCvj61367	fast reuse of source port can break ssl inspection
CSCvj67132	Policy deploy failure due to bgp neighbor CLI in wrong order
CSCvj73581	Traceback in `cli_xml_server` Thread
CSCvj74210	Traceback at ssh when executing `show service-policy inspect gtp pdp-context detail`
CSCvj79765	Netflow configuration on Active ASA is replicated in upside down order on Standby unit
CSCvj81287	Firepower Threat Defense rejecting syslog server TLS-X509 certificate due to EKU invalid purpose
CSCvj83316	Snort process exits while clearing XFF data.
CSCvj91619	1550 Block Depletions leading to ASA reload.
CSCvj97157	WebPage is not loading due to client rewriter issue on JS files
CSCvk00579	Slowness in the device list getting populated under the Deploy tab
CSCvk06176	SSEConnector is not coming up because of Wrong Executable
CSCvk07522	webvpn: Bookmark fails to render on Firefox and Chrome. IE fine.

Version 6.2.3.2 Resolved Issues

Table 75: Version 6.2.3.2 Resolved Issues

Bug ID	Headline
CSCuv68725	ASA unable to remove ACE with log disable option

Bug ID	Headline
CSCvd13182	AVT : Missing X-Content-Type-Options in ASA 9.5.2
CSCvd44525	ASA show tech some commands twice, show running-config/ak47 detailed/startup-config errors
CSCve94917	Stale VPN Context issue seen in 9.1 code despite fix for CSCvb29688
CSCvf18160	ASA traceback on failover sync with WebVPN and shared storage-url config
CSCvf39539	Netflow Returns Large Values for Bytes Sent/Received and IP address switch
CSCvf40179	ERROR: Unable to create crypto map: limit reached, when adding entry
CSCvf82832	ASA : ICMPv6 syslog messages after upgrade to 962.
CSCvf96773	Standby ASA has high CPU usage due to extremely large PAT pool range
CSCvg05442	ASA traceback due to deadlock between DATAPATH and webvpn processes
CSCvg43389	ASA traceback due to 1550 block exhaustion.
CSCvg72879	9.9.1/SecGW: Firepower 4100 w/ subsecond failover may have 10-20% packet loss for few mins
CSCvh14743	IKEv2 MOBIKE session with Strongswan/3rd party client fails due to DPD with NAT detection payload.
CSCvh23531	ASA TLS client connection fails with software DHE
CSCvh30261	ASA watchdog traceback during context modification/configuration sync
CSCvh47057	ASA - ICMP flow drops with `no-adjacency` on interface configured in zone when inspection enabled
CSCvh65500	Firepower 2100 Client in FTP active mode is not able to establish control channel with the Server
CSCvh81142	Snort Core Generated while running 6.2.3
CSCvh83934	Memory usage of User-ID component of SNORT exceeds the reserved limit of 10M
CSCvh91053	ASA sending DHCP decline | not assiging address to AC clients via DHCP
CSCvh91399	upgrade of ASA5500 series firewalls results in boot loop (not able to get past ROMMON)
CSCvh92381	ASA Traceback and goes to boot loop on 9.6.3.1
CSCvi01376	Upon reboot, non-default SSL commands are removed from the Firepower 4100
CSCvi07636	ASA: Traceback in Thread Name UserFromCert
CSCvi08450	CWS redirection on ASA doesn't treat SSL Client Hello retransmission properly in specific condition

Bug ID	Headline
CSCvi09305	Some SSL connections slow or fail under a Do-Not-Decrypt SSL policy action
CSCvi16264	ASA traceback and reload due to watchdog timeout when DATAPATH accesses compiling ACL structure
CSCvi19263	ASA 9.7.1.15 Traceback while releasing a vpn context spin lock
CSCvi22507	IKEv1 RRI : With Answer-only Reverse Route gets deleted during Phase 1 rekey
CSCvi23615	Sourcefire.agent_messages table becoming large preventing the agent messages from being consumed
CSCvi33962	WebVPN rewriter: drop down menu doesn't work in BMC Remedy
CSCvi35805	ASA Cut-Through Proxy allowing user to access website, but displaying `authentication failed`
CSCvi42965	ASA does not report accurate free memory under `show memory` output
CSCvi45567	Not able to do snmpwalk when snmpv1&2c host group configured.
CSCvi47847	Shell application not pin-holing for new tcp port for data transfer as expected
CSCvi48523	Not able to create SLA Monitor from static route page
CSCvi49383	Azure: ASAv running Cloud high availability gets in a watchdog crash loop
CSCvi55070	IKEv1 RRI : With Originate-only Reverse Route gets deleted during Phase 1 rekey
CSCvi57808	Continuously sfdatacorrelator process terminated unexpectedly
CSCvi58089	Memory leak on webvpn
CSCvi58865	SSL policy with URL category rules specifying decryption can cause browser errors
CSCvi63864	With SSL inspection in hardware mode and Malware protection, secure file transfers occasionally fail
CSCvi63888	SSL errors might occur when resumed sessions are not decrypted
CSCvi64007	Zeroize RSA key after Failover causes REST API to fail to changeto System context
CSCvi66905	PIM Auto-RP packets are dropped after cluster master switchover
CSCvi70680	Same groups from different AD not downloaded
CSCvi71039	Firepower Management Center: Change Reconciliation reports are failing intermittently
CSCvi76577	ASA:netsnmp:Snmpwalk is failed on some group of IPs of a host-group.
CSCvi77352	Illegal update occurs when device removes itself from the cluster
CSCvi82779	ASA generate traceback in DATAPATH thread

Bug ID	Headline
CSCvi84315	Unexpected failures on Firepower 2100 Series devices
CSCvi86799	ASA traceback during output of `show service-policy` with a high number of interfaces and qos
CSCvi87921	ASA self-signed RSA certificate is not allowed for TLS in FIPS mode
CSCvi95544	ASA not matching IPv6 traffic correctly in ACL with any keyword configured
CSCvj05140	Object description is not deployed with associated network object.
CSCvj07038	Firepower devices need to trust Threat Grid certificate
CSCvj07571	`Error 500` when saving some correlation policy rules
CSCvj07843	eStreamer using 100% CPU, event processing slows when File/FireAMP events enabled
CSCvj22491	Cluster: Enhance ifc monitor debounce-time for interface down->up scenario
CSCvj26450	ASA PKI OCSP failing - CRYPTO_PKI: failed to decode OCSP response data.
CSCvj47633	Non-SSL traffic causing SSL inspection to fail
CSCvj56008	Scansafe feature doesn't work at all for HTTPS traffic
CSCvj63196	Workaround for Sybase issue: After snort engine update, policy deployment fail abruptly

Version 6.2.3.1 Resolved Issues

Table 76: Version 6.2.3.1 Resolved Issues

Bug ID	Headline
CSCvf97979	NAT policy deployment failed during generating delta config after changing security zone in rule.
CSCvg00565	ASA crashes in `glib/g_slice` when do debug menu self testing
CSCvg36672	Need a way to prioritize user driven deployment tasks in Action Queue
CSCvg65072	Cisco ASA sw, FTD sw, and AnyConnect Secure Mobility Client SAML Auth Session Fixation Vulnerability
CSCvg78418	Evaluation of FireSIGHT / FirePOWER for Apache/Struts related vulnerabilities
CSCvg84495	Remote access VPN using an OpenLDAP realm/server doesn't use the correct naming attribute
CSCvh05081	ASA does not unrandomize the SLE and SRE values for SACK packet generated by ASA module

Bug ID	Headline
CSCvh22181	Failures loading websites, such as mail sites, using TLS 1.3 with SSL inspection enabled
CSCvh25433	New CLI for Supporting Legacy method SAML Auth using external browser on Endpoint with AC
CSCvh46202	Slow 2048 byte block leak due to fragmented traffic over VPN
CSCvh53616	ASA on Firepower Threat Defense devices traceback due to SSL
CSCvh63903	Failover of IPv6 addresses on 8000 series pair devices may not succeed
CSCvh79732	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh81474	Need to catch malformed JSON to allow rendering of Deploy button and notifications
CSCvh81737	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh81870	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh83012	SFDataCorrelator should not limit rate of duplicate flows
CSCvh99414	NFE failure causes Snort to constantly restart
CSCvi03546	User-IP mapping not updated on managed device due to error in updating current map
CSCvi18602	FSIC failed while downgrade ASA FirePOWER module (5585-x) from 6.2.2.2 to 6.2.2.1
CSCvi34137	With SSL decryption enabled and TCP Segmented HTTP requests, Snort does not capture URI correctly
CSCvi44365	After an upgrade the Firepower 4100 hostname is different than SFCLI hostname
CSCvi49752	`sfipproxy` may not be written correctly on a sensor when registered to a high availability pair
CSCvi55280	Deployment transcript does not indicate failed command if error is in last CLI of delta
CSCvi80849	Cisco Firepower 2100 Series POODLE TLS security scanner alerts

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.

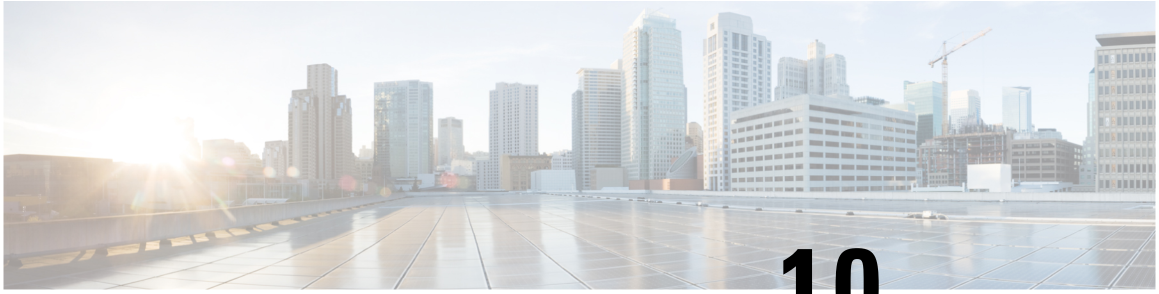
Important Bug lists are auto-generated once and are not subsequently updated. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes. You should regard the Cisco Bug Search Tool as the source of truth.

Version 6.2.3 Known Issues

Table 77: Version 6.2.3 Known Issues

Bug ID	Headline
CSCvf16001	SF Cli - "inside" or "outside" interface capture not giving all options
CSCvh73096	Firepower Management Center does not support userPrincipalName attribute for login with ISE 2.2+
CSCvh89068	Core in Firepower Management Center Perl
CSCvh95960	Using the match keyword in capture command causes IPv6 traffic to be ignored in capture
CSCvi07656	Small number of TLS connections can fail after TLS inspection in Hardware Mode is overloaded
CSCvi10758	With SSL inspection in software mode, a few TLS connections fail to close in a timely manner
CSCvi16024	SSL errors on session resume when server IP address changes - HW mode

Bug ID	Headline
CSCvi18123	Firepower Threat Defense show tech-support command output broken on 2100 from CLISH CLI
CSCvi19862	With SSL inspection enabled, TLS traffic throughput can drop following high-availability failover
CSCvi35176	Deployment Failed-Snort Restart Failure-APPLY_APP_CONFIG_APPLICATION_FAILURE SignalAppConfigFailed
CSCvi35588	Deployment failure due to Snort failed to restart PDTS Handle was NULL
CSCvi42539	Decrypted connections fail when SSLv2 is supported but a higher version is negotiated
CSCvi47264	Some indicators may stay pending when consuming TAXII feeds in parallel
CSCvi49538	Firepower Device Management fails on 2100 (6.2.3-51 (PortChannel))
CSCvi50731	Unable to delete certificate objects if there were previous used at ISE even it was deleted
CSCvi61411	Routed Threat Defense allows Transparent Configuration, but traffic fails (6.2.3-66) on KVM only
CSCvi62982	Firepower Threat Defense virtual on ESXi Firstboot config does not sync hostname correctly with FQHN
CSCvi63157	Firepower 2110 dropping connections
CSCvi63864	With SSL inspection in hardware mode and Malware protection, secure file transfers occasionally fail
CSCvi66189	CNP has been enabled in Firepower Management Center where it usage Satellite server for license
CSCvi70680	Same groups from different AD not downloaded
CSCvv14442	FMC backup restore fails if it contains files/directories with future timestamps



CHAPTER 10

For Assistance

Online Resources

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

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

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

Contact Cisco

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

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