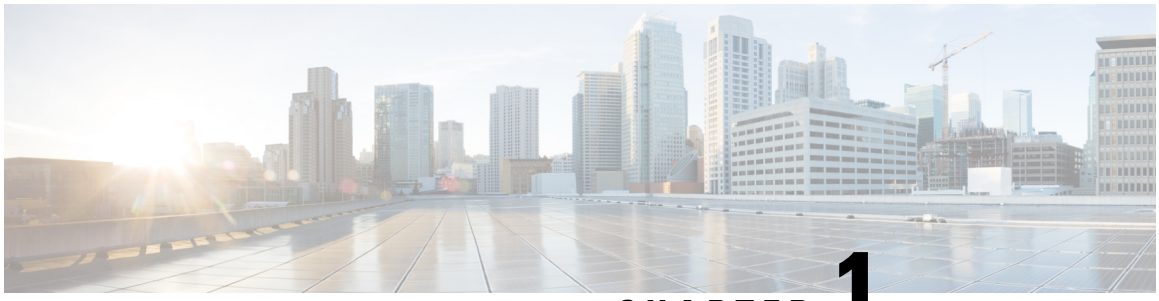
Cisco Firepower Release Notes, Version 6.5.0 Patches

First Published: 2019-11-20

Last Modified: 2022-03-08

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

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.

Table 1: Version 6.5.0 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.5.0	123	2020-02-03	FMC/FMCv	FMC/FMCv
6.5.0	120	2019-10-08	—	—
6.5.0	115	2019-09-26	All devices	All devices

Table 2: Version 6.5.0 Patch Dates

Version	Build	Date	Platforms
6.5.0.5	95	2021-02-09	All
6.5.0.4	57	2020-03-02	All
6.5.0.3	30	2020-02-03	No longer available.
6.5.0.2	57	2019-12-19	All
6.5.0.1	35	2019-11-20	No longer available.

Suggested Release

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

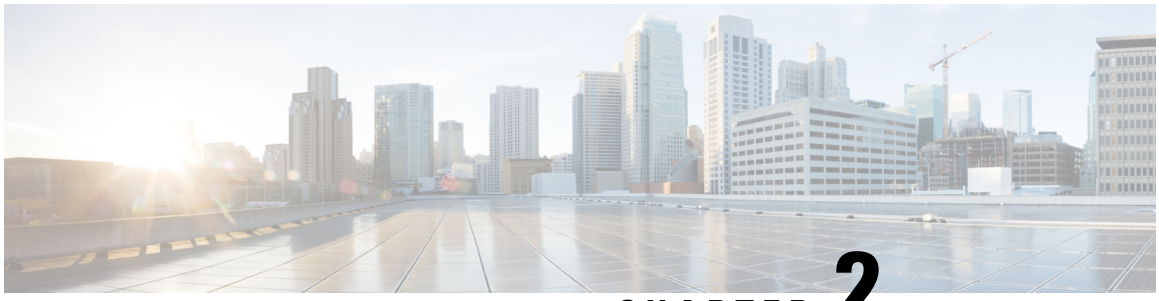
We also list the suggested release in the new feature guides:

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

Suggested Releases for Older Appliances

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

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



CHAPTER 2

Compatibility

For general compatibility information see:

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

For compatibility information for this version, see:

Firepower Management Center

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

Firepower Management Center

This release supports the following hardware FMC platforms:

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

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

Firepower Management Center Virtual

This release supports the following FMCv public cloud implementations:

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

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

- Firepower Management Center Virtual for Kernel-based virtual machine (KVM)
- Firepower Management Center Virtual for VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7

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

Firepower Devices

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

Note These release notes list the supported devices for *this* release. Even if an older device has reached EOL and you can no longer upgrade, you can still manage that device with a newer FMC, up to a few versions ahead. Similarly, newer versions of ASDM can manage older ASA FirePOWER modules. For supported management methods, including backwards compatibility, see Manager-Device Compatibility, on page 5.

Table 3: Firepower Threat Defense in Version 6.5.0

FTD Platform	OS/Hypervisor	Additional Details
Firepower 1010, 1120, 1140, 1150 Firepower 2110, 2120, 2130, 2140	—	—
Firepower 4110, 4120, 4140, 4150 Firepower 4115, 4125, 4145 Firepower 9300 with SM-24, SM-36, SM-44 modules Firepower 9300 with SM-40, SM-48, SM-56 modules	FXOS 2.7.1.92 or later build	Upgrade FXOS first. To resolve issues, you may need to upgrade FXOS to the latest build. To help you decide, see the Cisco FXOS Release Notes, 2.7(1).
ASA 5508-X, 5516-X ASA 5525-X, 5545-X, 5555-X ISA 3000	—	Although you do not separately upgrade the operating system on these devices in FTD deployments, you should make sure you have the latest ROMMON image on the ISA 3000, ASA 5508-X and 5516-X. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.

FTD Platform	OS/Hypervisor	Additional Details
FTDv	Any of: • AWS: Amazon Web Services • Azure: Microsoft Azure • KVM: Kernel-based Virtual Machine • VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7	For supported instances, see the appropriate FTDv Getting Started guide.

Table 4: NGIPS/ASA FirePOWER in Version 6.5.0

NGIPS/ASA FirePOWER Platform	OS/Hypervisor	Additional Details
ASA 5508-X, 5516-X ISA 3000	ASA 9.5(2) to 9.16(x)	There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues. See the Cisco ASA Upgrade Guide for order of operations. You should also make sure you have the latest ROMMON image on the ISA 3000, ASA 5508-X and 5516-X. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.
ASA 5525-X, 5545-X, 5555-X	ASA 9.5(2) to 9.14(x)	
NGIPSv	VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7	For supported instances, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.

Manager-Device Compatibility

Firepower Management Center

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

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

Table 5: FMC-Device Compatibility

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

Firepower Device Manager and Cisco Defense Orchestrator

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

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

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

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

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

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

Table 6: FDM/CDO Compatibility with FTD

FTD Platform	FDM Compatibility	CDO Compatibility
Firepower 1000 series	6.4.0+	6.4.0+
Firepower 2100 series	6.2.1+	6.4.0+
Firepower 4100/9300	6.5.0+	6.5.0+
ASA 5500-X series	6.1.0 to 7.0.x	6.4.0 to 7.0.x
ISA 3000	6.2.3+	6.4.0+
FTDv for AWS	6.6.0+	6.6.0+
FTDv for Azure	6.5.0+	6.5.0+
FTDv for KVM	6.2.3+	6.4.0+
FTDv for VMware	6.2.2+	6.4.0+

Adaptive Security Device Manager

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

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

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

Table 7: ASDM-ASA FirePOWER Compatibility

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

Web Browser Compatibility

Browsers

We test with the latest versions of the following popular browsers, running on currently supported versions of macOS and Microsoft Windows:

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

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

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

Browser Settings and Extensions

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

If you are using Microsoft Internet Explorer 11:

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

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

Securing Communications

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

To begin replacing the self-signed certificate:

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

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

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

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

Browsing from a Monitored Network

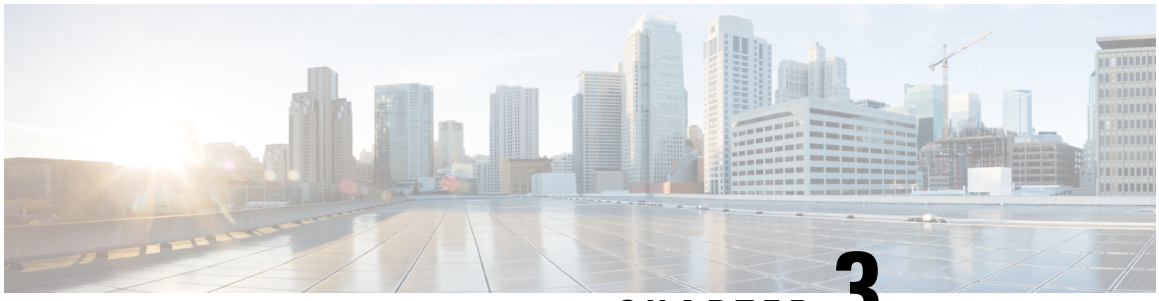
Many browsers use Transport Layer Security (TLS) v1.3 by default. If you are using an SSL policy to handle encrypted traffic, and people in your monitored network use browsers with TLS v1.3 enabled, websites that support TLS v1.3 may fail to load.

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

Screen Resolution Requirements

Table 8: Screen Resolution Requirements

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



CHAPTER 3

Features and Functionality

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

Features for Firepower Management Center Deployments

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 6.5.0 Patches

Table 9:

Feature	Description
Version 6.5.0.5 Default HTTPS server certificates	**Upgrade impact.** Unless the FMC's current *default* HTTPS server certificate already has an 800-day lifespan, upgrading to Version 6.5.0.5+ renews the certificate, which now expires 800 days from the date of the upgrade. All future renewals have an 800 day lifespan. Your old certificate was set to expire depending on when it was generated, as follows: • 6.5.0 to 6.5.0.4: 3 years • 6.4.0.9 and later patches: 800 days • 6.4.0 to 6.4.0.8: 3 years • 6.3.0 and all patches: 3 years • 6.2.3: 20 years

Deprecated Features in FMC Version 6.5.0 Patches

Table 10:

Feature	Upgrade Impact	Description
Version 6.5.0.2 Egress optimization	Patching turns off egress optimization processing.	To mitigate CSCvq34340, patching Firepower Threat Defense to Version 6.5.0.2+ turns off egress optimization processing. This happens regardless of whether the egress optimization feature is enabled or disabled. **Note** We recommend you upgrade to Version 6.6.0+, where this issue is fixed. That will turn egress optimization back on, if you left the feature 'enabled.' If you remain at Version 6.5.0 or 6.5.0.1, you should manually disable egress optimization from the FTD CLI: **no asp inspect-dp egress-optimization**. For more information, see the software advisory: FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature.

Features for Firepower Device Manager Deployments

New Features in FDM Version 6.5.0 Patches

Table 11:

Feature	Description
Version 6.5.0.5 Default HTTPS server certificates	**Upgrade impact.** Unless the device's current *default* HTTPS server certificate already has an 800-day lifespan, upgrading to Version 6.5.0.5+ renews the certificate, which now expires 800 days from the date of the upgrade. All future renewals have an 800 day lifespan. Your old certificate was set to expire depending on when it was generated, as follows: • 6.5.0 to 6.5.0.4: 3 years • 6.4.0.9 and later patches: 800 days • 6.4.0 to 6.4.0.8: 3 years • 6.3.0 and all patches: 3 years • 6.2.3: 20 years

Deprecated Features in FDM Version 6.5.0 Patches

Table 12:

Feature	Upgrade Impact	Description
Version 6.5.0.2 Egress optimization	Patching turns off egress optimization processing.	To mitigate CSCvq34340, patching a Firepower Threat Defense to Version 6.5.0.2+ turns off egress optimization processing. This happens regardless of whether the egress optimization feature is enabled or disabled. **Note** We recommend you upgrade to Version 6.6.0+, where this issue is fixed. That will turn egress optimization back on, if you left the feature 'enabled.' If you remain at Version 6.5.0 or 6.5.0.1, you should manually disable egress optimization from the FTD CLI: **no asp inspect-dp egress-optimization**. For more information, see the software advisory: FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature.

Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

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

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

Supported keywords depend on your Snort version:

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

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

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

How-To Walkthroughs for the FMC

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

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

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

Table 13: Troubleshooting Walkthroughs

Problem	Solution
Cannot find the **How To** link to start walkthroughs.	Make sure walkthroughs are enabled. From the drop-down list under your username, select **User Preferences** then click **How-To Settings**.
Walkthrough appears when you do not expect it.	If a walkthrough appears when you do not expect it, end the walkthrough.

Problem	Solution
Walkthrough disappears or quits suddenly.	If a walkthrough disappears: • Move your pointer. Sometimes the FMC stops displaying an in-progress walkthrough. For example, pointing to a different top-level menu can make this happen. • Navigate to a different page and try again. If moving your pointer does not work, the walkthrough may have quit.
Walkthrough is out of sync with the FMC: • Starts on the wrong step. • Advances prematurely. • Will not advance.	If a walkthrough is out of sync, you can: • Attempt to continue. For example, if you enter an invalid value in a field and the FMC displays an error, the walkthrough can prematurely move on. You may need to go back and resolve the error to complete the task. • End the walkthrough, navigate to a different page, and try again. Sometimes you cannot continue. For example, if you do not click **Next** after you complete a step, you may need to end the walkthrough.

Sharing Data with Cisco

Web Analytics tracking

In Version 6.2.3+, *Web analytics tracking* sends non-personally-identifiable usage data to Cisco, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your FMCs.

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

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

Cisco Success Network

In Version 6.2.3+, *Cisco Success Network* sends usage information and statistics to Cisco, which are essential to provide you with technical support.

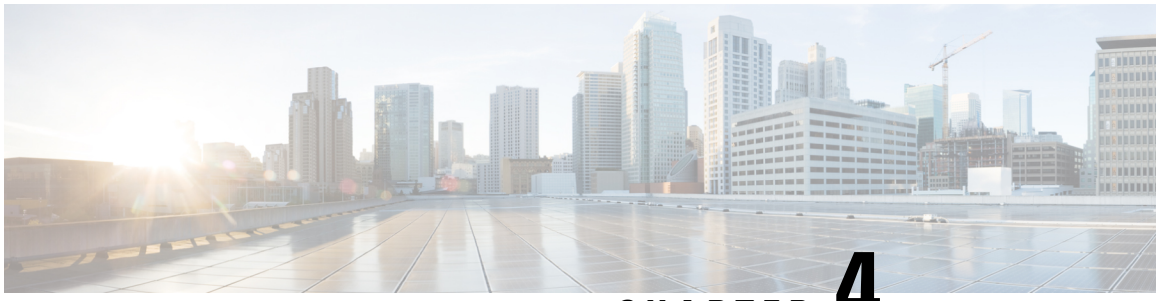
During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time.

Cisco Support Diagnostics

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

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

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



CHAPTER 4

Upgrade the Software

This chapter provides critical and release-specific information.

Planning Your Upgrade

Careful planning and preparation can help you avoid missteps. This table summarizes the upgrade planning process. For detailed checklists and procedures, see the the appropriate upgrade or configuration guide for full instructions: Upgrade Instructions, on page 28.

Table 14: Upgrade Planning Phases

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

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

Minimum Version to Upgrade

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

Upgrade Guidelines for Version 6.5.0.x Patches

There are no upgrade guidelines that apply specifically to Version 6.5.0 patches.

Unresponsive Upgrades

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

Traffic Flow and Inspection

Interruptions in traffic flow and inspection can occur when you:

- Reboot a device.
- Upgrade the device software, operating system, or virtual hosting environment.
- Uninstall the device software.
- Move a device between domains.

- Deploy configuration changes (Snort process restarts).

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

Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300

FXOS Upgrades

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

Table 15: Traffic Behavior: FXOS Upgrades

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

Software Upgrades for Standalone Devices

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

Table 16: Traffic Behavior: Software Upgrades for Standalone Devices

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

Software Upgrades for High Availability/Scalability

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

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

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

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

Software Uninstall (Patches)

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

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

- FTD with FDM: Not supported.

Deploying Configuration Changes

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

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

Table 17: 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 18: Traffic Behavior: Software Upgrades for Standalone Devices

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

Software Upgrades for High Availability/Scalability

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

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

Software Uninstall (Patches)

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

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

Deploying Configuration Changes

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

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

Table 19: Traffic Behavior: Deploying Configuration Changes

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

ASA FirePOWER Upgrade Behavior

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

Table 20: 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 21: 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 22: Traffic Behavior During NGIPSv Deployment

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

Time and Disk Space Tests

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

Time Tests

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

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

Table 23: Time Test Conditions for Software Upgrades

Condition	Details
Deployment	Times for FTD upgrades are from tests in a FMC deployments. Raw upgrade times for remotely and locally managed devices are similar, given similar conditions.
Versions	For major and maintenance releases, we test upgrades from all eligible previous major versions. For patches, we test upgrades from the base version. Upgrade time usually increases if your upgrade skips versions.
Models	In most cases, we test on the lowest-end models in each series, and sometimes on multiple models in a series.
Virtual appliances	We test with the default settings for memory and resources. However, note that upgrade time in virtual deployments is highly hardware dependent.
High availability/scalability	Unless otherwise noted, we test on standalone devices. In a high availability or clustered configuration, devices upgrade one at a time to preserve continuity of operations, with each device operating in maintenance mode while it upgrades. Upgrading a device pair or entire cluster, therefore, takes longer than upgrading a standalone device.
Configurations	We test on appliances with minimal configurations and traffic load. Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how those things are affected by the upgrade. For example, if you use a lot of access control rules and the upgrade needs to make a backend change to how those rules are stored, the upgrade can take longer.
Components	We report times for the software upgrade itself and the subsequent reboot *only*. This does not include time for operating system upgrades, transferring upgrade packages, readiness checks, VDB and intrusion rule (SRU/LSP) updates, or deploying configurations.

Disk Space Tests

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

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

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

Table 24: Checking Disk Space

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

Version 6.5.0.5 Time and Disk Space

Table 25: Version 6.5.0.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time	Reboot Time
FMC	4.4 GB	28 MB	—	47 min	8 min
FMCv: VMware	4.2 GB	25 MB	—	36 min	4 min
Firepower 1000 series	2.6 GB	2.6 GB	510 MB	9 min	11 min
Firepower 2100 series	2.5 GB	2.5 GB	530 MB	7 min	10 min
Firepower 4100 series	2.6 GB	2.6 GB	360 MB	5 min	8 min
Firepower 9300	2.6 GB	2.6 GB	360 MB	5 min	8 min
ASA 5500-X series with FTD	1.9 GB	120 MB	310 MB	9 min	8 min
FTDv: VMware	2.2 GB	120 MB	310 MB	7 min	6 min
ASA FirePOWER	4.3 GB	32 MB	610 MB	52 min	6 min
NGIPSv	2.2 GB	420 MB	470 MB	6 min	4 min

Version 6.5.0.4 Time and Disk Space

Table 26: Version 6.5.0.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
Firepower 1000 series	2.6 GB	2.6 GB	500 MB	20 min
Firepower 2100 series	2.5 GB	2.5 GB	530 MB	18 min
Firepower 4100 series	2.5 GB	2.5 GB	360 MB	13 min
Firepower 9300	2.5 GB	2.5 GB	360 MB	17 min
ASA 5500-X series with FTD	1.9 GB	110 MB	310 MB	16 min
FTDv: VMware	1.9 GB	110 MB	310 MB	9 min
ASA FirePOWER	2.6 GB	20 MB	340 MB	72 min
NGIPSv	740 MB	20 MB	230 MB	8 min

Version 6.5.0.3 Time and Disk Space

Version 6.5.0.3 was removed from the Cisco Support & Download site on 2019-02-04 (for FMCs) and 2020-03-02 (for devices). If you are running this version, it is safe to continue.

Version 6.5.0.2 Time and Disk Space

Table 27: Version 6.5.0.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	2.6 GB	20 MB	—	42 min
FMCv: VMware	2.7 GB	23 MB	—	34 min
Firepower 1000 series	2.5 GB	2.5 GB	480 MB	12 min
Firepower 2100 series	2.3 GB	2.3 GB	500 MB	17 min
Firepower 4100 series	2.3 GB	2.3 GB	340 MB	13 min
Firepower 9300	2.3 GB	2.3 GB	340 MB	17 min
ASA 5500-X series with FTD	1.9 GB	110 MB	280 MB	22 min
FTDv: VMware	1.7 GB	110 MB	280 MB	10 min
ASA FirePOWER	2.5 GB	20 MB	320 MB	56 min
NGIPSv	680 MB	18 MB	210 MB	9 min

Version 6.5.0.1 Time and Disk Space

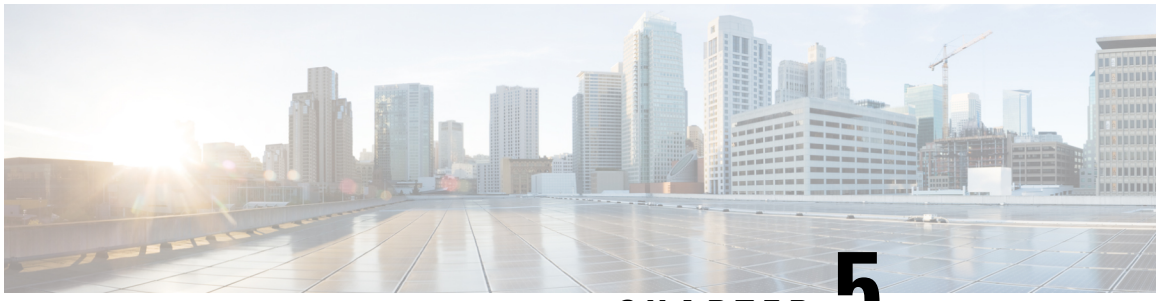
Version 6.5.0.1 was removed from the Cisco Support & Download site on 2019-12-19. If you are running this version, we recommend you upgrade.

Upgrade Instructions

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

Table 28: Firepower Upgrade Instructions

Task	Guide
Upgrade in Firepower Management Center deployments.	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
Upgrade Firepower Threat Defense with Firepower Device Manager.	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager See the *System Management* chapter in the guide for the Firepower Threat Defense version you are currently running—not the version you are upgrading to.
Upgrade FXOS on a Firepower 4100/9300 chassis.	Cisco Firepower 4100/9300 Upgrade Guide, Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1
Upgrade ASA FirePOWER modules with ASDM.	Cisco ASA Upgrade Guide
Upgrade the ROMMON image on the ISA 3000, ASA 5508-X, and ASA 5516-X.	Cisco ASA and Firepower Threat Defense Reimage Guide See the *Upgrade the ROMMON Image* section. You should always make sure you have the latest image.



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 6.5.0 Patches That Support Uninstall

This table lists supported uninstall scenarios for Version 6.5.0 patches. Remember that uninstalling returns you to the patch level you upgraded from. If uninstall will take you farther back than what is supported, we recommend you reimage and then upgrade to your desired patch level.

Table 29: Version 6.5.0 Patches That Support Uninstall

Current Version	Farthest Back You Should Uninstall		
	FTD/FTDv	ASA FirePOWER NGIPSv	FMC/FMCv
6.5.0.2+	6.5.0	6.5.0	6.5.0.1
6.5.0.1	6.5.0	6.5.0	—

Guidelines for Uninstalling Patches

Uninstall from Devices First, Using the Shell

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

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

- You cannot batch-uninstall patches from devices in high availability/scalability deployments. To plan an uninstall order that minimizes disruption, see Uninstall Order for HA/Scalability Deployments, on page 30.
- You cannot use the FMC or ASDM to uninstall a patch from a device.
- You cannot use FMC user accounts to log into and uninstall the patch from one of its managed devices. Devices maintain their own user accounts.
- You must have access to the device shell as the `admin` user for the device, or as another local user with CLI configuration access. If you disabled shell access, you cannot uninstall device patches. Contact Cisco TAC to reverse the device lockdown.

Uninstall from the FMC After Devices

Uninstall patches from the FMC after you uninstall from managed devices. As with upgrade, you must uninstall from high availability FMCs one at a time; see Uninstall Order for HA/Scalability Deployments, on page 30.

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

Uninstall Order for HA/Scalability Deployments

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

Note that in most cases, you will:

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

Table 30: Uninstall Order for FMCs in HA

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

Table 31: Uninstall Order for FTD devices in HA or Clusters

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

Table 32: Uninstall Order for ASA with FirePOWER Services Devices in ASA Failover Pairs/Clusters

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

Uninstall Instructions

Uninstall from a Standalone FMC

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

Before you begin

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

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

Deploying before you uninstall reduces the chance of failure.

Step 2 Perform prechecks.

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

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

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

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

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

Confirm that you want to uninstall and reboot the FMC.

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

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

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

Step 8 Verify success.

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

Step 9 Use the Message Center to recheck deployment health.

Step 10 Redeploy configurations.

Uninstall from High Availability FMCs

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

You uninstall from peers one at a time. With synchronization paused, first uninstall from the standby, then the active. When the standby FMC starts the uninstall, its status switches from standby to active, so that both peers are active. This temporary state is called *split-brain* and is *not* supported except during upgrade and uninstall. Do *not* make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you restart synchronization.

Before you begin

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

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

Deploying before you uninstall reduces the chance of failure.

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

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

Step 3 Pause synchronization.

a) Choose **System** > **Integration**.
b) On the **High Availability** tab, click **Pause Synchronization**.

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

Follow the instructions in Uninstall from a Standalone FMC, on page 32, 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 30.

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

Deploying before you uninstall reduces the chance of failure.

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

Step 2 Perform prechecks.

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

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

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

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

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

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

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

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

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

When you patch a Firepower appliance, an easily identifiable uninstaller for that patch is automatically created in the upgrade directory; see Uninstall Packages, on page 37.

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

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

Step 6 Monitor the uninstall.

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

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

Step 7 Verify success.

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

Step 8 Use the Message Center to recheck deployment health.

Step 9 Redeploy configurations.

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

What to do next

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

Uninstall from ASA FirePOWER (ASDM Managed)

Use this procedure to uninstall a patch from a locally managed ASA FirePOWER module. If you manage ASA FirePOWER with an FMC, see Uninstall from Any Device (FMC Managed), on page 34.

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 30.

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

Deploying before you uninstall reduces the chance of failure.

Step 2 Perform prechecks.

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

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

You can either SSH to the module's management interface (hostname or IP address) or use the console. Note that the console port defaults to the ASA CLI and you must use the `session sfr` command to access the Firepower CLI.

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

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

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

Do not untar signed (.tar) packages.

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

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

Step 6 Monitor the uninstall.

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

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

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

Step 7 Verify success.

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

Step 8 Redeploy configurations.

What to do next

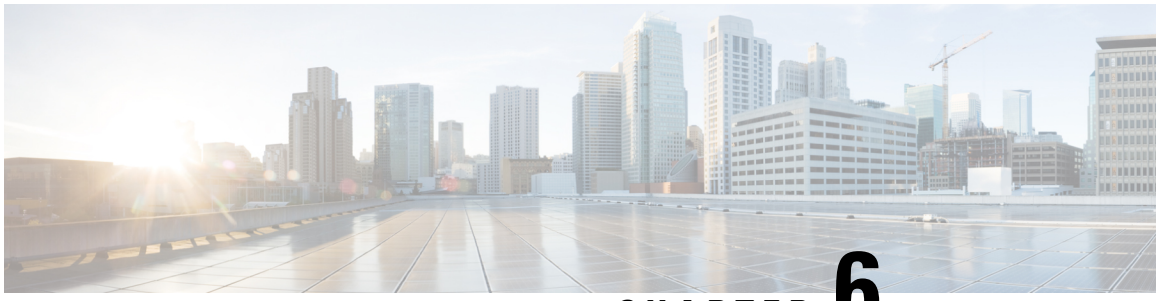
For ASA failover/cluster deployments, repeat this procedure for each device in your planned sequence.

Uninstall Packages

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

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

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



CHAPTER 6

Install the Software

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

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

Installation Checklist and Guidelines

Reimaging returns most settings to factory defaults, including the system password. This checklist highlights actions that can prevent common reimage issues. However, this checklist is *not* comprehensive. See the appropriate installation guide for full instructions: Installation Instructions, on page 42.

Table 33:

✓	Action/Check
	Check appliance access. If you do not have physical access to an appliance, the reimage process lets you keep management network settings. This allows you to connect to the appliance after you reimage to perform the initial configuration. If you delete network settings, you *must* have physical access to the appliance. You cannot use Lights-Out Management (LOM). **Note** Reimaging to an earlier version automatically deletes network settings. In this rare case, you must have physical access. For devices, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also able to access the FMC management interface without traversing the device.

✓	Action/Check
	Perform backups. Back up before reimaging, when supported. Note that if you are reimaging so that you don't have to upgrade, due to version restrictions you cannot use a backup to import your old configurations. You must recreate your configurations manually. **Caution** We *strongly* recommend you back up to a secure remote location and verify transfer success. Reimaging returns most settings to factory defaults, including the system password. It deletes any backups left on the appliance. And especially because backup files are unencrypted, do *not* allow unauthorized access. If backup files are modified, the restore process will fail. Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your deployment.
	Determine if you must remove devices from FMC management. If you plan to manually configure the reimaged appliance, remove devices from remote management before you reimage: • If you are reimaging the FMC, remove all its devices from management. • If you are reimaging a single device or switching from remote to local management, remove that one device. If you plan to restore from backup after reimaging, you do not need to remove devices from remote management.
	Address licensing concerns. Before you reimage *any* appliance, address licensing concerns. You may need to unregister from the Cisco Smart Software Manager (CSSM) to avoid accruing orphan entitlements, which can prevent you from reregistering. Or, you may need to contact Sales for new licenses. For more information, see: • The configuration guide for your product. • Unregistering Smart Licenses, on page 41 • Cisco Firepower System Feature Licenses Guide • Frequently Asked Questions (FAQ) about Firepower Licensing

Reimaging Firepower 1000/2100 Series Devices to Earlier Major Versions

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

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

Reimaging Version 5.x Hardware to Version 6.3.0+

The renamed installation packages in Version 6.3+ cause issues with reimaging older *physical* appliances: FMC 2000 and 4000. If you are currently running Version 5.x and need to freshly install Version 6.5.0, rename the installation package to the "old" name after you download it; see the *Renamed Upgrade and Installation Packages* information in the Cisco Firepower Release Notes, Version 6.3.0.

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

Unregistering Smart Licenses

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

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

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

Manually unregister from CSSM before you:

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

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

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

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

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

Installation Instructions

Table 34: Firepower Management Center Installation Instructions

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

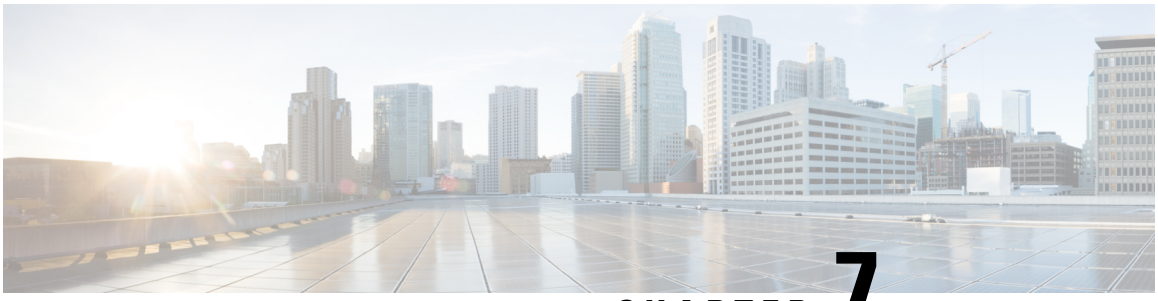
Table 35: Firepower Threat Defense Installation Instructions

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

Table 36: NGIPSv and ASA FirePOWER Installation Instructions

NGIPS Platform	Guide
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware

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



CHAPTER 7

Documentation

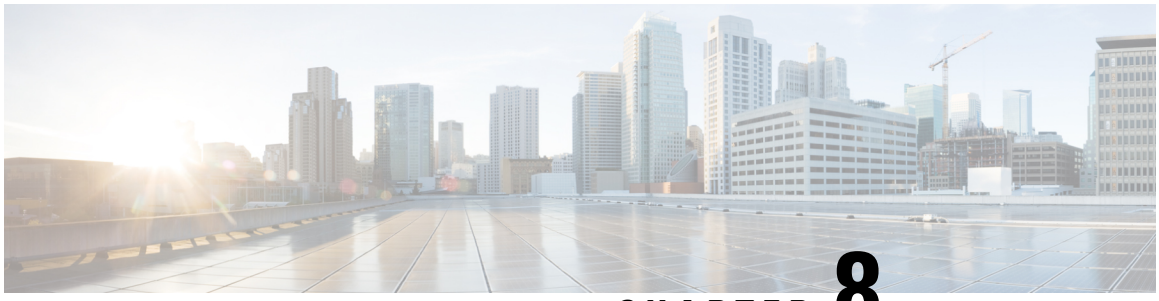
We update Firepower documentation if a patch requires it.

- Documentation Roadmaps, on page 45

Documentation Roadmaps

Documentation roadmaps provide links to currently available and legacy documentation:

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



CHAPTER 8

Resolved Issues

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

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

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

Version 6.5.0.5 Resolved Issues

Table 37: Version 6.5.0.5 Resolved Issues

Bug ID	Headline
CSCtb41710	ASA revocation-check to fall back to none only if CDP is unavailable
CSCuj60109	ENH: SFP transceivers attached to ASA-IC-6GE-SFP-A are not shown by CLI
CSCuw95798	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerabilities
CSCuy53106	ASA OS incorrectly calculates certificate expiry date in Syslog 717054
CSCuz24872	Original Client IP does not populate for dropped events when inline normalization enabled
CSCvb92169	ASA should provide better fragment-related logs and ASP drop reasons
CSCvg59385	ASA scansafe connector takes too long to failover to secondary CWS Tower

Bug ID	Headline
CSCvj00997	"show open-network-ports" not showing the proper information on FPR4100 Series
CSCvj93609	ASA traceback on spin_lock_release_actual
CSCvm77115	Lina Traceback due to invalid TSC values
CSCvn27043	Hostscan: LastSuccessfulInstallParams can not be detected by Hostscan
CSCvn64647	ASA traceback and reload due to tcp_retrans_timeout internal thread handling
CSCvn93683	ASA: cluster exec show commands not show all output
CSCvo60166	KP: Can't login to fxos due to disk full error
CSCvp57643	FTD/ASA - Cluster/HA - Master/Active unit does not update all the route changes to Slaves/Standby
CSCvp60088	2100 generating error on FMC "[FSM.FAILED].Retrieve application attributes"
CSCvp67033	ASA: Cannot distinguish name aliases for IPv6 and displays a "incomplete command" error message
CSCvp93468	Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability
CSCvp94478	ASA scp quite slow
CSCvp99327	FMC UI Unresponsive After Attempt To Register Smart License With Smart Satellite
CSCvq20707	Snort rendering block verdict for rules with action of alert.
CSCvq24258	Increase number of worker for mojo-server on large appliances
CSCvq34340	FTD traffic outage due to 9344 block size depletion caused by the egress-optimization feature
CSCvq37913	VPN-sessiondb does not replicate to standby ASA
CSCvq38889	slib memory manager : mempool mutex vs spinlock selection
CSCvq39344	Firepower managed devices may stop responding to SNMPv3 GET/WALK requests
CSCvq43920	Cisco Firepower Threat Defense Software Hidden Commands Vulnerability
CSCvq50944	OSPFv3 neighborship is flapping every ~30 minutes
CSCvq53902	Cisco Firepower Management Center Multiple Cross-Site Scripting Vulnerabilities
CSCvq55426	Adding an ipv6 default route causes CLI to hang for 50 seconds
CSCvq61601	OpenSSL vulnerability CVE-2019-1559 on FTD
CSCvq65864	Traceback in HTTP Cli Exec with rest-api agent enabled
CSCvq73464	ipv6 address of asa where ip-client is enabled is not showing in snmptrap logs

Bug ID	Headline
CSCvq78126	V route is missing even after setting the reverse route in Crypto map config in HA-IKEv2
CSCvq84430	ASA appliance mode shows port-channel member interfaces as "unassociated"
CSCvq93640	WRL6 and WRL8 commit id update in CCM layer (sprint 67)
CSCvq95826	DCD Causes Standby to send probes
CSCvq99107	Hot swap of SFP is not taking effect on the ASA
CSCvr02080	CPU Hogs observed in CERT API process while decoding the CRL with large number of entries in it
CSCvr07460	ASA traceback and reload related to crypto PKI operation
CSCvr09399	Dynamic flow-offload can't be disabled
CSCvr09468	ASA traceback and reload for the CLI "Show nat pool"
CSCvr15503	ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA
CSCvr17735	SFDataCorrelator high CPU during SI update
CSCvr19922	Cluster: BGP route may go in out of sync in some scenarios
CSCvr20449	Policy deployment is reported as successful on the FMC but it is actually failed
CSCvr20486	FTD 1010 Passive interfaces does not receive unicast packets
CSCvr20757	Block leak on ASA while running Cisco Umbrella DNS inspection
CSCvr20876	low memory causes kernel to invoke - oom and reload device - modified rlimit for KP
CSCvr20893	FTD in HA pair crashes in ids_event_proce process after policy deployment
CSCvr23986	Cisco ASA & FTD devices may reload under conditions of low memory and frequent complete MIB walks
CSCvr30694	FMC : FMC detect HA Sync Failed
CSCvr33586	FPR1010 - Add temperature/warnings for SSD when thresholds are exceeded
CSCvr35125	Packet loss over failover link triggers Split-Brain
CSCvr37502	libexpat Improper Parsing Denial of Service Vulnerability
CSCvr39556	Segfault in libclamav.so (in the context of SFDataCorrelator)
CSCvr42344	Traceback on snp_policy_based_route_lookup when deleting a rule from access-list configured for PBR
CSCvr43341	FDM 6.5.0 - FPR1000 GUI Unresponsive if upgraded with Trunk Interfaces

Bug ID	Headline
CSCvr49729	Fail-to-Wire ports showing down for FPR2100, FTW configuration API takes long to finish
CSCvr49833	Cisco Firepower 2100 Series Security Appliances ARP Denial of Service Vulnerability
CSCvr50509	Some 3DES related configurations are lost after booted
CSCvr50630	ASA Traceback: SCTP bulk sync and HA synchronization
CSCvr51955	Estreamer should terminate a connection when not receiving ACKs for a long time
CSCvr51998	ASA Static route disappearing from asp table after learning default route via BGP
CSCvr55518	Missing clean up on rule creation failure.
CSCvr56031	FTD/LINA Traceback and reload observed in thread name: cli_xml_server
CSCvr57605	ASA after reload had license context count greater than platform limits
CSCvr58411	RRI on static HUB/SPOKE config is not working on HUB when a new static SPOKE is added or deleted
CSCvr61252	systems must enforce controls that prevent confidential information from being stored within cookie
CSCvr66840	Management Interface operational state related fault is seen on fpr1000/fpr2100 platforms
CSCvr68146	Unable to auto-rejoin FTD cluster
CSCvr70895	LCMB: Dynamic medium page allocation can lead to memory depletion
CSCvr76029	FTD-HA: after restoring FTD-HA backup file, snort process will be down
CSCvr79974	Configuration might not replicated if packet loss on the failover Link
CSCvr80164	WR6 and WR8 commit id update in CCM layer(sprint 72)
CSCvr80621	FMC External Authentication with SecurID RSA fails with banner enabled
CSCvr86077	ASA Traceback/pagefault in Datapath due to re_multi_match_ascii
CSCvr89663	Traceback: with thread name: pix_flash_config_thread WM1010 went into reboot loop
CSCvr90965	FTDv Deployment in Azure causes unrecoverable traceback state due to no dns domain-lookup any"
CSCvr92168	Cisco ASA and Cisco FTD Software OSPF Packets Processing Memory Leak Vulnerability
CSCvr92311	Standby ASA logging %ASA-4-720022: (VPN-Secondary) Cannot find trust point __tmpCiscoM1Root__
CSCvr92327	ASA/FTD may traceback and reload in Thread Name 'PTHREAD-1533'

Bug ID	Headline
CSCvr92617	NPE in SecurityIntelligenceEoConvertor causes Lucene indexing failure
CSCvr93978	ASA traceback and reload on Thread DATAPATH-0-2064
CSCvr99222	NTP configuration is not synchronized to LINA on Multi Instance
CSCvs00023	port manager crashes with "shutdown" command from clish CLI
CSCvs01422	Lina traceback when changing device mode of FTD
CSCvs02954	ASA OSPF: Prefix removed from the RIB when topology changes, then added back when another SPF is run
CSCvs03023	Clustering module needs to skip the hardware clock update to avoid the timeout error and clock jump
CSCvs04067	Not able to access FMC devices with Chrome on Mac after upgrade to Catalina.
CSCvs04179	ASA - 9.8.4.12 traceback and reload in ssh or fover_rx Thread
CSCvs05066	Snort file mempool corruption leads to performance degradation and process failure.
CSCvs05262	Decrement TTL display wrong result
CSCvs07668	FTD traceback and reload on thread DATAPATH-1-15076 when SIP inspection is enabled
CSCvs07982	ASA TRACEBACK: sctpProcessNextSegment - SCTP_INIIT_CHUNK
CSCvs09533	FP2100: Traceback and reload when processing traffic through more than two inline sets
CSCvs10748	Cisco ASA Software and FTD Software Web Services Denial of Service Vulnerability
CSCvs15972	Network Performance Degradation when SSL policy is enabled
CSCvs16073	snmp poll failure with host and host-group configured
CSCvs16395	Unable to download bundles on FPR2100
CSCvs17319	[IMS_6_7_0] WM 'format everything' command bricks the device starting with fxos 82.9.1.112
CSCvs19968	Fix consoled from getting stuck and causing HA FTD policy deployment errors.
CSCvs23040	Expected output for time zone is not found while executing "show clock" command.
CSCvs24215	Firepower Device Manager (FDM) option to disable SSL rekey is not reflected on the config
CSCvs26402	NAT policy configuration range limit to be imposed for non service cmds as well
CSCvs27264	mroute entries on ASA not getting refreshed.

Bug ID	Headline
CSCvs28213	ASA Traceback in Thread Name SSH with assertion slib_malloc.c
CSCvs28290	Cisco Firepower Threat Defense Software SSL Input Validation Denial of Service Vulnerabili
CSCvs28580	Traceback when processing SSL traffic under heavy load
CSCvs29779	ASA may traceback and reload while waitinPC g for "DATAPATH-12-1899" process to finish.
CSCvs31159	Incorrect empty location handling inside CSCOGet_location wrapper
CSCvs31443	ASA reporting negative memory values on "%ASA-5-321001: Resource 'memory' limit'" message
CSCvs31470	OSPF Hello causing 9K block depletion, control point CPU 100% and cluster unstable.
CSCvs32907	Addition of debug counters for STRAP implementation.
CSCvs33102	ASA/FTD may traceback and reload in Thread Name 'EIGRP-IPv4'
CSCvs33416	Upgrade kernel to cpe:2.3:o:linux:linux_kernel:4.14.158:
CSCvs33852	After upgrade to version 9.6.4.34 is not possible to add an access-group
CSCvs34854	FMC generates referred interfaces cli delta after access-list cli delta
CSCvs37013	Prevent octeon_init from getting stuck and causing HA FTD policy deployment errors.
CSCvs38785	Inconsistent timestamp format in syslog
CSCvs40230	ICMP not working and failed with inspect-icmp-seq-num-not-matched
CSCvs42799	After FXOS upgrade, App Instance failed to start with Checksum Verification Fail
CSCvs43154	Secondary ASA is unable to join the failover due to aggressive warning messages.
CSCvs45111	WR6 and WR8 commit id update in CCM layer(sprint 75)
CSCvs45548	reactivation-mode timed causing untimely reactivation of failed server
CSCvs47252	ASA traceback and reload when running command "clear capture /"
CSCvs47283	Traffic may match an access-list incorrectly with object-group-search enabled
CSCvs50459	Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability
CSCvs50931	Policy deployment fails subsequent to SRU
CSCvs50952	Upgrade of 6.4.0.4-34 to 6.4.0.6 is deleting Static Route
CSCvs52169	ASA sends malformed RADIUS message when device-id from AnyConnect is too long

Bug ID	Headline
CSCvs55603	ICMP Reply Dropped when matched by ACL
CSCvs56888	Cisco Firepower Threat Defense Software TCP Flood Denial of Service Vulnerability
CSCvs59056	ASA/FTD Tunneled Static Routes are Ignored by Suboptimal Lookup if Float-Conn is Enabled
CSCvs59487	Observed crash in KP device while upgrading to 99.14.1.64 image.
CSCvs59866	Remove unsupported fast mode lacppolicy configuration from FXOS on Firepower 2100
CSCvs59966	false reported value for OID "cipSecGlobalActiveTunnels" - same as ASDM
CSCvs61392	On firepower devices, hardware rules are not updated after successful policy deployment
CSCvs61701	DME process crash due to memory leak on Firepower 2100
CSCvs63484	SAML tokens are not removed from hash table
CSCvs70260	IKEv2 vpn-filter drops traffic with implicit deny after volume based rekey collision
CSCvs71766	Cisco Firepower Management Center Software Open Redirect Vulnerability
CSCvs72393	FPR1010 temperature thresholds should be changed
CSCvs73663	ASA Traceback on IPsec message handler Thread
CSCvs73754	ASA/FTD: Block 256 size depletion caused by ARP of BVI not assigned to any physical interface
CSCvs74452	SFDatacorrelator and Snort process cores repeatedly while loading malware seed file
CSCvs76605	Wrong Module version listed for FXOS 2.6(1.174)
CSCvs77334	FTD failover due to error "Inspection engine in other unit has failed due to snort and disk failure"
CSCvs77818	Traceback: spin_lock_fair_mode_enqueue: Lock (np_conn_shrlock_t) is held for a long time
CSCvs78252	ASA/Lina Offloaded TCP flows interrupted if TCP sequence number randomizer is enabled and SACK used
CSCvs79023	ASA/FTD Traceback in Thread Name: DATAPATH due to DNS inspection
CSCvs80157	ASA Traceback Thread Name: IKE Daemon
CSCvs80536	FP41xx incorrect interface applied in ASA capture
CSCvs82726	Placeholder to address CSCvs31470 in Multi-Context Mode
CSCvs85467	Multiple Cisco Products Snort Application Detection Engine Policy Bypass Vulnerability

Bug ID	Headline
CSCvs87168	SNORT Fatal Error due to out of range interface ID
CSCvs88413	Port-channel bundling is failing after upgrade to 9.8 version
CSCvs90100	ASA/FTD may traceback and reload in Thread Name 'License Thread'
CSCvs91389	FTD Traceback Lina process
CSCvs91869	FPR-1000 Series Random Number Generation Error
CSCvs94061	NTP script error leading to clock drift and traffic interruption
CSCvs94486	CSCvs59487 requires additional fix for resolution
CSCvs97863	Reduce number of fsync calls during close in flash file system
CSCvs97908	Invalid scp session terminates other active http, scp sessions
CSCvs98634	catalina.<date>.log files can consume all disk space in their partition
CSCvt00113	ASA/FTD traceback and reload due to memory leak in SNMP community string
CSCvt01282	WR6 and WR8 commit id update in CCM layer(sprint 79)
CSCvt01397	Deployment is marked as success although LINA config was not pushed
CSCvt02409	Cisco Firepower Threat Defense Software Inline Pair/Passive Mode DoS Vulnerability
CSCvt03598	Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability
CSCvt04377	When maximum packet encapsulation is exceeded decoding errors are depleting disk space.
CSCvt05862	IPv6 DNS server resolution fails when the server is reachable over the management interface.
CSCvt06606	Flow offload not working with combination of FTD 6.2(3.10) and FXOS 2.6(1.169)
CSCvt06841	Incorrect access-list hitcount seen when configuring it with a capture on ASA
CSCvt09940	Cisco Firepower 4110 ICMP Flood Denial of Service Vulnerability
CSCvt11661	DOC - Clarify the meaning of mp-svc-flow-control under show asp drop
CSCvt11742	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCvt12463	ASA: Traceback in thread Unicorn Admin Handler
CSCvt13445	Cisco ASA and FTD Software FTP Inspection Bypass Vulnerability
CSCvt15062	FTD 2100: Packet drops during the transition of BYPASS to NON-BYPASS when device is rebooted

Bug ID	Headline
CSCvt15163	Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability
CSCvt18028	Cisco ASA and FTD WebVPN CRLF Injection Vulnerability
CSCvt21041	FTD Traceback in thread 'ctm_ipsec_display_msg'
CSCvt23643	VPN failover recovery is taking approx. 30 seconds for data to resume
CSCvt24328	FTD: Traceback and reload related to lina_host_file_open_raw function
CSCvt25225	ASA: Active unit HA traceback and reload during Config Sync state during OSPF sync
CSCvt26031	ASAv Unable to register smart licensing with IPv6
CSCvt26067	Active FTP fails when secondary interface is used on FTD
CSCvt26520	with FXOS 2.8.1.84, FDM UI installation of 6.5.0.2 patch fails. unzip -o fails to unzip all files
CSCvt27585	Observed traceback on 2100 while performing Failover Switch from Standby.
CSCvt28182	sctp-state-bypass is not getting invoked for inline FTD
CSCvt29049	FPR2100 - ASA in Appliance Mode - SNMP Delay
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
CSCvt33785	IPSec SAs are not being created for random VPN peers
CSCvt35897	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS Vuln
CSCvt35945	Encryption-3DES-AES should not be required when enabling ssh version 2 on 9.8 train
CSCvt36542	Multi-context ASA/LINA on FPR not sending DHCP release message
CSCvt41333	Dynamic RRI route is not destroyed when IKEv2 tunnel goes down
CSCvt43967	Pad packets received from RA tunnel which are less than or equal 46 bytes in length with zeros
CSCvt45863	Crypto ring stalls when the length in the ip header doesn't match the packet length
CSCvt46289	ASA LDAPS connection fails on Firepower 1000 Series
CSCvt46830	FPR2100 'show crypto accelerator statistics' counters do not track symmetric crypto

Bug ID	Headline
CSCvt48260	Standby unit traceback at fover_parse and boot loop when detecting Active unit
CSCvt48941	FTD Standby unit does not join HA due to "HA state progression failed due to APP SYNC timeout"
CSCvt50263	FMC Unable to fetch VPN troubleshooting logs from WM Model devices
CSCvt50946	Stuck uauth entry rejects AnyConnect user connections despite fix of CSCvi42008
CSCvt51346	PKI-CRL: Memory Leak on Download and Clear Large CRL
CSCvt51348	PKI-CRL: Memory Leak on Download Large CRL in loop without clearing it
CSCvt51349	Fragmented packets forwarded to fragment owner are not visible on data interface captures
CSCvt51987	Traffic outage due to 80 size block exhaustion on the ASA FPR9300 SM56
CSCvt52782	ASA traceback Thread name - webvpn_task
CSCvt54182	LINA cores are generated when FTD is configured to do SSL decryption.
CSCvt59015	KP IOQ driver. Add defensive parameter and state checks.
CSCvt59253	ASA 9.13.1.7 traceback and reload while processing hostscan data (process name LINA)
CSCvt60190	Cisco ASA and FTD Web Services File Upload Denial of Service Vulnerability
CSCvt63484	ASA High CPU with igb_saleen_io_sfp_mod_poll_thre process
CSCvt64035	remote acess mib - SNMP 64 bit only reporting 4Gb before wrapping around
CSCvt64270	ASA is sending failover interface check control packets with a wrong destination mac address
CSCvt64822	Cisco Adaptive Security Appliance Software SSL/TLS Denial of Service Vulnerability
CSCvt65982	Route Fallback doesn't happen on Slave unit, upon RRI route removal.
CSCvt66351	NetFlow reporting impossibly large flow bytes
CSCvt68131	FTD traceback and reload on thread "IKEv2 Mgd Timer Thread"
CSCvt68294	Adjust Firepower 4120 Maximum VPN Session Limit to 20,000
CSCvt70322	Cisco ASA Software and FTD Software Web Services Denial of Service Vulnerability
CSCvt73806	FTD traceback and reload on FP2120 LINA Active Box. VPN
CSCvt74037	Cisco FXOS Software Command Injection Vulnerability
CSCvt75241	Redistribution of VPN advertised static routes fail after reloading the FTD on FPR2100

Bug ID	Headline
CSCvt77813	High unmanaged disk usage on /ngfw due to cisco_uridb* files
CSCvt79709	FDM: Deployment Failure after editing NAT Policy containing Mapped Services
CSCvt79988	Policy deployment failure due to snmp configuration after upgrading FMC to 6.6
CSCvt83121	Cisco ASA and FTD Software OSPFv2 Link-Local Signaling Denial of Service Vulnerability
CSCvt83133	Unable to access anyconnect webvpn portal from google chrome using group-url
CSCvt86188	SNMP traps can't be generated via diagnostic interface
CSCvt90330	ASA traceback and reload with thread name coa_task
CSCvt91258	FDM: None of the NTP Servers can be reached - Using Data interfaces as Management Gateway
CSCvt92647	Connectivity over the state link configured with IPv6 addresses is lost after upgrading the ASA
CSCvt95517	Certificate mapping for AnyConnect on FTD stops working.
CSCvt97917	ASAv on AWS 9.13.1.7 BYOL image cannot be enabled for PLR
CSCvt98599	IKEv2 Call Admission Statistics "Active SAs" counter out of sync with the real number of sessions
CSCvu00112	tsd0 not reset when ssh quota limit is hit in ci_cons_shell
CSCvu03107	AnyConnect statistics is doubled in both %ASA-4-113019 and RADIUS accounting
CSCvu03562	Device loses ssh connectivity when username and password is entered
CSCvu03675	FPR2100: ASA console may hang & become unresponsive in low memory conditions
CSCvu04279	ASAv/AWS: Unable to upgrade or downgrade C5 ASAv code on AWS
CSCvu05216	cert map to specify CRL CDP Override does not allow backup entries
CSCvu05418	Import fails with local user password contains consecutive characters message
CSCvu07602	FPR-41x5: 'clear crypto accelerator load-balance' will cause a traceback and reload
CSCvu07880	ASA on QP platforms display wrong coredump filesystem space (50 GB)
CSCvu08013	DTLS v1.2 and AES-GCM cipher when used drops a particular size packet frequently.
CSCvu08422	Cisco Firepower Threat Defense Software Multi-Instance Container Escape Vulnerability
CSCvu12039	Cluster data unit might fail to synchronize SCTP configuration from the control unit after bootup

Bug ID	Headline
CSCvu12248	ASA-FPWR 1010 traceback and reload when users connect using AnyConnect VPN
CSCvu12684	HKT - Failover time increases with upgrade to 9.8.4.15
CSCvu15801	Cisco ASA and FTD Software SIP Denial of Service Vulnerability
CSCvu17924	FTD failover units traceback and reload on DATAPATH
CSCvu17965	ASA generated a traceback and reloaded when changing the port value of a manual nat rule
CSCvu20007	Config_XML_Response from LINA is not in the correct format,Lina reporting as No memory available.
CSCvu26296	ASA interface ACL dropping snmp control-plane traffic from ASA
CSCvu26561	WebVPN SSO Gives Unexpected Results when Integrated with Kerberos
CSCvu27868	ASA: Lack of specific syslog messages to external IPv6 logging server after ASA upgrade
CSCvu34413	SSH keys lost in ASA after reload
CSCvu40531	FXOS LACP packet logging to pktmgr.out and lacp.out fills up /opt/cisco/platform/logs to 100%
CSCvu43827	ASA & FTD Cluster unit traceback in thread Name "cluster config sync" or "fover_FSM_thread"
CSCvu44910	Cisco ASA Software and FTD Software Web Services Cross-Site Scripting Vulnerability
CSCvu46685	Cisco ASA and FTD Software SSL/TLS Session Denial of Service Vulnerability
CSCvu47925	Cisco ASA and FTD IP Fragment Memory Leak Vulnerability
CSCvu56286	FDM - New firewall session getting created after performing HA Failover for traffic in progress
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)
CSCvu70529	Binary rules (SO rules) are not loaded when snort reloads
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
CSCvu82743	Snort Generator ID 3 rules disabled following Snort reload
CSCvu83309	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities

Bug ID	Headline
CSCvu85346	Restore backup fails on FTD models 2100 or 1100 platforms
CSCvv02245	ASA 'session sfr' command disconnects from FirePOWER module for initial setup
CSCvv02925	OSPF neighbourship is not establising
CSCvv13835	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities
CSCvv13993	Cisco Firepower 1000 Series Bleichenbacher Attack Vulnerability
CSCvv20450	FMC 6.4 to 6.7 upgrade fails "Error running script 500_rpms/110_generate_dbaccess.sh"
CSCvv33712	Cisco ASA Software Web-Based Management Interface Reflected Cross-Site Scripting Vulnerabi
CSCvv52591	DMA memory leak in ctm_hw_malloc_from_pool causing management and VPN connections to fail
CSCvw07000	Snort busy drops with PDTS Tx queue stuck

Version 6.5.0.4 Resolved Issues

Table 38: Version 6.5.0.4 Resolved Issues

Bug ID	Headline
CSCvq35440	Upgrade Enhancements to STRAP verification for anyconnect - Cisco VPN session replay vulnerability
CSCvs55990	Deployment failure with SI DNS configured on FTD managed locally / FDM
CSCvs86257	FMC Upgrade is failing at 800_post/1025_vrf_policy_upgrade.pl

Version 6.5.0.3 Resolved Issues

Version 6.5.0.3 was removed from the Cisco Support & Download site on 2019-02-04 (for FMCs) and 2020-03-02 (for devices). If you are running this version, it is safe to continue. The bugs listed here are also fixed in Version 6.5.0.4.

Table 39: Version 6.5.0.3 Resolved Issues

Bug ID	Headline
CSCvd33448	fireamp.pl using 100% Cpu after restore backup.
CSCvk55766	Try to assign devices to platform settings policy list of devices randomly disappear under policy

Bug ID	Headline
CSCvm85823	Not able to ssh, ssh_exec: open(pager) error on console
CSCvo76866	Traceback on 2100 - watchdog
CSCvp04134	Traceback in HTTP Cli Exec when upgrading to 9.12.1
CSCvp06526	Manage the sfhassd thread CPU affinity to match the Snort CPU affinity
CSCvp70833	ASA/FTD: Twice nat Rule with same service displaying error "ERROR: NAT unable to reserve ports"
CSCvq29167	Physical interface goes to link UP state in spite of disable interface during bootingup.
CSCvq46587	After failover, Active unit tcp sessions are not removed when timeout reached
CSCvq50587	ASA/FTD may traceback and reload in Thread Name 'BGP Router'
CSCvq51284	FPR 2100, low block 9472 causes packet loss through the device.
CSCvq76198	Traffic interruptions for FreeBSD systems
CSCvq81516	VPN events between 12 and 1 PM UTC are not displayed on the FMC
CSCvq87797	Multiple context 5585 ASA, transparent context losing mangement interface configuration.
CSCvq88644	Traceback in tcp-proxy
CSCvq93572	Unable to add user on FTD using external authentication
CSCvq96495	Console connection for FPR2100 is disconnected randomly about 20 minutes.
CSCvr13278	PPPoE session not coming up after reload.
CSCvr20486	FTD 1010 Passive interfaces does not receive unicast packets
CSCvr21803	Mac address flap on switch with wrong packet injected on ingress FTD interface
CSCvr25768	ASA may traceback on display_hole_og
CSCvr29978	Changing a rule and saving quickly might remove configuration.
CSCvr38379	Upgraded FTD will not reimage to base FTD version with the use of 'auto-install' feature in FPR2100
CSCvr50266	Dual stack ASAv failover triggered by reload issue
CSCvr53058	AC policy lookup done for SYN+ACK packet when tcp-intercept and a monitor AC policy is configured
CSCvr54054	Mac Rewrite Occurring for Identity Nat Traffic
CSCvr54980	FPR2100: Power doesn't turn off after turned off the power button on back of chassis
CSCvr55400	FTD/LINA traceback and reload observed in thread name: cli_xml_server

Bug ID	Headline
CSCvr55678	ClamAV zip-bomb Migration Vulnerability for 6.5.0.2 and above
CSCvr60111	configurations getting wiped off from standby, while deployment fails on active
CSCvr61492	device loading slow, related REST API calls
CSCvr66768	Lina Traceback during FTD deployment when PBR config is being pushed
CSCvr72665	FMC upgrading to 6.3/6.4 shouldn't remove existing deprecated flexconfig
CSCvr73115	Initial FTD Deploy After Policy Import causes Unused Objects which bloat policy size
CSCvr78166	Deployment failed on FTD with reason "failed to retrieve running configuration"
CSCvr78832	SSH: Newly created Local Users unable to login when device is managed locally
CSCvr81457	FTD traceback when TLS tracker (tls_trk_sniff_for_tls) attempted to free a block.
CSCvr82133	Unable to add routes and select interface from Device management page after FMC upgrade to 6.5
CSCvr84572	FMC 6.5 - Failed user login on FMC does not record entry in audit log
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
CSCvs10443	6.5 CloudEvent code writes config files in a way that 6.4 code does not understand
CSCvs10526	Throttle SSE Attempts on FTDs
CSCvs15276	ERROR: entry for ::/0 exists when configuring ipv6 icmp
CSCvs32023	Disable egress-optimization by default
CSCvs39589	ASA doesn't honor SSH Timeout When Data Channel is not Negotiated
CSCvs40531	AnyConnect 4.8 is not working on the FPR1000 series
CSCvs53705	Anyconnect sessions limited incorrectly
CSCvs61555	Policy Deployment Failures and Intrusion Policy Editor hanging due to improper Snort deletion

Version 6.5.0.2 Resolved Issues

Table 40: Version 6.5.0.2 Resolved Issues

Bug ID	Headline
CSCvr52109	FTD may not match correct Access Control rule following a deploy to multiple devices
CSCvr88123	multi-deploy causes a sudden drop of intrusion events
CSCvs28768	Cisco Firepower Software WhatFix Walkthrough Data Issue

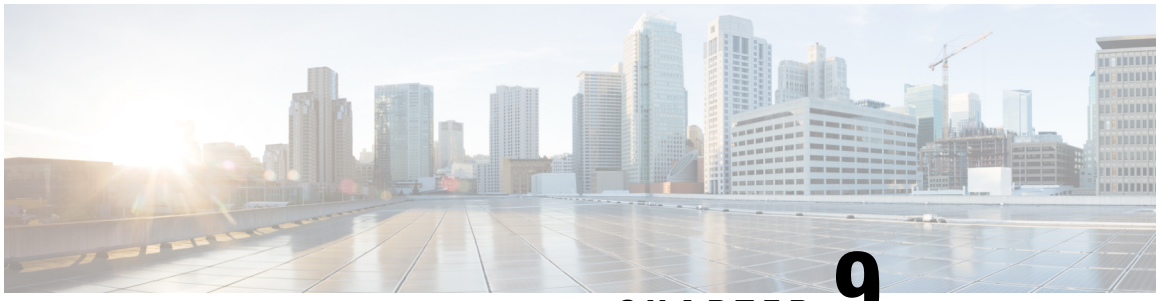
Version 6.5.0.1 Resolved Issues

Version 6.5.0.1 was removed from the Cisco Support & Download site on 2019-12-19. If you are running this version, we recommend you upgrade. The bugs listed here are also fixed in Version 6.5.0.2.

Table 41: Version 6.5.0.1 Resolved Issues

Bug ID	Headline
CSCva36446	ASA Stops Accepting Anyconnect Sessions/Terminates Connections Right After Successful SSL handshake
CSCvo88762	FTD inline/transparent sends packets back through the ingress interface
CSCvp29554	Watchdog traceback due to lina_host_file_stat calls
CSCvp69229	OpenSSL 0-byte Record Padding Oracle Information Disclosure Vulnerabil
CSCvp81083	ASA/Lina Traceback related to TLS/VPN
CSCvq09093	VPN Pre-deploy validations takes around 20 seconds for each device
CSCvq29969	Firepower Recommendations rule count changes even when not regenerated
CSCvq40943	FTD 4150 VPN s2s deployment failure with 6K spokes
CSCvq43453	Overrides cannot be added for port object if it is used in variable sets in sub domains
CSCvq45000	Policy deployment to FP 8000 sensor is failing when NAT is configured
CSCvq53915	Cisco Firepower Management Center Multiple Cross-Site Scripting Vulnerabilities
CSCvq56257	Cached malware disposition does not always expire as expected
CSCvq63024	Dual stacked ASAv manual failover issues
CSCvq67271	Retrieving an specfic rule by ID of a child Access Policy returns a 404 : Not Found status.
CSCvq70485	Slow "securityzones" REST API

Bug ID	Headline
CSCvq70775	FPR2100 FTD Standby unit leaking 9K blocks
CSCvq83019	Long processing time to insert policy deploy task if many application filter object used in ACPolicy
CSCvq83168	DNS lookup using mgmt VRF not possible because FMC doesn't allow interface after server address
CSCvq92126	ASA traceback in Thread IPsec Message Handler
CSCvq93640	WRL6 and WRL8 commit id update in CCM layer (sprint 67)
CSCvq94729	Deployment rollback causes momentary traffic drop when error in a LINA ONLY section of delta cli
CSCvq95058	IPSEC SA is deleted by failover which is caused by link down
CSCvr00892	where clause not working for external data base access
CSCvr04954	FMC 6.4.0 - Stack unit on different Domain fails the deployment after upgrade
CSCvr07421	Policy deployment fails with 400+ interfaces in security zone due to incorrect formation of deployDB
CSCvr10777	ASA Traceback in Ikev2 Daemon
CSCvr11395	Only a subset of devices where deployed from a device group during scheduled deploy
CSCvr12018	ASA: VPN traffic fails to take the tunnel route when the default route is learnt over BGP.
CSCvr23580	Can't delete 2 or more than two IP address-pool
CSCvr25954	FTD/LINA Standby may traceback and reload during logging command replication from Active
CSCvr27445	App-sync failure if unit tries to join HA during policy deployment
CSCvr29638	HA FTD on FPR2110 crash after deploy ACP from FMC
CSCvr35956	Block double-free when combining ServerKeyExchange and ClientKeyExchange fails --> lina crashes
CSCvr36687	Overrides cannot be added for network object if it is used in variable sets in sub domains
CSCvr37486	established rules in asp table are not un-installed on config removal
CSCvr44123	Unable to login via chassis Manager or Rest api in FPR2100 if session timeout is non-deafult
CSCvr95287	Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability



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 6.5.0 Known Issues, on page 65

Version 6.5.0 Known Issues

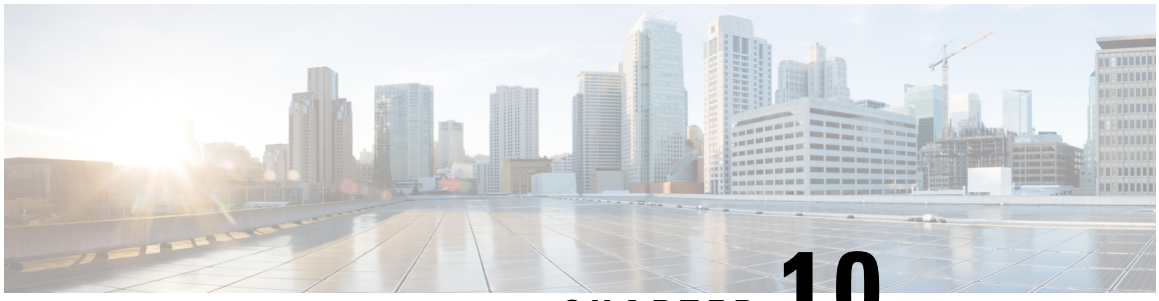
Table 42: Version 6.5.0 Known Issues

Bug ID	Headline
CSCvq03466	ISA 3000 FTD deployment fails with hardware-bypass activated
CSCvq11310	FTD performance has dropped approximately 5% in 6.5 SRTS runs
CSCvq30293	Bootstrap configuration is not updated after FTD version downgrade
CSCvq47804	FXOS security module will not power up after shutdown from FDM.
CSCvq91091	ASA 55xx series perform slower than expected on 6.5 in 1024B and MaxCPS tests
CSCvr09194	core.run_hm.pl found post FXOS upgrade
CSCvr17786	API GET call for access policy with HitCount "true" and filter "fetchZeroHitCount" returns all rules
CSCvr21119	Power cycling needed on FP1000 units when upgraded from 6.4 to 6.5 for SSD secure erase

Bug ID	Headline
CSCvr22260	Pair of HA FP2100 may exhibit crash in LINA when under load and low on memory
CSCvr23986	Cisco ASA & FTD devices may reload under conditions of low memory and frequent complete MIB walks
CSCvr24059	Source SGT correlation doesn't work for FMC and FTD 6.5
CSCvr28977	FTD: API Automatic Malware updates are downloaded even when its turned off in API
CSCvr34163	VLAN ID should not be seen under intrusion events when FTD is in routed or transparent mode
CSCvr35470	CloudAgent core on FMCv - 6.5.0
CSCvr37728	ADI process can crash and core after reconnecting to ISE in a corner case
CSCvr39516	lina segfault/reload caused by malloc failure in modexp-octeon
CSCvr39818	FTD: Switching interface IP from static to DHCP causes FTD to use different DHCP client-ids
CSCvr46892	Interface remains shutdown after switching between modes
CSCvr47499	Firepower FMC upgrade failure at 800_post/1028_latency_settings_upgrade.pl
CSCvr82603	Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability
CSCvr98881	Traceback: FTD ZeroMQ memory assertion
CSCvs02233	OpenSSH auth-gss2.c Information Disclosure Vulnerability
CSCvs02234	OpenSSH Bailout Delaying User Enumeration Vulnerability
CSCvs07159	Dev-side fix needed for online help: Fix Duplicate Help IDs
CSCvs07425	Max conn test will not reach 60 M conn after clear conns couple times
CSCvs08696	Firepower Chassis Manager Showing Smart Agent Disabled after upgrade to 2.7.1
CSCvs25517	Race condition for FMC API and GUI to fetch ACPs
CSCvs31114	Warning about not supported bypass revocation checking for FTD 6.5 and higher
CSCvs67534	Allowed to download zipped malware for first time
CSCvs79606	"dns server-group DefaultDNS" cli not getting negated
CSCvt22254	Auto Deploy fails after Restore if FDM cannot reach update server
CSCvt35770	Version mismatch errors after upgrade resulting in policy deployment failures
CSCvt43309	URL Filter license prevents policy deployment on all sensors if any one is missing the URL license

Bug ID	Headline
CSCvt45206	Event search may fail when searching events that existed before upgrade
CSCvt48260	Standby ASA Traceback at fover_parse and boot loop when detecting Active unit
CSCvt49308	ASA Traceback in thread name: CERT API memory leak while processing CRLs
CSCvt52604	Interfaces page from Objects section of the FMC does not load (domains page is likely affected also)
CSCvt52782	ASA traceback Thread name - webvpn_task
CSCvt54182	LINA cores are generated when FTD is configured to do SSL decryption.
CSCvt54286	FTD-UI: Self signed Certificate UI has hardcoded life of 5 years
CSCvt54286	FTD-UI: Self signed Certificate UI has hardcoded life of 5 years
CSCvt59253	ASA 9.13.1.7 traceback and reload on process name LINA
CSCvt63484	ASA High CPU with igb_saleen_io_sfp_mod_poll_thre process in 9.13(1)7
CSCvt63501	check heaps process failure seen on WM when uploading a 150Mb+ file
CSCvt63746	FDM /ngfw/var/sf/fwcfg/zones.conf is empty
CSCvt74893	FMCv Ethernet driver indicates vmxnet3 TCP performance compromised
CSCvt77813	High unmanaged disk usage on /ngfw due to cisco_uridb* files
CSCvt79777	duplicate ip addresses in sfipproxy.conf
CSCvt86439	marked version 0.3.6 and earlier is vulnerable to an XSS attack in the
CSCvt86583	marked is an application that is meant to parse and compile markdown.
CSCvt95268	idn in GNU libidn before 1.33 might allow remote attackers to obtain s
CSCvt95284	PCRE 7.8 and 8.32 through 8.37, and PCRE2 10.10 mishandle group empty
CSCvt95288	res_query in libresolv in glibc before 2.25 allows remote attackers to
CSCvt95323	Stack-based buffer overflow in the glob implementation in GNU C Librar
CSCvt95348	The makecontext function in the GNU C Library (aka glibc or libc6) bef
CSCvt95349	idn in libidn before 1.33 might allow remote attackers to obtain sensi
CSCvt95350	The idna_to_ascii_4i function in lib/idna.c in libidn before 1.33 allo
CSCvt95355	Stack-based buffer overflow in the getaddrinfo function in sysdeps/pos
CSCvt95375	The compile_branch function in pcre_compile.c in PCRE 8.x before 8.39
CSCvt95399	Memory leak in the __res_vinit function in the IPv6 name server manage

Bug ID	Headline
CSCvt95451	An SSE2-optimized memmove implementation for i386 in sysdeps/i386/i686
CSCvt95468	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-
CSCvt95469	The glob function in glob.c in the GNU C Library (aka glibc or libc6)
CSCvt95492	In shadow before 4.5, the newusers tool could be made to manipulate in
CSCvt95514	An issue was discovered in ide_dma_cb() in hw/ide/core.
CSCvt95564	In the GNU C Library (aka glibc or libc6) through 2.29,
CSCvt95651	GNU glibc elf/dl-load.c Local Privilege Escalation Vulnerability
CSCvt95675	Glibc in_realpath() Underflow Local Code Execution Vulnerability
CSCvt95719	GNU glibc getnetbyname Function Buffer Overflow Vulnerability
CSCvu05331	Cloud configuration links don't support the new APJ region
CSCvu05418	Import fails with local user password contains consecutive characters message
CSCvu20600	A use-after-free vulnerability introduced in glibc upstream version 2.
CSCvu26476	FTD Cluster unable to rejoin due to "process_create: out of stack memory "
CSCvu38870	The jQuery framework exchanges data using JavaScript Object Notation (
CSCvu43156	Upgrade appears hung on FMC at 11% but shows failed on sensor
CSCvu45952	Stack-based buffer overflow in the clntudp_call function in sunrpc/cln
CSCvu46890	FMCv300 requesting wrong license after migration using sf-migration.pl
CSCvu47941	Unexpected FTD traceback and reboot due to Lina core
CSCvu73496	Internal1/1 data interface goes down without any reason or logs.
CSCvu75855	stunnel process enabled on managed device when it should not be
CSCvu80802	FTD Traceback On Thread Name: CP DP SFR Event Processing
CSCvu82820	Traceback: ASDM Deployment causing ASA to reboot
CSCvu93834	FDM/FTD-API: Password cannot be changed on standby for the admin user
CSCvu94706	FXOS dynamically learning mac-address of external machine causing outage
CSCvu94715	FXOS "clear mac address-table dynamic" only removes entry from front end (not backend)
CSCvu95025	PPPoE fails to establish on ASA and FTD running on FP1010



CHAPTER 10

For Assistance

Online Resources

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

- Documentation: http://www.cisco.com/go/threatdefense-65-docs
- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.cisco.com/cisco/support/notifications.html

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

Contact Cisco

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

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