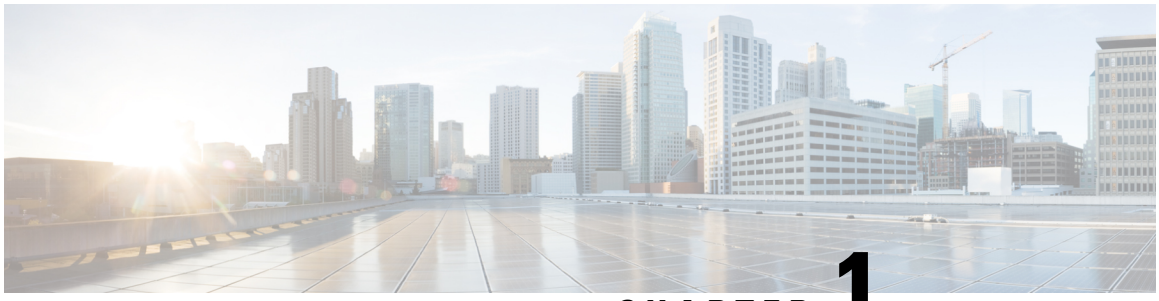
Cisco Firepower Release Notes, Version 6.2.3

First Published: 2018-03-29

Last Modified: 2022-12-21

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 release information for Version 6.2.3 of Cisco Firepower Threat Defense, Firepower Management Center, Firepower Device Manager, and Firepower Classic devices (Firepower 7000/8000 series, NGIPSv, ASA with FirePOWER Services).

Release Dates

Sometimes we release updated builds. In most cases, only the latest build for each platform is available on the Cisco Support & Download site. We *strongly* recommend you use the latest build. If you downloaded an earlier build, do not use it. For more information, see Resolved Bugs in New Builds, on page 65.

Table 1: Version 6.2.3 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.2.3.18	50	2022-02-16	All	—
6.2.3.17	30	2021-06-21	All	—
6.2.3.16	59	2020-07-13	All	—
6.2.3.15	39	2020-02-05	FTD/FTDv	—
	38	2019-09-18	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv	—
6.2.3.14	41	2019-07-03	All	—
	36	2019-06-12	All	—

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.2.3.13	53	2019-05-16	All	—
6.2.3.12	80	2019-04-17	All	—
6.2.3.11	55	2019-03-17	All	—
	53	2019-03-13	—	—
6.2.3.10	59	2019-02-07	All	—
6.2.3.9	54	2019-01-10	All	—
6.2.3.8	51	2019-01-02	No longer available.	—
6.2.3.7	51	2018-11-15	All	—
6.2.3.6	37	2018-10-10	All	—
6.2.3.5	53	2018-11-06	FTD/FTDv	—
	52	2018-09-12	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv	—
6.2.3.4	42	2018-08-13	All	—
6.2.3.3	76	2018-07-11	All	—
6.2.3.2	46	2018-06-27	All	—
	42	2018-06-06	—	—
6.2.3.1	47	2018-06-28	All	—
	45	2018-06-21	—	—
	43	2018-05-02	—	—

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.2.3	113	2020-06-01	FMC/FMCv	FMC/FMCv
	111	2019-11-25	—	FTDv: AWS, Azure
	110	2019-06-14	—	—
	99	2018-09-07	—	—
	96	2018-07-26	—	—
	92	2018-07-05	—	—
	88	2018-06-11	—	—
	85	2018-04-09	—	—
	84	2018-04-09	Firepower 7000/8000 series NGIPSv	—
	83	2018-04-02	FTD/FTDv ASA FirePOWER	FTD: Physical platforms FTDv: VMware, KVM Firepower 7000/8000 ASA FirePOWER NGIPSv
	79	2018-03-29	—	—

Suggested Release

Suggested Release: Version 7.2.5.x

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.

Sharing Data with Cisco

The following features share data with Cisco.

Cisco Success Network

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.

Web Analytics

Web analytics provides 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 by default but you can change your enrollment at any time after you complete initial setup. Note that ad blockers can block web analytics, so if you choose to remain enrolled, please disable ad blocking for the hostnames/IP addresses of your Cisco appliances.

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.

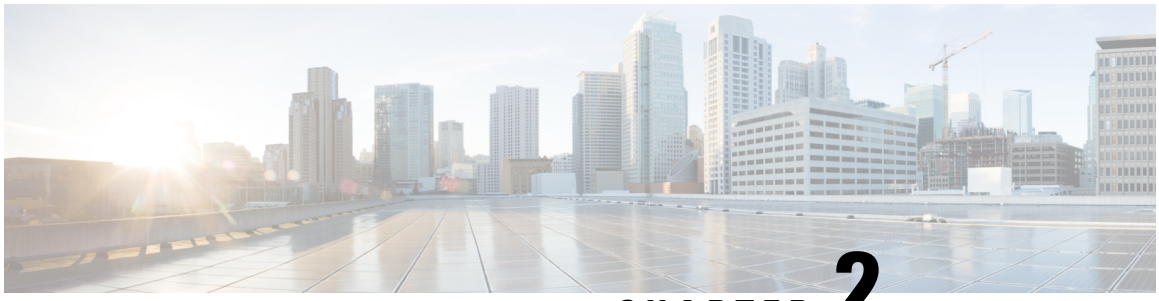
- Documentation: http://www.cisco.com/go/ftd-docs
- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.cisco.com/cisco/support/notifications.html

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



CHAPTER 2

System Requirements

This document includes the system requirements for Version 6.2.3.

FMC Platforms

The FMC provides a centralized firewall management console. For device compatibility with the FMC, see Device Management, on page 9. For general compatibility information, see the Cisco Secure Firewall Management Center Compatibility Guide.

FMC Hardware

Version 6.2.3 supports the following FMC hardware:

- Firepower Management Center 1000, 2500, 4500
- Firepower Management Center 2000, 4000
- Firepower Management Center 750, 1500, 3500 (high availability not supported for FMC 750)

You should also keep the BIOS and RAID controller firmware up to date; see the Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes.

FMCv

Version 6.2.3 supports FMCv deployments in both public and private clouds.

With the FMCv, you can purchase a license to manage 2, 10, or 25 devices. Some versions and platforms support 300 devices. For full details on supported instances, see the Cisco Secure Firewall Management Center Virtual Getting Started Guide.

Table 2: Version 6.2.3 FMCv Platforms

Platform	Devices Managed		High Availability
	2, 10, 25	300	
Public Cloud			
Amazon Web Services (AWS)	YES	—	—
Private Cloud			
Kernel-based virtual machine (KVM)	YES	—	—
VMware vSphere/VMware ESXi 5.5, 6.0, or 6.5	YES	—	—

Cloud-delivered Firewall Management Center

The Cisco Cloud-delivered Firewall Management Center is delivered via the Cisco Defense Orchestrator (CDO) platform, which unites management across multiple Cisco security solutions. We take care of feature updates. Note that a customer-deployed management center is often referred to as *on-prem*, even for virtual platforms.

At the time this document was published, the cloud-delivered Firewall Management Center could manage devices running threat defense . For up-to-date compatibility information, see the Cisco Cloud-Delivered Firewall Management Center Release Notes.

Device Platforms

Firepower devices monitor network traffic and decide whether to allow or block specific traffic based on a defined set of security rules. For details on device management methods, see Device Management, on page 9. For general compatibility information, see the Cisco Secure Firewall Threat Defense Compatibility Guide or the Cisco Firepower Classic Device Compatibility Guide.

FTD Hardware

Version 6.2.3 FTD hardware comes in a range of throughputs, scalability capabilities, and form factors.

Table 3: Version 6.2.3 FTD Hardware

Platform	FMC Compatibility		FDM Compatibility		Notes
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO	
Firepower 2110, 2120, 2130, 2140	YES	—	YES	—	—

Platform	FMC Compatibility		FDM Compatibility		Notes
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO	
Firepower 4110, 4120, 4140, 4150 Firepower 9300: SM-24, SM-36, SM-44 modules	YES	—	—	—	Requires FXOS 2.3.1.73 or later build. **Note** Firepower 6.2.3.16+ requires FXOS 2.3.1.157+. We recommend the latest firmware. See the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.
ASA 5506-X, 5506H-X, 5506W-X ASA 5512-X ASA 5515-X ASA 5508-X, 5516-X ASA 5525-X, 5545-X, 5555-X	YES	—	YES	—	ASA 5506-X, 5508-X, and 5516-X devices may require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
ISA 3000	YES	—	YES	—	May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

FTDv

Version 6.2.3 supports the following FTDv implementations. For information on supported instances, throughputs, and other hosting requirements, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.

Table 4: Version 6.2.3 FTDv Platforms

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO
Public Cloud				
Amazon Web Services (AWS)	YES	—	—	—

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO
Microsoft Azure	YES	—	—	—
Private Cloud				
Kernel-based virtual machine (KVM)	YES	—	YES	—
VMware vSphere/VMware ESXi 5.5, 6.0, or 6.5	YES	—	YES	—

Firepower Classic: Firepower 7000/8000, ASA FirePOWER, NGIPSv

Firepower Classic devices run NGIPS software on the following platforms:

- Firepower 7000/8000 series hardware comes in a range of throughputs, scalability capabilities, and form factors.
- ASA devices can run NGIPS software as a separate application (the *ASA FirePOWER module*). Traffic is sent to the module after ASA firewall policies are applied. Although there is wide compatibility between ASA and ASA FirePOWER versions, upgrading allows you to take advantage of new features and resolved issues.
- NGIPSv runs the software in virtualized environments.

Table 5: Version 6.2.3 NGIPS Platforms

Device Platform	FMC Compatibility	ASDM Compatibility	Notes
Firepower 7010, 7020, 7030, 7050 Firepower 7110, 7115, 7120, 7125 Firepower 8120, 8130, 8140 Firepower 8250, 8260, 8270, 8290 Firepower 8350, 8360, 8370, 8390 AMP 7150, 8050, 8150 AMP 8350, 8360, 8370, 8390	YES	—	—

Device Platform	FMC Compatibility	ASDM Compatibility	Notes
ASA 5506-X, 5506H-X, 5506W-X	YES	Requires ASDM 7.9(2).	Requires ASA 9.6(x) to 9.9(x). May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
ASA 5508-X, 5516-X	YES	Requires ASDM 7.9(2).	Requires ASA 9.5(2) to 9.16(x). May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
ASA 5512-X	YES	Requires ASDM 7.9(2).	Requires ASA 9.5(2) to 9.9(x).
ASA 5515-X	YES	Requires ASDM 7.9(2).	Requires ASA 9.5(2) to 9.12(x).
ASA 5525-X, 5545-X, 5555-X	YES	Requires ASDM 7.9(2).	Requires ASA 9.5(2) to 9.14(x).
NGIPSv	YES	—	Requires VMware vSphere/VMware ESXi 5.5, 6.0, or 6.5. For supported instances, throughputs, and other hosting requirements, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.

Device Management

Depending on device model and version, we support the following management methods.

FMC

All devices support remote management with FMC, which must run the *same or newer* version as its managed devices. This means:

- You *can* manage older devices with a newer FMC, usually a few major versions back. 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.
- You *cannot* upgrade a device past the FMC. Even for maintenance (third-digit) releases, you must upgrade the FMC first.

Note that in most cases you can upgrade an older device directly to the FMC's major version. However, sometimes you can manage an older device that you cannot directly upgrade, even though the target version is supported on the device. For release-specific requirements, see Minimum Version to Upgrade, on page 30.

Table 6: FMC-Device Compatibility

FMC Version	Oldest Device Version You Can Manage
7.4	7.0
7.3	6.7
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3
6.5	6.2.3
6.4	6.1
6.3	6.1
6.2.3	6.1
6.2.2	6.1
6.2.1	6.1
6.2	6.1
6.1	5.4.0.2/5.4.1.1
6.0.1	5.4.0.2/5.4.1.1
6.0	5.4.0.2/5.4.1.1
5.4.1	5.4.1 for ASA FirePOWER on the ASA-5506-X series, ASA5508-X, and ASA5516-X. 5.3.1 for ASA FirePOWER on the ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, and ASA-5585-X series. 5.3.0 for Firepower 7000/8000 series and legacy devices.

FDM

You can use FDM to locally manage a single FTD device.

ASDM

You can use ASDM to locally manage a single ASA FirePOWER module, which is a separate application on an ASA device. Traffic is sent to the module after ASA firewall policies are applied. Newer versions of ASDM can manage newer ASA FirePOWER modules.

Browser Requirements

Browsers

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

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer 10 and 11 (Windows only)

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

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

Browser Settings and Extensions

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

If you are using Microsoft Internet Explorer 10 or 11:

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

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

Screen Resolution

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

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:

- FMC or 7000/8000 series: Choose **System** (⚙) > **Configuration** > **HTTPS Certificate**.
- FDM: Click **Device**, then the **System Settings** > **Management Access** link, then the **Management Web Server** tab.

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

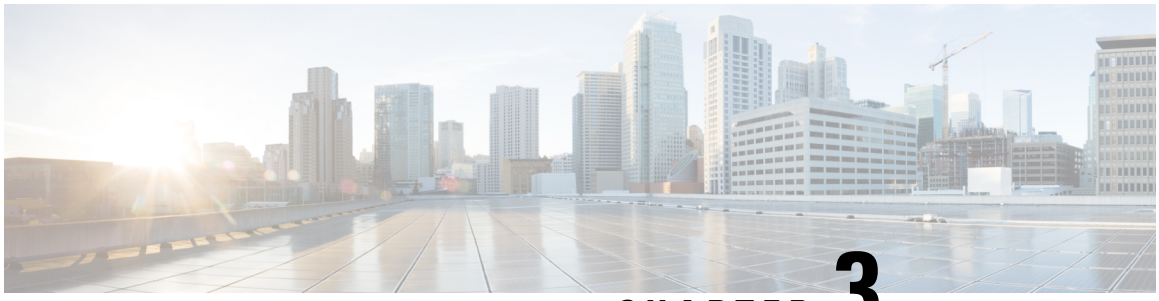
Note If you do not replace the self-signed certificate:

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

Browsing from a Monitored Network

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

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



CHAPTER 3

Features

This document describes new and deprecated features for Version 6.2.3, including upgrade impact.

Upgrade Impact

A feature has upgrade impact if upgrading and deploying can cause the system to process traffic or otherwise act differently without any other action on your part.

Upgrade impact is especially common with new threat detection and application identification capabilities. Or, sometimes the upgrade process has a special requirement; for example, if you must perform a specific task before or after upgrade (change configurations, apply health policies, redo FlexConfigs, and so on).

Upgrade impact can depend on your current platforms, version, and configurations. Note that sometimes a release reintroduces features, enhancements, and critical fixes that were included in some (but not all) previous releases. In that case, upgrade impact depends on whether you are upgrading from a supported/fixed version or from a version without the feature or fix.

Important The feature descriptions (and upgrade impact) below are for the current major version. For upgrade impact from earlier releases, see Upgrade Guidelines.

Upgrading Snort

If you are still using the Snort 2 inspection engine with threat defense, switch to Snort 3 now.

Snort 3 provides improved detection and performance. It is available starting in threat defense Version 6.7+ (with device manager) and Version 7.0+ (with management center). Snort 2 will be deprecated in a future release. You will eventually be unable to upgrade Snort 2 devices.

In management center deployments, upgrading to threat defense Version 7.2+ also upgrades eligible Snort 2 devices to Snort 3. For devices that are ineligible because they use custom intrusion or network analysis policies, manually upgrade to Snort 3. See *Migrate from Snort 2 to Snort 3* in the Firepower Management Center Snort 3 Configuration Guide.

For device manager, manually upgrade Snort. See *Intrusion Policies* in the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

New Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

Intrusion rule updates (SRUs/LSPs) provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. If a newer intrusion rule uses keywords that are not supported in your current version, that rule is not imported when you update the SRU/LSP. After you upgrade and those keywords become supported, the new intrusion rules are imported and, depending on your IPS configuration, can become auto-enabled and thus start generating events and affecting traffic flow.

The Snort release notes contain details on new keywords: https://www.snort.org/downloads.

Deprecated FlexConfig Commands

Upgrades can add web interface or Smart CLI support for features that previously required FlexConfig.

The upgrade does not convert FlexConfigs. After upgrade, configure the newly supported features in the web interface or Smart CLI. When you are satisfied with the new configuration, delete the deprecated FlexConfigs.

Caution Although you cannot newly assign or create FlexConfig objects using deprecated commands, in most cases existing FlexConfigs continue to work and you can still deploy. However, sometimes, using deprecated commands can cause deployment issues.

The feature descriptions below include deprecated FlexConfigs for the current major version. For a full list of deprecated FlexConfigs, see your configuration guide.

- FMC Features in Version 6.2.3, on page 14
- New Features in FDM Version 6.2.3, on page 22
- Intrusion Rules and Keywords, on page 26
- FlexConfig Commands, on page 27

FMC Features in Version 6.2.3

Although you can manage older devices with a newer management center, we recommend you always update your entire deployment. New traffic-handling features usually require the latest release on both the management center *and* device. Features where devices are not obviously involved (cosmetic changes to the web interface, cloud integrations) may only require the latest version on the management center, but that is not guaranteed.

Note Version 6.6 is the last release to support the Cisco Firepower User Agent software as an identity source. You cannot upgrade an FMC with user agent configurations to Version 6.7+. 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

Table 7: New Features in FMC Version 6.2.3 Patches

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

Table 8: New Features in FMC Version 6.2.3

Feature	Details
Platform	
FTD on the ISA 3000.	You can now run FTD on the ISA 3000 series. Note that the ISA 3000 supports the Threat license only. It does not support the URL Filtering or Malware licenses. Thus, you cannot configure features that require the URL Filtering or Malware licenses on an ISA 3000. Special features for the ISA 3000 that were supported with the ASA, such as Hardware Bypass, Alarm ports, and so on, are not supported with FTD in this release.
Support for VMware ESXi 6.5.	You can now deploy FMCv, FTDv, and NGIPSv virtual appliances on VMware vSphere/VMware ESXi 6.5.
Firepower Threat Defense: Encryption and VPN	
SSL hardware acceleration for Firepower 4100/9300	Firepower 4100/9300 with FTD now support SSL encryption and decryption acceleration in hardware, greatly improving performance. SSL hardware acceleration is disabled by default for all appliances that support it. **Note** This feature is renamed *TLS crypto acceleration* in Version 6.4.0+. Supported platforms: Firepower 4100/9300
Certificate enrollment improvements	Non-blocking work flow for certificate enrollment operation allows certificate enrollment on multiple FTD devices in parallel: • The administrator can now choose to have the Remote Access VPN Policy wizard enroll certificates for all devices in the policy by checking **Enroll the selected certificate object on the target devices** check box in the **Access & Certificate** step. If this is chosen, only deployment needs to be done after the wizard finishes. This is selected by default. • Administrators no longer have to initiate Remote Access VPN certificate enrollment on devices one at a time. The enrollment process for each device is now independent and can be done in parallel. • In the event of a PKS12 certificate enrollment failure, the administrator no longer needs to re-upload the PKS12 file again to retry enrollment, since it is now stored in the certificate enrollment object. Supported platforms: FTD
Firepower Threat Defense: High Availability and Clustering	
Automatically rejoin the FTD cluster after an internal failure	Formerly, many internal error conditions caused a cluster unit to be removed from the cluster, and you were required to manually rejoin the cluster after resolving the issue. Now, a unit will attempt to rejoin the cluster automatically at the following intervals: 5 minutes, 10 minutes, and then 20 minutes. Internal failures include: application sync timeout; inconsistent application statuses; and so on. New/modified command: **show cluster info auto-join** Supported platforms: Firepower 4100/9300

Feature	Details

FTD High Availability Hardening	Version 6.2.3 introduces the following features for FTD devices in high availability:
	• Whenever active or standby FTD devices in a high availability pair restart, the FMC may not display accurate high availability status for either managed device. However, the status may not upgrade on the FMC because the communication between the device and the FMC is not established yet. The **Refresh Node Status** option on the **Devices** > **Device Management** page allows you to refresh the high availability node status to obtain accurate information about the active and standby device in a high availability pair.
	• The **Devices** > **Device Management** page of the FMC UI has a new **Switch Active Peer** icon.
	• Version 6.2.3 includes a new REST API object, **Device High Availability Pair Services**, that contains four functions:
	  • **DELETE ftddevicehapairs**
	  • **PUT ftddevicehapairs**
	  • **POST ftddevicehapairs**
	  • **GET ftddevicehapairs**

Administration and Troubleshooting	
FMC High Availability Messaging	FMC high availability pairs have improved UI messaging. The UI now displays interim status messages while FMC pairs are being established and rephrased UI messaging to be more intuitive. Supported platforms: FMC
External Authentication added for FTD SSH Access	You can now configure external authentication for SSH access to FTD devices using LDAP or RADIUS. New/modified screen: **Devices** > **Platform Settings** > **External Authentication** Supported platforms: FTD
Enhanced Vulnerability Database (VDB) Installation	The FMC now warns you before you install a VDB that installing restarts the Snort process, interrupting traffic inspection and, depending on how the managed device handles traffic, possibly interrupting traffic flow. You can cancel the install until a more convenient time, such as during a maintenance window. These warnings can appear: • After you download and manually install a VDB. • When you create a scheduled task to install the VDB. • When the VDB installs in the background, such as during a previously scheduled task or as part of a Firepower software upgrade. Supported platforms: FMC

Feature	Details
Upgrade Package Push	You can now copy (or push) an upgrade package from the FMC to a managed device before you run the actual upgrade. This is useful because you can push during times of low bandwidth use, outside of the upgrade maintenance window. When you push to high availability, clustered, or stacked devices, the system sends the upgrade package to the active/control/primary first, then to the standby/data/secondary. New/modified screens: **System** > **Updates** Supported platforms: FMC
FTD serviceability	Version 6.2.3 improves the **show fail over** CLI command. The new keyword, **-history**, details to help troubleshooting. • **Show fail over history** displays failure reason along with its specific details. • **Show fail over history details** displays fail over history from the peer unit. **Note** This command includes fail over state changes and the reason for the state change for the peer unit. Supported platforms: FTD
Device list sorting	On the **Devices** > **Devices Management** page, you can use the **View by** drop-down list to sort and view the device list by any of the following categories: group, license, model, or access control policy. In a multidomain deployment, you can also sort and view by domain, which is the default display category in that deployment. Devices must belong to a leaf domain. Supported platforms: FMC
Audit log improvements	The audit log now denotes if a policy changed on the FTD Platform Settings **Devices** > **Platform Settings** page. Supported platforms: FMC with FTD
Updated FTD CLI commands	The **asa_mgmt_plane** and **asa_dataplane** options for FTD device CLI commands are renamed to **management-plane** and **data-plane** respectively. Supported platforms: FTD
Cisco Success Network	**Upgrade impact.** 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. For more information, see Sharing Data with Cisco, on page 3. Supported platforms: FMC

Feature	Details
Web Analytics Tracking	**Upgrade impact.** Web analytics provides 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. Initial setup enrolls you in web analytics tracking by default, but you can change your enrollment at any time after that. Upgrades can also enroll or re-enroll you in web analytics tracking. For more information, see Sharing Data with Cisco, on page 3. Supported platforms: FMC
Performance	
Snort restarts reduced for FTD devices	In Version 6.2.3, fewer FTD configuration changes restart the Snort process on FTD devices. The FMC now warns you before you deploy if the configuration deployment restarts the Snort process, interrupting traffic inspection and, depending on how the managed device handles traffic, possibly interrupting traffic flow. Supported platforms: FTD
Traffic Drop on Policy Apply	Version 6.2.3 adds the **configure snort preserve-connection {enable | disable}** command to the FTD CLI. This command determines whether to preserve existing connections on routed and transparent interfaces if the Snort process goes down. When disabled, all new or existing connections are dropped when Snort goes down and remain dropped until Snort resume. When enabled, connections that were already allowed remain established, but new connections cannot be established until Snort is again available. Note that you cannot permanently disable this command on a FTD device managed by FDM; existing connections may drop when the settings revert to default during the next configuration deployment.
Increased memory capacity for lower-end appliances	Versions 6.1.0.7, 6.2.0.5, 6.2.2.2, and 6.2.3 increase the memory capacity for lower-end Firepower appliances. This reduces the number of health alerts.
Faster ISE pxGrid discovery	If an ISE pxGrid deployed in high availability fails or becomes unreachable, the FMC now discovers the new active pxGrid faster.

Feature	Details
New result limits in reports.	**Upgrade can change report settings.** Version 6.2.3 limits the number of results you can use or include in a report section. For table and detail views, you can include fewer records in a PDF report than in an HTML/CSV report. For HTML/CSV report sections, the new limits are: • Bar and pie charts: 100 (top or bottom) • Table views: 400,000 • Detail views: 1,000 For PDF report sections, the new limits are: • Bar and pie charts: 100 (top or bottom) • Table views: 100,000 • Detail views: 500 If, before you upgrade the FMC, a section in a report template specifies a larger number of results than the HTML/CSV maximum, the upgrade process lowers the setting to the new maximum value. For report templates that generate PDF reports, if you exceed the PDF limit in any template section, the upgrade process changes the output format to HTML. To continue generating PDFs, lower the results limit to the PDF maximum. If you do this after the upgrade, set the output format back to PDF.
Firepower Management Center REST API	
FMC REST API Improvements	The new FMC REST APIs support the use of CRUD (create, retrieve, upgrade, and delete) operations for NAT rules, static routing configuration, and corresponding objects while migrating from ASA FirePOWER to FTD. Newly introduced APIs for NAT: • NAT rules • FTD NAT policies • Auto NAT rules • Manual NAT rules When deploying FTD devices in Cisco ACI, APIs enable APIC controller to add proper static routes in place, along with other configuration settings that are needed for a particular service graph. It also enables PBR service graph insertion, which is currently the most flexible way of inserting FTD in ACI. Newly introduced APIs for Static Route: • IPv4 static routes • IPv6 static routes • SLA monitors

Deprecated Features

Table 9: Deprecated Features in FMC Version 6.2.3

Feature	Details
Expired CA certificates for dynamic analysis with AMP for Networks.	On June 15, 2018, some Firepower deployments stopped being able to submit files for dynamic analysis. This occurred due to an expired CA certificate that was required for communications with the AMP Threat Grid cloud. Version 6.3 is the first major version with the new certificate. If you do not want to upgrade to Version 6.3+, you can patch to obtain the new certificate and reenable dynamic analysis, as follows: • Version 6.2.3 → patch to Version 6.2.3.4 • Version 6.2.2 → patch to Version 6.2.2.4 • Version 6.2.1 → no patches available • Version 6.2 → patch to Version 6.2.0.6 • Version 6.1 → patch to Version 6.1.0.7 • Version 6.0 → no patches available You can also apply a hotfix. For available hotfixes, see the Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes. Find the hotfix for your version and platform that applies to CSCvj07038*: Firepower devices need to trust Threat Grid certificate*. If this is your first time installing the patch or hotfix, make sure your firewall allows outbound connections to `fmc.api.threatgrid.com` (replacing `panacea.threatgrid.com`) from both the FMC and its managed devices. Note that upgrading a patched or hotfixed deployment to either Version 6.2.0 or Version 6.2.3 reverts to the old certificate and you must patch or hotfix again.
Deprecated: Geolocation details.	In May 2022 we split the GeoDB into two packages: a country code package that maps IP addresses to countries/continents, and an IP package that contains additional contextual data associated with routable IP addresses. The contextual data in the IP package can include additional location details, as well as connection information such as ISP, connection type, proxy type, domain name, and so on. The new country code package has the same file name as the old all-in-one package: Cisco_GEODB_Update-*date-build*. This allows deployments running Version 7.1 and earlier to continue to obtain GeoDB updates. If you manually download GeoDB updates—for example, in an air-gapped deployment—make sure you get the country code package and not the IP package. **Important** This split does not affect geolocation rules or traffic handling in any way—those rules rely only on the data in the country code package. However, because the country code package essentially replaces the all-in-one package, the contextual data is no longer updated and will grow stale. To obtain fresh data, upgrade or reimage the FMC to Version 7.2+ and update the GeoDB.

New Features in FDM Version 6.2.3

Table 10: New and Deprecated Features in FDM Version 6.2.3

Feature	Description
SSL/TLS decryption.	You can decrypt SSL/TLS connections so that you can inspect the contents of the connection. Without decryption, encrypted connections cannot be effectively inspected to identify intrusion and malware threats, or to enforce compliance with your URL and application usage polices. We added the **Policies** > **SSL Decryption** page and **Monitoring** > **SSL Decryption** dashboard. **Attention** Identity policies that implement active authentication automatically generate SSL decryption rules. If you upgrade from a release that does not support SSL decryption, the SSL decryption policy is automatically enabled if you have this type of rule. However, you must specify the certificate to use for Decrypt-Resign rules after completing the upgrade. Please edit the SSL decryption settings immediately after upgrade.
Security Intelligence blocking.	From the new **Policies** > **Security Intelligence** page you can configure a Security Intelligence policy, which you can use to drop unwanted traffic based on source/destination IP address or destination URL. Any allowed connections will still be evaluated by access control policies and might eventually be dropped. You must enable the Threat license to use Security Intelligence. We also renamed the **Policies** dashboard to **Access And SI Rules**, and the dashboard now includes Security Intelligence rule-equivalents as well as access rules.
Intrusion rule tuning.	You can change the action for intrusion rules within the pre-defined intrusion policies you apply with your access control rules. You can configure each rule to drop or generate events (alert) matching traffic, or disable the rule. You can change the action for enabled rules only (those set to drop or alert); you cannot enable a rule that is disabled by default. To tune intrusion rules, choose **Policies** > **Intrusion**.
Automatic network analysis policy (NAP) assignment based on intrusion policy.	In previous releases, the Balanced Security and Connectivity network analysis policy was always used for preprocessor settings, regardless of the intrusion policy assigned to a specific source/destination security zone and network object combination. Now, the system automatically generates NAP rules to assign the same-named NAP and intrusion policies to traffic based on those criteria. Note that if you use Layer 4 or 7 criteria to assign different intrusion policies to traffic that otherwise matches the same source/destination security zone and network object, you will not get perfectly matching NAP and intrusion policies. You cannot create custom network analysis policies.

Feature	Description
Drill-down reports for the Threats, Attackers, and Targets dashboards.	You can now click into the Threats, Attackers, and Targets dashboards to view more detail about the reported items. These dashboards are available on the Monitoring page. Because of these new reports, you will lose reporting data for these dashboards when upgrading from a pre-6.2.3 release.
Web Applications dashboard.	The new Web Applications dashboard shows the top web applications, such as Google, that are being used in the network. This dashboard augments the Applications dashboard, which provides protocol-oriented information, such as HTTP usage.
New Zones dashboard replaces the Ingress Zone and Egress Zone dashboards.	The new Zones dashboard shows the top security zone pairs for traffic entering and then exiting the device. This dashboard replaces the separate dashboards for Ingress and Egress zones.
New Malware dashboard.	The new Malware dashboard shows the top Malware action and disposition combinations. You can drill down to see information on the associated file types. You must configure file policies on access rules to see this information.
Self-signed internal certificates, and Internal CA certificates.	You can now generate self-signed internal identity certificates. You can also upload or generate self-signed internal CA certificates for use with SSL decryption policies. Configure these features on the **Objects** > **Certificates** page.
Ability to edit DHCP server settings when editing interface properties.	You can now edit settings for a DHCP server configured on an interface at the same time you edit the interface properties. This makes it easy to redefine the DHCP address pool if you need to change the interface IP address to a different subnet.
The Cisco Success Network sends usage and statistics data to Cisco to improve the product and provide effective technical support.	You can connect to the Cisco Success Network to send data to Cisco. By enabling Cisco Success Network, you are providing usage information and statistics to Cisco which are essential for Cisco to provide you with technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. You can enable the connection when you register the device with the Cisco Smart Software Manager, or later at your choice. You can disable the connection at any time. Cisco Success Network is a cloud service. The **Device** > **System Settings** > **Cloud Management** page is renamed **Cloud Services**. You can configure Cisco Defense Orchestrator from the same page.
FTDv for Kernel-based Virtual Machine (KVM) hypervisor device configuration.	You can configure Firepower Threat Defense on FTDv for KVM devices using FDM. Previously, only VMware was supported. **Note** You must install a new 6.2.3 image to get FDM support. You cannot upgrade an existing virtual machine from an older version and then switch to FDM.

Feature	Description
Support for VMware ESXi 6.5.	You can now deploy FTDv on VMware vSphere/VMware ESXi 6.5.
ISA 3000 (Cisco 3000 Series Industrial Security Appliances) device configuration.	You can configure Firepower Threat Defense on ISA 3000 devices using FDM. Note that the ISA 3000 supports the Threat license only. It does not support the URL Filtering or Malware licenses. Thus, you cannot configure features that require the URL Filtering or Malware licenses on an ISA 3000.
Optional deployment on update of the rules database or VDB.	When you update the intrusion rules database or VDB, or configure an update schedule, you can prevent the immediate deployment of the update. Because the update restarts the inspection engines, there is a momentary traffic drop during the deployment. By not deploying automatically, you can choose to initiate the deployment at a time when traffic drops will be least disruptive. **Note** A VDB download can also restart Snort all by itself, and then again cause a restart on deployment. You cannot stop the restart on download.
Improved messages that indicate whether a deployment restarts Snort. Also, a reduced need to restart Snort on deployment.	Before you start a deployment, FDM indicates whether the configuration updates require a Snort restart. Snort restarts result in the momentary dropping of traffic. Thus, you now know whether a deployment will not impact traffic and can be done immediately, or will impact traffic, so that you can deploy at a less disruptive time. In addition, in prior releases, Snort restarted on every deployment. Now, Snort restarts for the following reasons only: • you enable or disable SSL decryption policies • an updated rules database or VDB was downloaded • you changed the MTU on one or more physical interface (but not subinterface)
CLI console in FDM.	You can now open a CLI Console from FDM. The CLI Console mimics an SSH or console session, but allows a subset of commands only: **show**, **ping**, **traceroute**, and **packet-tracer**. Use the CLI Console for troubleshooting and device monitoring.

Feature	Description
Support for blocking access to the management address.	You can now remove all management access list entries for a protocol to prevent access to the management IP address. Previously, if you removed all entries, the system defaulted to allowing access from all client IP addresses. On upgrade to 6.2.3, if you previously had an empty management access list for a protocol (HTTPS or SSH), the system creates the default allow rule for all IP addresses. You can then delete these rules as needed. In addition, FDM will recognize changes you make to the management access list from the CLI, including if you disable SSH or HTTPS access. Ensure that you enable HTTPS access for at least one interface, or you will not be able to configure and manage the device.
EMS extension support.	Both the **Decrypt-Resign** and **Decrypt-Known Key** SSL policy actions now support the EMS extension during ClientHello negotiation, enabling more secure communications. The EMS extension is defined by RFC 7627. **Note** Version 6.2.3.8 was removed from the Cisco Support & Download site on 2019-01-07. Upgrading to Version 6.2.3.9 also enables EMS extension support. Version 6.3.0 discontinues EMS extension support. Support is reintroduced in Version 6.3.0.1. Minimum FTD: Version 6.2.3.8
TLS v1.3 downgrade CLI command for FTD.	A new CLI command allows you to specify when to downgrade TLS v1.3 connections to TLS v1.2. Many browsers use TLS v1.3 by default. If you are using an SSL policy to handle encrypted traffic, and people in your monitored network use browsers with TLS v1.3 enabled, websites that support TLS v1.3 fail to load. For more information, see the **system support** commands in the Cisco Secure Firewall Threat Defense Command Reference. We recommend you use these commands only after consulting with Cisco TAC. Minimum FTD: Version 6.2.3.7

Feature	Description
Smart CLI and FlexConfig for configuring features using the device CLI.	Smart CLI and FlexConfig allows you to configure features that are not yet directly supported through FDM policies and settings. FTD uses ASA configuration commands to implement some features. If you are a knowledgeable and expert user of ASA configuration commands, you can configure these features on the device using the following methods: • Smart CLI—(Preferred method.) A Smart CLI template is a pre-defined template for a particular feature. All of the commands needed for the feature are provided, and you simply need to select values for variables. The system validates your selection, so that you are more likely to configure a feature correctly. If a Smart CLI template exists for the feature you want, you must use this method. In this release, you can configure OSPFv2 using the Smart CLI. • FlexConfig—The FlexConfig policy is a collection of FlexConfig objects. The FlexConfig objects are more free-form than Smart CLI templates, and the system does no CLI, variable, or data validation. You must know ASA configuration commands and follow the ASA configuration guides to create a valid sequence of commands. **Caution** Cisco strongly recommends using Smart CLI and FlexConfig only if you are an advanced user with a strong ASA background and at your own risk. You may configure any commands that are not blacklisted. Enabling features through Smart CLI or FlexConfig may cause unintended results with other configured features.
FTD REST API, and an API Explorer.	You can use a REST API to programmatically interact with a Firepower Threat Defense device that you are managing locally through FDM. There is an API Explorer that you can use to view object models and test the various calls you can make from a client program. To open the API Explorer, log into FDM, and then change the path on the URL to /#/api-explorer, for example, https://ftd.example.com/#/api-explorer.

Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

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

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

You can find your Snort version in the *Bundled Components* section of the compatibility guide, or use one of these commands:

- FMC: Choose **Help** > **About**.
- FDM: Use the **show summary** CLI command.

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.

FlexConfig Commands

This document lists deprecated FlexConfig objects and commands along with the other deprecated features for this release. For a full list of prohibited commands, including those prohibited when FlexConfig was introduced and those deprecated in previous releases, see your configuration guide.

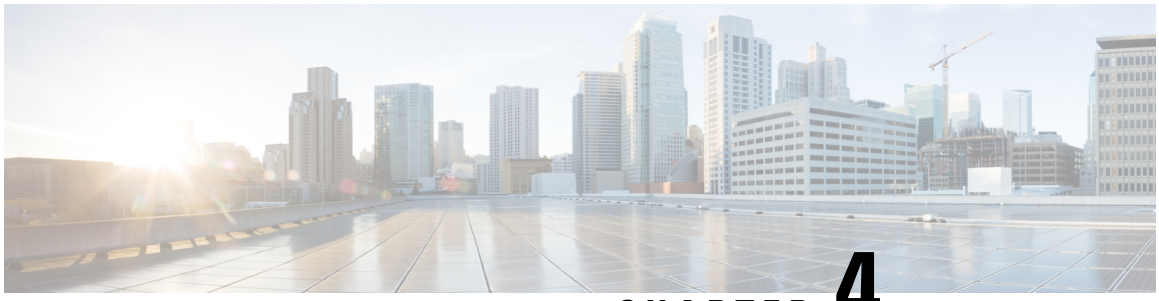
Caution In most cases, your existing FlexConfig configurations continue to work post-upgrade and you can still deploy. However, in some cases, using deprecated commands can cause deployment issues.

About FlexConfig

Some FTD features are configured using ASA configuration commands. You can use Smart CLI or FlexConfig to manually configure various ASA features that are not otherwise supported in the web interface.

Upgrades can add GUI or Smart CLI support for features that you previously configured using FlexConfig. This can deprecate FlexConfig commands that you are currently using; your configurations are *not* automatically converted. After the upgrade, you cannot assign or create FlexConfig objects using the newly deprecated commands.

After the upgrade, examine your FlexConfig policies and objects. If any contain commands that are now deprecated, messages indicate the problem. We recommend you redo your configuration. When you are satisfied with the new configuration, you can delete the problematic FlexConfig objects or commands.



CHAPTER 4

Upgrade Guidelines

This document provides critical and release-specific upgrade guidelines for Version 6.2.3.

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 appropriate upgrade or configuration guide.

Table 11: 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 configurations and events. 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 firmware on the Firepower 4100/9300. Upgrade FXOS on the Firepower 4100/9300. Upgrade ASA for ASA FirePOWER.
Final Checks	Check configurations. Check NTP synchronization. Deploy configurations. Run readiness checks. Check disk space. Check running tasks. Check deployment health and communications.

Minimum Version to Upgrade

Minimum Version to Upgrade

You can upgrade directly to Version 6.2.3 as follows.

Table 12: Minimum Version to Upgrade to Version 6.2.3

Platform	Minimum Version
FMC	6.1
FTD	6.1 with FMC 6.2 with FDM FXOS 2.3.1.73 is required for the Firepower 4100/9300. In most cases, we recommend you use the latest FXOS build in each major version. To help you decide, see the Cisco Firepower 4100/9300 FXOS Release Notes, 2.3(1). **Note** Firepower 6.2.3.16+ requires FXOS 2.3.1.157+.
Firepower 7000/8000 series	6.1

Platform	Minimum Version
ASA with FirePOWER Services	6.1 with FMC 6.2 with ASDM See Device Platforms, on page 6 for ASA requirements for your model. Although there is wide compatibility between ASA and ASA FirePOWER versions, upgrading allows you to take advantage of new features and resolved issues. To help you decide, see the Cisco Secure Firewall ASA Release Notes.
NGIPSv	6.1

Minimum Version to Patch

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

Upgrade Guidelines for Version 6.2.3

These checklists provide new and/or previously published upgrade guidelines that may apply to you.

Table 13: Upgrade Guidelines for FTD with FMC Version 6.2.3

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 30	Any	Any	Any
	Cisco Secure Firewall Management Center New Features by Release, for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	Bugs, on page 63, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 37	Firepower 4100/9300	Any	Any
	Patches That Support Uninstall	Any	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				
	Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure, on page 33	FTD	6.2.3 through 6.2.3.9	6.2.3.10

✓	Guideline	Platforms	Upgrading From	Directly To
	Version 6.2.3.3 FTD Device Cannot Switch to Local Management, on page 33	FTD	6.2.3 through 6.2.3.2	6.2.3.3
	Hotfix Before Upgrading Version 6.2.3-88 FMCs, on page 34	FMC	6.2.3-88	6.2.3.1 through 6.2.3.3
	Remove Site IDs from Version 6.1.x Firepower Threat Defense Clusters Before Upgrade, on page 34	FTD clusters	6.1.0.x	6.2.3+
	Edit/Resave Access Control Policies After Upgrade, on page 35	Any	6.1.0 through 6.2.2.x	6.2.3 only
	Access Control Can Get Latency-Based Performance Settings from SRUs, on page 36	FMC	6.1.0.x	6.2+
	'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 36	FTD	6.1.0.x	6.2+

Table 14: Upgrade Guidelines for FTD with FDM Version 6.2.3

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 30	Any	Any	Any
	Cisco Secure Firewall Device Manager New Features by Release, for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	Bugs, on page 63, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 37	Firepower 4100/9300	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				
	Version 6.2.3.3 FTD Device Cannot Switch to Local Management, on page 33	Any	6.2.3 through 6.2.3.2	6.2.3.3

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Can Unregister FDM from CSSM, on page 34	Any	6.2.3 through 6.2.3.1	6.2.3.2 through 6.2.3.5
	Upgrade Can Unregister FDM from CSSM, on page 34	Any	6.2.0 through 6.2.2.x	6.2.3+
	Upgrade Failure: Firepower 2100 Series from Version 6.2.2.5, on page 35	Firepower 2100 series	6.2.2.5	6.2.3 only
	Edit/Resave Realms After FTD/FDM Upgrade, on page 35	Any	6.2.0 through 6.2.2.x	6.2.3 only
	Edit/Resave Access Control Policies After Upgrade, on page 35	Any	6.1.0 through 6.2.2.x	6.2.3 only
	Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0, on page 35	Any	6.2.0 only	6.2.2+

Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure

Deployments: Firepower Threat Defense

Upgrading from: Version 6.2.3 through 6.2.3.9

Directly to: Version 6.2.3.10 only

Known issue: CSCvo39052

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

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

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

Version 6.2.3.3 FTD Device Cannot Switch to Local Management

Deployments: FTD wth FMC

Upgrading from: Version 6.2.3 through Version 6.2.3.2

Directly to: Version 6.2.3.3 only

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

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

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

Hotfix Before Upgrading Version 6.2.3-88 FMCs

Deployments: FMC

Upgrading from: Version 6.2.3-88

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

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

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

Remove Site IDs from Version 6.1.x Firepower Threat Defense Clusters Before Upgrade

Deployments: Firepower Threat Defense clusters

Upgrading from: Version 6.1.x

Directly to: Version 6.2.3 through 6.4.0

Firepower Threat Defense Version 6.1.x clusters do not support inter-site clustering (you can configure inter-site features using FlexConfig starting in Version 6.2.0).

If you deployed or redeployed a Version 6.1.x cluster in FXOS 2.1.1, and you entered a value for the (unsupported) site ID, remove the site ID (set to `0`) on each unit in FXOS before you upgrade. Otherwise, the units cannot rejoin the cluster after the upgrade.

If you already upgraded, remove the site ID from each unit, then reestablish the cluster. To view or change the site ID, see the Cisco FXOS CLI Configuration Guide.

Upgrade Can Unregister FDM from CSSM

Deployments: FTD with FDM

Upgrading from: Version 6.2 through 6.2.2.x

Directly to: Version 6.2.3 through 6.4.0

Note Upgrades from 6.2.3 and 6.2.3.1 directly to 6.2.3.2 through 6.2.3.5 are also affected.

Upgrading FTD with FDM may unregister the device from the Cisco Smart Software Manager. After the upgrade completes, check your license status.

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

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

Upgrade Failure: Firepower 2100 Series from Version 6.2.2.5

Deployments: Firepower 2100 series with FTD, managed by FDM

Upgrading from: Version 6.2.2.5

Directly to: Version 6.2.3 only

If you change the DNS settings on a Firepower 2100 series device running Version 6.2.2.5, and then upgrade to Version 6.2.3 without an intermediate deployment, the upgrade fails. You must deploy or execute an action that triggers a deployment, such as an SRU update, before you upgrade the device.

Edit/Resave Realms After FTD/FDM Upgrade

Deployments: FTD with FDM

Upgrading from: Version 6.2.0 through Version 6.2.2.x

Directly to: Version 6.2.3 only

Before Version 6.2.3, users were not automatically logged out after 24 hours of inactivity. After you upgrade Firepower Threat Defense to Version 6.2.3 when using Firepower Device Manager, if you are using identity policies with active authentication, update your realm before you deploy configurations. Choose **Objects** > **Identity Realm**, edit the realm (no changes are needed), and save it. Then, deploy.

Edit/Resave Access Control Policies After Upgrade

Deployments: Any

Upgrading from: Version 6.1 through 6.2.2.x

Directly to: Version 6.2.3 only

If you configured network or port objects that are used *only* in intrusion policy variable sets, deploying associated access control policies after the upgrade fails. If this happens, edit the access control policy, make a change (such as editing the description), save, and redeploy.

Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0

Deployments: FTD with FDM, running on a lower-memory ASA 5500-X series device

Upgrading from: Version 6.2.0

Directly to: Version 6.2.2 through 6.4.0

If you are upgrading from Version 6.2.0, the upgrade may fail with an error of: `Uploaded file is not a valid system upgrade file`. This can occur even if you are using the correct file.

If this happens, you can try the following workarounds:

- Try again.
- Use the CLI to upgrade.
- Upgrade to 6.2.0.1 first.

Access Control Can Get Latency-Based Performance Settings from SRUs

Deployments: FMC

Upgrading from: 6.1.x

Directly to: 6.2.0+

New access control policies in Version 6.2.0+ *by default* get their latency-based performance settings from the latest intrusion rule update (SRU). This behavior is controlled by a new **Apply Settings From** option. To configure this option, edit or create an access control policy, click **Advanced**, and edit the Latency-Based Performance Settings.

When you upgrade to Version 6.2.0+, the new option is set according to your current (Version 6.1.x) configuration. If your current settings are:

- Default: The new option is set to **Installed Rule Update**. When you deploy after the upgrade, the system uses the latency-based performance settings from the latest SRU. It is possible that traffic handling could change, depending on what the latest SRU specifies.
- Custom: The new option is set to **Custom**. The system retains its current performance settings. There should be no behavior change due to this option.

We recommend you review your configurations before you upgrade. From the Version 6.1.x FMC web interface, view your policies' Latency-Based Performance Settings as described earlier, and see whether the **Revert to Defaults** button is dimmed. If the button is dimmed, you are using the default settings. If it is active, you have configured custom settings.

'Snort Fail Open' Replaces 'Failsafe' on FTD

Deployments: FTD with FMC

Upgrading from: Version 6.1.x

Directly to: Version 6.2+

In Version 6.2, the Snort Fail Open configuration replaces the Failsafe option on FMC-managed Firepower Threat Defense devices. While Failsafe allows you to drop traffic when Snort is busy, traffic automatically passes without inspection when Snort is down. Snort Fail Open allows you to drop this traffic.

When you upgrade an FTD device, its new Snort Fail Open setting depends on its old Failsafe setting, as follows. Although the new configuration should not change traffic handling, we still recommend that you consider whether to enable or disable Failsafe before you upgrade.

Table 15: Migrating Failsafe to Snort Fail Open

Version 6.1 Failsafe	Version 6.2 Snort Fail Open	Behavior
Disabled (default behavior)	**Busy**: Disabled **Down**: Enabled	New and existing connections drop when the Snort process is busy and pass without inspection when the Snort process is down.
Enabled	**Busy**: Enabled **Down**: Enabled	New and existing connections pass without inspection when the Snort process is busy or down.

Note that Snort Fail Open requires Version 6.2 on the device. If you are managing a Version 6.1.x device, the FMC web interface displays the Failsafe option.

Upgrade Guidelines for the Firepower 4100/9300 Chassis

For the Firepower 4100/9300, major FTD upgrades also require a chassis upgrade (FXOS and firmware). Maintenance release and patches rarely require this, but you may still want to upgrade to the latest build to take advantage of resolved issues.

Table 16: Upgrade Guidelines for the Firepower 4100/9300 Chassis

Guideline	Details
FXOS upgrades.	FXOS 2.3.1.73+ is required to run threat defense Version 6.2.3 on the Firepower 4100/9300. **Note** Firepower 6.2.3.16+ requires FXOS 2.3.1.157+. You can upgrade to any later FXOS version from as far back as FXOS 2.2.2. For critical and release-specific upgrade guidelines, new and deprecated features, and open and resolved bugs, see the Cisco Firepower 4100/9300 FXOS Release Notes.
Firmware upgrades.	FXOS 2.14.1+ upgrades include firmware. If you are upgrading to an earlier FXOS version, see the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.
Time to upgrade.	Chassis upgrade can take up to 45 minutes and can affect traffic flow and inspection. For more information, see Traffic Flow and Inspection for Chassis Upgrades, on page 40.

Unresponsive Upgrades

Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down during upgrade. 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.

Uninstall a Patch

In FMC and ASDM deployments, you can uninstall most patches. If you need to return to an earlier major release, you must reimage. For guidelines, limitations, and procedures, see Uninstall a Patch in the FMC upgrade guide or Uninstall ASA FirePOWER Patches with ASDM, on page 38 in these release notes.

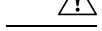
Uninstall ASA FirePOWER Patches with ASDM

Use the Linux shell (*expert mode*) to uninstall device patches. 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, contact Cisco TAC to reverse the lockdown.

For ASA failover pairs and clusters, minimize disruption by uninstalling from one appliance at a time. Wait until the patch has fully uninstalled from one unit before you move on to the next.

Table 17: Uninstall Order for ASA with FirePOWER Services in ASA Failover Pairs/Clusters

Configuration	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.



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

Before you begin

- In ASA failover/cluster deployments, make sure you are uninstalling from the correct device.
- Make sure your deployment is healthy and successfully communicating.

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

Deploying before you uninstall reduces the chance of failure. Make sure the deployment and other essential tasks are completed. Tasks running when the uninstall begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

Step 2 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 3 Use the `expert` command to access the Linux shell.

Step 4 Verify the uninstall package is in the upgrade directory.

```
ls /var/sf/updates
```

Patch uninstallers are named like upgrade packages, but have `Patch_Uninstaller` instead of `Patch` in the file name. When you patch a device, the uninstaller for that patch is automatically created in the upgrade directory. If the uninstaller is not there, contact Cisco TAC.

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

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

Caution The system does *not* ask you to confirm. 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. Note that using the `--detach` option ensures the uninstall process is not killed if your SSH session times out, which can leave the device in an unstable state.

Step 6 Monitor the uninstall until you are logged out.

For a detached uninstall, use `tail` or `tailf` to display logs:

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

Otherwise, monitor progress in the console or terminal.

Step 7 Verify uninstall success.

After the uninstall completes, 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

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

Traffic Flow and Inspection

Device upgrades (software and operating system) affect traffic flow and inspection. Schedule maintenance windows when this will have the least impact.

Traffic Flow and Inspection for Chassis Upgrades

Upgrading FXOS reboots the chassis. For FXOS upgrades to Version 2.14.1+ that include firmware upgrades, the device reboots twice—once for FXOS and once for the firmware.

Even in high availability/clustered deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade one chassis at a time.

Table 18: Traffic Flow and Inspection: FXOS Upgrades

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

Traffic Flow and Inspection for FTD Upgrades with FMC

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 19: Traffic Flow and Inspection: 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. For bridge group interfaces on the ISA 3000 only, you can use a FlexConfig policy to configure hardware bypass for power failure. This causes traffic to drop during software upgrades but pass without inspection while the device completes its post-upgrade reboot.
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force**	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby**	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**	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. 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.

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

Software Uninstall (Patches)

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.

Deploying Configuration Changes

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

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.

Table 20: Traffic Flow and Inspection: 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.	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.	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled.	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Traffic Flow and Inspection for FTD Upgrades with FDM

Software Upgrades

Traffic is dropped while you upgrade. In a high availability deployment, you can minimize disruption by upgrading devices one at a time.

For the ISA 3000 only, if you configured hardware bypass for power failure, traffic is dropped during the upgrade but is passed without inspection while the device completes its post-upgrade reboot.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

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.

Traffic Flow and Inspection for ASA FirePOWER Upgrades

Software Upgrades

Your ASA service policies for redirecting traffic to the ASA FirePOWER module determine how the module handles traffic during software upgrade.

Table 21: Traffic Flow and Inspection: ASA FirePOWER Upgrades

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

Software Uninstall (Patches)

Interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In ASA failover/cluster 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.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection. Traffic behavior while the Snort process restarts is the same as when you upgrade ASA FirePOWER. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

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.

Traffic Flow and Inspection for NGIPSv Upgrades with FMC

Software Upgrades

Interface configurations determine how NGIPSv handles traffic during the upgrade.

Table 22: Traffic Flow and Inspection: NGIPSv Upgrades

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

Software Uninstall (Patches)

Interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade.

Deploying Configuration Changes

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

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.

Table 23: Traffic Flow and Inspection: Deploying Configuration Changes

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 FMC and device software upgrades.

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 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.

Table 24: Time Test Conditions for Software Upgrades

Condition	Details
Deployment	Times for device 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 either /Volume or /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.

Without enough free disk space, the upgrade fails.

Table 25: 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 6.2.3.18 Time and Disk Space

Table 26: Time and Disk Space for Version 6.2.3.18

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

Version 6.2.3.17 Time and Disk Space

Table 27: Time and Disk Space for Version 6.2.3.17

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	3.4 GB	300 MB	—	32 min	7 min
FMCv: VMware	4.1 GB	230 MB	—	23 min	5 min
Firepower 2100 series	—	2.7 GB	600 MB	12 min	12 min
Firepower 4100 series	—	1.7 GB	390 MB	5 min	6 min
Firepower 9300	—	1.7 GB	390 MB	5 min	7 min
ASA 5500-X series with FTD	2.1 GB	200 MB	420 MB	18 min	37 min
FTDv: VMware	2.1 GB	190 MB	420 MB	7 min	5 min
Firepower 7000/8000 series	3.5 GB	200 MB	640 MB	10 min	15 min
ASA FirePOWER	3.8 GB	58 MB	580 MB	72 min	61 min
NGIPSv	2.5 GB	180 MB	480 MB	5 min	4 min

Version 6.2.3.16 Time and Disk Space

Table 28: Time and Disk Space for Version 6.2.3.16

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	3.6 GB	250 MB	—	40 min	9 min
FMCv: VMware	3.3 GB	220 MB	—	25 min	4 min
Firepower 2100 series	—	2.6 GB	620 MB	11 min	12 min
Firepower 4100 series	—	1.7 GB	410 MB	5 min	5 min
Firepower 9300	—	1.8 GB	410 MB	5 min	9 min
ASA 5500-X series with FTD	2.0 GB	200 MB	430 MB	18 min	33 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FTDv: VMware	2.0 GB	190 MB	430 MB	8 min	5 min
Firepower 7000/8000 series	3.5 GB	200 MB	670 MB	31 min	14 min
ASA FirePOWER	3.8 GB	58 MB	600 MB	74 min	77 min
NGIPSv	2.3 GB	180 MB	500 MB	6 min	4 min

Version 6.2.3.15 Time and Disk Space

Table 29: Time and Disk Space for Version 6.2.3.15

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	4.7 GB	260 MB	—	50 min
FMCv: VMware	4.7 GB	210 MB	—	Hardware dependent
Firepower 2100 series	—	2.3 GB	590 MB	27 min
Firepower 4100 series	—	1.7 GB	390 MB	10 min
Firepower 9300	—	2.4 GB	390 MB	11 min
ASA 5500-X series with FTD	2.0 GB	190 MB	410 MB	38 min
FTDv: VMware	2.4 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.5 GB	210 MB	640 MB	19 min
ASA FirePOWER	3.9 GB	56 MB	580 MB	100 min
NGIPSv	2.7 GB	180 MB	470 MB	Hardware dependent

Version 6.2.3.14 Time and Disk Space

Table 30: Time and Disk Space for Version 6.2.3.14

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	4.5 GB	260 MB	—	58 min
FMCv: VMware	4.7 GB	190 MB	—	Hardware dependent
Firepower 2100 series	—	1.9 GB	590 MB	23 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
Firepower 4100 series	—	1.7 GB	390 MB	11 min
Firepower 9300	—	1.7 GB	390 MB	10 min
ASA 5500-X series with FTD	2.0 GB	200 MB	410 MB	32 min
FTDv: VMware	2.4 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.4 GB	200 MB	630 MB	19 min
ASA FirePOWER	3.7 GB	53 MB	560 MB	106 min
NGIPSv	2.6 GB	190 MB	470 MB	Hardware dependent

Version 6.2.3.13 Time and Disk Space

Table 31: Time and Disk Space for Version 6.2.3.13

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	4.7 GB	290 MB	—	50 min
FMCv: VMware	4.6 GB	190 MB	—	Hardware dependent
Firepower 2100 series	—	2.6 GB	590 MB	25 min
Firepower 4100 series	—	1.7 GB	390 MB	11 min
Firepower 9300	—	1.8 GB	390 MB	11 min
ASA 5500-X series with FTD	2.4 GB	190 MB	410 MB	32 min
FTDv: VMware	2.3 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.8 GB	190 MB	620 MB	18 min
ASA FirePOWER	3.7 GB	51 MB	560 MB	105 min
NGIPSv	2.6 GB	180 MB	470 MB	Hardware dependent

Version 6.2.3.12 Time and Disk Space

Table 32: Time and Disk Space for Version 6.2.3.12

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

Version 6.2.3.11 Time and Disk Space

Table 33: Time and Disk Space for Version 6.2.3.11

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

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
NGIPSv	2.6 GB	130 MB	450 MB	Hardware dependent

Version 6.2.3.10 Time and Disk Space

Table 34: Time and Disk Space for Version 6.2.3.10

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

Version 6.2.3.9 Time and Disk Space

Table 35: Time and Disk Space for Version 6.2.3.9

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	3630 MB	190 MB	—	35 min
FMCv	3596 MB	172 MB	—	Hardware dependent
Firepower 2100 series	—	1677 MB	385 MB	21 min
Firepower 4100/9300	—	779 MB	184 MB	9 min
ASA 5500-X series with FTD	1105 MB	130 MB	206 MB	12 min
ISA 3000 with FTD	1071 MB	130 MB	206 MB	25 min
FTDv	1094 MB	130 MB	206 MB	Hardware dependent

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
Firepower 7000/8000 series	2975 MB	161 MB	538 MB	30 min
ASA FirePOWER	3211 MB	27 MB	462 MB	38 min
NGIPSv	1883 MB	146 MB	378 MB	Hardware dependent

Version 6.2.3.8 Time and Disk Space

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

Version 6.2.3.7 Time and Disk Space

Table 36: Time and Disk Space for Version 6.2.3.7

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	2909 MB	137 MB	—	25 min
FMCv	3972 MB	211 MB	—	Hardware dependent
Firepower 2100 series	—	1668 MB	384 MB	19 min
Firepower 4100/9300	—	795 MB	183 MB	8 min
ASA 5500-X series with FTD	1067 MB	130 MB	205 MB	9 min
ISA 3000 with FTD	1080 MB	130 MB	205 MB	20 min
FTDv	1146 MB	130 MB	205 MB	Hardware dependent
Firepower 7000/8000 series	3300 MB	136 MB	477 MB	20 min
ASA FirePOWER	2291 MB	26 MB	411 MB	80 min
NGIPSv	1588 MB	121 MB	327 MB	Hardware dependent

Version 6.2.3.6 Time and Disk Space

Table 37: Time and Disk Space for Version 6.2.3.6

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	2524 MB	47 MB	—	30 min

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

Version 6.2.3.5 Time and Disk Space

Table 38: Time and Disk Space for Version 6.2.3.5

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	1566 MB	24 MB	—	28 min
FMCv	2266 MB	80 MB	—	Hardware dependent
Firepower 2100 series	—	1001MB	257 MB	20 min
Firepower 4100/9300	—	370 MB	56 MB	7 min
ASA 5500-X series with FTD	587 MB	130 MB	78 MB	20 min
ISA 3000 with FTD	379 MB	130 MB	78 MB	20 min
Firepower 7000/8000 series	806 MB	17 MB	78 MB	22 min
ASA FirePOWER	1465 MB	15 MB	100 MB	70 min
NGIPSv	120 MB	17 MB	16 MB	Hardware dependent

Version 6.2.3.4 Time and Disk Space

Table 39: Time and Disk Space for Version 6.2.3.4

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

Version 6.2.3.3 Time and Disk Space

Table 40: Time and Disk Space for Version 6.2.3.3

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	1879 MB	88 MB	—	26 min
FMCv	2093 MB	90 MB	—	Hardware dependent
Firepower 2100 series	—	987 MB	255 MB	15 min
Firepower 4100/9300	—	313 MB	54 MB	5 min
ASA 5500-X series with FTD	553 MB	128 MB	77 MB	16 min
ISA 3000 with FTD	307 MB	90 MB	77 MB	15 min
FTDv	307 MB	90 MB	77 MB	Hardware dependent
Firepower 7000/8000 series	825 MB	17 MB	77 MB	15 min
ASA FirePOWER	634 MB	16 MB	98 MB	40 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
NGIPSv	102 MB	17 MB	77 MB	Hardware dependent

Version 6.2.3.2 Time and Disk Space

Table 41: Time and Disk Space for Version 6.2.3.2

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

Version 6.2.3.1 Time and Disk Space

Table 42: Time and Disk Space for Version 6.2.3.1

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

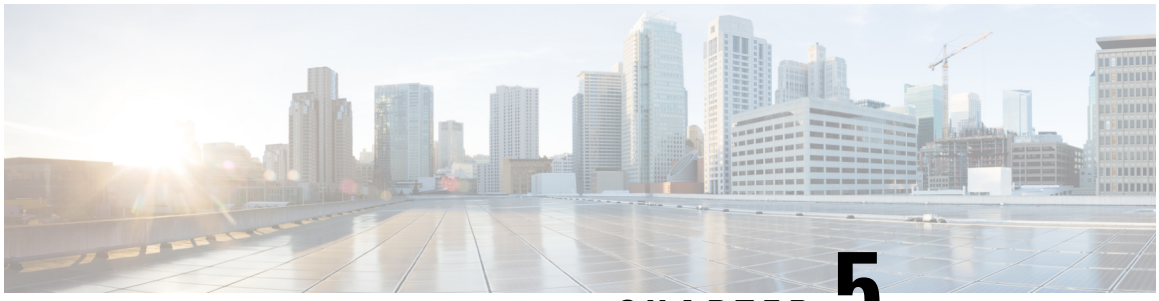
Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FTDv	275.5 MB	89.9 MB	67 MB	Hardware dependent
Firepower 7000/8000 series	99.8 MB	36 MB	10 MB	19 min
ASA FirePOWER	867.9 MB	15.45 MB	32 MB	60 min
NGIPSv	101.9 MB	17.18 MB	9 MB	Hardware dependent

Version 6.2.3 Time and Disk Space

Table 43: Time and Disk Space for Version 6.2.3

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
FMC	From 6.1.0: 7415 MB From 6.2.0: 8863 MB From 6.2.1: 8263 MB From 6.2.2: 11860 MB	From 6.1.0: 17 MB From 6.2.0: 24 MB From 6.2.1: 23 MB From 6.2.2: 24 MB	—	From 6.1.0: 38 min From 6.2.0: 43 min From 6.2.1: 37 min From 6.2.2: 37 min
FMCv	From 6.1.0: 7993 MB From 6.2.0: 9320 MB From 6.2.1: 11571 MB From 6.2.2: 11487 MB	From 6.1.0: 23 MB From 6.2.0: 28 MB From 6.2.1: 24 MB From 6.2.2: 24 MB	—	Hardware dependent
Firepower 2100 series	From 6.2.1: 7356 MB From 6.2.2: 11356 MB	From 6.2.1: 7356 MB From 6.2.2: 11356 MB	1000 MB	From 6.2.1: 15 min From 6.2.2: 15 min
Firepower 4100/9300	From 6.1.0: 5593 MB From 6.2.0: 5122 MB From 6.2.2: 7498 MB	From 6.1.0: 5593 MB From 6.2.0: 5122 MB From 6.2.2: 7498 MB	795 MB	From 6.1.0: 10 min From 6.2.0: 12 min From 6.2.2: 15 min
ASA 5500-X series with FTD	From 6.1.0: 4322 MB From 6.2.0: 6421 MB From 6.2.2: 6450 MB	From 6.1.0: .088 MB From 6.2.0: .092 MB From 6.2.2: .088 MB	1000 MB	From 6.1.0: 54 min From 6.2.0: 53 min From 6.2.2: 50 min
FTDv	From 6.1.0: 4225 MB From 6.2.0: 5179 MB From 6.2.2: 6450 MB	From 6.1.0: .076 MB From 6.2.0: .092 MB From 6.2.2: .092 MB	1000 MB	Hardware dependent

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time
Firepower 7000/8000 series	From 6.1.0: 5145 MB From 6.2.0: 5732 MB From 6.2.2: 6752 MB	From 6.1.0: 18 MB From 6.2.0: 18 MB From 6.2.2: 18 MB	840 MB	From 6.1.0: 29 min From 6.2.0: 31 min From 6.2.2: 31 min
ASA FirePOWER	From 6.1.0: 7286 MB From 6.2.0: 7286 MB From 6.2.2: 10748 MB	From 6.1.0: 16 MB From 6.2.0: 16 MB From 6.2.2: 16 MB	From 6.1.0: 1200 MB From 6.2.0: 1200 MB	From 6.1.0: 94 min From 6.2.0: 104 min From 6.2.2: 96 min
NGIPSv	From 6.1.0: 4115 MB From 6.2.0: 5505 MB From 6.2.2: 5871 MB	From 6.1.0: 18 MB From 6.2.0: 19 MB From 6.2.2: 19 MB	741 MB	Hardware dependent



CHAPTER 5

Install the Software

If you cannot or do not want to upgrade to Version 6.2.3, you can freshly install major releases. This is also called *reimaging*. We do not provide installation packages for patches. To run a particular patch, install the appropriate major release, then apply the patch.

Installation Guidelines

These guidelines can prevent common reimage issues, but are not comprehensive. For detailed checklists and procedures, see the appropriate installation guide.

Backups

Before you reimage, 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.

Note If you want to reimage 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.

Appliance 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's management interface without traversing the device.

Unregistering from Smart Software Manager

Before you reimage any appliance or switch device management, you may need to unregister from the Cisco Smart Software Manager (CSSM). This is to avoid accruing orphan entitlements, which can prevent you from reregistering.

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.

If you plan to restore from backup, do not unregister before you reimage and do not remove devices from the FMC. Instead, manually 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.

Table 44: Scenarios for Unregistering from CSSM (Not Restoring from Backup)

Scenario	Action
Reimage the FMC.	Unregister manually.
Model migration for the FMC.	Unregister manually, before you shut down the source FMC.
Reimage FTD with FMC.	Unregister automatically, by removing the device from the FMC.
Reimage FTD with FDM.	Unregister manually.
Switch FTD from FMC to FDM.	Unregister automatically, by removing the device from the FMC.
Switch FTD from device manager to FMC.	Unregister manually.

Removing Devices from the FMC

In FMC deployments, if you plan to manually configure the reimaged appliance, remove devices from the FMC before you reimage either. If you plan to restore from backup, you do not need to do this.

Table 45: Scenarios for Removing Devices from the FMC (Not Restoring from Backup)

Scenario	Action
Reimage the FMC.	Remove all devices from management.
Reimage FTD.	Remove the one device from management.
Switch FTD from FMC to FDM.	Remove the one device from management.

Fully Reimaging FTD Hardware to Downgrade FXOS

For FTD hardware models that use the FXOS operating system, reimaging to an earlier software version may require a full reimage, regardless of whether FXOS is bundled with the software or upgraded separately.

Table 46: Scenarios for Full Reimages

Model	Details
Firepower 2100 series	If you use the **erase configuration** method to reimage, FXOS may not downgrade along with the software. This can cause failures, especially in high availability deployments. We recommend that you perform full reimages of these devices.

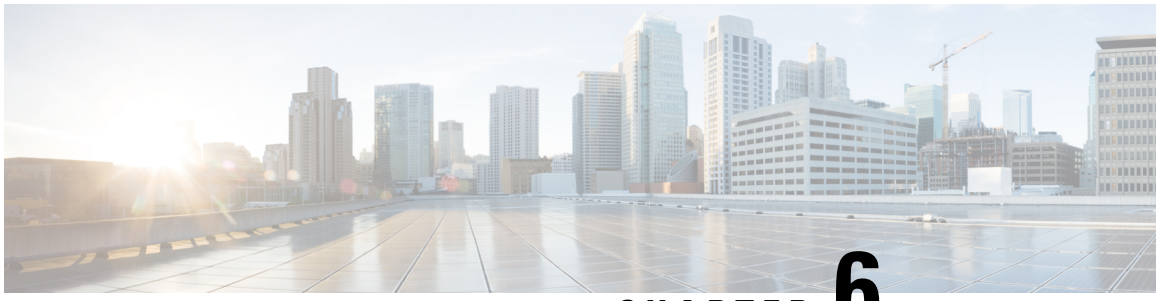
Model	Details
Firepower 4100/9300	Reverting FTD does not downgrade FXOS. For the Firepower 4100/9300, major FTD versions have a specially qualified and recommended companion FXOS version. After you return to the earlier version of FTD, you may be running a non-recommended version of FXOS (too new). Although newer versions of FXOS are backwards compatible with older FTD versions, we do perform enhanced testing for the recommended combinations. You cannot manually downgrade FXOS, so if you find yourself in this situation and you want to run a recommended combination, you will need a full reimage.

Installation Guides

Table 47: Installation Guides

Platform	Guide
FMC	
FMC 1000, 2500, 4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
FMC 750, 1500, 2000, 3500, 4000	Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide
FMCv	Cisco Secure Firewall Management Center Virtual Getting Started Guide
FTD	
Firepower 1000/2100 series	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with 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 Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide
ISA 3000	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide
FTDv	Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
ASA FirePOWER/NGIPSv	

Platform	Guide
Firepower 7000/8000 series	Cisco Firepower 7000 Series Getting Started Guide Cisco Firepower 8000 Series Getting Started Guide
ASA FirePOWER	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware



CHAPTER 6

Bugs

This document lists open and resolved bugs for threat defense and management center Version 6.2.3. For bugs in earlier releases, see the release notes for those versions. For cloud-delivered Firewall Management Center bugs, see the Cisco Cloud-Delivered Firewall Management Center Release Notes.

Important Bug lists are auto-generated once and may not be subsequently updated. If updated, the 'table last updated' date does not mean that the list was fully accurate on that date—only that some change was made. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes. If you have a support contract, you can obtain up-to-date bug lists with the Cisco Bug Search Tool.

- Open Bugs, on page 63
- Resolved Bugs, on page 65

Open Bugs

Important We do not list open bugs for patches.

Open Bugs in Version 6.2.3

Table last updated: 2022-11-02

Table 48: Open Bugs in Version 6.2.3

Bug ID	Headline
CSCvf16001	SF Cli - "inside" or "outside" interface capture not giving all options
CSCvh73096	Firepower Management Center does not support userPrincipalName attribute for login with ISE 2.2+
CSCvh89068	Core in Firepower Management Center Perl

Bug ID	Headline
CSCvh95960	Using the **match** keyword in capture command causes IPv6 traffic to be ignored in capture
CSCvi07656	Small number of TLS connections can fail after TLS inspection in Hardware Mode is overloaded
CSCvi10758	With SSL inspection in software mode, a few TLS connections fail to close in a timely manner
CSCvi16024	SSL errors on session resume when server IP address changes - HW mode
CSCvi18123	Firepower Threat Defense **show tech-support** command output broken on 2100 from CLISH CLI
CSCvi19862	With SSL inspection enabled, TLS traffic throughput can drop following high-availability failover
CSCvi35176	Deployment Failed-Snort Restart Failure-**APPLY_APP_CONFIG_APPLICATION_FAILURE** SignalAppConfigFailed
CSCvi35588	Deployment failure due to **Snort failed to restart** PDTS Handle was NULL
CSCvi42539	Decrypted connections fail when SSLv2 is supported but a higher version is negotiated
CSCvi47264	Some indicators may stay pending when consuming TAXII feeds in parallel
CSCvi50731	Unable to delete certificate objects if there were previous used at ISE even it was deleted
CSCvi61411	Routed Threat Defense allows Transparent Configuration, but traffic fails (6.2.3-66) on KVM only
CSCvi62982	Firepower Threat Defense virtual on ESXi Firstboot config does not sync hostname correctly with FQHN
CSCvi63157	Firepower 2110 dropping connections
CSCvi63864	With SSL inspection in hardware mode and Malware protection, secure file transfers occasionally fail
CSCvi66189	CNP has been enabled in Firepower Management Center where it usage Satellite server for license
CSCvi70680	Same groups from different AD not downloaded
CSCvv14442	FMC backup restore fails if it contains files/directories with future timestamps

Resolved Bugs

Resolved Bugs in New Builds

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

You cannot upgrade from one build to another for the same software version. If you are already running an affected build, determine if an upgrade or hotfix would work instead. If not, contact Cisco TAC. See the Cisco Firepower Hotfix Release Notes for quicklinks to publicly available hotfixes.

Table 49: Version 6.2.3 New Builds

Version	New Build	Released	Platforms: Upgrade	Platforms: Reimage	Resolves
6.2.3.15	39	2020-01-05	FTD/FTDv	—	CSCvs84578: Upgrading FTD on 4100/9300 Platform to 6.2.3.15 break SSHD, preventing FTD instance from booting up CSCvs84713: After upgrading FTD on ASA55XX to 6.2.3.15, cannot SSH to the device CSCvs95725: Virtual FTD Running on 6.2.3.15 blocks SSH request and loses connection with the FMC If you already upgraded your FTD device to Version 6.2.3.15-38, apply Hotfix DW to the device. For more information, see the Software Advisory for CSCvs84578 and CSCvs84713.
6.2.3.14	41	2019-07-03	All	—	CSCvq34224: Firepower Primary Detection Engine process terminated after Manager upgrade If you already upgraded to Version 6.2.3.14-36 and have FTD devices configured for high availability, apply Hotfix CY to the FMC.
6.2.3.11	55	2019-03-17	All	—	Cisco Firepower System User Agent issues. If you already downloaded and installed Version 6.2.3.11-53, contact Cisco TAC for a hotfix.

Version	New Build	Released	Platforms: Upgrade	Platforms: Reimage	Resolves
6.2.3.5	53	2018-11-06	FTD/FTDv	—	CSCvk67239: ASA Firewalls and Firepower Threat Defense devices may traceback and reload when the state of the unit in a Failover pair or multi-unit cluster changes. This also occurred when upgrading from Version 6.2.3.5 to Version 6.2.3.6. For more information, see the Software Advisory for CSCck67239.
6.2.3.2	46	2017-06-27	All	—	CSCvj25386: In some cases, if a device ever ran Version 6.0, upgrading to *any* version earlier than Version 6.2.2.3 failed. CSCvk06176: Even with this new build, if an FMC ever ran Version 6.2.3-88, the SSE cloud connection drops and telemetry cannot send data after you upgrade. If your FMC is affected, apply Hotfix T.
6.2.3.1	47	2017-06-28	All	—	CSCvj25386: In some cases, if a device ever ran Version 6.0, upgrading to *any* version earlier than Version 6.2.2.3 failed. CSCvk06176: Even with this new build, if an FMC ever ran Version 6.2.3-88, the SSE cloud connection drops and telemetry cannot send data after you upgrade. If your FMC is affected, apply Hotfix T.
	45 and 46	2017-06-21	All	—	Component issues.

Version	New Build	Released	Platforms: Upgrade	Platforms: Reimage	Resolves
6.2.3	113	2020-06-01	FMC/FMCv	FMC/FMCv	CSCvr95287: Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability If you are running an earlier build, apply Hotfix DO.
	111	2019-11-25	—	FTDv: AWS, Azure	Contact Cisco TAC.
	110	2019-06-14	—	—	CSCvn78174: Cisco ASA and Cisco FTD Software TCP Timer Handling Denial of Service Vulnerability
	99	2018-09-07	—	—	Contact Cisco TAC.
	96	2018-07-26	—	—	Contact Cisco TAC.
	92	2018-07-05	—	—	CSCvk06176: SSEConnector is not coming up because of Wrong Executable
	88	2018-06-11	—	—	CSCvj13327: Upgrade to 6.2.3 fails at 600_schema/100_update_database.sh - oom killer invoked
	85	2018-04-09	—	—	Contact Cisco TAC.
	84	2018-04-09	Firepower 7000/8000 NGIPSv	—	CSCvi74560: 6.2.3 does not properly deploy variables in variable sets and causes deploy failure CSCvi74623: 6.2.3 upgrade resets home_net variable to default "any" CSCvi77527: upgrade to 6.2.3 fails with post install database integrity check error
	83	2018-04-02	FTD/FTDv ASA FirePOWER	FTD: Physical platforms FTDv: VMware, KVM Firepower 7000/8000 ASA FirePOWER NGIPSv	Contact Cisco TAC.

Resolved Bugs in Version 6.2.3.18

Table last updated: 2022-02-16

Table 50: Resolved Bugs in Version 6.2.3.18

Bug ID	Headline
CSCvm05464	CVE-2018-5391 Remote denial of service via improper IP fragment handling
CSCvp16933	Cisco Firepower Threat Defense Software Shell Access Vulnerability
CSCvq41939	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DHCP DoS
CSCvx00496	QuoVadis root CA decommission on pix-asa
CSCvx19563	FDM: Need to update various items to use STO Certificate Trust Bundle (QuoVadis Root CA Issue)
CSCvx28070	Update QuoVadis root CA for Smart license as it is getting decommissioned
CSCvx30107	Default trustpoint _SmartCallHome_ServerCA using SHA1 which is not supported
CSCvx32283	Cisco Firepower Management Center Open Redirect Vulnerability
CSCvx46296	Cisco ASA and FTD Software Transparent Mode Denial of Service Vulnerability
CSCvx47895	Cisco ASA Software and FTD Software Identity-Based Rule Bypass Vulnerability
CSCvx52541	Update SSEConnector config to use the CA bundle /etc/ssl/certs.pem
CSCvx55664	Cisco Firepower Management Center Cross-site Scripting Vulnerability
CSCvx57417	Smart Tunnel Code signing certifcate renewal
CSCvy16573	Cisco Firepower Threat Defense Command Injection Vulnerability
CSCvy20504	Cisco ASA and FTD Software Web Services Interface Cross-Site Scripting Vulnerability
CSCvy36910	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS
CSCvy41771	Cisco Firepower Management Center Software Authenticated Directory Traversal Vulnerability
CSCvy58278	Denial of Service vulnerability handling the config-request request
CSCvy80325	Include the ios pem files into the patch upgrade package for vFTD
CSCvy93480	Cisco ASA and FTD Software IKEv2 Site-to-Site VPN Denial of Service Vulnerability
CSCwa46963	Security: CVE-2021-44228 -> Log4j 2 Vulnerability

Bug ID	Headline
CSCwa70008	Expired certs cause Security Intel. and malware file preclassification signature updates to fail
CSCwa88571	Unable to register FMC with the Smart Portal

Resolved Bugs in Version 6.2.3.17

Table last updated: 2021-06-14

Table 51: Resolved Bugs in Version 6.2.3.17

Bug ID	Headline
CSCvh64138	FXOS upgrade to 2.3.1.X causes FTD logical device to not come up
CSCvk08565	App-instance in start-failed with "Application Failing to Start by ProcMgr" error on container app
CSCvn82441	[SXP] Issue with establishing SXP connection between ASA on FPR-2110 and switches
CSCvn95731	ASA traceback and reload on Thread Name SSH
CSCvo60166	KP: Can't login to fxos due to disk full error
CSCvo86940	PROMPTING FOR PASSWORD WHEN TRYING TO CONFIGURE enic, vfio-pci , igb_uio ON BLADE
CSCvp16482	ASA reloads when establishing simultaneous ASDM sessions
CSCvp49481	Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability
CSCvp57643	FTD/ASA - Cluster/HA - Master/Active unit does not update all the route changes to Slaves/Standby
CSCvp93468	Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability
CSCvq43920	Cisco Firepower Threat Defense Software Hidden Commands Vulnerability
CSCvr35872	ASA traceback Thread Name: DATAPATH with PBR configured
CSCvr55973	Unable to ping out of management 1/1 interface on a KP
CSCvr80164	WR6 and WR8 commit id update in CCM layer(sprint 72)
CSCvs45111	WR6 and WR8 commit id update in CCM layer(sprint 75)
CSCvs56888	Cisco Firepower Threat Defense Software TCP Flood Denial of Service Vulnerability
CSCvs81504	WR6 and WR8 commit id update in CCM layer(sprint 77)
CSCvt01282	WR6 and WR8 commit id update in CCM layer(sprint 79)

Bug ID	Headline
CSCvt02409	Cisco Firepower Threat Defense Software Inline Pair/Passive Mode DoS Vulnerability
CSCvt13445	Cisco ASA and FTD Software FTP Inspection Bypass Vulnerability
CSCvt18028	Cisco ASA and FTD WebVPN CRLF Injection Vulnerability
CSCvt30731	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 80)
CSCvt31177	Cisco ASA and FTD Software for FP 1000/2100 Series Appliances Secure Boot Bypass Vulns
CSCvt31178	Cisco ASA and FTD Software for FP 1000/2100 Series Appliances Secure Boot Bypass Vulns
CSCvt60190	Cisco ASA and FTD Web Services File Upload Denial of Service Vulnerability
CSCvt70322	Cisco ASA Software and FTD Software Web Services Denial of Service Vulnerability
CSCvt74037	Cisco FXOS Software Command Injection Vulnerability
CSCvt83121	Cisco ASA and FTD Software OSPFv2 Link-Local Signaling Denial of Service Vulnerability
CSCvu15801	Cisco ASA and FTD Software SIP Denial of Service Vulnerability
CSCvu20257	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 85)
CSCvu40531	FXOS LACP packet logging to pktmgr.out and lacp.out fills up /opt/cisco/platform/logs to 100%
CSCvu44910	Cisco ASA Software and FTD Software Web Services Cross-Site Scripting Vulnerability
CSCvu46685	Cisco ASA and FTD Software SSL/TLS Session Denial of Service Vulnerability
CSCvu59817	Cisco ASA and FTD Software SSL VPN Direct Memory Access Denial of Service Vulnerability
CSCvu61919	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 87)
CSCvu75581	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities
CSCvu75615	Cisco ASA Software and FTD Software WebVPN Portal Access Rule Bypass Vulnerability
CSCvu83309	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities
CSCvu91097	Cisco Firepower Management Center Software Policy Vulnerability
CSCvv13835	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities
CSCvv33712	Cisco ASA Software Web-Based Management Interface Reflected Cross-Site Scripting Vulnerabi

Bug ID	Headline
CSCvv56644	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web DoS
CSCvv65184	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web DoS
CSCvv79459	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 94, seq 1)
CSCvv95277	FPR2100 High disk usage in partition /opt/cisco/platform/logs due to growth of httpd log files
CSCvw13348	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 98, seq 2)
CSCvw26544	Cisco ASA and FTD Software SIP Denial of Service Vulnerability
CSCvw52609	Cisco ASA and FTD Software Web Services Buffer Overflow Denial of Service Vulnerability
CSCvw53796	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerability
CSCvw53884	M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service
CSCvw90923	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 101, seq 4)
CSCvx06920	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 103, seq 5)
CSCvx16700	FXOS clock sync issue during blade boot up due to "MIO DID NOT RESPOND TO FORCED TIME SYNC"

Resolved Bugs in Version 6.2.3.16

Table last updated: 2020-07-13

Table 52: Resolved Bugs in Version 6.2.3.16

Bug ID	Headline
CSCvg84794	All Interfaces does not come up after booting KP ASA image
CSCvj49994	Failed to download FXOS package during upgrade due to no IPv6 address
CSCvm48451	Intrusion Event Performance Graphs load blank on 4100 and 9300
CSCvm84994	SSH idle timeout not working on FTD on Firepower 4100 and Firepower 9300
CSCvm85823	Not able to ssh, ssh_exec: open(pager) error on console
CSCvn93683	ASA: cluster exec show commands not show all output
CSCvo62077	Cisco Firepower Threat Defense Software VPN System Logging Denial of Service Vulnerability

Bug ID	Headline
CSCvo78789	Cisco Adaptive Security Appliance Smart Tunnel Vulnerabilities
CSCvo80853	Cisco Firepower Threat Defense Software Packet Flood Denial of Service Vulnerability
CSCvp04134	Traceback in HTTP Cli Exec when upgrading to 9.12.1
CSCvp16945	Cisco ASA Software and FTD Software MGCP Denial of Service Vulnerabilities
CSCvp16949	Cisco ASA Software and FTD Software MGCP Denial of Service Vulnerabilities
CSCvp45149	Traceback while Reverting the primary system as active
CSCvp49481	Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability
CSCvp55941	FILE RESUME BLOCK being randomly thrown causing access issues on files from SMB share.
CSCvp87623	Upload an update gives "update request entity too large" error when using CAC(HTTPS Client Certs)
CSCvp90847	Refresh Root CAs that SSL uses for resigning in FTD/FMC
CSCvp93468	Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability
CSCvq12070	Not able to establish more than 2 simultaneous ASDM sessions
CSCvq13442	When deleting context the ssh key-exchange goes to Default GLOBALLY!
CSCvq20910	Cisco Firepower 2100 Series Security Appliances ARP Denial of Service Vulnerability
CSCvq35440	Upgrade Enhancements to STRAP verification for anyconnect - Cisco VPN session replay vulnerability
CSCvq36042	lost heartbeat causing reload
CSCvq54034	WRL6 and WRL8 commit-id update in CCM Layer (sprint 65)
CSCvq56257	Cached malware disposition does not always expire as expected
CSCvq66092	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software BGP DoS
CSCvq70485	Slow "securityzones" REST API
CSCvq70775	FPR2100 FTD Standby unit leaking 9K blocks
CSCvq71217	High Disk Utilization due to mysql-server.err failing to rotate after CSCvn30118
CSCvq73534	Cisco ASA Software Kerberos Authentication Bypass Vulnerability
CSCvq73599	Cisco VPN session replay vulnerability : STRAP fix on ASA for SSL(OpenSSL 1.0.2) and SCEP proxy
CSCvq93640	WRL6 and WRL8 commit id update in CCM layer (sprint 67)

Bug ID	Headline
CSCvr07419	Cisco ASA and FTD Software IPv6 DNS Denial of Service Vulnerability
CSCvr09748	Cisco FXOS and FTD Software Command Line Interface Arbitrary File Read and Write Vuln
CSCvr11395	Only a subset of devices where deployed from a device group during scheduled deploy
CSCvr17735	SFDataCorrelator high CPU during SI update
CSCvr37502	libexpat Improper Parsing Denial of Service Vulnerability
CSCvr39556	Segfault in libclamav.so (in the context of SFDataCorrelator)
CSCvr49734	Cisco FXOS and UCS Manager Software CLI Command Injection Vulnerability
CSCvr55825	Cisco ASA and FTD Software Path Traversal Vulnerability
CSCvr63941	KP ASA diagnostic-cli channel stops functioning
CSCvr85295	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote
CSCvr86213	CD is required to ignore Cluster-Msg-Delivery-Confirmation in Cluster Node Release Lina State
CSCvr90768	FTD: Deployment through slow links may fail
CSCvr92327	ASA/FTD may traceback and reload in Thread Name 'PTHREAD-1533'
CSCvs12288	Snort unexpectedly exits with SSL policy enabled and debug_policy_all
CSCvs19968	Fix consoled from getting stuck and causing HA FTD policy deployment errors.
CSCvs33416	Upgrade Kernel to 4.14.158
CSCvs34844	pm process becomes randomly deadlocked when communicating with hardware.
CSCvs50459	Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability
CSCvs59487	Observed crash in KP device while upgrading to 99.14.1.64 image.
CSCvs60254	libxml2 xmlParseBalancedChunkMemoryRecover Memory Leak Vulnerability
CSCvs61701	DME process crash due to memory leak on Firepower 2100
CSCvs77334	FTD failover due to error "Inspection engine in other unit has failed due to snort and disk failure"
CSCvs84578	Upgrading FTD on 4100/9300 Platform to 6.2.3.15 prevents the FTD instance from booting up
CSCvs84713	Cannot SSH to the device after upgrading FTD on ASA55XX/ISA 3000/FTDv to 6.2.3.15 build 38

Bug ID	Headline
CSCvs87168	SNORT Fatal Error due to out of range interface ID
CSCvs94486	CSCvs59487 requires additional fix for resolution
CSCvs98311	FSIC Failure after upgrade from 6.2.3.15-38 > 6.2.3.16-29 in CC Mode
CSCvt03598	Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability
CSCvt15163	Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability
CSCvt39135	snort instances CPU spikes to >90% at low non-SSL traffic with SSL policy applied
CSCvt39299	6.2.3.15 to 6.4.0 upgrade broken for Series-3 Sensors
CSCvt80172	Supervisor software needs to be upgraded to address CVE-2017-11610
CSCvu30830	NGIPS sensor SSH broken due to bad CiscoSSH keywork in sshd_config file

Resolved Bugs in Version 6.2.3.15

Table last updated: 2019-09-17

Table 53: Resolved Bugs in Version 6.2.3.15

Bug ID	Headline
CSCve24102	GUI should allow max 256 addresses per DHCP pool
CSCvg49225	Canceling scheduled FXOS upgrade does not clear the event
CSCvg85687	Error messages seen on console when FXOS boots up
CSCvk43854	Cisco Firepower Threat Defense Detection Engine Policy Bypass Vulnerability
CSCvm64400	IKEv2: IKEv2-PROTO-2: Failed to allocate PSH from platform
CSCvm68648	review of CVE-2016-8858 (OpenSSH) on Firepower software
CSCvm82966	Linux Kernel 4.14 Vulnerabilities
CSCvn46390	Lina msglayer performance improvements: port Hotfix BO
CSCvn77125	FXOS: copy command should allow for wildcards to transfer multiple files
CSCvo29989	Cisco FirePower Threat Defense Information Disclosure Vulnerability
CSCvo47390	ASA traceback in thread SSH
CSCvo48838	Lina does not properly report the error for configuration line that is too long
CSCvo68184	management-only of diagnostic I/F on secondary FTD get disappeared

Bug ID	Headline
CSCvo68448	ASA report SFR module as 'Unresponsive' after reloading ASA module on 5585 platform
CSCvo85861	Propagate link-state not shown in FTD CLI
CSCvo86485	incorrect HTML <base> tag handling by Grammar Based Parser
CSCvo88762	FTD inline/transparent sends packets back through the ingress interface
CSCvo89224	FMC times out after 10 mins to fetch device list for deployment
CSCvo90998	LACPDUs should not be sent to snort for inline-set interfaces
CSCvp07616	[ciam] Python urllib Security Bypass Vulnerablity
CSCvp15176	FTD/ASA installed on firepower devices may report comm failure and assume itself as active/master.
CSCvp16536	ASA traceback and reload observed in Datapath due to SIP inspection.
CSCvp16618	URL inside HTML base tag is not rewritten after it is handled by GBP
CSCvp27263	Multiple ClamAV Vulnerabilities For Cisco Firepower Management Center for pre 6.5.0
CSCvp35141	ASA sends invalid redirect response for POST request
CSCvp35769	[ciam] Apache HTTP Server URL Normalization Denial of Service Vulnerability
CSCvp37779	FTD show tech from troubleshooting files incomplete
CSCvp46150	[ciam] GNU Wget Buffer Overflow Vulnerability
CSCvp48273	[ciam] Linux Kernel cipso_v4_validate Denial of Service Vulnerability
CSCvp49576	FTD Cluster traceback experienced when other unit leaves the Cluster
CSCvp53637	Flows are getting offloaded on inline-sets
CSCvp54261	Audit syslog for SFR module/7000/8000 devices uses TCP instead of UDP for syslog communication
CSCvp55880	Fail-Closed FTD passes packets through on Snort processes down
CSCvp55901	LINA traceback on ASA in HA Active Unit repeatedly
CSCvp58028	natd thread of nfm_exceptiond uses about 90% to 100% CPU time
CSCvp66559	Deploy fails on FTD HA due to exception when parsing big xml response
CSCvp67257	USGv6 Failures From Kernel Upgrade [3.10 to 4.14]
CSCvp67392	ASA/FTD HA Data Interface Heartbeat dropped due to Reverse Path Check

Bug ID	Headline
CSCvp70699	ASA Failover split brain (both units active) after rebooting a Firepower chassis
CSCvp72244	Evaluate Cisco 8000 series for CVE-2019-11815
CSCvp72488	Firepower: AMP for network connectivity failure after upgrading to 6.3.0.2+
CSCvp83437	serial console/SSH login using local account succeeds but immediately returns to login prompt
CSCvp97061	URL Filtering Shows All URLs as Uncategorized
CSCvp97799	Policy deploy failure 6.5.0-1148 post upgrade with CC mode with openSSL call during SSL pol Export
CSCvp97916	Executing 'failover' twice on active unit, clears interface configuration on standby unit
CSCvp98066	On reset CD not clearing its flags[parseFailoverReqIssued] which prevents further node join attempts
CSCvq00675	Linux Kernel sas_expander.c Race Condition Arbitrary Code Execution ...
CSCvq06790	Snort processes dump core with memory corruption on Series 3 devices
CSCvq13917	ADI does not learn VPN user logins anymore
CSCvq19525	Evaluation of sfims for TCP_SACK
CSCvq19641	Evaluation of Firepower 4k/9k Supervisor for TCP_SACK
CSCvq27010	Memory leak observed when ASA-SFR dataplane communication flaps
CSCvq32681	Fail to Wire configuration disabled for multiple interface-pair inline-sets during FTD upgrades
CSCvq33916	Linkdown between FP 4100 and switch when using 40gb bidi to 40/100 bidi
CSCvq39083	Security Intelligence does not drop HTTPS connections to blacklisted URLs when SSL policy is enabled
CSCvq44665	FTD/ASA : Traceback in Datapath with assert snp_tcp_intercept_assert_disabled
CSCvq54242	Warrning "There is an empty group in the source networks" in SSL policy
CSCvq56462	File policy not inspecting some malware document (.doc) and Adobe flash (.swf) files.
CSCvq57710	Firepower Primary Detection Engine process might terminated after Manager upgrade
CSCvq61651	URL DB download failure alerts on FMC; new URL DB updates not taking effect on FMC/FDM
CSCvq65092	Slow device related REST API calls
CSCvq98171	Unable to do Recovery using latest r241 images

Resolved Bugs in Version 6.2.3.14

Table last updated: 2019-07-03

Table 54: Resolved Bugs in Version 6.2.3.14

Bug ID	Headline
CSCvb15074	FMC health notifications for interfaces removed or added out-of-band get stuck
CSCvi63474	Unable to edit the system policy of a SFR module via ASDM after upgrading to 6.2.2
CSCvk69823	FlexConfig objects pushed to device in spite of no changes being made to that on either FMC or FTD
CSCvm70274	tcp proxy: ASA traceback on DATAPATH
CSCvn86777	Deployment on FTD with low memory results on interface nameif to be removed
CSCvo24145	ids_event_alerter high memory usage due to large firewall_rule_cache table
CSCvo33348	Mysql traffic on non standard port is not correctly classified
CSCvo33851	ngfwManager doesn't start if ngfw.properties is empty
CSCvo43679	FTD Lina traceback, due to packet looping in the system by normaliser
CSCvo50168	Audit Log Settings Failing Leading to being unable to edit System Settings
CSCvo60580	ASA traceback and reloads when issuing "show inventory" command
CSCvo60862	Internal Error when editing an Access Control Policy
CSCvo74745	cloud agent core after generating a large number of continuous URL lookups (>30M)
CSCvo90805	Cisco Firepower Management Center RSS Cross-Site Scripting Vulnerabilities
CSCvp16979	ssl and daq debug logs can't be enabled/disabled dynamically
CSCvp18878	ASA: Watchdog traceback in Datapath
CSCvp19549	FTD lina cored with Thread name: cli_xml_server
CSCvp24728	Random SGT tags added by FTD
CSCvp24787	(snort)File is not getting detected when going over HTTPS (SSL Resign)
CSCvp25583	FTD sets automatically metric 0 when we redistribute OSPF into BGP via FMC GUI.
CSCvp29692	FIPS mode gets disabled after rollback from a failed policy deploy
CSCvp33052	Firepower 8000 interfaces might flap due to unhandled resource temporarily unavailable issue
CSCvp43536	On upgraded FMC Device FXOS devices are shown dirty even after successful deployment.

Bug ID	Headline
CSCvp54634	Wrong rule matched when using ambiguous DND
CSCvp78197	Policy deployment remove and add back ospf neighbor
CSCvp81967	Slowness in loading Device Management page on FMC when there are over 500 managed devices
CSCvp82945	NAT policy apply failing with error duplicate
CSCvp96934	Ensure Error Message with Dup NATs Is Clear and Actionable
CSCvq13917	6.2.3.13 ADI does not learn VPN user logins anymore
CSCvq34224	Firepower Primary Detection Engine process terminated after Manager upgrade

Resolved Bugs in Version 6.2.3.13

Table last updated: 2019-07-03

Table 55: Resolved Bugs in Version 6.2.3.13

Bug ID	Headline
CSCve13816	MEMCACHED software needs to be upgraded to address several security vulnerabilities
CSCvf83160	Traceback on Thread Name: DATAPATH-2-1785
CSCvg01007	https pdf attachment issues
CSCvg74603	eStreamer archive events are not pruned correctly by diskmanager
CSCvi16224	snmp-server host command for SNMPv3 doesn't apply properly when deploy ASAv VM on NFVIS (KVM) system
CSCvi32569	Excessive logging in mysql-server.err log causes huge log files in FTD
CSCvi59887	OSPF Route may become stale and stuck in the routing table after failover events
CSCvj49623	Memory Leak In Smart Licensing
CSCvk14242	sfstunnel process in FTD is holding large cloud db files that are already deleted
CSCvk26612	"default Keyring's certificate is invalid, reason: expired" health alert
CSCvk29263	SSH session stuck after committing changes within a Configure Session.
CSCvk30739	ASA CP core pinning leads to exhaustion of core-local blocks
CSCvk44166	Cisco ASA and FTD TCP Proxy Denial of Service Vulnerability
CSCvk72958	Qos applied on interfaces doesn't work.
CSCvm00066	ASA is stuck on "reading from flash" for several hours

Bug ID	Headline
CSCvm08769	Standby unit sending BFD packets with active unit IP, causing BGP neighborship to fail.
CSCvm17985	Initiating write net command with management access for BVI interfaces does not succeed
CSCvm27111	FTD Lina traceback while removing OSPF configuration.
CSCvm36362	Route tracking failure
CSCvm80779	ASA not inspecting H323 H225
CSCvm82290	ASA core blocks depleted when host unreachable in IRB configuration
CSCvm85257	Spin lock traceback when changing vpn-mode with traffic
CSCvm86008	Policy Deployment: Delta config doesn't get copied to running config, LINA config remains unchanged
CSCvm88294	High Disk utilization due to partition force drain not occurring
CSCvn22833	ADI process fails to start on ASA on Firepower 4100
CSCvn30108	The 'show memory' CLI output is incorrect on ASAv
CSCvn30393	ASA Traceback in emweb/https during Anyconnect Auth/DAP assessment
CSCvn31347	ACL Unable to configure an ACL after access-group configuration error
CSCvn32620	IKEv2 Failed to obtain an Other VPN license
CSCvn34246	Loading AC policy editor takes too long, needs loading indicator
CSCvn38453	ASA: Not able to load Quovadis Root Certificate as trustpoint when FIPS is enabled
CSCvn45750	FMC Audit Logs will only display Admin and System as owners when deploying to 3D devices -GUI/SYSLOG
CSCvn50320	Firepower MySQL Server : Oracle MySQL October 2018 Critical Patch Update
CSCvn55007	DTLS fails after rekey
CSCvn57284	Unsupported EC curve x25519 on FTD
CSCvn66248	Configuring "boot config" has no effect if file was modified off-box and copied back on
CSCvn67137	ASA5506 may slowly leak memory when using NetFlow
CSCvn68527	FPR21xx: AnyConnect assigned addresses not marked allocated on Standby
CSCvn71592	After FMC reboot, intrusion events generated by Snort are not sent to FMC and show up in webGUI

Bug ID	Headline
CSCvn73962	ASA 5585 9.8.3.14 traceback in Datapath with ipsec
CSCvn76829	ASA as an SSL Client Memory Leak in Handshake Error path
CSCvn77248	Cisco Secure Boot Hardware Tampering Vulnerability
CSCvn78597	Firepower block page not displayed on MS IE11 and Edge for HTTPS blocked sites when proxy is enabled
CSCvn78674	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvn78870	ASA Multicontext traceback and reload due to allocate-interface out of range command
CSCvn94100	"Process Name: lina" | ASA traceback caused by Netflow
CSCvn95711	Traceback on Thread Name: Unicorn Admin Handler after adding protocol to IKEV2 ipsec-proposal
CSCvn96898	Memory Leak in DMA_Pool in binsize 1024 with SCP download
CSCvn97591	Packet Tracer fails with "ERROR: TRACER: NP failed tracing packet", with circular asp drop captures
CSCvo04444	Ikev2 tunnel creation fails
CSCvo06216	Support more than 255 chars for Split DNS-commit issue in hanover for CSCuz22961
CSCvo11406	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvo11416	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvo13497	Unable to remove access-list with 'log default' keyword
CSCvo15484	Unable to delete User IOC if user info is inconsistent between mysql & sybase - part fix
CSCvo17033	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvo23222	AnyConnect session rejected due to resource issue in multi context deployments
CSCvo27109	Standby may enter reboot loop upon upgrading to 9.6(4)20 from 9.6(4)6
CSCvo42174	ASA IPSec VPN EAP Fails to Load Valid Certificate in PKI
CSCvo45093	Validation Check when two objects with different name but same network is used in route without ECMP
CSCvo45209	FTD-CLUSTER:Adding new unit in cluster can cause traffic drop
CSCvo51265	SCP large file transfer to the box result in a traceback

Bug ID	Headline
CSCvo55151	crypto ipsec inner-routing-lookup should not be allowed to be configured with VTI present
CSCvo56616	Deployment times out in some cases resulting in non-terminated AQ
CSCvo56836	SCALE: with 500+ devices, UMS causes the UI to hang, especially during deploy
CSCvo58847	Enhancement to address high IKE CPU seen due to tunnel replace scenario
CSCvo60627	Policy failing to deploy after adding new cluster unit to setup
CSCvo62060	Telemetry not sent when FMC managing lots of devices
CSCvo66534	Traceback and reload citing Datapath as affected thread
CSCvo70866	SGT tag shows untagged in server packet for every client packet with SGT tag with some value
CSCvo72179	For SMB, remote storage configuration should allow configuring version string with dot(.)
CSCvo72232	ERR_SSL_BAD_RECORD_MAC_ALERT or SSL_ERROR_BAD_MAC_ALERT in the browser
CSCvo74350	ASA may traceback and reload. Potentially related to WebVPN traffic
CSCvo76727	No warning about possible policy deployment failure when in route is more than one object
CSCvo81073	Unable to load Device Management page or upgrade FMC due to missing NGFWHA EO
CSCvo83574	Device goes into a bad state when switching the inline set from TAP mode
CSCvo87930	HTTP with ipv6 using w3m is failing
CSCvo88188	SSL rules with App-ID conditions can limit decryption capability
CSCvo88306	NAT rules can get applied in the wrong order when you have duplicate rules
CSCvo93872	Memory leak while inspecting GTP traffic
CSCvo94486	Snort process exits while processing Security Intelligence.
CSCvp21837	Allow FTDs to perform URL lookups directly without having to go through the FMC
CSCvp42398	Series 3 8250: Upgrade 6.4.0-87 failed at 999_finish/989_flip_mbr.sh
CSCvp54634	Wrong rule matched when using ambiguous DND

Resolved Bugs in Version 6.2.3.12

Table last updated: 2019-05-13

Table 56: Resolved Bugs in Version 6.2.3.12

Bug ID	Headline
CSCvh26064	Unable to use "Change Reconciliation" on 7000/8000 sensors
CSCvj82652	Deployment changes are not pushed to the device due to disk0 mounted on read-only
CSCvk56988	Cisco ClamAV MEW unpacker Denial of Service Vulnerability
CSCvm16724	FXOS ASA/FTD needs means to poll Internal-data interface counters
CSCvm24210	One of the two schedule tasks running on same timestamp fails if they both access the same file
CSCvm35373	Pruner process fails to start due to configuration
CSCvm40545	downgrading FTD twice in a row without updating in between results in wrong lina version
CSCvn07452	712x devices become unstable when switching inline set from TAP to inline
CSCvn09383	Manual URL lookup returns Uncategorized if same URL is entered second time without "www." part
CSCvn38189	SFDataCorrelator is not restarted after backup scripts died
CSCvn46358	overloading of the lina msglyr infra due to the sending of VPN status messages
CSCvn49854	Subsequent HTTP requests not retrieving URL and XFF
CSCvn67570	amp-stunnel.conf does not point to correct amp cloud server post FMC upgrade
CSCvn67888	Object added using REST API result in policy deploy failure
CSCvn72570	Cisco ASA Software and FTD Software VPN SAML Authentication Bypass Vulnerability
CSCvn73848	Snort sessions are timing out earlier than configured idle timeouts.
CSCvn74112	FTDv does not have configuration on initial bringup with mix of vmxnet3 and ixgbevf interfaces
CSCvn75368	FPR platform IPsec VPN goes down intermittently
CSCvn78593	Control-plane ACL doesn't work correctly on FTD
CSCvn82895	Diskmanager may not track all event files
CSCvn87965	While associating FMC with TG account, FMC should not redirect users to TG console
CSCvn99712	Cisco Firepower Management Center Persistent Cross-Site Scripting Vulnerability

Bug ID	Headline
CSCvo02097	Upgrading ASA cluster to 9.10.1.7 cause traceback
CSCvo12057	DHCPRelay does not consume DHCP Offer packet with Unicast flag
CSCvo15545	nfm-burnin.sh system validation test fails for latest NFM release
CSCvo17775	EIGRP breaks when new sub-interface is added and "mac-address auto" is enabled
CSCvo20847	Active FTP fails through Cluster due to xlate allocation corruption upon sync
CSCvo23150	excessive DB queries for user identities causes slowness in user session processing.
CSCvo27164	SFDataCorrelator logs inappropriate "Resuming storage of old events" messages
CSCvo29973	ssl rules with cipher suite conditions can cause unneeded tls 1.3 downgrade
CSCvo31353	SSL connections may fail when URL categories are used and certificate common name doesn't match
CSCvo31953	Memory leak in SFDataCorelator process
CSCvo32329	Deleted realm is causing many user_id's loaded into user_identities cache
CSCvo38051	segfault in ctm_ipsec_pfkey_parse_msg at ctm_ipsec_pfkey.c:602
CSCvo39052	FSIC error after enable the CC mode
CSCvo39094	Delay/Longer processing time to insert policy deploy task after selecting the device for deploy
CSCvo40210	Update Talos RSS feed in dashboard widget
CSCvo43693	FTD HA creation fails due to multiple files modules*.tgz and vdb*.tgz being transferred from FMC
CSCvo44064	aggressive downgrade action is taken when url look up is pending due to no sni
CSCvo47562	VPN sessions failing due to PKI handles not freed during rekeys
CSCvo50230	SSL Connections to uncategorized URLs may fail repeatedly
CSCvo54799	ssh to device fails due to corrupted devpts entry in fstab
CSCvo55203	Registered devices do not appear in the Device Management page
CSCvo55282	Policy deploy fails when user is able to enter invalid inline port range in AC Rule accidentally
CSCvo56675	ASA or FTD traceback and reload due to failover state change or xlates cleared
CSCvo56895	Some donut charts on the Context Explorer failing to load
CSCvo61091	eStreamer memory and CPU grow when sending NAP policy metadata

Bug ID	Headline
CSCvo62031	ASA Traceback and reload while running IKE Debug
CSCvo63240	Smart Tunnel bookmarks don't work after upgrade giving certificate error
CSCvo66920	Enhancement: add counter for Duplicate remote proxy
CSCvo67454	Invalid port range object causes AC policy deploy to fail
CSCvo72462	Do not decrypt rule causes traffic interruptions.

Resolved Bugs in Version 6.2.3.11

Table last updated: 2019-03-13

Table 57: Resolved Bugs in Version 6.2.3.11

Bug ID	Headline
CSCuz28594	Diskmanager - critical alert on /var/storage due to disk manager not pruning till 99%
CSCvi54162	"ha-replace" action not working when peer not present
CSCvi55841	errors saving blacklist config file are not detected
CSCvi62112	Blocking BPDU via FlexConfig on FTD Transparent causes deployment and registration issues
CSCvk06386	FTD Files are Allowed Through Multiple Pre-existing Connections Despite the File Policy Verdict
CSCvm14875	Large number of stale cloudconfig EO causing performance issues
CSCvm58799	During deploy, if multiple Snorts are not responding, recovery takes too long
CSCvm60039	Custom DNS security intelligence feed fail to download intermittently
CSCvm96339	/dev/root partition will fill to 100% due to archive_cache_seed.sensor file
CSCvn10634	Files are not detected in HTTP flows when there's an Out of Order (ACK before actual data)
CSCvn16102	Diskmanager file capture data not increasing for hours at a time
CSCvn17347	Traceback and reload when displaying CPU profiling results
CSCvn38082	FMC should identify and recover from mongo corruption
CSCvn41903	Snort reload fails and causes restart due to dce2-mem-reloader memory adjustments taking too long
CSCvn47788	UI validation fails on a valid hostname IP for Audit Log Host in Firepower platform setting policy

Bug ID	Headline
CSCvn48739	FTD show tech taken from CLISH mode and in troubleshoot may be truncated
CSCvn53145	Policy deploy throws "Variable set has invalid execulded values"
CSCvn69019	usernames with single quotes are not written into user_ip_map file
CSCvn72683	FMC webGUI device management page loading time is too long around 45s with 25s fetching license
CSCvn73848	Snort sessions are timing out earlier than configured idle timeouts.
CSCvo00887	ssl client hello should not be modified if "Do Not Decrypt" rule will be the only possible verdict
CSCvo03186	Domain page in Firepower Management Center takes long time to load
CSCvo03808	Deploy from FMC fails due to OOM with no indication of why
CSCvo11077	Memory leak found in IPsec when we establish and terminate a new IKEv1 tunnel.
CSCvo39052	FSIC error after enable the CC mode

Resolved Bugs in Version 6.2.3.10

Table last updated: 2019-02-07

Table 58: Resolved Bugs in Version 6.2.3.10

Bug ID	Headline
CSCuu67159	ASA: traceback in DATAPATH-2-1157
CSCva62256	Appliance status widget taking too long with 500 sensors
CSCvf81672	ASA Routes flushed after failover when etherchannel fails
CSCvg40735	GTP inspection may spike cpu usage
CSCvg56122	SSL handshake fails with large certificate chain size
CSCvi09811	Traceback in DATAPATH, assertion "0" failed: file "./snp_cluster_transport.h", line 480
CSCvi28763	FTD Platform Settings: change default DH-group in SSL custom settings to 2
CSCvi34533	Cannot save modification in Access List if there's no SNMPv3 user defined
CSCvi71622	Traceback in DATAPATH on standby FTD
CSCvi97028	fmc GUI too slow when configuring unreachable syslog server
CSCvj01704	ASA is getting traceback with reboot only on ASA 5585-X after shutdown SFR module

Bug ID	Headline
CSCvj65154	FMC failing to communicate with SSM when proxy password contains @ character
CSCvj74643	Enabling Use CAC authentication and authorization on AD breaks RADIUS when changed.
CSCvj87287	simultaneous flood of REST-API requests to FMC results in inaccessibility
CSCvj89445	Inconsistent deployment status on GUI
CSCvj97229	'User Name Template' should be required filed for external authentication object for CAC in FMC
CSCvk18330	Active FTP Data transfers fail with FTP inspection and NAT
CSCvk19946	Sftunnel service broken due to cache archive data flooding
CSCvk39339	Unable to run the scheduling report generation on Japanese FMC
CSCvk40964	Deployment of empty interface config to device lead to traffic outage
CSCvk46038	ERROR: The entitlement is already acquired while the configuration is cached.
CSCvk50815	GTP inspection should not process TCP packets
CSCvk55634	Random policy deployment failure due to stuck notification for policy deployment
CSCvm24706	GTP delete bearer request is being dropped
CSCvm28730	ASA/FTD-LINA Tracebacks observed while getting CPU Profiling information
CSCvm33553	Clock drift causes Heartbeat misses from ndclientd
CSCvm46014	Copy config should not fail if standby device is corrupted on FTD HA
CSCvm55091	HA failed primary unit shows active while "No Switchover" status on FP platforms
CSCvm59983	The file-size directive returns invalid input error and breaks the captures from clish
CSCvm67273	ASA: Memory leak due to PC alloc_fo_ipsec_info_buffer_ver_1+136
CSCvm87315	FTD registration can fail because of TID in RegistrationTR::addToLamplighter
CSCvm88004	SSH Service on ASA echoes back each typed/pasted character in its own packet
CSCvn05797	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCvn06618	On LINA config rollback the startup-config is being merged with the default running
CSCvn09322	FTD device rebooted after taking Active State for less than 5 minutes
CSCvn09367	Prevent administrators from installing CXSC module on ASA 5500-X
CSCvn15757	ASA may traceback due to SCTP traffic inspection without NULL check
CSCvn16489	AMP Dynamic Analysis's clouds should be tracked separately for submission rates.

Bug ID	Headline
CSCvn19823	ASA : Failed SSL connection not getting deleted and depleting DMA memory
CSCvn20411	Device management page never loads and times out after an error message
CSCvn21899	Firepower: Disable TLS 1.0 permanently for SFTunnel communication
CSCvn23224	FTD-HA forming failed with SNMP configured
CSCvn23254	SNMPv2 pulls empty ifHCInOctets value if Nameif is configured on the interface
CSCvn23701	Deployment failed with - ftp_telnet.conf(4) => Invalid keyword 'memcap' for 'global' configuration.
CSCvn24756	Security intelligence feature can falsely block IP addresses (URL block)
CSCvn30118	mysql-server.err file is not fully deleted and keeps consuming Firepower disk space
CSCvn32657	ASA traceback when removing interface configuration used in call-home
CSCvn33943	Standby node traceback in wccp_int_statechange() with HA configuration sync
CSCvn36393	exclude tls1.0 and tls1.1 in stunnel config file
CSCvn37829	ASA should allow GCM(SSL) connections to use DMA_ALT1 when primary DMA pool is exhausted
CSCvn38010	Let remove_peers.pl scripts bailout when it is run in FTD HA setup
CSCvn43798	Deleting a domain fails to delete some objects if a Realm is in that domain
CSCvn44201	ASA discards OSPF hello packets with LLS TLVs sent from a neighbor running on IOS XE 16.5.1 or later
CSCvn46474	FP2120 FTD went unresponsive after power outage
CSCvn47599	RA VPN + SAML authentication causes 2 authorization requests against the RADIUS server
CSCvn47800	ASA stops authenticating new AnyConnect connections due to fiber exhaustion
CSCvn48790	Slave node kicked out of cluster if SI task running during policy apply
CSCvn49561	update FireAMP curl calls to use CA path
CSCvn53732	Modified SSL connections that are not decrypted should be closed
CSCvn54347	Entitlement release error in Failover switchover or disband on fp2100/1000 KP/WM
CSCvn56095	selective acking not happening with SSL crypto hardware offload
CSCvn61662	ASA 5500-X may reload without crashinfo written due to CXSC module continuously reloading

Bug ID	Headline
CSCvn62787	To support multiple retry on devcmd failure to CRUZ during flow table configuration update.
CSCvn63549	Python pop3lib apop() Method Denial of Service Vulnerability
CSCvn64418	ISA3000 interop issue with Nokia 7705 router
CSCvn65575	Snort termination can occur when active authentication is enabled and an SSL policy is not enabled
CSCvn68145	Snort Unexpectedly Exiting when using SSL decryption
CSCvn69213	ASA traceback and reload due to multiple threads waiting for the same lock - watchdog
CSCvn76763	Two versions of messages-X-SNAPSHOT.jar in FTD causes deployment failure
CSCvn77636	ASA/webvpn: FF and Chrome: Bookmark is not rendered with Grammar Based Parser
CSCvn93499	Snort/Data Correlator can crash while exiting on Firepower 4100/9300 devices.

Resolved Bugs in Version 6.2.3.9

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

Table last updated: 2019-01-10

Table 59: Resolved Bugs in Version 6.2.3.9

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

Resolved Bugs in Version 6.2.3.8

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

Table last updated: 2019-01-02

Table 60: Resolved Bugs in Version 6.2.3.8

Bug ID	Headline
CSCuy90400	Enhancement to support extended master secret in SSL
CSCvd03903	Firepower is affected by TCP Dump Vulnerability
CSCvd12834	FP Audit Logs do not log passed and failed SSH authentication attempts
CSCve29930	Cannot configure LOM on secondary FMC from HA pair
CSCvf20266	Firepower Management Center System Configuration Email Notification Password Length Too Short
CSCvf57596	After policy deploy has failed, ActionQueueScrape process did not exit
CSCvg10718	Correlation Policy With Traffic Profiles Doesn't Work
CSCvg36254	FTD Diagnostic Interface does Proxy ARP for br1 management subnet
CSCvh13022	SSL decryption is bypassed when client hello payload is < 6 bytes
CSCvh14743	IKEv2 MOBIKE session with Strongswan/3rd party client fails due to DPD with NAT detection payload.
CSCvi82404	Updating device can fail in 800_post/755_reapply_sensor_policy.pl
CSCvj67258	Change 2-tuple and 4-tuple hash table to lockless
CSCvj97213	ASA IKEv2 capture type isakmp is saving corrupted packets or is missing packets
CSCvk20292	FMC in HA mode, Health Policy is missing from Standby FMC when Active FMC failed
CSCvk30775	ENH: Addition of 'show fragment' to 'show tech' output
CSCvk30779	ENH: Addition of 'show ipv6 interface' to 'show tech' output
CSCvk30783	ENH: Addition of 'show aaa-server' to 'show tech' output
CSCvk33923	High disk usage after deleting managed FTD device from FMC
CSCvk51181	FTD IPV6 traffic outage after interface edit and deployment part 1/2
CSCvk62871	Firepower 2100 FTP Client in passive mode is not able to establish data channel with the Server
CSCvk72192	"Free memory" in "show memory" output is wrong as it includes memory utilisation due to overhead
CSCvm10968	CVE-2018-5391 Remote denial of service via improper IP fragment handling
CSCvm43975	Cisco ASA and FTD Denial of Service or High CPU due to SIP inspection Vulnerability

Bug ID	Headline
CSCvm47713	SSL policy disallows viewing of PDF on *.lightning.force.com when Chrome browser is used
CSCvm49283	Make Object Group Search Threshold disabled by default, and configurable. Causes outages.
CSCvm53531	Cisco Adaptive Security Appliance Software Privilege Escalation Vulnerability
CSCvm56371	ASA wrongly removes dACL for all Anyconnect clients which has the same dACL attached
CSCvm56719	Traceback high availability standby unit Thread Name: vpnfol_thread_msg
CSCvm60361	SSH public key auth not working on FTD on 5500
CSCvm62708	SSL connections negotiating NPN can fail with Do Not Decrypt SSL policy
CSCvm64230	verify_firmwareRunning() return code not checked
CSCvm65725	ASA kerberos auth fails switch to TCP if server has response too big (ERR_RESPONSE_TOO_BIG)
CSCvm67704	Memory Leak when handling KRB_ERR_RESPONSE_TOO_BIG (leak in krb5_extract_ticket)
CSCvm76760	FMC - External RADIUS authentication - Text in the "Shell Access Filter" field is not validated
CSCvm78449	Unable to modify access control license entry with log default command
CSCvm80933	ssl policy can match incorrect rule when server uses a cert with wildcard common name
CSCvm81052	local malware detection updates not downloading to FMC due to invalid certificate chain
CSCvm82966	Linux Kernel 3.10.107 Vulnerabilities
CSCvm91280	Intrusion Events Report Date, Hour Of Day, Day Of Week comes in UTC and Time comes in local timezone
CSCvm95669	ASA 5506 %Error copying http://x.x.x.x/asasfr-5500x-boot-6.2.3-4.img(No space left on device)
CSCvn03507	"set ip next-hop verify-availability" is removed from route-maps configuration with next deployment
CSCvn03966	FTD - When "object-group-search" is pushed through flexconfig, all ACLs get deleted causing outage.
CSCvn08146	Missing audit detail for changes to x509 certificates and keys

Bug ID	Headline
CSCvn09640	FTD: Need ability to trust ethertype ACLs from the parser. Need to allow BPDU to pass through
CSCvn09808	Captive portal bltd process fails on startup due to socket permission error
CSCvn11219	Policy deployment failed with error message "Not a directory"
CSCvn31753	ssl inspection policy may cause SEC_ERROR_REUSED_ISSUER_AND_SERIAL browser error

Resolved Bugs in Version 6.2.3.7

Table last updated: 2018-11-15

Table 61: Resolved Bugs in Version 6.2.3.7

Bug ID	Headline
CSCve34221	Internal server error seen on the UI when we enable CC mode
CSCvf54682	sudo : CVE-2017-1000368 : Sudo Parsed tty Information Privilege Escalation Vulnerability
CSCvh14743	IKEv2 MOBIKE session with Strongswan/3rd party client fails due to DPD with NAT detection payload.
CSCvi97500	AMP Cloud event on Firepower Management Center are seen with different file types
CSCvj14631	Appliance Information Widget shows IPv4 Address disabled if mgmt interface is not eth0
CSCvj58342	Multicast dropped after deleting a security context
CSCvj65064	Firepower 2100: Port-Channel down notification delayed
CSCvj67258	Change 2-tuple and 4-tuple hash table to lockless
CSCvj76858	Policy deployment take long time ~4 hours
CSCvj91795	SSL default policy action is taken when URL category lookup is pending
CSCvj97213	ASA IKEv2 capture type isakmp is saving corrupted packets or is missing packets
CSCvj98662	linux hotfix layer directory reorganisation
CSCvk18330	Active FTP Data transfers fail with FTP inspection and NAT
CSCvk30779	ENH: Addition of `show ipv6 interface` to `show tech` output
CSCvk31035	KVM (FTD): Mapping web server through outside not working consistent with other platforms

Bug ID	Headline
CSCvk33023	Policy deployment failure on Firepower module in cluster or failover
CSCvk48389	[`Error: Timed out communicating with DME`] when attempting to upgrade
CSCvk56513	Tor not blocked when traffic is passed through proxy.
CSCvk59260	On slower networks deployement may fail with **Resource temporarily unavailable** exception
CSCvk66529	FTD on FPR 9300 corrupts TCP headers with pre-filter enabled
CSCvk66771	The CPU profiler stops running without having hit the threshold and without collecting any samples.
CSCvk72192	show memory output shows wrong memory
CSCvk76146	Few devices /ngfw partition on 41xx shows 39GB whereas other shows 100 GB
CSCvm03931	software update downloads by Firepower failing due to newer CA certificates not being present
CSCvm04237	BusyBox `huft_build` Function Denial of Service Vulnerability
CSCvm05464	CVE-2018-5391 Remote denial of service via improper IP fragment handling
CSCvm08500	ASA cmd validation fails when deletion of NAT rule description includes Czech/Slovak characters
CSCvm09040	Resumption attempts for sessions using tickets and known-key action use full handshake
CSCvm19948	ssl connections without SNI could hit incorrect ssl rule
CSCvm32256	Slave unit fails to join FTD cluster when it is in disabled state
CSCvm32613	Format of syslog messages have changed after an update FMC 6.2.3.3 to 6.2.3.4
CSCvm43975	Cisco ASA and FTD Denial of Service or High CPU due to SIP inspection Vulnerability
CSCvm47595	FMC displays connections matching incorrect access control policy when not using SSL Policy
CSCvm49283	Make Object Group Search Threshold disabled by default, and configurable. Causes outages.
CSCvm51395	access control policy deploy fails in fwrulechecker due to memory limit
CSCvm56371	ASA wrongly removes dACL for all Anyconnect clients which has the same dACL attached
CSCvm56719	Traceback high availability standby unit Thread Name: `vpnfol_thread_msg`
CSCvm56851	eStreamer repeatedly exits after error deserializing File event or FireAMP event
CSCvm58672	Unable to deploy SSL policy while SSL Hardware offload feature is enabled

Bug ID	Headline
CSCvm60468	Linux Kernel `yurex_read` Privilege Escalation Vulnerability
CSCvm60548	Security Intelligence synchronization tasks fail
CSCvm60791	Linux Kernel `alarm_timer_nsleep()` Function Integer Overflow Vulnerab ...
CSCvm64255	SFNotificationd fails to stop
CSCvm65725	ASA kerberos auth fails switch to TCP if server has response too big `(ERR_RESPONSE_TOO_BIG)`
CSCvm67184	Audit Syslog messages are sent without User information
CSCvm67316	ASA: Add additional IKEv2/IPSec debugging for CSCvm70848
CSCvm67704	Memory Leak when handling `KRB_ERR_RESPONSE_TOO_BIG (leak in krb5_extract_ticket )`
CSCvm68467	Event alerting process CPU usage delays deployment on busy Firepower 2100
CSCvm71378	Policy Deployment failing due to NAT Rule
CSCvm78449	Unable to modify access control license entry with log default command
CSCvm80874	ASAv/FP2100 Smart Licensing - Unable to register/renew license
CSCvm82492	Snort process taking a long time to exit impacting traffic.
CSCvm82930	FTD: SSH to ASA Data interface fails if overlapping NAT statement is configured
CSCvm96634	Final stage of policy deployment is audit-logged under **admin** instead of current user
CSCvm96916	FMC is randomly sending **strong-encryption-disable** to ASA

Resolved Bugs in Version 6.2.3.6

Table last updated: 2018-10-10

Table 62: Resolved Bugs in Version 6.2.3.6

Bug ID	Headline
CSCux69220	WebVPN 'enable intf' with DHCP , CLI missing when ASA boot
CSCve95403	ASA boot loop caused by logs sent after FIPS boot test
CSCvf85831	asdm displays error uploading image
CSCvh16414	Health Monitoring can incorrectly show CPU on FTD as 100% or 150%
CSCvh69117	SFDataCorrelator log spam "Received an unknown event type"

Bug ID	Headline
CSCvh98781	ASA/FTD Deployment ERROR 'Management interface is not allowed as Data is in use by this instance'
CSCvi13054	scheduled rule recommendations update fails with "Attempted to store stale object"
CSCvi48170	ASA 9.4.4.8, SNMP causing slow memory leak
CSCvi71761	FTD cli prompt is stuck on Firepower 9300
CSCvi77340	race condition results in user id REST API not functioning
CSCvi90633	Edit GUI language on ASDM AC downloads but ignores the change FPR-21XX
CSCvi98909	RTP packets not matching the rule in AC policy
CSCvj42269	ASA 9.8.2 Receiving syslog 321006 reporting System Memory as 101%
CSCvj44032	snort premature connection closure during TCP 4-way teardown
CSCvj47256	ASA SIP and Skinny sessions drop, when two subsequent failovers take place
CSCvj67776	clear crypto ipsec ikev2 commands not replicated to standby
CSCvj72309	FTD does not send Marker for End-of-RIB after a BGP Graceful Restart
CSCvk04592	Flows get stuck in lina conn table in half-closed state
CSCvk12076	AnyConnect client profile doesn't show under group-policy not assigned under a connection profile.
CSCvk14768	ASA traceback with Thread Name: DATAPATH-1-2325
CSCvk23483	Elastic timeout not taking effect and enforcing 600 sec timeout
CSCvk24297	IKEv2 RA with EAP fails due to Windows 10 version 1803 IKEv2 fragmentation feature enabled.
CSCvk34648	Firepower 2100 tunnel flap at data rekey with high throughput Lan-to-Lan VPN traffic
CSCvk36087	When logging into the ASA via ASDM, syslog 611101 shows IP as 0.0.0.0 as remote IP
CSCvk36733	mac address is flapping on huasan switch when asa etherchannel is configued with active mode
CSCvk38176	Traceback and reload due to GTP inspection and Failover
CSCvk42473	QoS rule evaluation does not re-evaluate flows when applications change
CSCvk43865	Traceback: ASA 9.8.2.28 while doing mutex lock
CSCvk52667	FDM - Deployment is failing after latest SRU update in 6.2.3-83 build.
CSCvk62896	ASA IKEv2 crash while deleting SAs

Bug ID	Headline
CSCvk66722	Configuring DHCP option 'false' causes DHCP configuration to be not visible from GUI
CSCvk67239	ASA traceback and reload in "Thread Name: Logger Page fault: Address not mapped"
CSCvk68772	FMC UI not accessible if you enable client certificate and then upgrade
CSCvk68809	No soft link for ca-cert.pem file if you upgrade FMC from 5.4.0
CSCvk70676	Clientless webvpn fails when ASA sends HTTP as a message-body
CSCvk72652	FMC does not deploy 'crypto ikev1 am-disable' when aggressive mode is to be disabled
CSCvk74461	LDAP groups download but are not available in GUI
CSCvk76160	Unable to restore on KP 6.2.2.2 using FDM
CSCvk76547	IPS rule with flow established not blocking when retransmitted TCP handshake packets
CSCvm01396	Firepower block page not displayed on browser with proxy settings
CSCvm05821	Sensitive Data Detection being enabled automatically during SRU update
CSCvm07458	Using EEM to track VPN connection events may cause traceback and reload
CSCvm07643	FTD 6.2-Intrusion Events not displaying src and dst port
CSCvm09624	Protocol not updated based on AppID when enforcing IPS rules
CSCvm11389	Small percentage of ECDHE connections fail
CSCvm11714	EIGRP authentication key issue when using special character "&"
CSCvm15880	FPR 9k ASA cluster multicon mode/vpn-mode distribute causes a reboot-loop if transparent mode conf
CSCvm19585	Smart License getting deregistered after upgrade to 6.2.3.5.
CSCvm23370	ASA: Memory leak due to PC cssls_get_crypto_ctxt
CSCvm25972	ASA Traceback: Thread Name NIC Status Poll.
CSCvm26004	Incorrect calculation of AAB in ASA causes random AAB invocations.
CSCvm29973	False positive for DNS SI events!
CSCvm44905	ssl inspection may continue processing a flow without flow information
CSCvm56019	Cisco Adaptive Security Appliance WebVPN - VPN not connecting through Browser

Resolved Bugs in Version 6.2.3.5

Table last updated: 2018-09-12

Table 63: Resolved Bugs in Version 6.2.3.5

Bug ID	Headline
CSCvb19750	Cisco Firepower Management Center Cross-Site Request Forgery Vulnerability
CSCve39071	Option to disable attempts to connect to the ThreatGRID cloud
CSCve85565	Traceback when syslog sent over VPN tunnel
CSCvg33300	Unable to modify Integer Host Attributes after creating them
CSCvg51412	Unable to establish a estreamer sftunnel between managed device and estreamer client
CSCvg54724	Firepower Dynamic Analysis Association Only Redirects to US address
CSCvg75144	All apps matching the filter deletes all objects
CSCvg91631	URL Reputation shows high risk or Unknown in Encore
CSCvg94363	Prefix List "le 32" does not work on Firepower Threat Defense
CSCvh21219	"set ip next-hop verify-availability" is removed from PBR configuration with next deployment
CSCvh89017	Configure user add command does not accept numeric user
CSCvi01312	webvpn: multiple rendering issues on Confluence and Jira applications
CSCvi31540	Traceback and reload with 'show tech' on ASA with No Payload Encryption (NPE)
CSCvi34164	ASA does not send 104001 and 104002 messages to TCP/UDP syslog
CSCvi37644	PKI:- ASA fails to process CRL's with error "Add CA req to pool failed. Pool full."
CSCvi45989	Query Cisco CSI for Unknown URLs option being reset by ASA managed by ASDM (Regression)
CSCvi51370	race condition can result in syslog alerts without rule messages
CSCvi53708	ASA NAT position discrepancy between CLI and REST-API causing REST to delete wrong config
CSCvi69343	ids_event_processor leaks memory when resetting communications
CSCvi69356	SFDataCorrelator reports "Invalid column value name" error-eStreamer does not work on managed device
CSCvi76808	File detection failing for encrypted SMTP TLS with Decrypt - Known Key SSL rule action
CSCvi79691	LDAP over SSL crypto engine error

Bug ID	Headline
CSCvi79999	256 Byte block leak observed due to ARP traffic when using VTI
CSCvi85382	ASA5515 Low DMA memory when ASA-IC-6GE-SFP-A module is installed
CSCvi93500	snort's handling of x-forward-for-like headers is incorrect when there are multiple proxies
CSCvi94239	IDSEventAlerter log spam "Unable to get SSL certificate fingerprint"
CSCvi96442	Slave unit drops UDP/500 and IPSec packets for S2S instead of redirecting to Master
CSCvi97894	Several hardware rules are truncated when running capture traffic.
CSCvi98424	IDSEventAlerter and IDSEventProcessor stop working and spam logs after file read error
CSCvi99743	Standby traceback in Thread "Logger" after executing "failover active" with telnet access
CSCvj07038	Firepower devices need to trust Threat Grid certificate
CSCvj11442	Firepower Threat Defense: BGP order of deployment operation of neighbor causes failure
CSCvj19835	Decrypted connections using ECDHE-RSA-RC4-SHA cipher fail in the application data phase
CSCvj38002	SNMPv3 user engineID mismatch with Active engineID causes 'user not found' error on SNMP request
CSCvj44517	List of trusted CAs in SSL policy duplicates
CSCvj49452	sftunnel using weak SSL/TLS versions and ciphers
CSCvj54840	create/delete context stress test causes traceback in nameif_install_arp_punt_service
CSCvj65581	Excessive logging from ftdrpcd process on 2100 series appliances
CSCvj67504	Deploy of policy fails when adding users/groups to the ssl policy
CSCvj67740	Static IPv6 route prefix will be removed from the ASA configuration
CSCvj75793	2100/4100/9300: stopping/pausing capture from Management Center doesn't lower the CPU usage
CSCvj85516	Packet capture fails for interface named "management" on Firepower Threat Defense
CSCvj88514	IP Local pools configured with the same name.
CSCvj91449	ASA traceback when logging host command is enable for IPv6 after each reboot
CSCvj92040	TLS client offers some ciphersuites in CC mode that are not allowed by CC
CSCvj95451	webvpn-l7-rewriter: Bookmark logout fails on IE

Bug ID	Headline
CSCvj96173	After upgrading to 6.2.3, FMC still generates sha1 certificate for eStreamer clients
CSCvj97326	Unable to create SSL policy on Firepower Services
CSCvj98964	ASA may traceback due to SCTP traffic
CSCvk01577	Pigtail from CLISH mode in FTD 6.2.3 not allowed
CSCvk01981	users shows up as unknown after user purge
CSCvk06249	SFDataCorrelator alerting can cause deadlock restart when si_uuid not in firewall_rule_cache
CSCvk06336	FMC displays connections matching incorrect access control policy rules packet count is zero
CSCvk06368	Evaluation of FMC kernel vulnerabilities
CSCvk08377	ASA 5525 running 9.8.2.20 memory exhaustion.
CSCvk10252	SI Category may be incorrect for alerts or eStreamer; also performance and memory problems
CSCvk11898	GTP soft traceback seen while processing v2 handoff
CSCvk14910	SFDataCorrelator keeps exiting when processing FireAMP event without agent uuid
CSCvk16568	AppID stop processing traffic if Application ID has been detected
CSCvk17382	Snort exiting unexpectedly while processing rule evaluation.
CSCvk18378	ASA Traceback and reload when executing show process (rip: inet_ntop6)
CSCvk18578	Enabling compression necessary to load ASA SSLVPN login page customization
CSCvk18846	Firepower Management Center WebUI performance degraded due to sfdccsm logging level.
CSCvk19435	Unwanted IE present error when parsing GTP APN Restriction
CSCvk26887	Certificate import from Local CA fails due to invalid Content-Encoding
CSCvk27686	ASA may traceback and reload when acessing qos metrics via ASDM/Telnet/SSH
CSCvk28023	WebVPN: Grammar Based Parser fails to handle META tags
CSCvk30212	FMC negates BGPv6 commands and generates again if neighbor IPv6 address contains leading 0 in group
CSCvk30665	ASA "snmp-server enable traps memory-threshold" hogs CPU resulting in "no buffer" drops
CSCvk33947	Sensitive Data Threshold Configuration is incorrect

Bug ID	Headline
CSCvk35323	With Objects having override configured, copy config was not happening
CSCvk35761	Sensitive Data is not working as expected when processing multiple patterns in a single session.
CSCvk37890	Firepower 2110, Webvpn conditional debugging causes Threat Defense to traceback
CSCvk40332	UDP traffic without zone information will match incorrect AC rule
CSCvk49527	Add application level timeout for switchprimarynode API call
CSCvk50364	NGIPSV "system support capture-traffic" not working for inline-sets
CSCvk50732	AnyConnect 4.6 Web-deploy fails on MAC using Safari 11.1.x browsers
CSCvk52305	Snort process terminated with segfault in daq
CSCvk54078	Firepower Threat Defense high availability Creation with VPN configuration fails
CSCvk54491	Race condition processing Reputation causes Snort process to exit.
CSCvk54779	Async queue issues with fragmented packets leading to block depletion 9344
CSCvk55355	User/group download fails is at least one user belongs to two groups with same common name
CSCvk57516	Firepower Threat Defense: Low DMA memory leading to VPN failures due to incorrect crypto maps
CSCvk58188	Snort configuration validation failed due to Value specified for max_sessions is out of bounds
CSCvk66012	Policy deployment fails if a member of a cluster is shutdown/Disabled on the FMC
CSCvk71511	SFDataCorrelator event backlog grows when event storage is large and device count is high
CSCvk72602	Incorrect TCP checksum causes snort retries
CSCvk73990	Change Reconciliation report: simplify the rule deletion event
CSCvm01497	Scheduled reports not stored in correct domain when using another domain's report template
CSCvm06114	RDP bookmark plugin won't launch
CSCvm16686	Threat Defense interfaces goes down during high availability creation using redundant interface

Resolved Bugs in Version 6.2.3.4

Table last updated: 2018-08-13

Table 64: Resolved Bugs in Version 6.2.3.4

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

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

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

Resolved Bugs in Version 6.2.3.3

Table last updated: 2018-07-11

Table 65: Resolved Bugs in Version 6.2.3.3

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

Bug ID	Headline
CSCvi15830	wrong configurations on Threat Defense device when network group object is used on identity policy
CSCvi16024	SSL errors on session resume when server IP address changes
CSCvi19220	ASA fails to encrypt after performing IPv6 to IPv4 NAT translation
CSCvi36434	Cisco Firepower System Software SSL Denial of Service Vulnerability
CSCvi37374	SSL connections fail to complete when passing through a single inline set multiple times
CSCvi38151	ASA pair: IPv6 static/connected routes are not sync/replicated between Active/Standby pairs.
CSCvi42008	Stuck uauth entry rejects AnyConnect user connections
CSCvi51515	REST-API:`500 Internal Server Error`
CSCvi53420	User/Group Download fails when same user is part of multiple groups with comma (,) in common name
CSCvi58032	Management Center Internal Error creates an Auto-NAT rule which causes a policy deployment failure
CSCvi58183	Custom SI feed update in Firepower Management Center is not propagated to managed devices
CSCvi59000	SecGW - Data Loss during ASR
CSCvi59148	Sessions can remain active on managed device if they are from same IP address but different realms
CSCvi62671	users/groups download takes long time in 6.2.2.1 with high number of user/group mappings
CSCvi63968	`Internal Error is preventing Policy Validation` Cannot save access control policy.
CSCvi70606	ASA 9.6(4): WebVPN page not loading correctly
CSCvi73414	Unable to delete User Indication of Compromise if user info is inconsistent between mysql and sybase
CSCvi80928	HW Mode - SSL errors may occur when resumed sessions are not decrypted
CSCvi89194	pki handles: increase and fail to decrement
CSCvi97479	Snort restart while deploying access control policy changes
CSCvi97721	The memcap for Security Intelligence URL feeds needs to be increased for devices 4GB total memory

Bug ID	Headline
CSCvi98251	SMTP: Could not allocate SMTP mempool causing Policy Apply Failure and Snort Outage
CSCvj00918	(1 of 2) high memory usage of `user_id/user_group` broadcast in SFDataCorrelator(on sensor)
CSCvj06418	Custom SI DNS feed not synced to secondary Firepower Management Center
CSCvj09571	Firepower Management Center UI slow when managing large number of device with classic licenses
CSCvj10011	Management Center: IGMP gets enabled on interfaces which it has been configured but not enabled
CSCvj17609	synchronization failed (Cannot open file) entries in action queue when file is empty
CSCvj22491	Cluster: Enhance ifc monitor debounce-time for interface down->up scenario
CSCvj24036	Messaging on Firepower Management Center UI informing of ports required by RAVPN
CSCvj25386	Missing default Identity realm EOs causing upgrade failure
CSCvj25817	ASA responds to MOBIKE but clears SA due to DPD.
CSCvj26819	modifying `ssl_debug` settings requires a detection engine restart
CSCvj32264	ASA - zonelabs-integrity : Traceback and High CPU due to `Process Integrity FW task`
CSCvj33202	Cannot save Intrusion Policy with Firepower recommendations and shared policy layers
CSCvj37448	ASA : Device sends only ID certificate in SSL server certificate packet after reload
CSCvj37858	performance impact from `action_queue` queries
CSCvj37924	CWE-20: Improper Input Validation
CSCvj39858	Traceback: Thread Name: IPsec message handler
CSCvj40636	S2S VPN support for Firepower Threat Defense Cluster for the classic centralized VPN clustering
CSCvj42450	ASA traceback in Thread Name: DATAPATH-14-17303
CSCvj42680	Slowness due to frequent device registration queries on Firepower Management Center pair
CSCvj44262	portal-access-rule changing from **deny** to **permit**
CSCvj45594	SFDataCorrelator core when timing-out old host info on a slow Firepower Management Center

Bug ID	Headline
CSCvj46777	Firepower Threat Defense 2100 asa traceback for unknown reason
CSCvj48168	The `show memory` command returns low used memory numbers
CSCvj48340	ASA memory Leak - snp_svc_insert_dtls_session
CSCvj48931	Firepower recommendation updates task never runs
CSCvj49883	ASA traceback on Firepower Threat Defense 2130-ASA-K9
CSCvj50024	ASA portchannel lacp max-bundle 1 hot-sby port not coming up after link failure
CSCvj56008	Scansafe feature doesn't work at all for HTTPS traffic
CSCvj56909	ASA does not unrandomize the SLE and SRE values for SACK packet generated by ASA module
CSCvj56963	Management Center error about `Only 8 equal cost routes are allowed` when adding the fifth route
CSCvj61367	fast reuse of source port can break ssl inspection
CSCvj67132	Policy deploy failure due to bgp neighbor CLI in wrong order
CSCvj73581	Traceback in `cli_xml_server` Thread
CSCvj74210	Traceback at **ssh** when executing `show service-policy inspect gtp pdp-context detail`
CSCvj79765	Netflow configuration on Active ASA is replicated in upside down order on Standby unit
CSCvj81287	Firepower Threat Defense rejecting syslog server TLS-X509 certificate due to EKU invalid purpose
CSCvj83316	Snort process exits while clearing XFF data.
CSCvj91619	1550 Block Depletions leading to ASA reload.
CSCvj97157	WebPage is not loading due to client rewriter issue on JS files
CSCvk00579	Slowness in the device list getting populated under the Deploy tab
CSCvk06176	SSEConnector is not coming up because of Wrong Executable
CSCvk07522	webvpn: Bookmark fails to render on Firefox and Chrome. IE fine.

Resolved Bugs in Version 6.2.3.2

Table last updated: 2018-06-06

Table 66: Resolved Bugs in Version 6.2.3.2

Bug ID	Headline
CSCuv68725	ASA unable to remove ACE with **log disable** option
CSCvd13182	AVT : Missing X-Content-Type-Options in ASA 9.5.2
CSCvd44525	ASA **show tech** some commands twice, show running-config/ak47 detailed/startup-config errors
CSCve94917	Stale VPN Context issue seen in 9.1 code despite fix for CSCvb29688
CSCvf18160	ASA traceback on failover sync with WebVPN and shared storage-url config
CSCvf39539	Netflow Returns Large Values for Bytes Sent/Received and IP address switch
CSCvf40179	ERROR: Unable to create crypto map: limit reached, when adding entry
CSCvf82832	ASA : ICMPv6 syslog messages after upgrade to 962.
CSCvf96773	Standby ASA has high CPU usage due to extremely large PAT pool range
CSCvg05442	ASA traceback due to deadlock between DATAPATH and webvpn processes
CSCvg43389	ASA traceback due to 1550 block exhaustion.
CSCvg72879	9.9.1/SecGW: Firepower 4100 w/ subsecond failover may have 10-20% packet loss for few mins
CSCvh14743	IKEv2 MOBIKE session with Strongswan/3rd party client fails due to DPD with NAT detection payload.
CSCvh23531	ASA TLS client connection fails with software DHE
CSCvh30261	ASA watchdog traceback during context modification/configuration sync
CSCvh47057	ASA - ICMP flow drops with `no-adjacency` on interface configured in zone when inspection enabled
CSCvh65500	Firepower 2100 Client in FTP active mode is not able to establish control channel with the Server
CSCvh81142	Snort Core Generated while running 6.2.3
CSCvh83934	Memory usage of User-ID component of SNORT exceeds the reserved limit of 10M
CSCvh91053	ASA sending DHCP decline | not assiging address to AC clients via DHCP
CSCvh91399	upgrade of ASA5500 series firewalls results in boot loop (not able to get past ROMMON)

Bug ID	Headline
CSCvh92381	ASA Traceback and goes to boot loop on 9.6.3.1
CSCvi01376	Upon reboot, non-default SSL commands are removed from the Firepower 4100
CSCvi07636	ASA: Traceback in Thread Name UserFromCert
CSCvi08450	CWS redirection on ASA doesn't treat SSL Client Hello retransmission properly in specific condition
CSCvi09305	Some SSL connections slow or fail under a **Do-Not-Decrypt** SSL policy action
CSCvi16264	ASA traceback and reload due to watchdog timeout when DATAPATH accesses compiling ACL structure
CSCvi19263	ASA 9.7.1.15 Traceback while releasing a vpn context spin lock
CSCvi22507	IKEv1 RRI : With Answer-only Reverse Route gets deleted during Phase 1 rekey
CSCvi23615	Sourcefire.agent_messages table becoming large preventing the agent messages from being consumed
CSCvi33962	WebVPN rewriter: drop down menu doesn't work in BMC Remedy
CSCvi35805	ASA Cut-Through Proxy allowing user to access website, but displaying `authentication failed`
CSCvi42965	ASA does not report accurate free memory under `show memory` output
CSCvi45567	Not able to do snmpwalk when snmpv1&2c host group configured.
CSCvi47847	Shell application not pin-holing for new tcp port for data transfer as expected
CSCvi48523	Not able to create SLA Monitor from static route page
CSCvi49383	Azure: ASAv running Cloud high availability gets in a watchdog crash loop
CSCvi55070	IKEv1 RRI : With Originate-only Reverse Route gets deleted during Phase 1 rekey
CSCvi57808	Continuously sfdatacorrelator process terminated unexpectedly
CSCvi58089	Memory leak on webvpn
CSCvi58865	SSL policy with URL category rules specifying decryption can cause browser errors
CSCvi63864	With SSL inspection in hardware mode and Malware protection, secure file transfers occasionally fail
CSCvi63888	SSL errors might occur when resumed sessions are not decrypted
CSCvi64007	Zeroize RSA key after Failover causes REST API to fail to changeto System context
CSCvi66905	PIM Auto-RP packets are dropped after cluster master switchover
CSCvi70680	Same groups from different AD not downloaded

Bug ID	Headline
CSCvi71039	Firepower Management Center: Change Reconciliation reports are failing intermittently
CSCvi76577	ASA:netsnmp:Snmpwalk is failed on some group of IPs of a host-group.
CSCvi77352	Illegal update occurs when device removes itself from the cluster
CSCvi82779	ASA generate traceback in DATAPATH thread
CSCvi84315	Unexpected failures on Firepower 2100 Series devices
CSCvi86799	ASA traceback during output of `show service-policy` with a high number of interfaces and qos
CSCvi87921	ASA self-signed RSA certificate is not allowed for TLS in FIPS mode
CSCvi95544	ASA not matching IPv6 traffic correctly in ACL with **any** keyword configured
CSCvj05140	Object description is not deployed with associated network object.
CSCvj07038	Firepower devices need to trust Threat Grid certificate
CSCvj07571	`Error 500` when saving some correlation policy rules
CSCvj07843	eStreamer using 100% CPU, event processing slows when File/FireAMP events enabled
CSCvj22491	Cluster: Enhance ifc monitor debounce-time for interface down->up scenario
CSCvj26450	ASA PKI OCSP failing - CRYPTO_PKI: failed to decode OCSP response data.
CSCvj47633	Non-SSL traffic causing SSL inspection to fail
CSCvj56008	Scansafe feature doesn't work at all for HTTPS traffic
CSCvj63196	Workaround for Sybase issue: After snort engine update, policy deployment fail abruptly

Resolved Bugs in Version 6.2.3.1

Table last updated: 2018-05-02

Table 67: Resolved Bugs in Version 6.2.3.1

Bug ID	Headline
CSCvf97979	NAT policy deployment failed during generating delta config after changing security zone in rule.
CSCvg00565	ASA crashes in `glib/g_slice` when do **debug menu** self testing
CSCvg36672	Need a way to prioritize user driven deployment tasks in Action Queue

Bug ID	Headline
CSCvg65072	Cisco ASA sw, FTD sw, and AnyConnect Secure Mobility Client SAML Auth Session Fixation Vulnerability
CSCvg78418	Evaluation of FireSIGHT / FirePOWER for Apache/Struts related vulnerabilities
CSCvg84495	Remote access VPN using an OpenLDAP realm/server doesn't use the correct naming attribute
CSCvh05081	ASA does not unrandomize the SLE and SRE values for SACK packet generated by ASA module
CSCvh22181	Failures loading websites, such as mail sites, using TLS 1.3 with SSL inspection enabled
CSCvh25433	New CLI for Supporting Legacy method SAML Auth using external browser on Endpoint with AC
CSCvh46202	Slow 2048 byte block leak due to fragmented traffic over VPN
CSCvh53616	ASA on Firepower Threat Defense devices traceback due to SSL
CSCvh63903	Failover of IPv6 addresses on 8000 series pair devices may not succeed
CSCvh79732	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh81474	Need to catch malformed JSON to allow rendering of **Deploy** button and notifications
CSCvh81737	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh81870	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh83012	SFDataCorrelator should not limit rate of duplicate flows
CSCvh99414	NFE failure causes Snort to constantly restart
CSCvi03546	User-IP mapping not updated on managed device due to error in updating current map
CSCvi18602	FSIC failed while downgrade ASA FirePOWER module (5585-x) from 6.2.2.2 to 6.2.2.1
CSCvi34137	With SSL decryption enabled and TCP Segmented HTTP requests, Snort does not capture URI correctly
CSCvi44365	After an upgrade the Firepower 4100 hostname is different than SFCLI hostname
CSCvi49752	`sfipproxy` may not be written correctly on a sensor when registered to a high availability pair
CSCvi55280	Deployment transcript does not indicate failed command if error is in last CLI of delta
CSCvi80849	Cisco Firepower 2100 Series POODLE TLS security scanner alerts

Resolved Bugs in Version 6.2.3

Table last updated: 2020-04-21

Table 68: Resolved Bugs in Version 6.2.3

Bug ID	Headline
CSCuw57184	Not keep URL entries in cache forever.
CSCuw73747	DST for Europe/Istanbul time zone is now on a different date
CSCux17501	SSL inspection blocks traffic with decryption errors for sites with 3072 bit key RSA certificates
CSCux42313	Cisco ASA module captive portal redirect gets stuck
CSCux61395	UserIDs get lost if an error occurs while streaming to the sensor
CSCuy10223	ASA Security Zone cannot be used in Active Authentication identity rules
CSCuy18154	ADISubscriber shuts down before session receive in SFDataCorrelator
CSCuy21943	Firepower Threat Defense / Unable to deploy after restoring a backup
CSCuy56306	SCP Expect during backup to remote server times out and fails
CSCuy57310	Cisco Adaptive Security Appliance Traffic Flow Confidentiality Denial of Service Vulnerability
CSCuz09515	Active/Passive authentication does not work with predefined objects
CSCuz85967	New added management interface does not have "management-only" configuration
CSCuz92983	Policy deployment fails with mode 10 Gbit Full-Duplex for lag interface
CSCva21702	Traffic capture BPF validation
CSCva34909	DNS blacklist has an 81 character limit
CSCva36446	ASA Stops Accepting Anyconnect Sessions/Terminates Connections Right After Successful SSL handshake
CSCva44278	Policy apply fails due to orphaned database objects
CSCvb13949	Readiness Check option should NOT be enabled for VDB updates
CSCvb28202	False warnings in DB Integrity Check for PlatformSettings object
CSCvc03899	Firepower Threat Defense managed by Management Center- High unmanaged disk usage on /ngfw
CSCvc37876	Policy deploy fails due to inconsistency in Primary Threat Defense device pair in the backend
CSCvc44535	Under rare circumstances captive portal is very slow and even unresponsive

Bug ID	Headline
CSCvc48180	Application categories and tags are missing in Version 6.1 or 6.2.1
CSCvc48768	Search Option does not work for network objects under NAP editor
CSCvc50598	Comparison reports for intrusion policy between two revisions is not working correctly
CSCvc55341	Intermittent error 500 when trying to review an event from the packet view
CSCvc56921	Altering logging settings like disabling syslog causes IPS and File policies to become disabled
CSCvc65909	ASDM:Importing access control policy leads to duplicate objects
CSCvc77913	Custom configuration for SFDataCorrelator should be checked on updates otherwise it may remain down
CSCvc84585	Firepower sensor will not ingest users from ISE using EAP chaining
CSCvc91092	Cisco FireSIGHT System Software Arbitrary Code Execution Vulnerability
CSCvc92934	When SSL decryption is enabled, URL constraints in access control policy are not applied correctly
CSCvd19749	Upgrade from 6.1.0 to 6.1.0.1 failed at 000_start/113_EO_integrity_check.pl
CSCvd28906	ASA traceback at first boot in 5506 due to unable to allocate enough LCMB memory
CSCvd29303	Disk status health monitoring should be disabled for virtual ASA 5500-X series
CSCvd32767	Unable to use objects inside IPS rules
CSCvd35049	Hard-coded query limit needed to prevent QueryEngine and Report Generation failures
CSCvd39729	Firepower Enterprise Objects Missing References Causes Multiple Problems
CSCvd51066	URL cloud lookup has URL category as Uncategorized
CSCvd59044	Access Control Policy does not match condition with URL SI lists for HTTPS traffic
CSCvd59268	possible to have data-interfaces + Firepower Management Center from cli_firstboot wizard
CSCvd61462	Partial match of DNS Queries if DNS Feed or DNS List contains single word entry
CSCvd72150	Deleted objects continue to show up as available to add to variable sets on the Management Center UI
CSCvd83845	SafeSearch-specific codes get hit even if SafeSearch rule is disabled in Firepower Management Center
CSCvd84471	Connections not blacklisted by Security Intelligence due to memory (memcap) issues
CSCvd91889	Unable to change logical name of interface and add sub-interface

Bug ID	Headline
CSCve00330	Document details on what synchronizes between Firepower Management Centers in High Availabilty
CSCve03600	SMTP traffic prematurely reaching SafeSearch engine rule.
CSCve11879	Ping traffic is dropped for 1 minute during high availability switchover
CSCve12096	Failure on deleting port object used in manual NAT rule
CSCve17433	Policy deployment failing on AWS Firepower Management Center
CSCve23827	Restore from backup fails when clock is behind on restore device
CSCve31929	Firepower Management Center does not show any network discovery data when using security zones
CSCve42340	URL Database Updates Use IP for Proxy Connection in HTTP Header
CSCve42379	SCALE : Avoid queueing Sync Sybase to MySQL task if similar PENDING task already there
CSCve42542	not allowed to choose Firepower Threat Defense as Secondary Peer during High Availability creation
CSCve45573	Internal error message while loading access control policy in Japanese environment
CSCve48087	Deploy policy tab failed to populate the device list from Firepower Management Center
CSCve49433	Threat Defence Platform Settings Policy does not check the NTP input value properly
CSCve49546	Policy apply failed at "FINALIZE" prevents future policy apply from succeeding
CSCve49643	User logins with double byte characters are not recorded on Firepower Management Center correctly
CSCve49722	Can't export if intrusion policy inherits intrusion layer from parent domain
CSCve49778	Threat Defense ICMP platform settings security zones with multiple interfaces not handled properly
CSCve55618	DNS policy generates DNS responses for already generated responses, if it is seen over the wire
CSCve56743	Firepower Threat Defense pair: Snort is dropping traffic inspite of having a trust rule.
CSCve57521	For NGFW rules processing, always use first packet of flow to determine initiator direction
CSCve57858	Sites with large certificate not loading with SSL policy turned on even with "Do not decrypt" action
CSCve60167	Upgrade framework needs to review onbox scripts NEVER_SKIP

Bug ID	Headline
CSCve61540	Cisco Adaptive Security Appliance Application Layer Protocol Inspection DoS Vulnerabilities
CSCve73129	DB query does not terminate when upgrade to 6.2.1 fails
CSCve77286	Intrusion policy rule filter is not working properly
CSCve79555	ASA/Threat Defense traceback when clearing capture-assertion "0" failed: mps_hash_table_debug.c file
CSCve84791	Capturing asp-drop causes unexpected ASA failure
CSCve87945	Cannot install new https certificate
CSCve88764	Don't restore Primary Firepower Management Center backup to secondary
CSCve90384	high availability break/Config Deployment fails on 2100 platforms when in secondary is Active
CSCve98443	User Identity count tracking may be incorrect
CSCve98877	Dashboard Drilldown Does Not Match Top Level Report
CSCve99511	Traceback and reload in thread name: sfr-vpn-status-watcher when unit takes active role
CSCve99818	Time window setting for Connection events gets reset to different range
CSCvf01839	vFMC getting logged out for "An unauthorized action has been detected" after some idle time
CSCvf04102	Error generating report preview for Vulnerabilities section
CSCvf06031	After adding a secondary Firepower Threat Defense to cluster, deploy can fail
CSCvf12392	Security Intelligence category may be incorrect in alert response from correlation policy
CSCvf12828	Device stuck at HA state progression failed due to App sync issue on QP FTD HA pair
CSCvf15067	Sync hostname to ASA when device is managed by Firepower Management Center/no manager
CSCvf18641	Connection events are not generated for unmonitored hosts in ND rules
CSCvf18966	Adding Port Group Object to Extended Access Control Entry causes ERROR: Invalid Protocol
CSCvf25032	FMC: Ownership of sydb.out changes to root and prevents vmsDbEngine/dbsrv16 to start
CSCvf25058	Firepower Threat Defense Security Intelligence DNS memcap exceeded health alert

Bug ID	Headline
CSCvf25444	Copying Realm and replacing users in SSL policy criteria corrupts policy
CSCvf27979	Unable to view access control policy with the error "End value is less than start value"
CSCvf34791	Install 6.2.2-1290 on an ASA with Firepower Services-- ASA fails unexpectedly.
CSCvf35266	Deployment failure if group policy is unassigned from connection profile and deleted in advanced tab
CSCvf41793	High memory usage of ids_event_processor/ids_event_alerter when threshold.conf file is not pruned
CSCvf42199	Core seen while running snort restart automated regression suite for more than 14 hours.
CSCvf45952	high availability progression failed for secondary when pair is rebooted due to App-sync failure
CSCvf46168	"no capture <name> stop" doesn't change capture status from Stopped
CSCvf46886	Security Analyst User Role not permitted to download file from malware event
CSCvf49737	Add state-checking options on H323 policy inspect map
CSCvf53734	access control rules and Categories duplication on Firepower Management Center UI
CSCvf55897	Disable Intrusion Policy controls on Default action in Access Policy Page
CSCvf56476	DNS Flexconfig removed after enabling LDAPS on Firepower 2120 device
CSCvf56533	Cannot re-register Firepower 9300 cluster to a different Firepower Management Center
CSCvf57862	Snort install silently fails and automatic deploy after Snort is installed is skipped
CSCvf60738	Elektra Registration failures due to RPC call failures
CSCvf61157	Firepower Management Center DB corruption name mismatch
CSCvf64643	ERROR on Firepower Threat Defense device: Captive-portal port not available. Try again
CSCvf64882	Deployment Failing on high availability pair due to Cluster Hold Request Timed Out by ASA
CSCvf64914	updates to local URL filtering database and/or cloud dispositions need to supersede cached data
CSCvf65014	Having custom "End Time" in "Intrusion Events" Analysis returns a blank page with no events
CSCvf65226	OSPF Redistribution command not getting deleted on Firepower Threat Defense device
CSCvf65245	Monitor rule does not log large sessions (such as file transfers)

Bug ID	Headline
CSCvf68502	Unable to assign FQDN for hostname in Certificate Signing Request
CSCvf71365	Log appropriate message if SFDataCorrelator exits during startup due to empty VDB tables
CSCvf73465	re-registration failed due to stale entry in ID_MAPPING table post device delete
CSCvf74023	Smart License registration failures when Proxy Authentication is configured on Management Center
CSCvf74113	Firepower Intrusion rule UI policy deploy fails when threshold seconds of rules set to 00, 08, 09
CSCvf75062	Deployment failed with 'ERROR: Trustpoint not enrolled'
CSCvf77836	FTD HA - both devices go into unknown state when HA break is performed
CSCvf78629	Custom Fingerprint GUI offers "Defense Center" instead of "Firepower Management Center" option
CSCvf81725	syncd uses high memory and exits when loading firewall_rule_cache table
CSCvf82315	IP address for 10G interfaces cannot be changed from GUI.
CSCvf91371	Invalid certificate error seen when internal CA is used for SSL Decrypt-Resign rule
CSCvf95633	Management Center: Interface "mac-address-table" command not sent to the Firepower Threat Defense
CSCvf98386	FDM pre-shared key changed to random value after upgrade
CSCvg02051	Large user/group tables due to duplicated entries when group names are not ASCII
CSCvg03671	FMC policy deployment slows down due to multiple failed attempts by Snort to load SI data
CSCvg04309	Micro-Engine failure due to TCAM leads to bb-heath not generating auto-troubleshoot.
CSCvg06811	Add captive_portal.log to logrotate.d
CSCvg09316	Cisco Firepower Threat Defense Software Policy Bypass Vulnerability
CSCvg20782	Identified Vulnerabilities associated with the CVEs from Oracle MySQL Patch Updates
CSCvg21939	Parts of Firepower Management Center GUI not loading in Firefox 56
CSCvg23945	ASA panic/crash spin_lock_fair_mode_enqueue: Lock (mps_shash_bucket_t) is held for a long time
CSCvg24416	FTW inline interfaces do not go into hardware bypass during Firepower 4100 Series
CSCvg24892	6.2.3 Snort configuration validation failed due to ERROR: SMTP: Could not allocate SMTP mempool.

Bug ID	Headline
CSCvg27431	Applying large access control policy fails on AWS - 6.2.2.1
CSCvg27511	Network Object - getting 'missing entry' while trying to delete an existing object
CSCvg27590	Daily Change reconciliation report lacks details and users on Firepower 6.2.2
CSCvg29442	When IPSec is enabled, high availability goes in Active-Failed state
CSCvg29791	FlexConfig - System variable should contain subinterface ID
CSCvg30947	more than one default route with same metric allows on Threat Defense device's routing table
CSCvg32590	6.1-6.2.3 upgrade: FTD upgrade failed with /ngfw/var/lib/mysql/sfsnort: not accessible error
CSCvg37391	Migrated access control policy deploy fails since it has FQDN objects
CSCvg37456	Deployment to high availability pair successful on active unit; standby unit will be updated message
CSCvg38612	Upgrade failure from 6.2.0 -> 6.2.3-10646 on FDM
CSCvg38789	Nested entities not deleted when deploying an object
CSCvg39981	Firepower Management Center not displaying Firepower Threat Defense cluster names correctly
CSCvg43759	URL filter matching fails - Two SSL Certificate CNs Concatenated
CSCvg45236	Lower-than-expected 256 byte block count with fast-path pre-filter SSL policy
CSCvg46466	Cisco FMC and Firepower System Software SF Tunnel Control Channel Command Execution Vulnerability
CSCvg47696	Not able to create RA VPN after removing DfltGrpPolicy
CSCvg48363	With verbose SSL logging enabled, logs can consume all available disk space
CSCvg50707	Firepower Threat Defense high availability policy deploy fails with Found more than one NGFW Policy
CSCvg52545	9300 pair NGFWs in inlineIPS mode do not trigger SNAP packet updates with proper VLAN tags
CSCvg58777	Multiple Vulnerabilities in Apache tomcat
CSCvg58825	Report generated from access control policy using object group in sub-domain is blank/0 bytes
CSCvg61624	Deployment fails when Secondary-Active Primary-Disabled (by doing suspend operation in device)

Bug ID	Headline
CSCvg61737	Deployement failed due to "Snort validation failed due to Unable to open rules file snort.conf file"
CSCvg61760	Not all the syslog messages on Firepower Threat Defense are available for editing
CSCvg61799	Sysopt permit-vpn behavior change to prevent unintended clear-text traffic
CSCvg62337	Memory calculation in Snort incorrect for Firepower Threat Defense devices
CSCvg66727	sysopt connection tcpmss 0 not removed after removing jumboframe
CSCvg67377	Malware correlation rule is missing Device condition
CSCvg71501	ASA/FTD device needs to be rebooted after adding Base license with export-controlled function
CSCvg73042	SSL Cache missing session info leading to ERR_SSL_PROTOCOL_ERROR in the browser for SSL websites
CSCvg76789	MASTER_KEY_INVALID flow error on FMC shown when having DND on few websites
CSCvg76907	Repeated SFDaco crashes if current_user_ip_map references invalid realm, somehow caused by RA-VPN?
CSCvg78622	Deployment failed in policy and object collection
CSCvg80346	Init Process Respawning on FMCv/FTDv/NGIPSv
CSCvg83924	Traffic not hitting the access control rule which has deprecated Application in it
CSCvg85613	Smart call home does not work properly with HTTP Proxy, when Authentication is turned on
CSCvg86139	After breaking Firepower Threat Defense high availability pair, policy deploy fails
CSCvg86366	Change Reconciliation Report not generated after upgrade
CSCvg87754	Unable to disable certain VPN related Syslog IDs from Management Center (like 402114 or 402119)
CSCvg90403	Blocks of size 80 leak observed when IRB is used in conjunction with multicast traffic
CSCvg93202	Dashboard custom analysis flow_chunk queries block event processing for hours
CSCvg93556	Deployment on a healthy KP HA pair failed with message "ssp_ha_state_improper"
CSCvg94796	Security Intelligence Connection Events showing '0' for Initiator User
CSCvg95046	Customer Success Network fails after upgrade of high-availability Firepower Management Centers
CSCvg98609	Management Center REST API - Threat Defense pairare not reported as targets on GET policyassignments

Bug ID	Headline
CSCvg98640	Cluster-Hold-Abort and Cluster-Hold-Timeout during policy deployment not handled correctly
CSCvg99285	[ERROR] Failed to init octeon -- FATAL ERROR: Can't initialize DAQ oct_ssl (-1)
CSCvh01213	An ASA may Traceback and reload when processing traffic
CSCvh03962	Cisco Firepower Management Center Command Injection Vulnerability
CSCvh05658	NAT policy assignment by device group does not update UI after moving device to different group
CSCvh05897	Firepower Threat Defense Cluster Registration with Group may fail
CSCvh07577	Cannot remove "management-access" configuration via flexconfig
CSCvh12923	Need to update docs that Firepower Threat Defense in cluster mode does not support Remote Access VPN
CSCvh14447	Rule parsing error was ignored in 602_log_package.pl.log during Snort update
CSCvh14478	policy deployment fails with QoS policy on firewall rulechecker
CSCvh15228	Firepower Threat Defense Traffic Zone Member Causes Traffic Interruption
CSCvh16252	ASA may traceback and reload in Thread Name: fover_rep during conn replication
CSCvh19991	User/Group Download fails when an Included Group is missing from the AD Server
CSCvh20742	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvh23085	Cisco Adaptive Security Appliance Application Layer Protocol Inspection DoS Vulnerabilities
CSCvh25000	custom user role unable to generate CSV reports without "health" privileges enabled
CSCvh25562	Cannot modify an access control rules / "An internal error occurred" error
CSCvh25977	blank space must be remove at the end of device name - cannot find events
CSCvh26084	SFDataCorrelator core in deserialization of corrupt flow event
CSCvh28733	Firepower Management Center allows wrong NAT rule when switching policy from Static to Dynamic
CSCvh31939	Firepower Management Center allows deleting Interface Object being used in SLA monitor object
CSCvh47069	Firepower Management Center Data purge causes managed sensor to wipe out user sessions upon reboot
CSCvh49388	Cisco FireSIGHT System VPN Policy Bypass Vulnerability

Bug ID	Headline
CSCvh49748	Malware.exe getting downloaded in the first try bypassing file detection due to unknown app-id
CSCvh53414	Access control policy deployment failing when object description contains "?" character
CSCvh53597	Policy deploy fails if SSL Policy has deprecated AppDetector
CSCvh53901	SFDataCorrelator cores when reading invalid fingerprint type from database
CSCvh59772	Deployment fails after S2S/RA VPN is deleted/unassigned following some edits and testing on it.
CSCvh59884	Notifications about pruned events contains invalid date/time (Thu Jan 1 00:00:01 1970)
CSCvh62164	ASA standby stuck in Bulk-Sync state with high CPS traffics on active
CSCvh63896	ASA/FTD traceback in threadname CP Processing
CSCvh67237	Policy deployment failing due to incomplete copying of deployment package
CSCvh67930	Management Center doesn't allow site to site tunnel with both IPv4 and IPv6 protected networks
CSCvh68253	Creation of two S2S VPN topologies with the same endpoints (nodes) leads to unpredictable results
CSCvh68311	Cisco Firepower System Software Cross-Origin Domain Protection Vulnerability
CSCvh68521	On 8000 series stack, with "Maint on sec fail" setting enabled, stack health is in compromised state
CSCvh70474	SFDataCorrelator/SFDCNotificationd connection log spam after expiring many hosts
CSCvh73463	Documentation and logs specify Firepower remote storage via SSH uses SCP, when it actually uses SFTP
CSCvh77456	Cisco Firepower Threat Defense Software FTP Inspection Denial of Service Vulnerability
CSCvh77845	SSL errors on session resume when server IP address changes
CSCvh78133	Firepower 2100 process_stderr.log getting flooded with errors causing /ngfw high disk
CSCvh79172	Phase-1 solution for momentary traffic drop during ASA policy apply rollback tracked w/ CSCvc56570
CSCvh83145	ASA interface IP and subnet mask changes to 0.0.0.0 0.0.0.0 causing outage of services on interface
CSCvh84511	Cisco FireSIGHT System URL-based Access Control Policy Bypass Vulnerability
CSCvh85246	ssl inspection can be limited by a "do not decrypt" rule specifying one or more common names

Bug ID	Headline
CSCvh85580	ids_event_alerter core when processing connection events
CSCvh89340	Cisco Firepower Threat Defense SSL Engine High CPU Denial Of Service Vulnerability
CSCvh90092	AQ task selection ignores few groups when large no of groups present causing 8 hr delays in deploy
CSCvh92840	Failing to deploy after adding a URL literal from REST API
CSCvh95396	Policy deployment failure due to Invalid preprocessor normalize_tcp option 'ftp'
CSCvh95456	Cisco Adaptive Security Appliance Application Layer Protocol Inspection DoS Vulnerabilities
CSCvh95807	SSL FLow Errors reported when accessing ECDSA signed websites
CSCvh95960	Using the "match" keyword in capture command causes IPv6 traffic to be ignored in capture
CSCvh97258	unable to render any of monitoring screens in any browser
CSCvh97594	ssl inspection cache can become unbalanced, leading to premature removal of recently used items
CSCvh97782	KP traceback illegal memory access inside a vendor Modular Exponentiation implementation
CSCvh98781	ASA/FTD Deployment ERROR 'Management interface is not allowed as Data is in use by this instance'
CSCvh98897	Data interfaces on Firepower devices shut down on upgrade failure, causing management interruptions
CSCvi02989	Access control policy not able to be edited or deployed after upgrade to Version 6.2.2.1
CSCvi09340	Policy deployment failed on multiple devices because of large size of policy deployment DB
CSCvi31174	FTD:Deployment takes lot of time when node in cluster is down/unreachable from FMC
CSCvi39938	Traffic outage while downloading large number of users and groups
CSCvi43661	Static Route:Proper Interface is not being assigned while configuring the route, causing problem.
CSCvi44246	Port-channel's subinterfaces share same MAC address on both unit of Threat Defense pair
CSCvi44365	After an upgrade the Firepower 4100 hostname is different than SFCLI hostname
CSCvi54162	"ha-replace" action not working when peer not present
CSCvi58729	6.2.3 Upgrade Resume Fails on KP-Onbox at 200_pre/600_ftd_onbox_data_export.sh

Bug ID	Headline
CSCvi59968	Firepower 2100 Incorrect reply for SNMP get request 1.3.6.1.2.1.1.2.0
CSCvi74560	6.2.3 does not properly deploy variables in variable sets and causes deploy failure
CSCvi74623	6.2.3 upgrade resets home_net variable to default "any"
CSCvi77527	upgrade to 6.2.3 fails with post install database integrity check error
CSCvi79043	Add warning to configure manager delete/add command
CSCvi80012	CD state incorrect if failover happens during snort policy application on Active FTD
CSCvi80849	Cisco Firepower 2100 Series POODLE TLS security scanner alerts
CSCvj00363	ASA may traceback and reload with combination of packet-tracer and captures
CSCvj05640	Traceback at snmp address not mapped when snmp-server not enabled
CSCvj13327	Upgrade to 6.2.3 fails at 600_schema/100_update_database.sh - oom killer invoked
CSCvj18111	FTD: Flow-preserve N1 flag shouldn't apply for IPS interfaces
CSCvj42450	ASA traceback in Thread Name: DATAPATH-14-17303
CSCvj47119	"clear capture /all" might crash
CSCvj50373	Doc: Table 1 has incorrect information on Configuration Guide Version 6.2.3
CSCvj58342	Multicast dropped after deleting a security context
CSCvj62504	Cisco Firepower 2100 Series Security Appliances Denial of Service Vulnerability
CSCvj65581	Excessive logging from ftdrpcd process on 2100 series appliances
CSCvj72309	FTD does not send Marker for End-of-RIB after a BGP Graceful Restart
CSCvj74210	Traceback at "ssh" when executing 'show service-policy inspect gtp pdp-context detail'
CSCvj82652	Deployment changes are not pushed to the device due to disk0 mounted on read-only
CSCvj85516	Packet capture fails for interface named "management" on Firepower Threat Defense
CSCvj89470	Cisco Adaptive Security Appliance Direct Memory Access Denial of Service Vulnerability
CSCvj98499	Linux Kernel cdrom_ioctl_media_changed Function Kernel Memory Read Vul
CSCvj98512	Doc: Procedure of changing FTD management IP address should be corrected.
CSCvj99658	ASA/Lina HA failover interface testing rendering control channel unresponsive
CSCvk02250	"show memory binsize" and "show memory top-usage" do not show correct information (Complete fix)
CSCvk04592	Flows get stuck in lina conn table in half-closed state

Bug ID	Headline
CSCvk07522	webvpn: Bookmark fails to render on Firefox and Chrome. IE fine.
CSCvk18330	Active FTP Data transfers fail with FTP inspection and NAT
CSCvk18578	Enabling compression necessary to load ASA SSLVPN login page customization
CSCvk20381	Traceback loop seen on fresh ASAv Azure, KVM and VMWare deployments
CSCvk25729	Large ACL taking long time to compile on boot causing outage
CSCvk30228	ASAv and FTDv deployment fails in Microsoft Azure and/or slow console response
CSCvk31035	KVM (FTD): Mapping web server through outside not working consistent with other platforms
CSCvk44166	Cisco ASA and FTD TCP Proxy Denial of Service Vulnerability
CSCvk45443	ASA cluster: Traffic loop on CCL with NAT and high traffic
CSCvk47253	Flow offload for UDP/TCP traffic is not working
CSCvk50732	AnyConnect 4.6 Web-deploy fails on MAC using Safari 11.1.x browsers
CSCvk51181	FTD IPV6 traffic outage after interface edit and deployment part 1/2
CSCvk57516	Low DMA memory leading to VPN failures due to incorrect crypto maps
CSCvk66732	Cisco Adaptive Security Appliance Software IPsec Denial of Service Vulnerability
CSCvk67239	FTD or ASA traceback and reload in "Thread Name: Logger Page fault: Address not mapped"
CSCvm06114	RDP bookmark plugin won't launch
CSCvm23370	ASA: Memory leak due to PC cssls_get_crypto_ctxt
CSCvm27111	FTD Lina traceback while removing OSPF configuration.
CSCvm31905	OpenSSH Bailout Delaying User Enumeration Vulnerability
CSCvm32267	Not blocking EICAR files through HTTPS connection with SSL policy in place
CSCvm53531	Cisco Adaptive Security Appliance Software Privilege Escalation Vulnerability
CSCvm64400	IKEv2: IKEv2-PROTO-2: Failed to allocate PSH from platform
CSCvm70274	tcp proxy: ASA traceback on DATAPATH
CSCvm72145	Cisco ASA Software and FTD Software MOBIKE Denial of Service Vulnerability
CSCvm80011	FTD Cluster in transparent mode; Inline set: FTP/SCP flows get stalled and never recover.
CSCvm86658	FTD traceback and reload in snap_get_retaddr_mips at snap.h:285

Bug ID	Headline
CSCvm91893	FMC does not update time and display events when using sliding time window option for event analysis
CSCvn09322	FTD device rebooted after taking Active State for less than 5 minutes
CSCvn09612	ASA/FTD Connection Idle Timers Not Increasing For Inactive Offloaded Sessions
CSCvn09640	FTD: Need ability to trust ethertype ACLs from the parser. Need to allow BPDU to pass through
CSCvn23254	SNMPv2 pulls empty ifHCInOctets value if Nameif is configured on the interface
CSCvn31390	Computing Processor PortSmash Side-Channel Information Disclosure Vuln
CSCvn33943	Standby node traceback in wccp_int_statechange() with HA configuration sync
CSCvn46358	overloading of the lina msglyr infra due to the sending of VPN status messages
CSCvn55563	Port group objects not listed while creating extended access list (FMC GUI)
CSCvn56095	selective acking not happening with SSL crypto hardware offload
CSCvn69213	ASA traceback and reload due to multiple threads waiting for the same lock - watchdog
CSCvn69270	Add troubleshooting for VPN Client Assignment
CSCvn75368	IPsec VPN goes down intermittently during a re-key
CSCvn76023	Firepower:when deploy policy, device list is empty with error message "failed to fetch device list"
CSCvn78174	Cisco ASA and Cisco FTD Software TCP Timer Handling Denial of Service Vulnerability
CSCvn78593	Control-plane ACL doesn't work correctly on FTD
CSCvn86777	Deployment on FTD with low memory results on interface nameif to be removed - finetune mmap thresh
CSCvo11077	Cisco ASA Software and FTD Software IKEv1 Denial of Service Vulnerability
CSCvo12985	ASA: EIGRP neighborship formation delayed after failover due to delay in sending out Hello packet
CSCvo39356	Traceback at Thread Name: IP Address Assign
CSCvo41572	FMC shows connection events with packet count as 0
CSCvo43679	FTD Lina traceback, due to packet looping in the system by normaliser
CSCvo47562	VPN sessions failing due to PKI handles not freed during rekeys
CSCvo48838	Lina does not properly report the error for configuration line that is too long

Bug ID	Headline
CSCvo56675	ASA or FTD traceback and reload due to failover state change or xlates cleared
CSCvo58847	Enhancement to address high IKE CPU seen due to tunnel replace scenario
CSCvo62031	ASA Traceback and reload while running IKE Debug
CSCvo68184	management-only of diagnostic I/F on secondary FTD get disappeared
CSCvo72462	Do not decrypt rule causes traffic interruptions.
CSCvo88762	FTD inline/transparent sends packets back through the ingress interface
CSCvo90998	LACPDUs should not be sent to snort for inline-set interfaces
CSCvp16536	ASA traceback and reload observed in Datapath due to SIP inspection.
CSCvp18878	ASA: Watchdog traceback in Datapath
CSCvp19549	FTD lina cored with Thread name: cli_xml_server
CSCvp24728	Random SGT tags added by FTD
CSCvp25236	FTD Lina traceback -Thread Name: cli_xml_server
CSCvp30505	FDM Error: There were some connectivity problems while loading archived backups.
CSCvp36425	Cisco ASA & FTD Software Cryptographic TLS and SSL Driver Denial of Service Vulnerability
CSCvp43150	FP9300 Cluster - Master unit does not update all the route changes to slaves
CSCvp45149	Traceback while Reverting the primary system as active
CSCvp47525	Upgrade times out after 1 hour for slow FMC-to-sensor bandwidth
CSCvp49576	FTD traceback due to watchdog on xlate_detach
CSCvp53637	Flows are getting offloaded on inline-sets
CSCvp55880	Fail-Closed FTD passes packets through on Snort processes down
CSCvp55901	LINA traceback on ASA in HA Active Unit repeatedly
CSCvp57643	FP9300 Cluster - Master unit does not update all the route changes to slaves
CSCvp67392	ASA/FTD HA Data Interface Heartbeat dropped due to Reverse Path Check
CSCvp70699	ASA Failover split brain (both units active) after rebooting a Firepower chassis
CSCvp81083	ASA/Lina Traceback related to TLS/VPN
CSCvq27010	Memory leak observed when ASA-SFR dataplane communication flaps
CSCvq44665	FTD/ASA : Traceback in Datapath with assert snp_tcp_intercept_assert_disabled

Bug ID	Headline
CSCvq54034	WRL6 and WRL8 commit-id update in CCM Layer (sprint 65)
CSCvq70775	FPR2100 FTD Standby unit leaking 9K blocks
CSCvq75634	Management interface configuration leads to immediate traceback and reload
CSCvq79042	FQDN ACL entries incomplete due to DNS response from server is large and truncated
CSCvq80735	Cannot add neighbor in BGP when the neighbor is on the same subnet as one interface
CSCvq93640	WRL6 and WRL8 commit id update in CCM layer (sprint 67)
CSCvr21803	Mac address flap on switch with wrong packet injected on ingress FTD interface
CSCvr23986	Cisco ASA & FTD devices may reload under conditions of low memory and frequent complete MIB walks
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
CSCvr68146	Unable to auto-rejoin FTD cluster
CSCvs01422	Lina traceback when changing device mode of FTD
CSCvs03023	Clustering module needs to skip the hardware clock update to avoid the timeout error and clock jump
CSCvs26402	NAT policy configuration range limit to be imposed for non service cmds as well
CSCvs59056	ASA/FTD Tunneled Static Routes are Ignored by Suboptimal Lookup if Float-Conn is Enabled
CSCvs80536	FP41xx incorrect interface applied in ASA capture
CSCvs81504	WR6 and WR8 commit id update in CCM layer(sprint 77)
CSCvt06606	Flow offload not working with combination of FTD 6.2(3.10) and FXOS 2.6(1.169)
CSCvt28182	sctp-state-bypass is not getting invoked for inline FTD