

Cisco Firepower Release Notes, Version 7.0.x

First Published: 2021-05-26

Last Modified: 2026-09-16

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

© 2021 –2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Welcome** 1

Release Highlights 1

Release Dates 2

Sharing Data with Cisco 3

For Assistance 4

CHAPTER 2 **System Requirements** 7

Firewall Management Center Platforms 7

Device Platforms 8

Device Management 11

CHAPTER 3 **Features** 15

FMC Features in Version 7.0.10 16

FMC Features in Version 7.0.9 17

FMC Features in Version 7.0.8 17

FMC Features in Version 7.0.7 17

FMC Features in Version 7.0.6 19

FMC Features in Version 7.0.5 21

FMC Features in Version 7.0.4 21

FMC Features in Version 7.0.3 22

FMC Features in Version 7.0.2 22

FMC Features in Version 7.0.1 24

FMC Features in Version 7.0.0 25

FDM Features in Version 7.0.x 38

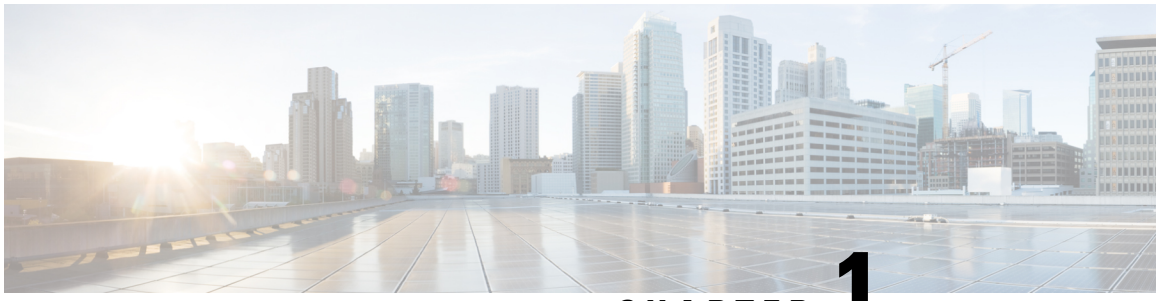
CHAPTER 4 **Upgrade Guidelines** 43

Planning Your Upgrade 43
Minimum Version to Upgrade 44
Upgrade Guidelines for Version 7.0 45
Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0 47
Reconnect with Cisco Threat Grid for High Availability Firewall Management Centers 47
Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs 47
Firewall Management Center Virtual Requires 28 GB RAM for Upgrade 48
Firepower 1000 Series Devices Require Post-Upgrade Power Cycle 49
Historical Data Removed During Firewall Threat Defense Upgrade with Firewall Device Manager 49
New URL Categories and Reputations 49
Pre-Upgrade Actions for URL Categories and Reputations 51
Post-Upgrade Actions for URL Categories and Reputations 52
Guidelines for Rules with Merged URL Categories 53
Upgrade Guidelines for Cloud-Delivered Firewall Management Center 55
Upgrade Guidelines for the Firepower 4100/9300 Chassis 55
Unresponsive Upgrades 56
Revert or Uninstall the Upgrade 56
Uninstall ASA FirePOWER Patches with ASDM 57
Traffic Flow and Inspection 59
Traffic Flow and Inspection for Chassis Upgrades 59
Traffic Flow and Inspection for Firewall Threat Defense Upgrades with Firewall Management Center 60
Traffic Flow and Inspection for Firewall Threat Defense Upgrades with Firewall Device Manager 61
Traffic Flow and Inspection for ASA FirePOWER Upgrades 62
Traffic Flow and Inspection for NGIPSv Upgrades with FMC 62
Traffic Flow and Inspection when Deploying Configurations 63
Time and Disk Space 64

CHAPTER 5 **Install the Software** 67
Installation Guidelines 67
Installation Guides 69

CHAPTER 6 **Bugs** 71
Open Bugs 71

Open Bugs in Version 7.0.0 71
Resolved Bugs 73
Resolved Bugs in Version 7.0.10 73
Resolved Bugs in Version 7.0.9 75
Resolved Bugs in Version 7.0.8.1 80
Resolved Bugs in Version 7.0.8 80
Resolved Bugs in Version 7.0.7 81
Resolved Bugs in Version 7.0.6.3 90
Resolved Bugs in Version 7.0.6.2 97
Resolved Bugs in Version 7.0.6.1 106
Resolved Bugs in Version 7.0.6 111
Resolved Bugs in Version 7.0.5.1 152
Resolved Bugs in Version 7.0.5 152
Resolved Bugs in Version 7.0.4 165
Resolved Bugs in Version 7.0.3 170
Resolved Bugs in Version 7.0.2.1 171
Resolved Bugs in Version 7.0.2 171
Resolved Bugs in Version 7.0.1.1 186
Resolved Bugs in Version 7.0.1 187
Resolved Bugs in Version 7.0.0.1 194
Resolved Bugs in Version 7.0.0 194



CHAPTER 1

Welcome

This document contains release information for Version 7.0 of Cisco Secure Firewall Threat Defense, Secure Firewall Management Center, Secure Firewall Device Manager, and Firepower Classic devices (NGIPSv, ASA with FirePOWER Services).

For Security Cloud Control (Security Cloud Control) deployments, see the Release Notes for Cloud-Delivered Firewall Management Center or *What's New for Security Cloud Control*.

- Release Highlights, on page 1
- Release Dates, on page 2
- Sharing Data with Cisco, on page 3
- For Assistance, on page 4

Release Highlights

Release Numbering: Why Version 7.0?

Release numbering skips from Version 6.7 to Version 7.0.

This emphasizes the superior value due to the key new features and functionality introduced over the last several releases, in addition to the multiple performance and security enhancements. There are no unexpected incompatibilities with or limitations to upgrading to Version 7.0. Read these release notes for specific details on compatibility, upgrade requirements, deprecated features and functionality, and so on.

Note that Version 7.0 is an *extra long-term release*, as described in the Cisco's Next Generation Firewall Product Line Software Release and Sustaining Bulletin.

Snort 3 for FTD with FMC Deployments

For new FTD deployments, Snort 3 is now the default inspection engine. Upgraded deployments continue to use Snort 2, but you can switch at any time.

Advantages to using Snort 3 include, but are not limited to:

- Improved performance.
- Improved SMBv2 inspection.
- New script detection capabilities.
- HTTP/2 inspection.

- Custom rule groups.
- Syntax that makes custom intrusion rules easier to write.
- Reasons for 'would have dropped' inline results in intrusion events.
- No Snort restarts when deploying changes to the VDB, SSL policies, custom application detectors, captive portal identity sources, and TLS server identity discovery.
- Improved serviceability, due to Snort 3-specific telemetry data sent to Cisco Success Network, and to better troubleshooting logs.

A Snort 3 intrusion rule update is called an *LSP* (Lightweight Security Package) rather than an SRU. The system still uses SRUs for Snort 2; downloads from Cisco contain both the latest LSP and SRU. The system automatically uses the appropriate rule set for your configurations.

The FMC can manage a deployment with both Snort 2 and Snort 3 devices, and will apply the correct policies to each device. However, unlike Snort 2, you cannot update Snort 3 on a device by upgrading the FMC only and then deploying. With Snort 3, new features and resolved bugs require you upgrade the software on the FMC *and* its managed devices. For information on the Snort included with each software version, see the *Bundled Components* section of the Cisco Firepower Compatibility Guide.



Important Before you switch to Snort 3, we *strongly* recommend you read and understand the Firepower Management Center Snort 3 Configuration Guide. Pay special attention to feature limitations and migration instructions. Although upgrading to Snort 3 is designed for minimal impact, features do not map exactly. Careful planning and preparation can help you make sure that traffic handled as expected.

You can also visit the Snort 3 website: https://snort.org/snort3.

Release Dates

Table 1: Version 7.0 Dates

Version	Build	Date	Platforms
7.0.10	63	2026-09-15	All
7.0.9	25	2026-02-17	All
7.0.8.1	4	2025-09-25	All
7.0.8	174	2025-08-12	All
7.0.7	519	2025-02-14	Firewall Threat Defense
	518	2025-01-29	Firewall Management Center, including virtual ASA FirePOWER NGIPSv
7.0.6.3	50	2024-09-10	All

Version	Build	Date	Platforms
7.0.6.2	65	2024-04-15	All
7.0.6.1	36	2023-11-13	All
7.0.6	236	2023-07-18	All
7.0.5.1	5	2023-04-26	NGIPSv For devices with security certifications compliance enabled (CC/UCAPL mode). Use with a Version 7.0.5 FMC.
7.0.5	72	2022-11-17	All
7.0.4	55	2022-08-10	All
7.0.3	37	2022-06-30	All
7.0.2.1	10	2022-06-27	All
7.0.2	88	2022-05-05	All
7.0.1.1	11	2022-02-17	All
7.0.1	84	2021-10-07	All
7.0.0.1	15	2021-07-15	All
7.0.0	94	2021-05-26	All

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.

Cisco Support Diagnostics

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

During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time. This feature is not supported with Firewall Device Manager.

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 Firewall Management Centers.

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

Upgrade Guides

In Firewall Management Center deployments, the Firewall Management Center must run the same or newer maintenance (third-digit) release as its managed devices. Upgrade the Firewall Management Center first, then devices. Use the upgrade guide for the version you are *currently* running—not your target version.

Table 2: Upgrade Guides

Platform	Upgrade Guide	Link
Firewall Management Center	Firewall Management Center version you are *currently* running.	https://cisco.com/go/fmc-upgrade
Firewall Threat Defense with Firewall Management Center	Firewall Management Center version you are *currently* running.	https://cisco.com/go/ftd-fmc-upgrade
Firewall Threat Defense with device manager	Firewall Threat Defense version you are *currently* running.	https://cisco.com/go/ftd-fdm-upgrade
Firewall Threat Defense with Cloud-Delivered Firewall Management Center	Cloud-Delivered Firewall Management Center.	https://cisco.com/go/ftd-cdfmc-upgrade

Install Guides

If you cannot or do not want to upgrade, you can freshly install major and maintenance releases. This is also called *reimaging*. You cannot reimage to a patch. Install the appropriate major or maintenance release, then apply the patch. If you are reimaging to an earlier Firewall Threat Defense version on an FXOS device, perform a full reimage—even for devices where the operating system and software are bundled.

Table 3: Install Guides

Platform	Install Guide	Link
Firewall Management Center hardware	Getting started guide for your Firewall Management Center hardware model.	https://cisco.com/go/fmc-install

Platform	Install Guide	Link
Firewall Management Center Virtual	Getting started guide for the Firewall Management Center Virtual.	https://cisco.com/go/fmcv-quick
Firewall Threat Defense hardware	Getting started or reimage guide for your device model.	https://cisco.com/go/ftd-quick
Firewall Threat Defense Virtual	Getting started guide for your Firewall Threat Defense Virtual version.	https://cisco.com/go/ftdv-quick
FXOS for the Firepower 4100/9300	Configuration guide for your FXOS version, in the *Image Management* chapter.	https://cisco.com/go/firepower9300-config
FXOS for the Firepower 1000/2100 and Secure Firewall 3100	Troubleshooting guide, in the *Reimage Procedures* chapter.	*Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense*

More 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.

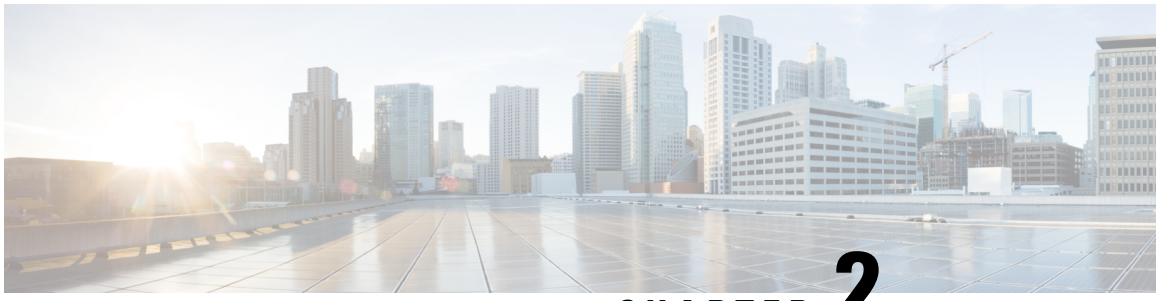
- Documentation: https://cisco.com/go/threatdefense-70-docs
- Cisco Support & Download site: https://cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://cisco.com/cisco/support/notifications.html

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 7.0.

- Firewall Management Center Platforms, on page 7
- Device Platforms, on page 8
- Device Management, on page 11

Firewall Management Center Platforms

The Firewall Management Center provides a centralized firewall management console. For device compatibility with the Firewall Management Center, see Device Management, on page 11. For general compatibility information, see the *Cisco Secure Firewall Management Center Compatibility Guide*.

Firewall Management Center Hardware

Version 7.0 supports the following Firewall Management Center hardware:

- Firepower Management Center 1600, 2600, 4600
- Firepower Management Center 1000, 2500, 4500

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

Firewall Management Center Virtual

Version 7.0 supports Firewall Management Center Virtual deployments in both public and private clouds.

With the Firewall Management Center Virtual, you can purchase a license to manage 2, 10, or 25 devices. Some platforms support 300 devices. Note that two-device licenses do not support Firewall Management Center high availability. For full details on supported instances, see the *Cisco Secure Firewall Management Center Virtual Getting Started Guide*.

Table 4: Version 7.0 Firewall Management Center Virtual Platforms

Platform	Devices Managed		High Availability
	2, 10, 25	300	
Public Cloud			

Platform	Devices Managed		High Availability
	2, 10, 25	300	
Amazon Web Services (AWS)	YES	—	—
Google Cloud Platform (GCP)	YES	—	—
Microsoft Azure	YES	—	—
Oracle Cloud Infrastructure (OCI)	YES	—	—
Private Cloud			
Cisco HyperFlex	YES	—	YES
Kernel-based virtual machine (KVM)	YES	—	—
Nutanix Enterprise Cloud	YES	—	—
OpenStack	YES	—	—
VMware vSphere/VMware ESXi 6.5, 6.7, or 7.0	YES	YES	YES

Cloud-Delivered Firewall Management Center

is delivered via Security Cloud Control, which unites management across multiple Cisco security solutions. We take care of feature updates. Note that a customer-deployed Firewall Management Center is referred to as *on-prem*, even for public cloud deployments.

For up-to-date compatibility information, see the *Cisco Secure Firewall Management Center Compatibility Guide*.

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 11. For general compatibility information, see the *Cisco Secure Firewall Threat Defense Compatibility Guide* or the *Cisco Firepower Classic Device Compatibility Guide*.

Firewall Threat Defense Hardware

Version 7.0 Firewall Threat Defense hardware comes in a range of throughputs, scalability capabilities, and form factors.

Table 5: Version 7.0 Firewall Threat Defense Hardware

Platform	Firewall Management Center Compatibility		Firewall Device Manager Compatibility		Notes
	Customer Deployed	Cloud Delivered	Firewall Device Manager Only	Firewall Device Manager + CDO	
Firepower 1010, 1120, 1140, 1150	YES	YES Requires Version 7.0.3+	YES	YES	—
Firepower 2110, 2120, 2130, 2140	YES	YES Requires Version 7.0.3+	YES	YES	—
Firepower 4110, 4120, 4140, 4150 Firepower 4112, 4115, 4125, 4145 Firepower 9300: SM-24, SM-36, SM-44 modules Firepower 9300: SM-40, SM-48, SM-56 modules	YES	YES Requires Version 7.0.3+	YES	YES	Requires FXOS 2.10.1.331 or later build. We recommend the latest firmware. See the *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*.
ASA 5508-X, 5516-X	YES	YES Requires Version 7.0.3+	YES	YES	ASA 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 Requires Version 7.0.3+	YES	YES	May require a ROMMON update. See the *Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide*.

Firewall Threat Defense Virtual

Version 7.0 Firewall Threat Defense Virtual implementations support performance-tiered Smart Software Licensing, based on throughput requirements and remote access VPN session limits. Options run from FTDv5 (100 Mbps/50 sessions) to FTDv100 (16 Gbps/10,000 sessions). For more information on supported instances, throughputs, and other hosting requirements, see the appropriate *Getting Started Guide*.

Table 6: Version 7.0 Firewall Threat Defense Virtual Platforms

Device Platform	Firewall Management Center Compatibility		Firewall Device Manager Compatibility	
	Customer Deployed	Cloud Delivered	Firewall Device Manager Only	Firewall Device Manager + CDO
Public Cloud				
Amazon Web Services (AWS)	YES	YES Requires Version 7.0.3+	YES	YES
Microsoft Azure	YES	YES Requires Version 7.0.3+	YES	YES
Google Cloud Platform (GCP)	YES	YES Requires Version 7.0.3+	—	—
Oracle Cloud Infrastructure (OCI)	YES	YES Requires Version 7.0.3+	—	—
Private Cloud				
Cisco Hyperflex	YES	YES Requires Version 7.0.3+	YES	YES
Kernel-based virtual machine (KVM)	YES	YES Requires Version 7.0.3+	YES	YES
Nutanix Enterprise Cloud	YES	YES Requires Version 7.0.3+	YES	YES
OpenStack	YES	YES Requires Version 7.0.3+	—	—
VMware vSphere/VMware ESXi 6.5, 6.7, or 7.0	YES	YES Requires Version 7.0.3+	YES	YES

Firepower Classic: ASA FirePOWER, NGIPSv

Firepower Classic devices run NGIPS software on the following platforms:

- 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 7: Version 7.0 NGIPS Platforms

Device Platform	FMC Compatibility (Customer Deployed)	ASDM Compatibility	Notes
ASA 5508-X, 5516-X	YES	Requires ASDM 7.16(1).	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*.
ISA 3000	YES	Requires ASDM 7.16(1).	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*.
NGIPSv	YES	—	Requires VMware vSphere/VMware ESXi 6.5, 6.7, or 7.0. 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.

On-Prem Firewall Management Center

All devices support remote management with a customer-deployed (*on-prem*) Firewall Management Center.

Versions are major (A.x), maintenance (A.x.y), or patch (A.x.y.z). The Firewall Management Center should run the same or newer version as its devices. New features and resolved issues often require the latest version on both the Firewall Management Center and its devices. Upgrade the Firewall Management Center first—you will still be able to manage older devices, usually a few major versions back.

Note You cannot upgrade a device past the Firewall Management Center to a newer major or maintenance version. Although a patched device (fourth-digit) can be managed with an unpatched Firewall Management Center, fully patched deployments undergo enhanced testing.

Note that in most cases you can upgrade an older device directly to the Firewall Management Center's major or maintenance version. However, sometimes you can manage an older device that you cannot directly upgrade, even though the target version is supported on the device. Rarely, there are issues with specific Firewall Management Center-device combinations. For release-specific requirements, see Upgrade Guidelines, on page 43.

Table 8: On-Prem Firewall Management Center-Device Compatibility

Firewall Management Center Version	Oldest Device Version You Can Manage
10.x	7.3
7.7	7.2
7.6	7.1
7.4 Last support for NGIPS device management.	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
6.4	6.1
6.2.3	6.1

Cloud-Delivered Firewall Management Center

For Firewall Threat Defense compatibility with Cloud-Delivered Firewall Management Center, see the *Cisco Secure Firewall Threat Defense Compatibility Guide*.

Firewall Device Manager

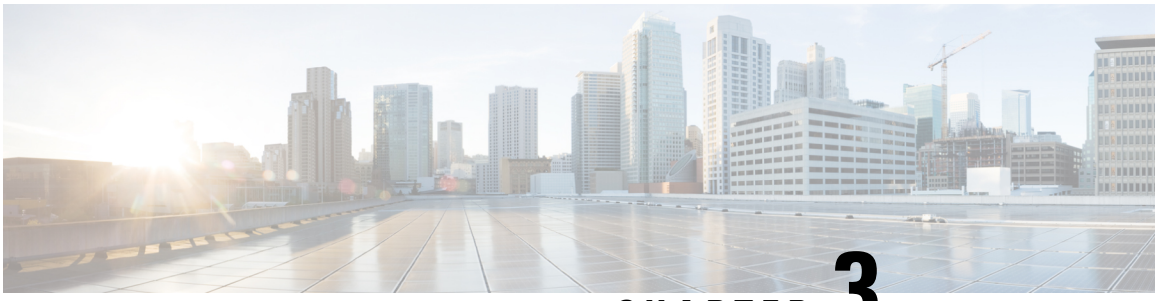
You can use Firewall Device Manager to locally manage a single Firewall Threat Defense device. Most models suppport local management.

Optionally, add Security Cloud Control to remotely manage multiple Firewall Threat Defense devices, as an alternative to the Firewall Management Center. Although some configurations still require Firewall Device

Manager, Security Cloud Control allows you to establish and maintain consistent security policies across your Firewall Threat Defense deployment.

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.



CHAPTER 3

Features

For features in earlier releases, see *Cisco Secure Firewall Management Center New Features by Release* and *Cisco Secure Firewall Device Manager New Features by Release*.

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. This is especially common with new threat detection and application identification capabilities. A feature can also have upgrade impact if upgrading requires that you take action before or after upgrade to avoid an undesirable outcome; for example, if you must change a configuration.

The feature descriptions here include upgrade impact where appropriate.

Features in Maintenance Releases

Features, enhancements, and critical fixes included in maintenance releases (third-digit) and patches (fourth-digit) can skip future releases, depending on release date, release type (short term vs. long term), and other factors. Minimize upgrade and other impact by going directly to the latest maintenance release in your chosen version. See .

If you are using the web interface in a language other than English, features introduced in maintenance releases and patches may not be translated until the next major release.

Snort Features

Snort 3 is the default inspection engine for Firewall Threat Defense. Snort 3 features for Firewall Management Center deployments also apply to Firewall Device Manager, even if they are not listed as new Firewall Device Manager features. However, keep in mind that the Firewall Management Center may offer more configurable options than Firewall Device Manager.



Important Snort 2 is deprecated in Version 7.7+, and prevents Firewall Threat Defense upgrade. If you are still using Snort 2 on older devices, switch to Snort 3 for improved detection and performance.

Intrusion Rules and Keywords

Upgrades can import and auto-enable 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.

For details on new keywords, see the Snort release notes: https://www.snort.org/downloads.

FlexConfig

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

The feature descriptions here include information on deprecated FlexConfigs when appropriate. For a full list of deprecated FlexConfigs, see your configuration guide.

Integrations and Logging

These integrations and logging facilities may have new features associated with threat defense and management center releases:

- Syslog: *Cisco Secure Firewall Threat Defense Syslog Messages*
- Cisco Success Network: Cisco Success Network Telemetry Data Collected from Cisco Firepower Management Center
- REST API: *Secure Firewall Management Center REST API Quick Start Guide* and *Cisco Secure Firewall Threat Defense REST API Guide*

- FMC Features in Version 7.0.10, on page 16
- FMC Features in Version 7.0.9, on page 17
- FMC Features in Version 7.0.8, on page 17
- FMC Features in Version 7.0.7, on page 17
- FMC Features in Version 7.0.6, on page 19
- FMC Features in Version 7.0.5, on page 21
- FMC Features in Version 7.0.4, on page 21
- FMC Features in Version 7.0.3, on page 22
- FMC Features in Version 7.0.2, on page 22
- FMC Features in Version 7.0.1, on page 24
- FMC Features in Version 7.0.0, on page 25
- FDM Features in Version 7.0.x, on page 38

FMC Features in Version 7.0.10

There are no new features in this release. See Resolved Bugs in Version 7.0.10, on page 73.

FMC Features in Version 7.0.9

There are no new features in this release. See Resolved Bugs in Version 7.0.9, on page 75.

FMC Features in Version 7.0.8

Table 9: FMC Features in Version 7.0.8

Feature	Minimum FMC	Minimum FTD	Details
Licensing			
Updated internet access requirements for Smart Licensing.	7.0.8 7.2.10 7.3.0	Any	**Upgrade impact. The system connects to new resources.** When communicating with the Cisco Smart Software Manager, the Firewall Management Center now connects to smartreceiver.cisco.com instead of tools.cisco.com.

FMC Features in Version 7.0.7

Table 10: FMC Features in Version 7.0.7

Feature	Minimum FMC	Minimum FTD	Details
Access Control: File and Malware			

Feature	Minimum FMC	Minimum FTD	Details
New Cisco AMP cloud connection method. Deprecated Cisco AMP Cloud connection backups.	7.0.7 7.2.10 7.6.1 7.7.0	Any	**Upgrade impact. The system connects to new resources. US public cloud connections replace AMP private cloud connections.** We replaced the AMP cloud connection method with one that is more secure, as well as easier to maintain and enhance. As a result of these changes: • The system connects to new resources. Success is reported in the Message Center (as Update Legacy AMP Public Cloud Connections). See the section for *Secure Firewall (AMP For Networks)* on Required Server Addresses for Proper Cisco Secure Endpoint & Malware Analytics Operations. • AMP cloud connections, both public and private, are no longer included in Firewall Management Center configuration backups. You must reconfigure them after restore. • Upgrade replaces AMP private cloud connections with US public cloud connections. Pre-upgrade, the readiness check fails once if you have private AMP connections. **Tip** To avoid this, delete private cloud connections before upgrade and reconnect after upgrade. Use **Integration** > **AMP Management**. Other restrictions: Version 7.0.7 Firewall Management Centers are not listed on **Management** > **Computers** in the Secure Endpoint console. Although you can still integrate with Secure Endpoint, you cannot use the console to run diagnostics, see a risk score, quick-link to events and trajectories, apply policies, and so on.
Administration			
Cisco Security Cloud regions: India and Australia.	7.0.7 7.2.9 7.6.0	7.0.7 7.2.9 7.6.0	Cisco Security Cloud integration now supports the India and Australia regional clouds. New/modified screens: • Version 7.6.0+ : **Integration** > **Cisco Security Cloud** > **Current Region** • Version 7.4.x and earlier: **Integration** > **SecureX** > **Current Region**
Security and Hardening			

Feature	Minimum FMC	Minimum FTD	Details
Require the Message-Authenticator attribute in all RADIUS responses.	7.0.7 7.2.10 7.4.3 7.6.1 7.7.0	7.0.7 7.2.10 7.4.3 7.6.1 7.7.0	**Upgrade impact. For the Firepower 4100/9300, check FXOS compatibility before you upgrade Firewall Threat Defense. After Firewall Threat Defense upgrade, enable the option for existing servers.** You can now require the Message-Authenticator attribute in all RADIUS responses, ensuring that the Firewall Threat Defense VPN gateway securely verifies every response from the RADIUS server, whether for RA VPN or access to the device itself. The **RADIUS Server-Enabled Message Authenticator** option is enabled by default for new RADIUS servers. We also recommend you enable it for existing servers. Disabling it may expose firewalls to potential attacks. New/modified screens: • **Objects** > **AAA Server** > **RADIUS Server Group** > **Add RADIUS Server Group** > **Add RADIUS Server** • **System** (⚙) > **Users** > **External Authentication** > **Add External Authentication Object (RADIUS)** New CLI commands: **message-authenticator-required** Version restrictions: For the Firepower 4100/9300, this feature may require an FXOS upgrade. For minimum builds, see *Cisco Secure Firewall Threat Defense Compatibility Guide*. Other restrictions: This feature introduced a login bug where the Firewall Management Center treats the RADIUS Class attribute (25) as octets instead of a string, which can break role mapping and cause login failures. For a list of fixed releases, or a workaround if you cannot upgrade, see CSCwq03404.

FMC Features in Version 7.0.6

Table 11: FMC Features in Version 7.0.6

Feature	Minimum FMC	Minimum FTD	Details
Access Control: Threat Detection and Application Identification			

Feature	Minimum FMC	Minimum FTD	Details
Smaller VDB for lower memory Snort 2 devices.	6.4.0.17 7.0.6 7.2.4 7.3.1.1 7.4.0	Any with Snort 2	**Upgrade impact. Application identification on lower memory devices is affected.** For VDB 363+, the system now installs a smaller VDB (also called *VDB lite*) on lower memory devices running Snort 2. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Lower memory devices: ASA 5506-X series, ASA-5508-X, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X Version restrictions: The ability to install a smaller VDB depends on the version of the Firewall Management Center, not managed devices. If you upgrade the Firewall Management Center from a supported version to an unsupported version, you cannot install VDB 363+ if your deployment includes even one lower memory device. For a list of affected releases, see CSCwd88641.
Administration			
Updated web analytics provider.	7.0.6 7.2.6 7.4.1	Any	**Upgrade impact. Your browser connects to new resources.** While using the Firewall Management Center, your browser now contacts Amplitude (amplitude.com) instead of Google (google.com) for web analytics.
Deprecated Features			
Deprecated: `high unmanaged disk usage` alerts.	7.0.6 7.2.4 7.4.0	7.0.6 7.2.4 7.4.0	The Disk Usage health module no longer alerts with `high unmanaged disk usage`. After FMC upgrade, you may continue to see these alerts until you either deploy health policies to managed devices (stops the display of alerts) or upgrade the devices (stops the sending of alerts). **Note** Versions 7.0–7.0.5, 7.1.x, 7.2.0–7.2.3, and 7.3.x continue to support these alerts. If your Firewall Management Center is running any of these versions, you may also continue to see alerts. For information on the remaining Disk Usage alerts, see Disk Usage and Drain of Events Health Monitor Alerts.

FMC Features in Version 7.0.5

Table 12: FMC Features in Version 7.0.5

Feature	Minimum FMC	Minimum FTD	Details
ISA 3000 System LED support for shutting down.	Any	7.0.5 7.3.0	When you shut down the ISA 3000, the System LED turns off. Wait at least 10 seconds after that before you remove power from the device.
Automatically update CA bundles.	7.0.5 7.1.0.3 7.2.4 7.3.0	7.0.5 7.1.0.3 7.2.4 7.3.0	**Upgrade impact. The system connects to new resources.** The local CA bundle contains certificates to access several Cisco services. The system now automatically queries Cisco for new CA certificates at a daily system-defined time. Previously, you had to upgrade the software to update CA certificates. You can use the CLI to disable this feature. New resources: https://cisco.com/security/pki/ New/modified CLI commands: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** See: Firepower Management Center Command Line Reference and *Cisco Secure Firewall Threat Defense Command Reference*

FMC Features in Version 7.0.4

There are no new features in this release.

FMC Features in Version 7.0.3

Table 13: FMC Features in Version 7.0.3

Feature	Minimum FMC	Minimum FTD	Details
Threat defense support for Cloud-Delivered Firewall Management Center.	7.2.0 for analytics-only support	7.0.3 7.2.0	Version 7.0.3–7.0.x and 7.2.0+ threat defense devices support management by the Cloud-Delivered Firewall Management Center in Security Cloud Control. cannot manage Firewall Threat Defense devices running Version 7.1, or Classic devices running any version. You cannot upgrade a cloud-managed device from Version 7.0.x to Version 7.1 unless you unregister and disable cloud management. We recommend you upgrade directly to a later version. **Important** ended support for Version 7.0.x Firewall Threat Defense devices on December 15, 2025. For more information, see FAQ and Support. New/modified CLI commands: **configure manager add**, **configure manager delete**, **configure manager edit**, **show managers** For more information, see *Cisco Security Cloud Control: Cloud-Delivered Firewall Management Center for Firewall Threat Defense*.

FMC Features in Version 7.0.2

Table 14: FMC Features in Version 7.0.2

Feature	Minimum FMC	Minimum FTD	Details
ISA 3000 support for shutting down.	Any	7.0.2 7.2.0	You can now shut down the ISA 3000; previously, you could only reboot the device.
Dynamic object names now support the dash character.	7.0.2 7.1.0	7.0.2 7.1.0	Dynamic object names now support the dash character. This is especially useful if you are using the ACI endpoint update app (where the dash character is allowed), to create dynamic objects on the FMC that represent tenant endpoint groups.

Feature	Minimum FMC	Minimum FTD	Details
Improved SecureX integration, SecureX orchestration.	7.0.2 7.2.0	Any	**Upgrade impact. Cannot upgrade Version 7.0.x → 7.1 with feature enabled.** We have streamlined the SecureX integration process. Now, as long as you already have a SecureX account, you just choose your cloud region on the new **Integration > SecureX** page, click **Enable SecureX**, and authenticate to SecureX. The option to send events to the cloud, as well as to enable Cisco Success Network and Cisco Support Diagnostics, are also moved to this new page. When you enable SecureX integration on this new page, licensing and management for the system's cloud connection switches from Cisco Smart Licensing to SecureX. If you already enabled SecureX the "old" way, you must disable and re-enable to get the benefits of this cloud connection management. Note that this page also governs the cloud region for and event types sent to the Secure Network Analytics (Stealthwatch) cloud using Security Analytics and Logging (SaaS), even though the web interface does not indicate this. Previously, these options were on **System**(⚙) **> Integration > Cloud Services**. Enabling SecureX does not affect communications with the Secure Network Analytics cloud; you can send events to both. The Firewall Management Center also now supports SecureX orchestration—a powerful drag-and-drop interface you can use to automate workflows across security tools. After you enable SecureX, you can enable orchestration. As part of this feature, you can no longer use the REST API to configure SecureX integration. You must use the FMC web interface. Version restrictions: Not supported with Version 7.0.0-7.0.1, 7.1.x. If you use the new method to enable SecureX integration in Version 7.0.x, you cannot upgrade to Version 7.1 unless you disable the feature. We recommend you upgrade to Version 7.2+. See: *Cisco Secure Firewall Threat Defense and SecureX Integration Guide*

Feature	Minimum FMC	Minimum FTD	Details
Web interface changes: SecureX, threat intelligence, and other integrations.	7.0.2 7.2.0	Any	We changed these FMC menu options. **AMP > AMP Management** is now **Integration > AMP > AMP Management** **AMP > Dynamic Analysis Connections** is now **Integration > AMP > Dynamic Analysis Connections** **Intelligence > Sources** is now **Integration > Intelligence > Sources** **Intelligence > Elements** is now **Integration > Intelligence > Elements** **Intelligence > Settings** is now **Integration > Intelligence > Settings** **Intelligence > Incidents** is now **Integration > Intelligence > Incidents** **System (⚙) > Integration** is now **Integration > Other Integrations** **System (⚙) > Logging > Security Analytics & Logging** is now **Integration > Security Analytics & Logging** **System (⚙) > SecureX** is now **Integration > SecureX**

FMC Features in Version 7.0.1

Table 15: FMC Features in Version 7.0.1

Feature	Minimum FMC	Minimum FTD	Details
Device Management			
New default password for ISA 3000 with ASA FirePOWER Services.	7.0.1 7.1.0	7.0.1 7.1.0	For new devices, the default password for the admin account is now Adm!n123. Previously, the default admin password was Admin123. Upgrading or reimaging to Version 7.0.1+ does not change the password. However, we do recommend that all user accounts—especially those with Admin access—have strong passwords.
Access Control: Threat Detection and Application Identification			

Feature	Minimum FMC	Minimum FTD	Details
Snort 3 rate_filter inspector.	7.0.1 7.1.0	7.0.1 7.1.0	We introduced the Snort 3 rate_filter inspector. This allows you to change the action of an intrusion rule in response to excessive matches on that rule. You can block rate-based attacks for a specific length of time, then return to allowing matching traffic while still generating events. For more information, see the Snort 3 Inspector Reference. New/modified pages: Configure the inspector by editing the Snort 3 version of a custom network analysis policy. Version restrictions: Requires lsp-rel-20210816-1910 or later.

FMC Features in Version 7.0.0

Table 16: FMC Features in Version 7.0.0

Feature	Minimum FMC	Minimum FTD	Details
Platform			
VMware vSphere/VMware ESXi 7.0 support.	7.0	7.0	You can now deploy FMCv, FTDv, and NGIPSv virtual appliances on VMware vSphere/VMware ESXi 7.0. Note that Version 7.0 also discontinues support for VMware 6.0. Upgrade the hosting environment to a supported version before you upgrade the Firepower software.
FMCv for HyperFlex, Nutanix, and OpenStack.	7.0	Any	We now support FMCv2, v10, and v25 for Cisco HyperFlex, Nutanix Enterprise Cloud, and OpenStack. FMCv for HyperFlex supports high availability with FMCv10 and v25. If you are managing FTD devices, you need two identically licensed FMCs, as well as one FTD entitlement for each managed device. For example, to manage 10 devices with an FMCv10 high availability pair, you need two FMCv10 entitlements and 10 FTD entitlements. If you are managing Classic devices only (NGIPSv or ASA FirePOWER), you do not need FMCv entitlements.
FTDv for HyperFlex, Nutanix, and OpenStack.	7.0	7.0	We now support FTDv for Cisco HyperFlex, Nutanix Enterprise Cloud, and OpenStack.

Feature	Minimum FMC	Minimum FTD	Details
FTDv performance tiered Smart Licensing.	7.0	7.0	**Upgrade impact. Upgrading automatically assigns devices to the FTDv Variable tier.** FTDv now supports performance-tiered Smart Software Licensing, based on throughput requirements and RA VPN session limits. Options run from FTDv5 (100 Mbps/50 sessions) to FTDv100 (16 Gbps/10,000 sessions). Before you add a new device, make sure your account contains the licenses you need. To purchase additional licenses, contact your Cisco representative or partner contact. Upgrading FTDv to Version 7.0 automatically assigns the device to the FTDv Variable tier, although you can change this later. For more information on changing performance tiers, supported instances, throughputs, and other hosting requirements, see the appropriate *Getting Started Guide*. New/modified pages: • You can now specify a performance tier when adding or editing an FTDv device on the **Device > Device Management** page. • You can bulk-edit performance tiers on **System** (⚙) > **Licenses** > **Smart Licenses** > page.
FTD Clustering			
Improved PAT port block allocation for clustering	7.0	7.0	The improved PAT port block allocation ensures that the control unit keeps ports in reserve for joining nodes, and proactively reclaims unused ports. To best optimize the allocation, you can set the maximum nodes you plan to have in the cluster using the **cluster-member-limit** command using FlexConfig. The control unit can then allocate port blocks to the planned number of nodes, and it will not have to reserve ports for extra nodes you don't plan to use. The default is 16 nodes. You can also monitor syslog 747046 to ensure that there are enough ports available for a new node. New/modified commands: **cluster-member-limit** (FlexConfig), **show nat pool cluster [summary]**, **show nat pool ip detail** Supported platforms: Firepower 4100/9300
FTD CLI **show cluster history** improvements.	7.0	7.0	New keywords allow you to customize the output of the **show cluster history** command. New/modified commands: **show cluster history** [**brief**] [**latest**] [**reverse**] [**time**] Supported platforms: Firepower 4100/9300
FTD CLI command to permanently leave a cluster.	7.0	7.0	You can now use the FTD CLI to permanently remove a unit from the cluster, converting its configuration to a standalone device. New/modified commands: **cluster reset-interface-mode** Supported platforms: Firepower 4100/9300

Feature	Minimum FMC	Minimum FTD	Details
FTD NAT			
Prioritized system-defined NAT rules for FTD.	7.0	7.0	We added a new Section 0 to the NAT rule table. This section is exclusively for the use of the system. Any NAT rules that the system needs for normal functioning are added to this section, and these rules take priority over any rules you create. Previously, system-defined rules were added to Section 1, and user-defined rules could interfere with proper system functioning. You cannot add, edit, or delete Section 0 rules, but you will see them in **show nat detail** command output.
FTD Routing			
Virtual router support for the ISA 3000.	7.0	7.0	You can now configure up to 10 virtual routers on an ISA 3000 device.
FTD VPN: Site to Site			
Backup virtual tunnel interfaces (VTI) for route-based site-to-site VPN.	7.0	6.7	When you configure a site-to-site VPN that uses virtual tunnel interfaces, you can select a backup VTI for the tunnel. Specifying a backup VTI provides resiliency, so that if the primary connection goes down, the backup connection might still be functional. For example, you could point the primary VTI to the endpoint of one service provider, and the backup VTI to the endpoint of a different service provider. New/modified pages: We added the ability to add a backup VTI to the site-to-site VPN wizard when you select Route-Based as the VPN type for a point-to-point connection.
FTD VPN: Remote Access			
Load balancing.	7.0	7.0	We now support RA VPN load balancing. The system distributes sessions among grouped devices by number of sessions; it does not consider traffic volume or other factors. New/modified screens: We added load balancing options to the Advanced settings in an RA VPN policy.

Feature	Minimum FMC	Minimum FTD	Details
Local authentication.	7.0	7.0	We now support local authentication for RA VPN users. You can use this as the primary or secondary authentication method, or as a fallback in case the configured remote server cannot be reached. **1.** Create a local realm. Local usernames and passwords are stored in local realms. When you create a realm (**System** (⚙) > **Integration** > **Realms**) and select the new **LOCAL** realm type, the system prompts you to add one or more local users. **2.** Configure RA VPN to use local authentication. Create or edit an RA VPN policy (**Devices > VPN > Remote Access**), create a connection profile within that policy, then specify **LOCAL** as the primary, secondary, or fallback authentication server in that connection profile. **3.** Associate the local realm you created with an RA VPN policy. In the RA VPN policy editor, use the new **Local Realm** setting. Every connection profile in the RA VPN policy that uses local authentication will use the local realm you specify here.
Dynamic access policies.	7.0	Any	The new dynamic access policy allows you to configure remote access VPN authorization that automatically adapts to a changing environment: **1.** Configure HostScan by uploading the AnyConnect HostScan package as an AnyConnect file (**Objects > Object Management > VPN > AnyConnect File**). There is a new **HostScan Package** option in the **File Type** drop-down list. This module runs on endpoints and performs a posture assessment that the dynamic access policy will use. **2.** Create a dynamic access policy (**Devices > Dynamic Access Policy**). Dynamic access policies specify session attributes (such as group membership and endpoint security) that you want to evaluate each time a user initiates a session. You can then deny or grant access based on that evaluation. **3.** Associate the dynamic access policy you created with an RA VPN policy. In the remote access VPN policy editor, use the new **Dynamic Access Policy** setting.
Multi-certificate authentication.	7.0	7.0	We now support multi-certificate authentication for remote access VPN users. You can validate the machine or device certificate, to ensure the device is a corporate-issued device, in addition to authenticating the user's identity certificate to allow VPN access using the AnyConnect client during SSL or IKEv2 EAP phase.

Feature	Minimum FMC	Minimum FTD	Details
AnyConnect custom attributes.	7.0	7.0	We now support AnyConnect custom attributes, and provide an infrastructure to configure AnyConnect client features without adding explicit support for these features in the system.
Access Control: Threat Detection and Application Identification			
Snort 3 for FTD.	7.0	7.0	For new FTD deployments, Snort 3 is now the default inspection engine. Upgraded deployments continue to use Snort 2, but you can switch at any time. Advantages to using Snort 3 include, but are not limited to: • Improved performance. • Improved SMBv2 inspection. • New script detection capabilities. • HTTP/2 inspection. • Custom rule groups. • Syntax that makes custom intrusion rules easier to write. • Reasons for 'would have dropped' inline results in intrusion events. • No Snort restarts when deploying changes to the VDB, SSL policies, custom application detectors, captive portal identity sources, and TLS server identity discovery. • Improved serviceability, due to Snort 3-specific telemetry data sent to Cisco Success Network, and to better troubleshooting logs. A Snort 3 intrusion rule update is called an *LSP* (Lightweight Security Package) rather than an SRU. The system still uses SRUs for Snort 2; downloads from Cisco contain both the latest LSP and SRU. The system automatically uses the appropriate rule set for your configurations. The FMC can manage a deployment with both Snort 2 and Snort 3 devices, and will apply the correct policies to each device. However, unlike Snort 2, you cannot update Snort 3 on a device by upgrading the FMC only and then deploying. With Snort 3, new features and resolved bugs require you upgrade the software on the FMC *and* its managed devices. For information on the Snort included with each software version, see the *Bundled Components* section of the Cisco Firepower Compatibility Guide. **Important** Before you switch to Snort 3, we *strongly* recommend you read and understand the Firepower Management Center Snort 3 Configuration Guide. Pay special attention to feature limitations and migration instructions. Although upgrading to Snort 3 is designed for minimal impact, features do not map exactly. Careful planning and preparation can help you make sure that traffic handled as expected. You can also visit the Snort 3 website: https://snort.org/snort3.

Feature	Minimum FMC	Minimum FTD	Details
Access Control: Identity			
Cross-domain trust for Active Directory domains.	7.0	Any	You can now configure user identity rules with users from Microsoft Active Directory forests (groupings of AD domains that trust each other). New/modified pages: • You now configure a realm and directories at the same time. • A new Sync Results page (**System** (⚙) > **Integration** > **Sync Results**) displays any errors related to downloading users and groups in a cross-domain trust relationship.
Event Logging and Analysis			
Improved process for storing events in a Secure Network Analytics on-prem deployment.	7.0	7.0	A new Cisco Security Analytics and Logging (On Premises) app and a new FMC wizard make it easier to configure remote data storage for on-prem Secure Network Analytics solutions: **1.** Deploy hardware or virtual Stealthwatch appliances. You can use a Stealthwatch Management Console alone, or you can configure Stealthwatch Management Console, flow collector, and data store. **2.** Install the new Cisco Security Analytics and Logging (On Premises) app on your Stealthwatch Management Console to configure Stealthwatch as a remote data store. **3.** On the FMC, use one of the new wizards on **System** (⚙) > **Logging** > **Security Analytics & Logging** to connect to your Stealthwatch deployment. Note that the wizards replace the narrower-focus page where you used to configure Stealthwatch contextual cross-launch; that is now a step in the wizard. For upgraded deployments where you were using syslog to send Firepower events to Stealthwatch, disable those configurations before you use the wizard. Otherwise, you will get double events. To remove the syslog connection to Stealthwatch use FTD platform settings (**Devices > Platform Settings**); to disable sending events to syslog, edit your access control rules. For more information, including Stealthwatch hardware and software requirements, see *Cisco Security Analytics and Logging (On Premises): Firewall Event Integration Guide*.

Feature	Minimum FMC	Minimum FTD	Details
Work with events stored remotely in a Secure Network Analytics on-prem deployment.	7.0	Any	You can now use the FMC to work with connection events stored remotely in a Secure Network Analytics on-prem deployment. A new **Data Source** option on the connection events page (**Analysis > Connections > Events**) and in the unified event viewer (**Analysis > Unified Events**) allows you to choose which connection events you want to work with. The default is to display locally stored connection events, unless there are none in the time range. In that case, the system displays remotely stored events.. We also added a data source option to report templates (**Overview > Reporting > Report Templates**), so that you can generate reports based on remotely stored connection events. **Note** This feature is supported for connection events only; cross-launch is still the only way to examine remotely stored Security Intelligence, intrusion, file and malware events. Even in the unified event viewer, the system only displays locally stored events of those types. However, note that for every Security Intelligence event, there is an identical connection event—these are the events with reasons such as 'IP Block' or 'DNS Block.' You can work with those duplicated events on the connection events page or in the unified event viewer, but not on the dedicated Security Intelligence events page.
Store all connection events in the Secure Network Analytics cloud.	7.0	Any	You can now store all connection events in the Stealthwatch cloud using Cisco Security Analytics and Logging (SaaS). Previously, you were limited to security events: Security Intelligence, intrusion, file, and malware events, as well as their associated connection events. To change the events you send to the cloud, choose **System** (⚙) **> Integration**. On the **Cloud Services** tab, edit the **Cisco Cloud Event Configuration**. The old option to send high priority connection events to the cloud has been replaced with a choice of **All**, **None**, or **Security Events**. **Note** These settings also control which events you send to SecureX. However, even if you choose to send all connection events to the cloud, SecureX consumes only the security (higher priority) connection events. Also note that you now configure the SecureX connection itself on **Analysis > SecureX**.
Unified event viewer.	7.0	Any	The unified event viewer (**Analysis** > **Unified Events**) displays connection, Security Intelligence, intrusion, file, and malware events in a single table. This can help you look relationships between events of different types. A single search field allows you to dynamically filter the view based on multiple criteria, and a **Go Live** option displays events received from managed devices in real time.

Feature	Minimum FMC	Minimum FTD	Details
SecureX ribbon.	7.0	Any	The SecureX ribbon on the FMC pivots into SecureX for instant visibility into the threat landscape across your Cisco security products. To connect with SecureX and enable the ribbon, use **System** (⚙) > **SecureX**. Note that you must still use **System** (⚙) > **Integration** > **Cloud Services** to choose your cloud region and to specify which events to send to SecureX. For more information, see the *Cisco Secure Firewall Threat Defense and SecureX Integration Guide*.
Exempt all connection events from rate limiting when you turn off local storage.	7.0	Any	Event rate limiting applies to all events sent to the FMC, with the exception of security events: Security Intelligence, intrusion, file, and malware events, as well as their associated connection events. Now, disabling local connection event storage exempts *all* connection events from rate limiting, not just security events. To do this, set the **Maximum Connection Events** to zero on **System** (⚙) > **Configuration** > **Database**. **Note** Other than turning it off by setting it to zero, **Maximum Connection Events** does not govern connection event rate limiting. Any non-zero number in this field ensures that *all* lower-priority connection events are rate limited. Note that disabling local event storage does not affect remote event storage, nor does it affect connection summaries or correlation. The system still uses connection event information for features like traffic profiles, correlation policies, and dashboard displays.
Port and protocol displayed together in file and malware event tables.	7.0	Any	In file and malware event tables, the port field now displays the protocol, and you can search port fields for protocol. For events that existed before upgrade, if the protocol is not known, the system uses "tcp." New/modified pages: • **Analysis** > **Files** > **Malware Events** • **Analysis** > **Files** > **File Events**
Health Monitoring			

Feature	Minimum FMC	Minimum FTD	Details
New health modules.	7.0	Module dependent	We added the following health modules: • AMP Connection Status • AMP Threat Grid Status • ASP Drop • Advanced Snort Statistics • Chassis Status FTD • Event Stream Status • FMC Access Configuration Changes • FMC HA Status (replaces HA Status) • FTD HA Status • File System Integrity Check • Flow Offload • Hit Count • MySQL Status • NTP Status FTD • Rabbit MQ Status • Routing Statistics • SSE Connection Status • Sybase Status • Unresolved Groups Monitor • VPN Statistics • xTLS Counters Additionally, full support returns for the Configuration Memory Allocation module, which was introduced in Version 6.6.3 as the Appliance Configuration Resource Utilization module, but was not fully supported in Version 6.7.
Deployment and Policy Management			

Feature	Minimum FMC	Minimum FTD	Details
Dynamic objects.	7.0	7.0	You can now use *dynamic objects* in access control rules. A dynamic object is just a list of IP addresses/subnets (no ranges, no FQDN). But unlike a network object, changes to dynamic objects take effect immediately, without having to redeploy. This is useful in virtual and cloud environments, where IP addresses often dynamically map to workload resources. To create and manage dynamic objects, we recommend the Cisco Secure Dynamic Attributes Connector. The connector is a separate, lightweight application that quickly and seamlessly updates firewall policies based on workload changes. To do this, it gets workload attributes from tagged resources in your environment, and compiles an IP list based on criteria you specify (a "dynamic attributes filter"). It then creates a dynamic object on the FMC and populates it with the IP list. When your workload changes, the connector updates the dynamic object and the system immediately starts handling traffic based on the new mappings. For more information, see the *Cisco Secure Dynamic Attributes Connector Configuration Guide*. After you create a dynamic object, you can add it to access control rules on the new **Dynamic Attributes** tab in the access control rule editor. This tab replaces the narrower-focus **SGT/ISE Attributes** tab; continue to configure rules with SGT attributes here. **Note** You can also create a dynamic object on the FMC: **Objects > Object Management > External Attributes > Dynamic Objects**. However, this creates the container only; you must then populate and manage it using the REST API. See the Firepower Management Center REST API Quick Start Guide, Version 7.0. Supported virtual/cloud workloads for Cisco Secure Dynamic Attributes Connector integration: Microsoft Azure, AWS, VMware
Global search for policies and objects.	7.0	Any	You can now search for certain policies by name, and for certain objects by name and configured value. This feature is not available with the Classic theme. New/modified pages: We added capabilities to the **Search** icon and field on the FMC menu bar, to the left of the **Deploy** menu.
Selectively deploy RA and site-to-site VPN policies.	7.0	Any	Selective policy deployment, which was introduced in Version 6.6, now supports remote access and site-to-site VPN policies for FTD. New/modified pages: We added VPN policy options on the **Deploy > Deployment** page.
FTD Upgrade			
Improved FTD upgrade performance and status reporting.	7.0	7.0	FTD upgrades are now easier faster, more reliable, and take up less disk space. A new **Upgrades** tab in the Message Center provides further enhancements to upgrade status and error reporting.

Feature	Minimum FMC	Minimum FTD	Details
Upgrade wizard for FTD.	7.0	Any	A new device upgrade page (**Devices** > **Device Upgrade**) on the FMC provides an easy-to-follow wizard for upgrading Version 6.4+ FTD devices. It walks you through important pre-upgrade stages, including selecting devices to upgrade, copying the upgrade package to the devices, and compatibility and readiness checks. To begin, use the new **Upgrade Firepower Software** action on the Device Management page **Devices** > **Device Management** > **Selection**. As you proceed, the system displays basic information about your selected devices, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a device does not "pass" a stage in the wizard, it does not appear in the next stage. If you navigate away from wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the wizard. **Note** You must still use **System** > **Updates** to upload or specify the location of FTD upgrade packages. You must also use the System Updates page to upgrade the FMC itself, as well as all non-FTD managed devices. **Note** In Version 7.0, the wizard does not correctly display devices in clusters or high availability pairs. Even though you must select and upgrade these devices as a unit, the wizard displays them as standalone devices. Device status and upgrade readiness are evaluated and reported on an individual basis. This means it is possible for one unit to appear to "pass" to the next stage while the other unit or units do not. However, these devices are still grouped. Running a readiness check on one, runs it on all. Starting the upgrade on one, starts it on all. To avoid possible time-consuming upgrade failures, *manually* ensure all group members are ready to move on to the next step of the wizard before you click **Next**.
Upgrade more FTD devices at once.	7.0	Upgrades to 6.7+	The number of devices you can upgrade at once is now limited by your management network bandwidth—not the system's ability to manage simultaneous upgrades. Previously, we recommended against upgrading more than five devices at a time. **Important** Only upgrades to FTD Version 6.7+ using the FTD upgrade wizard see this improvement. If you are upgrading devices to an older FTD release—even if you are using the new upgrade wizard—we still recommend you limit to five devices at a time.

Feature	Minimum FMC	Minimum FTD	Details
Upgrade different device models together.	7.0	Any	You can now use the FTD upgrade wizard to queue and invoke upgrades for all FTD models at the same time, as long as the system has access to the appropriate upgrade packages. Previously, you would choose an upgrade package, then choose the devices to upgrade using that package. That meant that you could upgrade multiple devices at the same time *only* if they shared an upgrade package. For example, you could upgrade two Firepower 2100 series devices at the same time, but not a Firepower 2100 series and a Firepower 1000 series.
Administration and Troubleshooting			
Zero-touch restore for the ISA 3000 using the SD card.	7.0	7.0	When you perform a local backup, the backup file is copied to the SD card if present. To restore the configuration on a replacement device, simply install the SD card in the new device, and depress the Reset button for 3 to 15 seconds during the device bootup.
Security and Hardening			
New default password for AWS deployments.	7.0	7.0	For FMCv/FTDv for AWS, the default password for the admin account is now the AWS Instance ID, unless you define a default password with user data (**Advanced Details > User Data**) during the initial deployment. Previously, the default admin password was Admin123.
EST for certificate enrollment.	7.0	7.0	Support for Enrollment over Secure Transport for certificate enrollment was provided. New/modified pages: New enrollment options when configuring **Objects > PKI > Cert Enrollment > CA Information** tab.
Support for EdDSA certificate type.	7.0	7.0	A new certificate key type- EdDSA was added with key size 256. New/modified pages: New certificate key options when configuring **Objects > PKI > Cert Enrollment > Key** tab.
AES-128 CMAC authentication for NTP servers.	7.0	Any	You can now use AES-128 CMAC keys to secure connections between the FMC and NTP servers. New/modified pages: **System** (⚙) > **Configuration** > **Time Synchronization**.
SNMPv3 users can authenticate using a SHA-224 or SHA-384 authorization algorithm.	7.0	7.0	SNMPv3 users can now authenticate using a SHA-224 or SHA-384 algorithm. New/modified pages: **Devices > Platform Settings > SNMP > Users > Auth Algorithm Type**
Usability			
Report appearance has changed.	7.0	Any	To make reports appear cleaner and easier to read, we changed red color accents to gray and blue, removed background shading on table and chart titles, and removed alternating row colors in tables. New/modified pages: **Overview** > **Reporting**

Feature	Minimum FMC	Minimum FTD	Details
How-to location has changed.	7.0	Any	**Help** > **How-Tos** now invokes walkthroughs. Previously, you clicked **How-Tos** at the bottom of the browser window.
Performance			
Hardware crypto acceleration on FTDv using Intel QuickAssist Technology (QAT).	7.0	7.0	We now support hardware crypto acceleration (CBC cipher only) on FTDv for VMware and FTDv for KVM. This feature requires a Intel QAT 8970 PCI adapter/Version 1.7+ driver on the hosting platform. After you reboot, hardware crypto acceleration is automatically enabled.
Improved CPU usage and performance for many-to-one and one-to-many connections.	7.0	7.0	The system no longer creates local host objects and locks them when creating connections, except for connections that involve dynamic NAT/PAT and scanning threat detection and host statistics. This improves FTD performance and CPU usage in situations where many connections are going to the same server (such as a load balancer or web server), or one endpoint is making connections to many remote hosts. We changed the following commands: **clear local-host** (deprecated), **show local-host**
Deprecated Features			
End of support: VMware vSphere/VMware ESXi 6.0.	7.0	7.0	We discontinued support for virtual deployments on VMware vSphere/VMware ESXi 6.0. Upgrade the hosting environment to a supported version before you upgrade the Firepower software.
Deprecated: RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm.	7.0	7.0	**Prevents post-upgrade VPN connections through FTD devices.** We removed support for RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm. Before you upgrade, use the object manager to update your PKI certificate enrollments with stronger options: **Objects > PKI > Cert Enrollment**. Otherwise, although the upgrade preserves your current settings, VPN connections through the device will fail. To continue managing older FTD devices only (Version 6.4–6.7.x) with these weaker options, select the new **Enable Weak-Crypto** option for each device on the **Devices > Certificates** page.
Deprecated: MD5 authentication algorithm and DES encryption for SNMPv3 users.	7.0	7.0	**Deletes Users. Prevents post-upgrade deploy.** We removed support for the MD5 authentication algorithm and DES encryption for SNMPv3 users on FTD devices. Upgrading FTD to Version 7.0+ deletes these users from the device, regardless of the configurations on the FMC. If you are still using these options in your platform settings policy, change and verify your configurations before you upgrade FTD. These options are in the **Auth Algorithm Type** and **Encryption Type** drop-downs when creating or editing an SNMPv3 user in a Threat Defense platform settings policy: **Devices > Platform Settings**.

Feature	Minimum FMC	Minimum FTD	Details
Deprecated: Port 32137 comms with AMP clouds.	7.0	Any	**Prevents FMC upgrade.** We deprecated the FMC option to use port 32137 to obtain file disposition data from public and private AMP clouds. Unless you configure a proxy, the FMC now uses port 443/HTTPS. Before you upgrade, disable the **Use Legacy Port 32137 for AMP for Networks** option on the **System** (⚙) > **Integration** > **Cloud Services** page. Do not proceed with upgrade until your AMP for Networks deployment is working as expected.
Deprecated: HA Status health module.	7.0	Any	We renamed the HA Status health module to the *FMC* HA Status health module. This is to distinguish it from the new FTD HA Status module.
Deprecated: Legacy API Explorer.	7.0	Any	We removed support for the FMC REST API legacy API Explorer.
Deprecated: Geolocation details.	Any	Any	We no longer provide the geolocation IP package, which contained contextual data associated with routable IP addresses. This saves disk space and does not affect geolocation rules or traffic handling in any way. Any contextual data is now stale, and upgrading to most later versions deletes the IP package. Options to view contextual data have no effect, and are removed in later versions.

FDM Features in Version 7.0.x

Table 17: FDM Features in Version 7.0.x

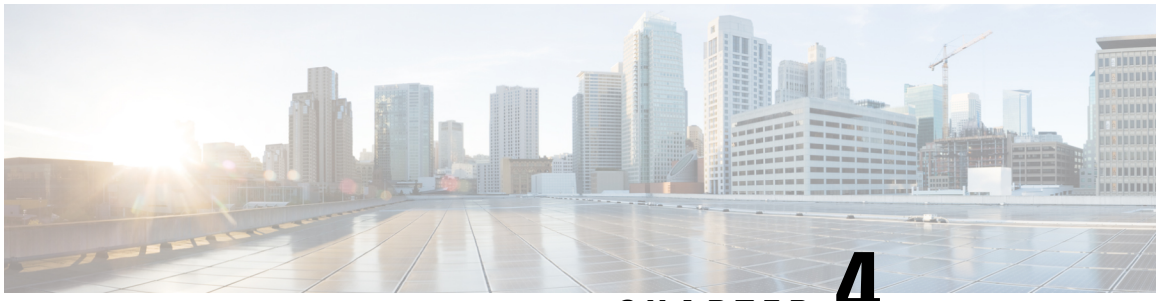
Feature	Description
Platform Features	
FTDv for HyperFlex and Nutanix.	We introduced FTDv for Cisco HyperFlex and Nutanix Enterprise Cloud.
FTDv for VMware vSphere/VMware ESXi 7.0.	You can now deploy FTDv on VMware vSphere/VMware ESXi 7.0. Note that Version 7.0 also discontinues support for VMware 6.0. Upgrade the hosting environment to a supported version before you upgrade the FTD.
New default password for the Firewall Threat Defense Virtual on AWS.	On AWS, the default admin password for the Firewall Threat Defense Virtual is the AWS Instance ID, unless you define a default password with user data (**Advanced Details** > **User Data**) during the initial deployment.

Feature	Description
ISA 3000 support for shutting down.	In Version 7.0.2+, you can shut down the ISA 3000; previously, you could only reboot the device. In Version 7.0.5+, when you shut down the ISA 3000, the System LED turns off. Wait at least 10 seconds after that before you remove power from the device. Version restrictions: Version 7.1 temporarily deprecates support for this feature. Support returns in Version 7.2.
Firewall and IPS Features	
New Section 0 for system-defined NAT rules.	A new Section 0 has been added to the NAT rule table. This section is exclusively for the use of the system. Any NAT rules that the system needs for normal functioning are added to this section, and these rules take priority over any rules you create. Previously, system-defined rules were added to Section 1, and user-defined rules could interfere with proper system functioning. You cannot add, edit, or delete Section 0 rules, but you will see them in **show nat detail** command output.
Custom intrusion rules for Snort 3.	You can use offline tools to create custom intrusion rules for use with Snort 3, and upload them into an intrusion policy. You can organize custom rules in your own custom rule groups, to make it easy to update them as needed. You can also create the rules directly in Firewall Device Manager, but the rules have the same format as uploaded rules. Firewall Device Manager does not guide you in creating the rules. You can duplicate existing rules, including system-defined rules, as a basis for a new intrusion rule. We added support for custom groups and rules to the **Policies** > **Intrusion** page, when you edit an intrusion policy.
Snort 3 new features for Firewall Device Manager-managed systems.	You can now configure the following additional features when using Snort 3 as the inspection engine on an Firewall Device Manager-managed system: • Time-based access control rules. (Firewall Threat Defense API only.) • Multiple virtual routers. • The decryption of TLS 1.1 or lower connections using the SSL Decryption policy. • The decryption of the following protocols using the SSL Decryption policy: FTPS, SMTPS, IMAPS, POP3S.
DNS request filtering based on URL category and reputation.	You can apply your URL filtering category and reputation rules to DNS lookup requests. If the fully-qualified domain name (FQDN) in the lookup request has a category and reputation that you are blocking, the system blocks the DNS reply. Because the user does not receive a DNS resolution, the user cannot complete the connection. Use this option to apply URL category and reputation filtering to non-web traffic. You must have the URL filtering license to use this feature. We added the **Reputation Enforcement on DNS Traffic** option to the access control policy settings.

Feature	Description
Smaller VDB for lower memory devices with Snort 2.	**Upgrade impact. Application identification on lower memory devices is affected.** For Version 7.0.6+ devices with Snort 2, for VDB 363+, the system now installs a smaller VDB (also called *VDB lite*) on lower memory devices running Snort 2. This smaller VDB contains the same applications, but fewer detection patterns. Devices using the smaller VDB can miss some application identification versus devices using the full VDB. Lower memory devices: ASA-5508-X, ASA-5516-X Version restrictions: The smaller VDB is not supported in all versions. If you upgrade from a supported version to an unsupported version, you cannot install VDB 363+ on lower memory devices running Snort 2. For a list of affected releases, see CSCwd88641.
VPN Features	
Firewall Device Manager SSL cipher settings for remote access VPN.	You can define the TLS versions and encryption ciphers to use for remote access VPN connections in Firewall Device Manager. Previously, you needed to use the Firewall Threat Defense API to configure SSL settings. We added the following pages: **Objects** > **SSL Ciphers**; **Device** > **System Settings** > **SSL Settings**.
Support for Diffie-Hellman group 31.	You can now use Diffie-Hellman (DH) group 31 in IKEv2 proposals and policies.
The maximum number of Virtual Tunnel Interfaces on the device is 1024.	The maximum number of Virtual Tunnel Interfaces (VTI) that you can create is 1024. In previous versions, the maximum was 100 per source interface.
IPsec lifetime settings for site-to-site VPN security associations.	You can change the default settings for how long a security association is maintained before it must be re-negotiated. We added the **Lifetime Duration** and **Lifetime Size** options to the site-to-site VPN wizard.
Routing Features	
Virtual router support for the ISA 3000.	You can configure up to 10 virtual routers on an ISA 3000 device.
Equal-Cost Multi-Path (ECMP) routing.	You can configure ECMP traffic zones to contain multiple interfaces, which lets traffic from an existing connection exit or enter the Firewall Threat Defense device on any interface within the zone. This capability allows Equal-Cost Multi-Path (ECMP) routing on the Firewall Threat Defense device as well as external load balancing of traffic to the Firewall Threat Defense device across multiple interfaces. ECMP traffic zones are used for routing only. They are not the same as security zones. We added the **ECMP Traffic Zones** tab to the Routing pages. In the Firewall Threat Defense API, we added the ECMPZones resources.
Interface Features	
New default inside IP address.	The default IP address for the inside interface is being changed to **192.168.95.1** from 192.168.1.1 to avoid an IP address conflict when an address on 192.168.1.0/24 is assigned to the outside interface using DHCP.

Feature	Description
Default outside IP address now has IPv6 autoconfiguration enabled; new default IPv6 DNS server for Management.	The default configuration on the outside interface now includes IPv6 autoconfiguration, in addition to the IPv4 DHCP client. The default Management DNS servers now also include an IPv6 server: 2620:119:35::35.
EtherChannel support for the ISA 3000.	You can now use Firewall Device Manager to configure EtherChannels on the ISA 3000. New/modified screens: **Devices** > **Interfaces** > **EtherChannels**
Licensing Features	
Performance-Tiered Licensing for Firewall Threat Defense Virtual.	The Firewall Threat Defense Virtual now supports performance-tiered Smart Licensing based on throughput requirements and RA VPN session limits. When the Firewall Threat Defense Virtual is licensed with one of the available performance licenses, two things occur. First, a rate limiter is installed that limits the device throughput to a specified level. Second, the number of VPN sessions is capped to the level specified by the license.
Administrative and Troubleshooting Features	
DHCP relay configuration using the Firewall Threat Defense API.	**Upgrade impact. Can prevent post-upgrade deploy.** You can use the Firewall Threat Defense API to configure DHCP relay. Using DHCP relay on an interface, you can direct DHCP requests to a DHCP server that is accessible through the other interface. You can configure DHCP relay on physical interfaces, subinterfaces, EtherChannels, and VLAN interfaces. You cannot configure DHCP relay if you configure a DHCP server on any interface. Note that if you used FlexConfig in prior releases to configure DHCP relay (the **dhcprelay** command), you must re-do the configuration using the API, and delete the FlexConfig object, after you upgrade. We added the following model to the Firewall Threat Defense API: dhcprelayservices
Faster bootstrap processing and early login to Firewall Device Manager.	The process to initially bootstrap an Firewall Device Manager-managed system has been improved to make it faster. Thus, you do not need to wait as long after starting the device to log into Firewall Device Manager. In addition, you can now log in while the bootstrap is in progress. If the bootstrap is not complete, you will see status information on the process so you know what is happening on the device.
Improved CPU usage and performance for many-to-one and one-to-many connections.	The system no longer creates local host objects and locks them when creating connections, except for connections that involve dynamic NAT/PAT and scanning threat detection and host statistics. This improves performance and CPU usage in situations where many connections are going to the same server (such as a load balancer or web server), or one endpoint is making connections to many remote hosts. We changed the following commands: **clear local-host** (deprecated), **show local-host**
Upgrade readiness check for Firewall Device Manager-managed devices.	You can run an upgrade readiness check on an uploaded Firewall Threat Defense upgrade package before attempting to install it. The readiness check verifies that the upgrade is valid for the system, and that the system meets other requirements needed to install the package. Running an upgrade readiness check helps you avoid failed installations. A link to run the upgrade readiness check was added to the **System Upgrade** section of the **Device** > **Updates** page.

Feature	Description
Automatically update CA bundles.	**Upgrade impact. The system connects to Cisco for something new.** The local CA bundle contains certificates to access several Cisco services. The system now automatically queries Cisco for new CA certificates at a daily system-defined time. Previously, you had to upgrade the software to update CA certificates. You can use the CLI to disable this feature. New resources: https://cisco.com/security/pki/ New/modified CLI commands: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** Version restrictions: Requires Version 7.0.5, 7.1.0.3, or 7.2.4+. See: *Cisco Secure Firewall Threat Defense Command Reference*
Require the Message-Authenticator attribute in all RADIUS responses.	**Upgrade impact. For the Firepower 4100/9300, check FXOS compatibility before you upgrade Firewall Threat Defense. After Firewall Threat Defense upgrade, enable the option for existing servers.** You can now require the Message-Authenticator attribute in all RADIUS responses, ensuring that the Firewall Threat Defense VPN gateway securely verifies every response from the RADIUS server, whether for RA VPN or access to the device itself. The **Require Message-Authenticator for all RADIUS Responses** option is enabled by default for new RADIUS servers. We also recommend you enable it for existing servers. Disabling it may expose firewalls to potential attacks. New CLI commands: **message-authenticator-required** Version restrictions: Requires Version 7.0.7, 7.2.10, 7.4.3, 7.6.1, or 7.7+. For the Firepower 4100/9300, may require an FXOS upgrade; for minimum builds, see *Cisco Secure Firewall Threat Defense Compatibility Guide*.
Firewall Threat Defense REST API version 6.1 (v6).	The Firewall Threat Defense REST API for software version 7.0 is version 6.1 You can use v6 in the API URLs, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. Note that the URL version path element for 6.1 is the same as 6.0: v6. Please re-evaluate all existing calls, as changes might have been mode to the resource models you are using. To open the API Explorer, where you can view the resources, log into Firewall Device Manager, then click the more options button (⋮) and choose **API Explorer**.



CHAPTER 4

Upgrade Guidelines

This document provides critical and release-specific upgrade guidelines for Version 7.0.

- Planning Your Upgrade, on page 43
- Minimum Version to Upgrade, on page 44
- Upgrade Guidelines for Version 7.0, on page 45
- Upgrade Guidelines for Cloud-Delivered Firewall Management Center, on page 55
- Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 55
- Unresponsive Upgrades, on page 56
- Revert or Uninstall the Upgrade, on page 56
- Traffic Flow and Inspection, on page 59
- Traffic Flow and Inspection when Deploying Configurations, on page 63
- Time and Disk Space, on page 64

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: https://cisco.com/go/threatdefense-70-docs.

Table 18: 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.

Planning Phase	Includes
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.
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 7.0, including maintenance releases, as follows.

Table 19: Minimum Version to Upgrade to Version 7.0

Platform	Minimum Version
FMC	6.4
FTD	6.4 FXOS 2.10.1.331 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, 2.10(1).
ASA with FirePOWER Services	6.4 See Device Platforms, on page 8 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	6.4

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 7.0

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

Table 20: Upgrade Guidelines for Firewall Threat Defense with Firewall Management Center Version 7.0

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 44	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 71, 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 Cloud-Delivered Firewall Management Center, on page 55	Firewall Threat Defense	Any	Any
	Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 55	Firepower 4100/9300	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				
	Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0, on page 47	Any	7.0.4+	7.1.0 only
	End of Support for Cisco Secure Firewall Threat Defense 7.0.x with Cloud-delivered Firewall Management Center	Any	7.0.3–7.0.x	Any
	Reconnect with Cisco Threat Grid for High Availability Firewall Management Centers, on page 47	Firewall Management Center	6.4.0 through 6.7.x	7.0+

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 47	Firepower 1010	6.4.0 through 6.6.x	6.7+
	Firewall Management Center Virtual Requires 28 GB RAM for Upgrade, on page 48	FMCv	6.2.3 through 6.5.0.x	6.6+
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 49	Firepower 1000 series	6.4.0.x	6.5+
	New URL Categories and Reputations, on page 49	Any	6.2.3 through 6.4.0.x	6.5+

Table 21: Upgrade Guidelines for Firewall Threat Defense with Firewall Device Manager Version 7.0

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 44	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 71, 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 55	Firepower 4100/9300	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				
	Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0, on page 47	Any	7.0.4+	7.1.0 only
	Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 47	Firepower 1010	6.4.0 through 6.6.x	6.7+
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 49	Firepower 1000 series	6.4.0.x	6.5+

✓	Guideline	Platforms	Upgrading From	Directly To
	Historical Data Removed During Firewall Threat Defense Upgrade with Firewall Device Manager, on page 49	Any	6.2.3 through 6.4.0.x	6.5+
	New URL Categories and Reputations, on page 49	Any	6.2.3 through 6.4.0.x	6.5+

Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0

Deployments: Any

Upgrading from: Version 7.0.4 or later maintenance release

Directly to: Version 7.1.0 only

Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4+ to Version 7.1.0. We recommend you upgrade directly to Version 7.2+.

Reconnect with Cisco Threat Grid for High Availability Firewall Management Centers

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

Upgrading from: Version 6.4.0 through 6.7.x

Directly to: Version 7.0.0+

Related bug: CSCvu35704

Version 7.0.0 fixes an issue with high availability where, after failover, the system stopped submitting files for dynamic analysis. For the fix to take effect, you must reassociate with the Cisco Threat Grid public cloud.

After you upgrade the high availability pair, on the primary Firewall Management Center:

1. Choose **AMP** > **Dynamic Analysis Connections**.
2. Click **Associate** in the table row corresponding to the public cloud.

   A portal window opens. You do not have to sign in. The reassociation happens in the background, within a few minutes.

Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs

Deployments: Firepower 1010

Upgrading from: Version 6.4 through 6.6

Directly to: Version 6.7+

For the Firepower 1010, Firewall Threat Defense upgrades to Version 6.7+ will fail if you configured switch ports with a VLAN ID in the 3968–4047 range. These IDs are for internal use only.

Firewall Management Center Virtual Requires 28 GB RAM for Upgrade

Deployments: Firewall Management Center Virtual

Upgrading from: Version 6.2.3 through 6.5

Directly to: Version 6.6+

All Firewall Management Center Virtual implementations now have the same RAM requirements: 32 GB recommended, 28 GB required (64 GB for FMCv 300). Upgrades to Version 6.6+ will fail if you allocate less than 28 GB to the virtual appliance. After upgrade, the health monitor will alert if you lower the memory allocation.

These new memory requirements enforce uniform requirements across all virtual environments, improve performance, and allow you to take advantage of new features and functionality. We recommend you do not decrease the default settings. To improve performance, you can increase a virtual appliance's memory and number of CPUs, depending on your available resources. For details, see the *Cisco Secure Firewall Management Center Virtual Getting Started Guide*.



Note As of the Version 6.6.0 release, lower-memory instance types for cloud-based Firewall Management Center Virtual deployments (AWS, Azure) are fully deprecated. You cannot create new instances using them, even for earlier versions. You can continue running existing instances.

This table summarizes pre-upgrade requirements for lower-memory deployments.

Table 22: Firewall Management Center Virtual Memory Requirements for Version 6.6+ Upgrades

Platform	Pre-Upgrade Action	Details
VMware	Allocate 28 GB minimum/32 GB recommended.	Power off the virtual machine first. For instructions, see the VMware documentation.
KVM	Allocate 28 GB minimum/32 GB recommended.	For instructions, see the documentation for your KVM environment.
AWS	Resize instances: • **From** c3.xlarge **to** c3.4xlarge. • **From** c3.2.xlarge **to** c3.4xlarge. • **From** c4.xlarge **to** c4.4xlarge. • **From** c4.2xlarge **to** c4.4xlarge. We also offer a c5.4xlarge instance for new deployments.	Stop the instance before you resize. Note that when you do this, data on the instance store volume is lost, so migrate your instance store-backed instance first. Additionally, if your management interface does not have an Elastic IP address, its public IP address is released. For instructions, see the documentation on changing your instance type in the AWS user guide for Linux instances.

Platform	Pre-Upgrade Action	Details
Azure	Resize instances: • **From** Standard_D3_v2 **to** Standard_D4_v2.	Use the Azure portal or PowerShell. You do not need to stop the instance before you resize, but stopping may reveal additional sizes. Resizing restarts a running virtual machine. For instructions, see the Azure documentation on resizing a Windows VM.

Firepower 1000 Series Devices Require Post-Upgrade Power Cycle

Deployments: Firepower 1000 series

Upgrading from: Version 6.4.0.x

Directly to: Version 6.5.0+

Version 6.5.0 introduces an FXOS CLI 'secure erase' feature for Firepower 1000/2100 and Firepower 4100/9300 series devices.

For Firepower 1000 series devices, you must power cycle the device after you upgrade to Version 6.5.0+ for this feature to work properly. The automatic reboot is not sufficient. Other supported devices do not require the power cycle.

Historical Data Removed During Firewall Threat Defense Upgrade with Firewall Device Manager

Deployments: Firewall Threat Defense with Firewall Device Manager

Upgrading from: Version 6.2.3 through 6.4.0.x

Directly to: 6.5.0+

All historical report data is removed during the upgrade due to a database schema change. After the upgrade, you cannot query historical data, nor view historical data in dashboards.

New URL Categories and Reputations

Deployments: Any

Upgrading from: Version 6.2.3 through 6.4.0.x

Directly to: Version 6.5.0+

Talos Intelligence Group has introduced new categories and renamed reputations to classify and filter URLs. For detailed lists of category changes, see the Cisco Firepower Release Notes, Version 6.5.0. For descriptions of the new URL categories, see the Talos Intelligence Categories site.

Also new are the concepts of uncategorized and reputationless URLs, although rule configuration options stay the same:

- *Uncategorized URLs* can have a Questionable, Neutral, Favorable, or Trusted reputation.

You can filter **Uncategorized** URLs but you cannot further constrain by reputation. These rules will match all uncategorized URLs, regardless of reputation.

Note that there is no such thing as an Untrusted rule with no category. Otherwise uncategorized URLs with an Untrusted reputation are automatically assigned to the new Malicious Sites threat category.

- *Reputationless URLs* can belong to any category.

  You cannot filter reputationless URLs. There is no option in the rule editor for 'no reputation.' However, you can filter URLs with **Any** reputation, which includes reputationless URLs. These URLs must also be constrained by category. There is no utility to an Any/Any rule.

The following table summarizes the changes on upgrade. Although they are designed for minimal impact and will not prevent post-upgrade deploy for most customers, we *strongly* recommend you review these release notes and your current URL filtering configuration. Careful planning and preparation can help you avoid missteps, as well as reduce the time you spend troubleshooting post-upgrade.

Table 23: Deployment Changes on Upgrade

Change	Details
Modifies URL rule categories.	The upgrade modifies URL rules to use the nearest equivalents in the new category set, in the following policies: • Access control • SSL • QoS (FMC only) • Correlation (FMC only) These changes may create redundant or preempted rules, which can slow performance. If your configuration includes merged categories, you may experience minor changes to the URLs that are allowed or blocked.
Renames URL rule reputations.	The upgrade modifies URL rules to use the new reputation names: **1.** Untrusted (was *High Risk*) **2.** Questionable (was *Suspicious sites*) **3.** Neutral (was *Benign sites with security risks*) **4.** Favorable (was *Benign sites*) **5.** Trusted (was *Well Known*)
Clears the URL cache.	The upgrade clears the URL cache, which contains results that the system previously looked up in the cloud. Your users may temporarily experience slightly longer access times for URLs that are not in the local data set.
Labels 'legacy' events.	For already-logged events, the upgrade labels any associated URL category and reputation information as `Legacy`. These legacy events will age out of the database over time.

Pre-Upgrade Actions for URL Categories and Reputations

Before upgrade, take the following actions.

Table 24: Pre-Upgrade Actions

Action	Details

Make sure your appliances can reach Talos resources.	The system must be able to communicate with the following Cisco resources after the upgrade:
	• https://regsvc.sco.cisco.com/ — Registration
	• https://est.sco.cisco.com/ — Obtain certificates for secure communications
	• https://updates-talos.sco.cisco.com/ — Obtain client/server manifests
	• http://updates.ironport.com/ — Download database (note: uses port 80)
	• https://v3.sds.cisco.com/ — Cloud queries
	
	The cloud query service also uses the following IP address blocks:
	• IPv4 cloud queries:
	  • 146.112.62.0/24
	  • 146.112.63.0/24
	  • 146.112.255.0/24
	  • 146.112.59.0/24
	• IPv6 cloud queries:
	  • 2a04:e4c7:ffff::/48
	  • 2a04:e4c7:fffe::/48

Identify potential rule issues.	Understand the upcoming changes. Examine your current URL filtering configuration and determine what post-upgrade actions you will need to take (see the next section). **Note** You may want to modify URL rules that use deprecated categories now. Otherwise, rules that use them will prevent deploy after the upgrade. In FMC deployments, we recommend you generate an *access control policy report*, which provides details on the policy's current saved configuration, including access control rules and rules in subordinate policies (such as SSL). For each URL rule, you can see the current categories, reputations, and associated rule actions. On the FMC, choose **Policies** > **Access Control**, then click the report icon () next to the appropriate policy.

Post-Upgrade Actions for URL Categories and Reputations

After upgrade, you should reexamine your URL filtering configuration and take the following actions as soon as possible. Depending on deployment type and the changes made by the upgrade, some — but not all — issues may be marked in the GUI. For example, in access control policies on FMC/FDM, you can click **Show Warnings** (FMC) or **Show Problem Rules** (FDM).

Table 25: Post-Upgrade Actions

Action	Details
Remove **deprecated categories** from rules. Required.	The upgrade does not modify URL rules that use deprecated categories. Rules that use them will prevent deploy. On the FMC, these rules are marked.
Create or modify rules to include the **new categories**.	Most of the new categories identify threats. We strongly recommend you use them. On the FMC, these new categories are not marked after *this* upgrade, but Talos may add additional categories in the future. When that happens, new categories are marked.
Evaluate rules changed as a result of **merged categories**.	Each rule that included any of the affected categories now include all of the affected categories. If the original categories were associated with different reputations, the new rule is associated with the broader, more inclusive reputation. To filter URLs as before, you may have to modify or delete some configurations; see Guidelines for Rules with Merged URL Categories, on page 53. Depending on what changed and how your platform handles rule warnings, changes may be marked. For example, the FMC marks wholly redundant and wholly preempted rules, but not rules that have partial overlap.
Evaluate rules changed as a result of **split categories**.	The upgrade replaces each old, single category in URL rules with *all* the new categories that map to the old one. This will not change the way you filter URLs, but you can modify affected rules to take advantage of the new granularity. These changes are not marked.
Understand which categories were **renamed** or are **unchanged**.	Although no action is required, you should be aware of these changes. These changes are not marked.
Evaluate how you handle **uncategorized** and **reputationless** URLs.	Even though it is now possible to have uncategorized and reputationless URLs, you cannot still cannot filter uncategorized URLs by reputation, nor can you filter reputationless URLs. Make sure that rules that filter by the **Uncategorized** category, or by **Any** reputation, will behave as you expect.

Guidelines for Rules with Merged URL Categories

When you examine your URL filtering configuration before the upgrade, determine which of the following scenarios and guidelines apply to you. This will ensure that your post-upgrade configuration is as you expect, and that you can take quick action to resolve any issues.

Table 26: Guidelines for Rules with Merged URL Categories

Guideline	Details
Rule Order Determines Which Rule Matches Traffic	When considering rules that include the same category, remember that traffic matches the first rule in the list that includes the condition.
Categories in the Same Rule vs Categories in Different Rules	Merging categories in a single rule will merge into a single category in the rule. For example, if Category A and Category B are merging to become Category AB, and you have a rule with both Category A and Category B, then after merge the rule will have a single Category AB. Merging categories in different rules will result in separate rules with the same category in each rule after the merge. For example, if Category A and Category B are merging to become Category AB, and you have Rule 1 with Category A and Rule 2 with Category B, then after merge Rule 1 and Rule 2 will each include Category AB. How you choose to resolve this situation depends on the rule order, on the actions and reputation levels associated with the rules, on the other URL categories included in the rule, and on the non-URL conditions that are included in the rule.
Associated Action	If merged categories in different rules were associated with different actions, then after merge you may have two or more rules with different actions for the same category.
Associated Reputation Level	If a single rule includes categories that were associated with different reputation levels before merging, the merged category will be associated with the more inclusive reputation level. For example, if Category A was associated in a particular rule with **Any reputation** and Category B was associated in the same rule with reputation level **3 - Benign sites with security risks**, then after merge Category AB in that rule will be associated with **Any reputation**.
Duplicate and Redundant Categories and Rules	After merge, different rules may have the same category associated with different actions and reputation levels. Redundant rules may not be exact duplicates, but they may no longer match traffic if another rule earlier in the rule order matches instead. For example, if you have pre-merge Rule 1 with Category A that applies to Any Reputation, and Rule 2 with Category B that applies only to Reputation 1-3, then after merge, both Rule 1 and Rule 2 will have Category AB, but Rule 2 will never match if Rule 1 is higher in the rule order. On the FMC, rules with an identical category and reputation will show a warning. However, these warnings will not indicate rules that include the same category but a different reputation. Caution: Consider all conditions in the rule when determining how to resolve duplicate or redundant categories.

Guideline	Details
Other URL Categories in a Rule	Rules with merged URLs may also include other URL categories. Therefore, if a particular category is duplicated after merge, you may want to modify rather than delete these rules.
Non-URL Conditions in a Rule	Rules with merged URL categories may also include other rule conditions, such as application conditions. Therefore, if a particular category is duplicated after merge, you may want to modify rather than delete these rules.

The examples in the following table use Category A and Category B, now merged into Category AB. In two-rule examples, Rule 1 comes before Rule 2.

Table 27: Examples of Rules with Merged URL Categories

Scenario	Before Upgrade	After Upgrade
Merged categories in the same rule	Rule 1 has Category A and Category B.	Rule 1 has Category AB.
Merged categories in different rules	Rule 1 has Category A. Rule 2 has Category B.	Rule 1 has Category AB. Rule 2 has Category AB. The specific result varies by the rules' order in the list, reputation levels, and associated actions. You should also consider all other conditions in the rule when determining how to resolve any redundancy.
Merged categories in different rules have different actions (Reputation is the same)	Rule 1 has Category A set to Allow. Rule 2 has Category B set to Block. (Reputation is the same)	Rule 1 has Category AB set to Allow. Rule 2 has Category AB set to Block. Rule 1 will match all traffic for this category. Rule 2 will never match traffic, and will display a warning indicator if you show warnings after merge, because both category and reputation are the same.
Merged categories in the same rule have different reputation levels	Rule 1 includes: Category A with Reputation Any Category B with Reputation 1-3	Rule 1 includes Category AB with Reputation Any.

Scenario	Before Upgrade	After Upgrade
Merged categories in different rules have different reputation levels	Rule 1 includes Category A with Reputation Any. Rule 2 includes Category B with Reputation 1-3.	Rule 1 includes Category AB with Reputation Any. Rule 2 includes Category AB with Reputation 1-3. Rule 1 will match all traffic for this category. Rule 2 will never match traffic, but you will not see a warning indicator because the reputations are not identical.

Upgrade Guidelines for Cloud-Delivered Firewall Management Center

You do not upgrade the Cloud-Delivered Firewall Management Center. We take care of feature updates. To upgrade Firewall Threat Defense with the Cloud-Delivered Firewall Management Center, see the Secure Firewall Threat Defense upgrade guides for Cloud-Delivered Firewall Management Center.

Upgrade Guidelines for the Firepower 4100/9300 Chassis

For the Firepower 4100/9300, major Firewall Threat Defense 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 28: Upgrade Guidelines for the Firepower 4100/9300 Chassis

Guideline	Details
FXOS upgrades.	FXOS 2.10.1.331+ is required to run threat defense Version 7.0 on the Firepower 4100/9300. 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 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 59.

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.

Unresponsive Firewall Management Center or Classic Device Upgrade

Do not restart an upgrade in progress. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Unresponsive Firewall Threat Defense Upgrade

For major and maintenance upgrades, you can manually cancel failed or in-progress upgrades, and retry failed upgrades:

- Firewall Management Center: Use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page, and from the Message Center.
- Firewall Device Manager: Use the System Upgrade panel.

You can also use the Firewall Threat Defense CLI.

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

This feature is not supported for patches or for upgrades from Version 6.6 and earlier.

Revert or Uninstall the Upgrade

If an upgrade succeeds but the system does not function to your expectations, you may be able to revert or uninstall:

- Revert is supported for major and maintenance upgrades to FTD with FDM.

  See System Management in the FDM configuration guide.

- Uninstall is supported for most patches in FMC and ASDM deployments.

  See Uninstall a Patch in the FMC upgrade guide, or Uninstall ASA FirePOWER Patches with ASDM, on page 57 in these release notes.

If this will not work for you and you still need to return to an earlier version, you must reimage.

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 29: 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.

Procedure

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 30: Traffic Flow and Inspection: FXOS Upgrades

Firewall Threat Defense 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 Firewall Threat Defense Upgrades with Firewall Management Center

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 31: 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.

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 32: 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 Firewall Threat Defense Upgrades with Firewall Device Manager

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.

Software Revert (Major/Maintenance Releases)

Traffic is dropped while you revert. In a high availability deployment, revert is more successful when you revert both units simultaneously. Traffic flow and inspection resume when the first unit comes back online.

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 33: 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 34: 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 35: 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.

Traffic Flow and Inspection when Deploying Configurations

Snort typically restarts during the first deployment immediately after upgrade. This means that for Firewall Management Center upgrades, Snort could restart on all managed devices. Snort does not restart after subsequent deployments unless, before deploying, you modify specific policy or device configurations.

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.

Table 36: 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.

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.

Time and Disk Space

Time to Upgrade

We recommend you track and record your own upgrade times so you can use them as future benchmarks. The following table lists some things that can affect upgrade time.

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not 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, you can find troubleshooting information in the upgrade guide: https://www.cisco.com/go/ftd-upgrade. If you continue to have issues, contact Cisco TAC.

Table 37: Upgrade Time Considerations

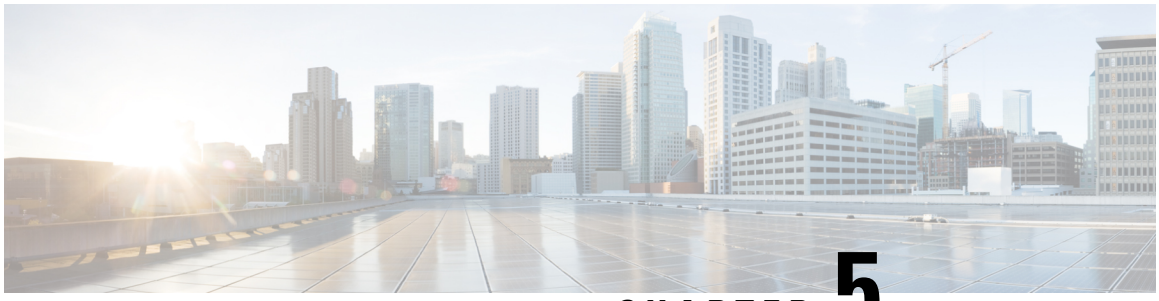
Consideration	Details
Versions	Upgrade time usually increases if your upgrade skips versions.
Models	Upgrade time usually increases with lower-end models.
Virtual appliances	Upgrade time in virtual deployments is highly hardware dependent.
High availability and clustering	In a high availability or clustered 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	Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how they 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	You may need additional time to perform operating system or virtual hosting upgrades, upgrade package transfers, readiness checks, VDB and intrusion rule (SRU/LSP) updates, configuration deployment, and other related tasks.

Disk Space to Upgrade

To upgrade, the upgrade package must be on the appliance. For device upgrades, you must also have enough space on the Firewall Management Center (in either /Volume or /var) for the device upgrade package. Or, you can use an internal server to store them. Readiness checks should indicate whether you have enough disk space to perform the upgrade. Without enough free disk space, the upgrade fails.

Table 38: Checking Disk Space

Platform	Command
Firewall Management Center	Choose **System** (⚙) > **Monitoring** > **Statistics** and select the Firewall Management Center. Under Disk Usage, expand the By Partition details.
Firewall Threat Defense with Firewall Management Center	Choose **System** (⚙) > **Monitoring** > **Statistics** and select the device you want to check. Under Disk Usage, expand the By Partition details.
Firewall Threat Defense with Firewall Device Manager	Use the **show disk** CLI command.



CHAPTER 5

Install the Software

If you cannot or do not want to upgrade to Version 7.0, you can freshly install major and maintenance releases. This is also called *reimaging*. We do not provide installation packages for patches. To run a particular patch, install the appropriate major or maintenance release, then apply the patch.

- Installation Guidelines, on page 67
- Installation Guides, on page 69

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

If you do not have physical access to an appliance, reimaging to the current major or maintenance release lets you keep management network settings. This allows you to connect to the appliance after you reimage to perform the initial configuration. Note that if you delete network settings or if you reimage to an earlier release, you must have physical access to the appliance. You cannot use Lights-Out Management (LOM).

For devices, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In Firewall Management Center deployments, you should also able to access the Firewall Management Center'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 Firewall Management Center. 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 39: Scenarios for Unregistering from CSSM (Not Restoring from Backup)

Scenario	Action
Reimage the Firewall Management Center.	Unregister manually.
Model migration for the Firewall Management Center.	Unregister manually, before you shut down the source Firewall Management Center.
Reimage Firewall Threat Defense with Firewall Management Center.	Unregister automatically, by removing the device from the Firewall Management Center.
Reimage Firewall Threat Defense with Firewall Device Manager.	Unregister manually.
Switch Firewall Threat Defense from Firewall Management Center to Firewall Device Manager.	Unregister automatically, by removing the device from the Firewall Management Center.
Switch Firewall Threat Defense from device manager to Firewall Management Center.	Unregister manually.

Removing Devices from the Firewall Management Center

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

Table 40: Scenarios for Removing Devices from the Firewall Management Center (Not Restoring from Backup)

Scenario	Action
Reimage the Firewall Management Center.	Remove all devices from management.
Reimage Firewall Threat Defense.	Remove the one device from management.
Switch Firewall Threat Defense from Firewall Management Center to Firewall Device Manager.	Remove the one device from management.

Fully Reimaging Firewall Threat Defense Hardware to Downgrade FXOS

For Firewall Threat Defense 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 41: Scenarios for Full Reimages

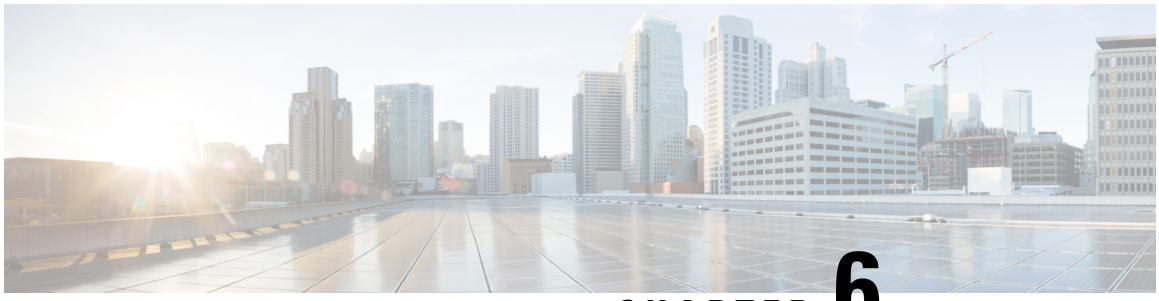
Model	Details
Firepower 1000 series Firepower 2100 series	If you use the **erase configuration** method to reimage, FXOS may not downgrade along with the software. This can cause failures, especially in high availability deployments. We recommend that you perform full reimages of these devices.
Firepower 4100/9300	Reverting Firewall Threat Defense does not downgrade FXOS. Major Firewall Threat Defense versions have a specially qualified and recommended companion FXOS version. After you return to the earlier version of Firewall Threat Defense, you may be running a non-recommended version of FXOS (too new). Although newer versions of FXOS are backwards compatible with older Firewall Threat Defense 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 42: Installation Guides

Platform	Guide
Firewall Management Center	
FMC 1600, 2600, 4600	*Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide*
FMC 1000, 2500, 4500	*Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide*
Firewall Management Center Virtual	*Cisco Secure Firewall Management Center Virtual Getting Started Guide*
Firewall Threat Defense	
Firepower 1000/2100 series	*Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide* *Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense*

Platform	Guide
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*
Firewall Threat Defense Virtual	Secure Firewall Threat Defense Virtual getting started guides
ASA FirePOWER/NGIPSv	
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

For bugs in earlier releases, see the release notes for those versions. For cloud deployments, see the Release Notes for Cloud-Delivered Firewall Management Center.

Important We do not list open bugs for maintenance releases or patches.

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 71
- Resolved Bugs, on page 73

Open Bugs

Open Bugs in Version 7.0.0

Table last updated: 2025-06-17

Table 43: Open Bugs in Version 7.0.0

Bug ID	Headline
CSCvr74863	CIP-Multiservice shows wrong service Attributes
CSCvx21050	Snort3 UDP performance down up to 50% relative to snort2
CSCvx25425	snort3 ssl - tickets from undecrypted sessions are not cached for subsequent policy decisions
CSCvx30175	Snort3 - SMTP closing TCP flags are not propagated correctly

Bug ID	Headline
CSCvx63788	Edit policy in new window for AC Policy default action IPS policy shows error pop-up
CSCvx64252	Event Search errors out when using FQDN object search for initiator
CSCvx67856	FTD7.0: Promethues process doesnt come up when system ungracefully rebooted
CSCvx89720	User-based access control rules for RA VPN users may not apply as expected after 7.0.0 upgrade
CSCvx96452	Some HTTP2 TLS traffic ends with TCP RST, not TCP FIN, after complete payload transmission
CSCvx96452	Snort3 - Connection events sporadically show Allow action for traffic hitting SSL Block with Reset
CSCvx99179	FDM-VMWARE: nikita-incremen core during upgrade from 6.5 or higher to 7.0/7.1
CSCvy07113	7.0.0-1459 :FTPs traffic(malware file) is not blocked with file policy config,specifi to QP platform
CSCvy13572	7.0 - Downgrade to LSP version used in 6.7 causes deployment failure
CSCvy19415	After switching FTD HA, (secondary,active) sends primary device name in syslog message
CSCvy26742	Deployment failure when 1k rules are uploaded on 7.0.0-62 KVM vFTD
CSCvy27261	Snort2 and Snort3 Events view need enhancements to provide more clarity
CSCvy31096	Host rediscovery in case of snort configuration reload
CSCvy32550	Correlation fiiltering on snort3 custom rule message fails because rule is not built with GID 2000
CSCvy35352	Error handling for Suppression settings needed in certain conditions
CSCvy38070	File/Malware Event Report fails when date is x-axis and count y-axis for table chart
CSCvy39840	SI TALOS feed updates are not synced to rule file
CSCvy43483	Snort Toggle sometimes takes longer time to toggle to Snort 2
CSCvy43740	vFDM ISA HA Security Intelligence feed update throws java.lang.NullPoin
CSCvy44701	Version 7.0 FMC online help for the Snort 3 HTTP/2 inspector contains incorrect content.
CSCvy48764	SSH access with public key authentication requires user password
CSCwa16654	Firepower release 7.0.x does not support ssl_state or ssl_version keywords for Snort 3
CSCwh76499	After GeoDB update, using a new country in an access control rule replaces country names with (deleted) as the country name

Resolved Bugs

Resolved Bugs in Version 7.0.10

Table last updated: 2026-09-16

Table 44: Resolved Security Bugs in Version 7.0.10

Bug ID	Headline
CSCwo83926	Cisco Secure Firewall Threat Defense Software TLS 1.3 Denial of Service Vulnerability
CSCwr31700	RADIUS external auth doing one request per interface when bad username/password attempted
CSCws43281	Cisco Secure Firewall Management Center and Secure Firewall Threat Defense Software sftunnel Memory Exhaustion Denial of Service Vulnerability
CSCwt42671	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software IKEv2 Certificate Authentication Denial of Service Vulnerability
CSCwt50719	Clear the IPv4 rp_filter setting to allow FMC with dual management interfaces in same subnet
CSCwt61597	Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense
CSCwt81457	Cisco Secure Firewall Management Center Software Session Fixation Issue
CSCwt95974	Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability
CSCwt95997	Cisco Secure Firewall Management Center Software Static Credential Vulnerability
CSCwu03757	Cisco Secure Firewall Threat Defense Software Snort 2 SSL/TLS Denial of Service Vulnerability
CSCwu14285	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software TCP DNS Denial of Service Vulnerability
CSCwu14331	Cisco Secure Firewall Management Center Software sftunnel Root Arbitrary Code Execution Vulnerability
CSCwu16938	Cisco Secure Firewall Management Center Software Java Deserialization Remote Code Execution Vulnerability
CSCwu16954	Cisco Secure Firewall Management Center Software sftunnel Deserialization Root Command Execution Vulnerability
CSCwu16965	Cisco Secure Firewall Management Center Software Single Sign-On Token Forgery of Administrator Account Vulnerability

Bug ID	Headline
CSCwu24501	Cisco Secure Firewall Management Center Software SQL Injection Vulnerability
CSCwu27275	Cisco Secure Firewall Management Center Software Deserialization Arbitrary Root Command Execution Vulnerability
CSCwu27279	Cisco Secure Firewall Management Center Software Impersonated sftunnel Connection Vulnerability
CSCwu42586	Cisco Secure Firewall Management Center Software Low Privileged Arbitrary File Download Vulnerability
CSCwv96220	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability

Table last updated: 2026-09-15

Table 45: Resolved Functional Bugs in Version 7.0.10

Bug ID	Headline
CSCwf01318	sfhassd process keeps running after FTD upgrade/downgrade before deploy in snort3 mode
CSCwj68220	Unable to copy NAT policy on FMC
CSCwq27767	Deployment fails deployment with "Deployment failed due to failure in retrieving running configuration information from device."
CSCwq35960	"OSPF: High CPU, Route flaps, Lina Traceback and Reload in High Availability Setup."
CSCwq85473	FP 4115 ASA Cluster: GTP inspection causing high lina CPU 70% - 90%+ depend on traffic
CSCws31237	High cpu in spin lock due to excessive hash lookup's.
CSCws41206	Memory Leak issue binsize 131072 and 8192
CSCwt24048	FMC-created capture for FTD causes generation of excessive 'capture_*' files to FTD disk
CSCwt64074	'document.cookie = "CSRFtoken="' appears intermittently on the Clientless VPN login page
CSCwu95619	Lina core found on QW MI cluster

Resolved Bugs in Version 7.0.9

Table last updated: 2026-03-04

Table 46: Resolved Security Bugs in Version 7.0.9

Bug ID	Headline
CSCwh64704	FDM should provide a way to disable WebVPN portal on FTD
CSCwm83088	Cisco FXOS and UCS Manager Software Stored Cross-Site Scripting Vulnerability
CSCwm83089	Cisco FXOS and UCS Manager Software Stored Cross-Site Scripting Vulnerability
CSCwn48245	SEC-PWD-CONTROL - PSB - Proxy password showing in plain text on FMC
CSCwn49805	Multiple Cisco Products Snort 3 TBD Denial of Service Vulnerability
CSCwn69075	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF Heap Corruption Vulnerability
CSCwn69076	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability
CSCwn69078	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability
CSCwn69079	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF Memory Exhaustion Vulnerability
CSCwn69081	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability
CSCwn72848	Lina interface fragment db queue size is incorrectly stuck at 4294967295 - ASA/FTD
CSCwo00332	Firepower wiping SSL trustpoint config after reloading.
CSCwo01785	Memory leak in RAVPN
CSCwo40957	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software IPsec Denial of Service Vulnerability
CSCwo49925	Cisco Secure Firewall ASA Software and Secure FTD Software IKEv2 DoS Vulnerability
CSCwo49932	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Authentication Denial of Service Vulnerability
CSCwo49934	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Memory Exhaustion Denial of Service Vulnerability
CSCwo71552	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF DoS Vulnerability

Bug ID	Headline
CSCwo73885	Cisco Secure Firewall ASA Software and Secure FTD Software Authenticated Command Injection Vulnerability
CSCwo73886	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Unauthenticated Memory Exhaustion Denial of Service Vulnerability
CSCwo73888	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Lua Code Injection Vulnerability
CSCwo73889	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Lua Interpreter Denial of Service Vulnerability
CSCwo73891	Cisco Secure Firewall ASA Software and Secure FTD Software Remote Access SSL VPN Authenticated Memory Exhaustion Denial of Service Vulnerability
CSCwo74009	Cisco FXOS and UCS Manager Software Command Injection Vulnerability
CSCwo95774	Vulnerable version of Highcharts used by Context Explorer
CSCwo97439	ACL: ASA may show false "OOB Access-list config change detected" warning after AAA authorization command is applied
CSCwp22451	Cisco Secure Firepower Management Center Software SQL Injection Vulnerability
CSCwp29401	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software SAML Reflected Cross-Site Scripting Vulnerability
CSCwp34291	Cisco Secure Firewall Threat Defense Software Snort Deep Inspection Bypass Vulnerability
CSCwp68059	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Services Cross-Site Scripting Vulnerability
CSCwp98488	PSB: SEC-LOG-NOSENS-FR2 - P12 cert passphrase logged in plaintext in FMC logs
CSCwq01517	Cisco Secure Firepower Management Center Software SQL Injection Vulnerability
CSCwq01519	Cisco Secure FTD Software Authenticated Command Injection Vulnerability
CSCwq01526	Cisco Secure FTD Software Authenticated DoS Vulnerability
CSCwq01530	Multiple Cisco Products Snort 3 TBD Denial of Service Vulnerability
CSCwq02055	Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software VPN Web Services Client-Side Request Smuggling Vulnerability
CSCwq23375	Cisco Secure Firewall Management Center Software Command Injection Vulnerability
CSCwq32051	Cisco Adaptive Security Appliance and Firepower Threat Defense Software Command Injection Vulnerability
CSCwq56017	Cisco Secure Firewall Management Center and Secure Firewall Threat Defense Software Path Traversal Vulnerability

Bug ID	Headline
CSCwq73656	Cisco Secure Firewall ASA Software and Secure FTD Software OSPF Memory Corruption Vulnerability
CSCwq75339	Multiple Cisco Products Snort 3 DCERPC Vulnerabilities
CSCwq75359	Multiple Cisco Products Snort 3 DCERPC Vulnerabilities
CSCwq78991	Firewall joins a cluster although gets incomplete ACL policy rules during replication
CSCwq85267	Late Release of Memory after Effective Lifetime vulnerability in Apache HTTP Server.
CSCwq85285	HTTP response splitting in the core of Apache HTTP Server allows an attacker who can manipulate the Content-Type response headers
CSCwr50762	DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTM
CSCwr50784	DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTM
CSCwr50785	DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTM
CSCwr50836	DOMPurify before 3.2.4 has an incorrect template literal regular express
CSCwr96008	Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability
CSCwt14636	Cisco Secure Firewall Management Center Software Remote Code Execution Vulnerability

Table last updated: 2026-02-19

Table 47: Resolved Functional Bugs in Version 7.0.9

Bug ID	Headline
CSCvx55760	Out of compliance is not showing at entitlement level and Overconsumption of VIRTUAL license on vFMC
CSCwc87963	ASAv "Unable to retrieve license info. Please try again later"
CSCwe28608	Snort returns "Blocked by SSL" with no SSL policy.
CSCwf25454	Stale anyconnect entries causing issues with routing
CSCwh17965	[Display]FXOS: PC member interface is shown as down & unassociated/unassigned after reload
CSCwk28058	FTD memory depletion resulting in traceback and reload
CSCwk46737	ASA on HA: alloc_ch() alloc from chunk mem Failed message on one context in Standby device
CSCwk63586	App instance stuck in STOP_FAILED with error message
CSCwm28007	Browser redirects to blank page when the user clicks the WebVPN bookmark

Bug ID	Headline
CSCwm35730	LINA may traceback in Thread Name: Datapath with NAT config
CSCwm36631	FTD Secondary Unit got stuck in Bulk sync state.
CSCwm37455	ASA/FTD will allow local IP pool with invalid netmask
CSCwm44412	FTD inline-set ignore reverse flag for inject/rewrite
CSCwm49721	ASA Traceback and Reload due to MEMORY CORRUPTION WAS DETECTED
CSCwm52931	ASA/FTD may traceback and reload in Thread Name "fover_parse"
CSCwm56864	show run access-list command returns warning
CSCwm63868	FTD - Missing routes on BGP advertised-routes after FTD HA failover event
CSCwm68211	ASA traceback and reload on thread snmp_inspect
CSCwm70835	ASA traceback and reload due to stack overflow while using APCF file
CSCwm71265	ASA traceback and reload on thread DATAPATH when processing gtpv1 end marker msg for PDP
CSCwm85228	ASA/FTD may traceback and reload in Thread Name "IKEv2 Daemon" while joining failover
CSCwm90905	GTP inspection drops packet with error ERROR-DROP:MsgType:32
CSCwm92310	FQDNs are unresolved via DNS on data interface after reboot or traceback
CSCwm97054	ASA/FTD traceback and reload with high rate of SIP connections
CSCwm98278	TCP Conn not being flagged as Half-Closed after receiving the ACK for the FIN.
CSCwn00475	Memory Blocks 80 and 9344 leak due to priority-queue
CSCwn01281	GTP inspection not allowing GTP data packets if session create response has cause type 18
CSCwn14447	ASA/FTD may traceback and reload in Thread Name 'ldap_client_thread'
CSCwn15104	FTD reload with traceback on swapcontext function
CSCwn17121	ASA/FTD may traceback and reload in Thread Name 'cli_xml_request_process'.
CSCwn20024	ASA may traceback and reload in Thread Name 'ssh'
CSCwn22456	GTPv2 IE-type 157 (Signaling Priority Indication) is dropped with reason as unknown IE type
CSCwn24577	ASA booting process may freeze when including 'no pim' or 'no igmp' config
CSCwn26165	FTD/ASA May Traceback and Reload - During Deployment / Radius changes - Due to Radius Packets

Bug ID	Headline
CSCwn27819	Jumbo frame packets are being fragmented
CSCwn34259	Monitored interfaces may go in waiting state after upgrade to 9.20.3.7
CSCwn34707	Multiple Unicorn Admin Handler processes consume all the control plane CPU.
CSCwn35470	Serviceability : FQDN Packet based debug and capture trace support
CSCwn36120	Enhanced Debug Image with Lina and PDTS Capabilities for FQDN Issue Resolution
CSCwn38761	DNS FQDN obj doesn't go unresolved upon FQDN obj deleted on server/intf to reach sever is down in 7.7
CSCwn39780	FTD Deployment Resilience: Skip non-critical / non-existing commands to avoid deployment failures.
CSCwn42949	Implementing forwarder flow on non-owner units handling distributed secondary flow connections
CSCwn49391	Frequent traceback after upgrading FTD HA
CSCwn65415	ASA: floating-conn not closing UDP conns if conn was created without ARP entry for next hop
CSCwn73351	Asia/Bangkok timezone option not listed in ASA running on firepower1k
CSCwn84557	Lina traceback and reload due to "spin_lock_fair_mode_enqueue"
CSCwn90900	High ASA/FTD memory usage due to polling of RA VPN related SNMP OIDs
CSCwn92894	Occasionally, 'show chunkstat top-usage' output does not show all entries
CSCwn93319	ASA/FTD may traceback and reload in Thread Name "DATAPATH"
CSCwo01557	ASA traceback and reload on DATAPATH thread due to memory corruption
CSCwo08042	ASAv reloaded unexpectedly with traceback on Unicorn Proxy Thread
CSCwo09060	SSL trustpoint with 4096 bit RSA keys not allowed by ASA if renewed via CLI
CSCwo31094	Virtual ASA Traceback and Reload Caused by Disk Access Issues with NFS Enabled
CSCwo41250	Traceback & Reload in thread named: DATAPATH-1-23988 during low memory condition
CSCwp11382	ASA/FTD: the ssl trust-point command deleted after a reload
CSCwp26815	CPU usage by "WebVPN Timer Process" on standby ASA device
CSCwp34610	IKEv2-EAP Authentication Fails with Windows and MacOS Native VPN Clients
CSCwp37284	"CSRF Token Mismatch" error seen when users click logout from Clientless VPN page

Bug ID	Headline
CSCwq07808	FP3105 Traceback and Reload after changing the speed on Ethernet interface
CSCwq46058	ASA SNMP Response Issue - Responses Sent Only for Odd OIDs, Not for Even
CSCws06991	Few FQDNs are not resolving after FTD upgrade
CSCws19823	80, 1550 and 9472 block depletion seen on ASA/FTD 2100 when SMB multichannel traffic is sent
CSCws31035	Lina Traceback and reload in Thread: "cli_xml_request_process"

Resolved Bugs in Version 7.0.8.1

Table last updated: 2025-09-25

Table 48: Resolved Security Bugs in Version 7.0.8.1

Bug ID	Headline
CSCwq79815	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Unauthorized Access Vulnerability
CSCwq79831	Cisco Secure Firewall Adaptive Security Appliance Software and Secure Firewall Threat Defense Software VPN Web Server Remote Code Execution Vulnerability

Resolved Bugs in Version 7.0.8

Table last updated: 2025-08-12

Table 49: Resolved Security Bugs in Version 7.0.8

Bug ID	Headline
CSCwq03404	External auth login with RADIUS to FMC UI may fail if Class attribute is used
CSCwq10344	FMC RADIUS external authentication access requests missing 6 attributes after FMC upgrade

Table last updated: 2025-08-12

Table 50: Resolved Functional Bugs in Version 7.0.8

Bug ID	Headline
CSCvx66624	Write cache is disabled on some FMC M5 appliances
CSCvy28590	Snort3: Wrong action on events page for Sinkhole block and log connection
CSCwh08441	ENH: Add a command or a script to regenerate CA Certificate on FTD

Bug ID	Headline
CSCwh13312	Disable Notification Daemon heartbeat action
CSCwi91166	Need to add reasons for blocks in stream
CSCwj28437	Snort3: TCP traffic failure after upgrade due to large invalid sequence numbers and invalid ACKs
CSCwj62984	Snort3: MSSQL query traffic corrupted by stream_tcp overlap handling causing SQL HY000
CSCwk12673	TCP Session Interrupted if Keep-Alive with 1 Byte is Received
CSCwk48026	Increase connection retry count in 200_pre/100_get_snort_from_dc.pl
CSCwn84340	Talos registration cert may fail to generate if smart licensing VA name contains certain characters
CSCwo16016	Users from legacy radius server can login to Standby FMC domain when MA is enabled
CSCwo61240	After renewal FMC CA, the certificate cannot be used for ArcSight integration
CSCwo71835	The NAS-IP-Address attribute is missing from the Access-Request in FMC
CSCwo77662	Certain special characters or spaces in RADIUS user passwords cause login failure in FMC

Resolved Bugs in Version 7.0.7

Table last updated: 2025-02-14

Table 51: Additional Resolved Bugs in Version 7.0.7-519 (FTD/FTDv Only)

Bug ID	Headline
CSCwo06545	Readiness Check Failure for Upgrade to Version 7.0.7: "DEV Keys Not Installed"

Table last updated: 2025-01-29

Table 52: Resolved Bugs in Version 7.0.7-518 (All Platforms)

Bug ID	Headline
CSCvu95526	Disable "ca-check" option should be available on FDM
CSCvz83863	Snort3 crash in Http2StreamSplitter
CSCwa14524	Snort cores in pdts_sftls_daq_acquire with SSL activated
CSCwa82791	ENH: Support for snapshots of RX queues on InternalData interfaces when "Blocks free curr" goes low
CSCwc15032	Unable to configure suppression/threshold for an intrusion rule

Bug ID	Headline
CSCwc28374	Search Feature of Large Access Control Policy Not Able to Find Searched-For Values
CSCwc57500	Remove bootlogd package from FXOS to avoid ASA boot log problems
CSCwc87387	Valid DNS requests are being dropped by Lina DNS inspection when Umbrella DNS is configured
CSCwc96780	FMC module specific health exclusion disables all health checks
CSCwd08098	cacert.pem on FMC expired and all the devices showing as disabled.
CSCwd08448	FMC to provide health alert 60 days prior to cacert.pem certificate expiry
CSCwd27186	All traffic blocked due to access-group command missing from FTD config
CSCwd49767	System popover is empty for Network Admin and Security Approver users
CSCwd65598	cdFMC: SFDataCorrelator cores and user to group map not updated on sensor
CSCwd80284	Import/export fails with backend error
CSCwd86226	Standby FMC show FMC-HA as healthy when Active unit Sybase is down
CSCwe16730	Deployment failing - "Error while printing show-xml-response file contents" XML response too big
CSCwe18216	null connection error seen in logs
CSCwe22431	[SXP-UserIP Muted Leader]FMC HA Join flushes FW IP_SGT Mapping and restreams in registered sensors.
CSCwe42986	Classic and Unified Events should handle cases when SMC is unreachable
CSCwe58635	Readiness Check Failed [ERROR] Fatal error: Enterprise Object integrity check failed with errors
CSCwe59889	Create Identity Services Engine via API returns 404 Client Error: Not Found
CSCwe63686	Upgrade readiness failed in WM FDM @009_check_snort_preproc.sh but upgrade to 7.3.1-19 passed
CSCwe66360	Snort3 out of memory and process exit unexpectedly due to memory not released by flows
CSCwe68917	Snort3 fails to match SMTPS traffic to ACP rules
CSCwe75055	[FMC model migration] Health monitoring on FMC reporting errors
CSCwe78674	User Group Download fetches less data than available or fails with "Size limit exceeded" error
CSCwe81135	ac-policy rule section showing non-existing index page in old ac-policy UI
CSCwe93925	Deployment fails to FTD when reusing/reassigning existing vlan id to diff interface

Bug ID	Headline
CSCwf00849	Unable to remove host directory from realm
CSCwf08320	SSE does not update relevant information after first discovery of an asset.
CSCwf10295	Snort3 is not closing the pcap file handle and disk is getting full
CSCwf12521	Unable to load intrusion policy page on FMC GUI
CSCwf16001	HashiCorp Vault's implementation of Shamir's secret sharing used precomp
CSCwf17314	FMC deploy logs rotating faster because of /internal_rest_api/accesscontrol/rapplicationsavailable
CSCwf25642	High Disk Utilization and Performance issue due to large MariaDB Undo Logs
CSCwf26264	FMC backup restore page takes around 5 mins to load when remote storage is unreachable
CSCwf30542	Snort3 crash found during cleaning up a CHP object
CSCwf32338	Multi-tenancy sub-domain - HealthMonitor menu layout should be based on FTD device version
CSCwf35346	FMC should handle error appropriately when ISE reports error during SXP download
CSCwf45091	Snort3 matches SMTP_RESPONSE_OVERFLOW (IPS rule 124:3) when SMTPS hosts exchange certificates
CSCwf66818	FMC VPN Monitoring Dashboard incorrectly shows Standby FTD as VPN Session owner in HA pair
CSCwf69576	Snort Crash with SMB inspection traffic
CSCwf71602	FMC not generating FTD S2S VPN alerts when down or idle
CSCwf80183	Snort3 core in navl seen during traffic flow
CSCwf92371	HA secondary unit disabled after reboot - Process Manager failed to secure LSP
CSCwf92439	Deployment blocked due to port object with IP range max limit 131838 in NAT64
CSCwh01312	ENH: FMC External Authentication doesn't work for SSH when configured with IPv6.
CSCwh02621	add a confirmation message when using on manage_HADC.pl options 9,10,11,12
CSCwh10087	core-compressor fails due to core filename with white space
CSCwh13182	FTD fails upgrade from 7.2.4 to 7.4.1 and revert fails to take device out of maintenance mode
CSCwh18704	Certifi is a curated collection of Root Certificates for validating th
CSCwh20307	FMC fails deployment after removing NAT or ACL rule

Bug ID	Headline
CSCwh21337	FTD - Issue with the LSP package code during deploy rollback.
CSCwh22317	LILO validation during Readiness Check missing
CSCwh28779	Unable to save intrusion policy after upgrade to 7.x as the name exceeds 40 characters
CSCwh36167	DAP: FMC adds &#13 characters in a LUA script
CSCwh36328	Test tool config params are shared by HTTP and HTTP/2 causing a race condition -regression test only
CSCwh37655	Snort2:Skip writing malware seed file duing process shutdown
CSCwh38492	FMC Restore is stuck in vault clear stage after mysql restore completed
CSCwh39258	Occasionally External auth may not work after HA failover to Active
CSCwh41606	Extensive logging for a problematic deployment caused logs to rollover important logs
CSCwh51872	Message asa_log_client exited 1 time(s) seen multiple times
CSCwh52526	FMC SSO timesout when user session is active for more than 1 hr (idle timeout)
CSCwh52710	evaluate open-vm-tools / VMware Tools on FMC for VMware -- CVE-2023-20900 and VMSA-2023-0019
CSCwh57814	The html/template package does not apply the proper rules for handling o
CSCwh58490	FMC Deployment failed due to internal errors after upgrade
CSCwh63663	Cannot use .k12 domain on realm AD Primary Domain configuration
CSCwh80131	S3_Core: crashinfo: increase buffer space to print longer function names
CSCwh83854	Cannot configure Correlation rule because there are no values for GID that exceed 2000
CSCwh89289	Snort is getting reloaded during deploy due to diff in timerange and nap conf contents in each run
CSCwh90813	FDM Upgrade failure due to expired certificates.
CSCwh95003	Init process spikes to 100% CPU usage after a failed backup
CSCwi01895	Connection drops during file transfers due to HeartBeat failures
CSCwi07068	SFDataCorrelator logs "Killing MySQL connection" every minute, causing performance problems
CSCwi08374	FMC backup fails with "Registration Blocking" failure caused by DCCSM issues
CSCwi08392	Configuring /32 makse PPoE address: "Invalid value of IPV4 address or subnet or network overlap"

Bug ID	Headline
CSCwi16571	Capture-traffic Clish command with snort3 not producing a proper resulting capture
CSCwi28645	User assigned to a read only custom role is not able to view content of intrusion policy for snort2
CSCwi38708	FDM deployment failure
CSCwi40674	Umbrella Profile and others cleared incorrectly when editing group policy in the UI
CSCwi41666	MonetDB startup enhancement to clean up large files
CSCwi45408	Monetdb having 14GB of unknown BAT data causing "High unmanaged disk usage on /Volume"
CSCwi46163	Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.
CSCwi46676	API:/operational/commands not working as swagger indicate
CSCwi49128	Update logs - SSP object serialization during HA
CSCwi55009	Error thrown if Security Analytics user tries to access Packet Capture page
CSCwi58187	Incorrect NAT warnings threshold limit of 131838 IPs
CSCwi59453	Bootstrap after upgrade failed - Resume HA with reason deployment already exists
CSCwi64429	MonetDB memory usage grows slowly over time
CSCwi72294	FTD: Improve or optimize LSP package verification logic to run it faster
CSCwi81503	HTTP/HTTPS detection for application needs to fail it's detection earlier
CSCwi81771	Unable to send unknown file disposition to ThreatGrid due to mem cache issue
CSCwi98274	unzip 5.52 is from 2005 is contains multiple vulnerabilities
CSCwj01321	FMC Stored XSS via Edit AnyConnect custom Attribute
CSCwj02259	Backup failures needs to be displayed with the correct state on GUI
CSCwj05464	FMC Server Certificate shows Only First 20 Objects
CSCwj08030	libexpat through 2.5.0 allows a resource consumption denial of service event
CSCwj08031	libexpat through 2.5.0 allows recursive XML Entity Expansion if XML_DT
CSCwj08203	FMC: fireamp generating too many logs
CSCwj14589	FMC-SSE Cloud Configuration SSE Enrollment Failure alert due to empty connector.toml file on the FTD
CSCwj17852	FMC - Inheritance Settings Select Base Policy Menu disappears while scrolling using Light or Dusk UI

Bug ID	Headline
CSCwj23192	extra file check is not reporting with pmtool SecureLSP lsp-rel-xxx command
CSCwj23777	Missing Column(s) in eventdb table
CSCwj24517	LSP Deployment fails in multi instance FP 41xx / 93xx
CSCwj26595	FMC allows loading a binary certificate in the External Authentication Object
CSCwj31904	After upgrade FDM deployment fails "Timeout waiting for snort detection engines to process traffic"
CSCwj31918	Segmentation fault with "logger_msg_dispatch" while HA sync
CSCwj33503	Snort3 event PCAPs contain only header data when decrypting HTTP/2
CSCwj33734	The Portable Network Graphics library (libpng) 1.0.15 and earlier allows
CSCwj34374	SecureX / Cisco Security Cloud registration fails if FMC is behind a proxy server
CSCwj39212	SFDataCorrelator memory growth when processing a huge number of expired user identities
CSCwj43379	libexpat through 2.6.1 allows an XML Entity Expansion attack when ther
CSCwj45075	Critical Processes show twice after upgrade to 7.0.6.x
CSCwj45439	Internal Certificate Import Error : Failed to validate Cert Based EO: Unsupported Key Type
CSCwj50024	Add support for new Cloud SSX regions for India and Australia
CSCwj50557	Snort creating too many snort-unified log files when frequent policy deploys
CSCwj53725	Traceback observed while applying 'no failover' and 'failover' in the ASA standby
CSCwj54042	Crypto ikev2 policy sequence order alters on interface/sub-interface config changes
CSCwj62959	Deployment failure and rollback when changing parent of subinterface with failover MAC address
CSCwj65811	FMC gets flooded with"Unable to find SSL rule id for policy" if TLS server identity discovery is on
CSCwj67947	ASA5516: SNMPv3 poll to SFR failing with error "Unknown user name"
CSCwj72013	PAT communication via using PAT pool fails for about 40 seconds when a device joins a cluster
CSCwj72022	Deployment time increased by 30-45 seconds after the upgrade when applying specific Platform Setting
CSCwj72369	sync call got stuck resulting in boot loop
CSCwj79229	FMC - plain-text passwords for External Authentication Profile "Radius Server Key"

Bug ID	Headline
CSCwj85103	Unable to download group/user due to error in SQL syntax on rebuild indexes
CSCwj85106	FMC on upgrade results in FTDv losing its performance tier
CSCwj89126	HTTP Response splitting in multiple modules in Apache HTTP Server allows
CSCwj89228	FTD /mnt 100% disk utilization due to snort memory mapped files
CSCwj90826	Snort2 SSL decryption with known key fails on Chrome v124 and above.
CSCwj98451	FMC got deregistered from Smart License after upgrade
CSCwk02332	Snort2 - SSL decryption failing and some websites not loading on Chrome v124+
CSCwk04216	Realm download task failing with ADI process is not currently available
CSCwk04893	FTD does not compact files that are used to communicate updates to the SGT/IP mappings
CSCwk06216	Loss of interface mapping with security zones after deployment
CSCwk07563	Force deploy not re-generating export-cache in the device
CSCwk08241	FTD is not resolving FQDN for ACLs intermittently
CSCwk08476	FTD/ASA traceback and reload due to 'show bgp summary' memory leak
CSCwk10884	Connectivity failure due to mismatch between l2_table and subinterface mac address
CSCwk24440	Backups may fail on remote storage when the filebackup.tar contents are so huge
CSCwk33516	MonetDB down due to a corrupt table (table missing columns)
CSCwk35710	FTD/LINA may traceback and reload when "show capture" command is executed in EEM script
CSCwk38440	if conn_meta null, dont send packet to snort
CSCwk45679	DOC: cdFMC page help needs to be improved for Interface used to connect to Directory server
CSCwk48488	Cisco FTD for Cisco Firepower 2100 Series TCP UDP Snort 2 and Snort 3 DoS Vulnerability
CSCwk54033	FMC can not connect to private AMP when proxy is enabled in management interface
CSCwk56388	GRE traffic getting dropped after failover
CSCwk61157	FTD LINA Traceback and Reload dhcp_daemon Thread
CSCwk63733	HA-monitored interfaces are going into "waiting" state and subsequently to "Failed"
CSCwk66255	urllib3 is a user-friendly HTTP client library for Python. When using

Bug ID	Headline
CSCwk67346	DAP policies not working with attribute TRUE/FALSE
CSCwk67859	FTD and FXOS: RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS): July 2024
CSCwk69454	FDM: Blast-RADIUS CVE-2024-3596
CSCwk71817	FMC: Blast-RADIUS CVE-2024-3596
CSCwk71992	BlastRADIUS vulnerability phase-1 fix for pix-asa - Message Authenticator
CSCwk73512	Deployment fails on cluster node "snort3 command for 'IPRepReload' failed" no response was received"
CSCwk75956	ASA/FTD may traceback and reload in Thread Name SSH
CSCwk76142	ASA crashing in thread PIX Garbage Collector with inspect-rtsp enabled.
CSCwk77241	Traffic outage due to 9k block depletion (tcpmod proc) observed on FPR 3100 (HA)
CSCwk78075	FTD does not mark stuck ongoing deployments as failed leading to subsequent deployment failures
CSCwk87457	ASA/FTD may traceback and reload in Process Name "lina" after device was reloaded
CSCwk88182	FTDv50 traceback during normal operation at PTHREAD-8141 spin_lock_fair_mode_enqueue
CSCwk88913	Keep a FMC backup locally until we copy the file to remote server successfully
CSCwk89127	Backup_info table is not being pruned, causing DB queries to slow down
CSCwk89836	ASA/FTD may traceback and reload in Thread Name 'strlen'
CSCwk94382	FTD: Lina might fail to respond to CONFIG_XML_REQUEST leading to stuck deployments
CSCwm01544	Lina traceback and reload in data-path thread
CSCwm03227	FTD upgrade failure due to multiple DB folders in /ngfw/var/cisco/deploy/tmp_bundle/db/ path
CSCwm04650	Increase memory usage leading to tracebacks in Lina.
CSCwm05520	Disable cluster syn cookie decoding when FTD cluster is deployed with inline-set
CSCwm13141	FTD CLISH/CLI gets locked up when trying to run any show command
CSCwm13199	SIP traffic is affected due to unexpected behavior with NAT untranslations.
CSCwm14509	Wrong drops seen with Invalid length for 23, 24 and 25 IE-Types during GTP inspection
CSCwm29469	FMC GUI has a limitation to display only 50 SSH rules for FTD (Under platform settings >> SSH)

Bug ID	Headline
CSCwm29768	Connection been logged for rules with no logging enabled
CSCwm29876	Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.5
CSCwm29879	In the Linux kernel, the following vulnerability has been resolved: b
CSCwm29929	QoS policy editor on FMC GUI lacks functional pagination when QoS policy has more than 50 rules
CSCwm30731	The ASA's OSPF routing table is not properly synchronized with the neighbors
CSCwm33613	Default Group Policy is applied when receiving multiple Group Policies in SAML assertion attributes
CSCwm35051	hostname/IP Address field does not accept domains ending in a number
CSCwm35251	FMC4700 displays premature fan speed alerts
CSCwm36646	After FMC upgrade results in standby FTDv losing its performance tier for FTD HA
CSCwm38635	TACACS+ traffic is dropped by TLS Server Identity in XTLS module
CSCwm40278	S2S VPN config removed unexpectedly after deployment
CSCwm41847	Serviceability to capture PDTS writing/reading block to help root cause CSCwm36314
CSCwm43186	In the Linux kernel, the following vulnerability has been resolved: x
CSCwm43304	In the Linux kernel, the following vulnerability has been resolved: p
CSCwm47775	FMC Deployment Failure When Modifying NAT Policy with Block Allocation and Round-Robin Enabled
CSCwm49153	Cisco Adaptive Security Appliance Software SSH Server Resource DoS Vulnerability
CSCwm49410	Misconfigured Cross-Origin-Opener-Policy
CSCwm51923	Deployment transcript showing "Enable management access: false"
CSCwm57472	In the Linux kernel, for filelock: Remove locks reliably when fcntl/close race is detected
CSCwm57484	In the Linux kernel, within mm: avoid overflows in dirty throttling logic
CSCwm58772	snort2 instances restart unexpectedly with OOM during policy deployment
CSCwm60536	SQLNet traffic getting dropped intermittently in Clustering data unit.
CSCwm61282	ASA/FTD: RA VPN tunnel causing memory leak leading to traceback & Reload
CSCwm67414	Unable to edit/delete client module in the RAVPN group policy
CSCwm78351	Potential High CPU usage in Multi-Context Cluster setup with unconditional execution of capture code

Bug ID	Headline
CSCwm92397	LINA core observed pointing to "IP RIB Update" thread
CSCwm95116	ADI crashes on FTD due to both FMC ADIs going unmuted
CSCwm95328	Copy/Paste for a rule on any UI page other than page 1 results in policy UI loading back to page 1.
CSCwn05183	FTD HA active node interfaces went down after failed policy deploy
CSCwn23992	Push messages including UMS are broken when the FMC is reached on port 443
CSCwn34659	Firewall not initiating TCP request even after receiving the TC bit in server response

Resolved Bugs in Version 7.0.6.3

Table last updated: 2024-09-10

Table 53: Resolved Bugs in Version

Bug ID	Headline
CSCvy51481	FTD should show error/warning when attaching a not valid certificate to the interface for VPN
CSCwb03293	IKEv2 debugs: Received Policies and Expected Policies are empty
CSCwe11754	Nodes randomly fail to join cluster due to internal clustering error
CSCwe12645	Secondary state flips between Ready & Failed when node is rebooted and mgmt interface is shutdown
CSCwe18462	ASA/FTD: Improve GTP Inspection Logging
CSCwe18467	ASA/FTD: GTP Inspection engine serviceability
CSCwe37132	TLS Server Identity may cause certain clients to produce mangled Client Hello
CSCwe86923	In Apache MINA, a specifically crafted, malformed HTTP request may cause
CSCwf49254	cannot unregister FTD from Cisco Cloud in FDM if already unregistered/unenrolled from cloud side
CSCwf70275	FTD: TLS Server Identity does not work if size of client hello more than TCP MSS bytes
CSCwf75694	ASA - The GTP inspection dropped the message 'Delete PDP Context Response' due to an invalid TEID=0
CSCwf84318	ASA/FTD traceback and reload on thread DATAPATH
CSCwh10931	ASA/FTD traceback and reload when invoking "show webvpn saml idp" CLI command

Bug ID	Headline
CSCwh29276	ASA: Traceback and reload when switching from single to multiple mode
CSCwh43945	FTD/ASA traceback and reload may occur when ssl packet debugs are enabled
CSCwh48776	An issue was discovered in Python before 3.8.18, 3.9.x before 3.9.18,
CSCwh49085	Avoid unnecessary DB operations when processing derived fingerprints
CSCwh59222	SNORT3 - FTD - TSID high cpu, daq polling when ssl enabled is not pulling enough packets
CSCwh60971	NAT pool is not working properly despite is not reaching the 32k object ID limit.
CSCwh68068	Firepower WCCP router-id changes randomly when VRFs are configured
CSCwh71262	A flaw was found in glibc. In an uncommon situation, the gaih_inet fun
CSCwh83021	ASA/FTD HA pair EIGRP routes getting flushed after failover
CSCwh87058	FTD: Internal certificate generation results to certificate and private key mismatch
CSCwh94029	A flaw was found in the Netfilter subsystem in the Linux kernel. The n
CSCwh94116	A flaw was found in the Netfilter subsystem in the Linux kernel. The x
CSCwh94193	urllib3 is a user-friendly HTTP client library for Python. urllib3 doe
CSCwh95443	Datapath hogs causing clustering units to get kicked out of the cluster
CSCwi00713	A memory leak flaw was found in Libtiff's tiffcrop utility. This issue
CSCwi05240	ASA - Traceback the standby device while HA sync ACL-DAP
CSCwi06797	ASA/FTD traceback and reload on thread DATAPATH
CSCwi23964	Python 3.x through 3.10 has an open redirection vulnerability in lib/h
CSCwi24007	An issue was discovered in the Linux kernel before 6.3.3. There is an
CSCwi24116	Twisted is an event-based framework for internet applications. Prior t
CSCwi36244	In buc Traceroute 2.0.12 through 2.1.2 before 2.1.3, the wrapper scrip
CSCwi38662	FTD HA should not be created partially on FMC
CSCwi43492	ASA traceback and reload on Thread Name: DATAPATH
CSCwi44912	ISA3000 Traceback and reload boot loop
CSCwi49770	ASA|FTD Traceback & reload in thread name Datapath
CSCwi52008	Snort3 traceback and restarts with race conditions
CSCwi56499	Cut-Through Proxy feature spikes CP CPU with a flood of un-authenticated traffic

Bug ID	Headline
CSCwi60430	CVE-2023-51385 (Medium Sev) In ssh in OpenSSH before 9.6, OS command injection might occur if a us
CSCwi68625	Continuous snmpd restarts observed if SNMP host is configured before the IP is configured
CSCwi78191	An issue was discovered in drivers/input/input.c in the Linux kernel b
CSCwi78193	An issue was discovered in the Linux kernel before 6.6.8. do_vcc_ioctl
CSCwi78200	A vulnerability was found in GnuTLS. The response times to malformed c
CSCwi78206	A vulnerability was found in GnuTLS, where a cockpit (which uses gnuTL
CSCwi78941	FDM deployment fails with error "Some interfaces have been added to or removed from the device"
CSCwi79037	IKEv2 client services is not getting enabled - XML profile is not downloaded
CSCwi84314	ASA CLI hangs with 'show run' on multiple SSH
CSCwi85951	A use-after-free flaw was found in the __ext4_remount in fs/ext4/super
CSCwi85953	In rds_recv_track_latency in net/rds/af_rds.c in the Linux kernel thro
CSCwi90751	FTD/ASA - SNMP queries using snmpwalk are not displaying all "nameif" interfaces
CSCwi92924	A memory leak problem was found in ctnetlink_create_conntrack in net/n
CSCwi92927	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tab
CSCwi92930	linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a den
CSCwi92932	copy_params in drivers/md/dm-ioctl.c in the Linux kernel through 6.7.1
CSCwi95796	FTD SNMP OID 1.3.6.1.4.1.9.9.109.1.1.1.1.7 always returns 0% for SysProc Average
CSCwi97836	ASA traceback and reload after configuring capture on nlp_int_tap and deleting context
CSCwi97948	EIGRP bandwidth is changing after upgrade or after "shutdown"/"no shutdown" commands
CSCwi98147	Tomcat restarts in the middle of the LTP flow due to certificate update
CSCwi99429	Policy deployment failure rollback didnt reconfigure the FTD devices
CSCwj00956	Snort process spamming syslog-ng messages so our on KP platform syslog-ng is being killed
CSCwj03112	pmtool restart of monetdb fails to bring up monetdb, too many files in monetdb Volume directory
CSCwj05151	ASA/FTD may traceback and reload in Thread Name DATAPATH due to GTP Spin Lock Assertion

Bug ID	Headline
CSCwj08021	The DNS message parsing code in 'named' includes a section whose compu
CSCwj08023	Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6
CSCwj08066	A denial of service vulnerability due to a deadlock was found in sctp_
CSCwj08083	An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.1
CSCwj08153	An out-of-memory flaw was found in libtiff that could be triggered by
CSCwj10451	The secondary device reloaded while rebooting the primary device.
CSCwj12924	A flaw was found in the Netfilter subsystem in the Linux kernel. The i
CSCwj14624	Backup exits with memory allocation error on 4115
CSCwj14798	TSS_Daemon process is exiting every minute
CSCwj17447	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-6-26174'
CSCwj17969	rna_ip_os_map can grow very large that causes SFDataCorrelator to stop processing events
CSCwj22235	Lina traceback and reload due to mps_hash_memory pointing to null hash table
CSCwj22990	After upgrading the ASA, “Slot 1: ATA Compact Flash memory” shows a ditterent value
CSCwj24828	Issue when two FQDN objects with same IP are added in source or destination (FTD/ASA)
CSCwj25975	FTD/ASA : CSR generation with comma between “Company Name” attribute does not work expected
CSCwj28153	Lina contains outdated libexpat source code
CSCwj30980	Addition of debugs & a show command to capture the ID usage in the CTS SXP flow.
CSCwj32035	Clientless VPN users are unable to reach pages with HTTP Basic Authentication
CSCwj33487	ASA/FTD may traceback and reload while handling DTLS traffic
CSCwj33580	IKEv2 tunnels flap due to fragmentation and throttling caused by multiple ciphers/proposal
CSCwj40597	Backups fail on multi-instance (or standalone) with error "Backup died unexpectedly"
CSCwj43345	SNMP poll for some OIDs may cause CPU hogs and high latency can be observed for ICMP packets
CSCwj43355	A bug in QEMU could cause a guest I/O operation otherwise addressed to
CSCwj43466	A heap-buffer-overflow vulnerability was found in LibTIFF, in extractI

Bug ID	Headline
CSCwj44398	when set the route-map in route RIP on FTD, routes update is not working after FTD reload
CSCwj45822	Cisco Secure Client Unable to complete connection. Cisco Secure Desktop not installed on the client.
CSCwj48704	ASA traceback and reload when accessing file system from ASDM
CSCwj49958	Crypto IPSEC Negotiation Failing At "Failed to compute a hash value"
CSCwj51115	FMC backup remote server copy to Solar Winds remote server failing after upgrading to 7.x versions.
CSCwj55036	ASA/FTD: A delay in an async crypto command induces a traceback and subsequently a reload.
CSCwj59861	ASA/FTD may traceback and reload in Thread Name 'lina' due to SCP/SSH process
CSCwj60265	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-1-16803'
CSCwj61885	File descriptor leak when validating upgrade images
CSCwj68783	FTD/ASA-HA configs not in sync as the command sync process is sending configs with special chars
CSCwj72683	ASA - Bookmarks on the WebVPN portal are unreachable after successful login.
CSCwj72721	Deployment failure and rollback when BGP communities added or removed in route-map match clause
CSCwj73061	SNMP OID for CPUTotal1min omits snort cpu cores entries when polled
CSCwj74323	ASAv Memory leak involving PKI/Crypto for VPN
CSCwj76503	Syslogs continue to be sent after disabling logging class on ASA
CSCwj82285	ASA/FTD may traceback and reload in Thread Name 'sdi_work'
CSCwj82736	TLS Handshake Fails if Fragmented Client Hello Packet is Received Out of Order
CSCwj83185	FTD/ASA : Standby FTD traceback and reload after enabling memory tracking
CSCwj83634	Seeing message "reg_fover_nlp_sessions: failover ioctl C_FOREG failed"
CSCwj86116	High LINA CPU observed due to NetFlow configuration
CSCwj87501	ASA/FTD may traceback and reload in Thread Name 'fover_FSM_thread'
CSCwj88400	FTD may traceback and reload in process name lina while processing appAgent msg reply
CSCwj88414	CVE-2023-48795 is not addressed on FMC 7.0.6.2 version
CSCwj89050	Faulty input validation in the core of Apache allows malicious or expl

Bug ID	Headline
CSCwj89051	In GNU tar before 1.35, mishandled extension attributes in a PAX archi
CSCwj89054	An attacker may cause an HTTP/2 endpoint to read arbitrary amounts of
CSCwj89264	FTD HA: Traceback and reload in netsnmp_oid_compare_ll
CSCwj89315	HTTP Response splitting in multiple modules in Apache HTTP Server allo
CSCwj89402	In the Linux kernel, the following vulnerability has been resolved: n
CSCwj89404	In the Linux kernel, the following vulnerability has been resolved: b
CSCwj89406	In the Linux kernel, the following vulnerability has been resolved: b
CSCwj89417	In the Linux kernel, the following vulnerability has been resolved: d
CSCwj89425	In the Linux kernel, the following vulnerability has been resolved: B
CSCwj89434	wall in util-linux through 2.40, often installed with setgid tty permi
CSCwj89445	The iconv() function in the GNU C Library versions 2.39 and older may
CSCwj89447	less through 653 allows OS command execution via a newline character i
CSCwj95590	Browser redirects to logon page when the user clicks the WebVPN bookmark
CSCwk02804	WebVPN connections stuck in CLOSEWAIT state
CSCwk02928	ASA/FTD may traceback and reload in Thread Name PTHREAD
CSCwk04492	ASA CLI hangs with 'show run' with multiple ssh sessions
CSCwk05826	nscd: Stack-based buffer overflow in netgroup cache If the Name Servi
CSCwk05828	nscd: netgroup cache may terminate daemon on memory allocation failure
CSCwk05851	"set ip next-hop" line deleted from config at reload if IP address is matched to a NAME
CSCwk06564	Add New Syslog for Routes for NP add/delete
CSCwk07934	Clock skew between FXOS and Lina causes SAML assertion processing failure
CSCwk08576	command to print the debug menu setting of service worker
CSCwk12497	Traceback and reload on active unit due to HA break operation.
CSCwk12698	SNMP polling of admin context mgmt interface fails to show all interfaces across all contexts
CSCwk13812	ASA/FTD incorrectly forwards extended community attribute after upgrade.
CSCwk14909	Traffic drop with 'rule-transaction-in-progress' after failover with TCM cfgd in multi-ctx mode

Bug ID	Headline
CSCwk17637	State Link Stops Sending Hello Messages Post-Failover Triggered by Snort Crash in FTD HA
CSCwk17854	FTD doesn't send Type A query after receiving a refuse error from one DNS server in AAAA query.
CSCwk21561	Add warning message when configuring CCL MTU
CSCwk22034	Snmpwalk displays incorrect interface speeds for values greater or equal than 10G
CSCwk22759	Issue with Setting Certain Timezones (e.g. GMT+1) on Cisco ASA Firepower in Appliance Mode
CSCwk22993	In the Linux kernel, the following vulnerability has been resolved: t
CSCwk24176	FTD/ASA - VPN traffic flowing through the device may trigger tracebacks and reloads.
CSCwk25117	ENH: Add application support for blocking consecutive AAA failures on LINA
CSCwk25506	Multiple snort binaries are present (Patch or HF) at /var/sf/bin/ making tar command to fail
CSCwk25755	In the Linux kernel, the following vulnerability has been resolved: n
CSCwk25756	Requests is a HTTP library. Prior to 2.32.0, when making requests thro
CSCwk25759	In the Linux kernel, the following vulnerability has been resolved: B
CSCwk25761	In the Linux kernel, the following vulnerability has been resolved: b
CSCwk25762	In the Linux kernel, the following vulnerability has been resolved: i
CSCwk25764	In the Linux kernel, the following vulnerability has been resolved: H
CSCwk26968	Backup feature does not save/restore DAP configuration in multiple context mode.
CSCwk27830	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwk32501	256/1550 block depletion process fover_thread
CSCwk36312	High cpu on "update block depletion" causing BGP flap terminated on FTD
CSCwk40726	FMC REST API calls to get AC policy data times out, AC policy GUI slowness with larger rule query
CSCwk41806	Need to Protect LINA from getting killed by OOM
CSCwk44245	In the Linux kernel, the following vulnerability has been resolved: i
CSCwk44246	In the Linux kernel, the following vulnerability has been resolved: i
CSCwk48975	Packet-tracer output incorrectly appends 'control-plane' to drops for data-plane access-group

Bug ID	Headline
CSCwk50044	The various Is methods (IsPrivate, IsLoopback, etc) did not work as ex
CSCwk50055	url.c in GNU Wget through 1.24.5 mishandles semicolons in the userinfo
CSCwk56443	Network address API calls taking long time to complete.
CSCwk57933	Vulnerabilities in linux-kernel CVE-2023-52439
CSCwk57949	Vulnerabilities in linux-kernel CVE-2023-52435
CSCwk62296	Address SSP OpenSSH regreSSHion vulnerability
CSCwk62381	ASA might traceback and reload due to ssh/client hitting a null pointer while using SCP.
CSCwk75030	The IPv6 implementation in the Linux kernel before 6.3 has a net/ipv6/
CSCwk75033	In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can cause inva
CSCwk75035	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vul
CSCwk75036	null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and

Resolved Bugs in Version 7.0.6.2

Table last updated: 2024-05-17

Table 54: Resolved Bugs in Version 7.0.6.2

Bug ID	Headline
CSCvu22491	FMC fails to connect to SSM with error "Failed to send the message to the server"
CSCvx37329	Remove Syslog Messages 852001 and 852002 in Firewall Threat Defense
CSCvx94744	FMC UI inaccessible due to flood of TSA (version 1.3) REST-API calls to FMC
CSCvy47786	Deployment preview will show unchanged/unadded comments to ACP rules
CSCvy90949	import of iips sfo with some overriden rules across sibling domains
CSCvz03407	IPTables.conf file is disappearing resulting in backup and restore failure.
CSCvz10481	sfo import fails when "import as new" option is selected
CSCvz70310	ASA may fail to create NAT rule for SNMP with: "error NAT unable to reserve ports."
CSCvz77254	Hotfix patch upgrade doesn't clean old snort3 binaries
CSCwa08084	FMC hardware appliance restore ends with an error "Unknown Failure Condition"
CSCwa22766	FMC4500/4600 shows virtual license

Bug ID	Headline
CSCwb41189	LINA time-sync correction
CSCwb55243	snort3 crashinfo sometimes fails to collect all frames
CSCwb95850	Snort down due to missing lua files because of disabled application detectors (PM side)
CSCwc31953	Prevention of RSA private key leaks regardless of root cause.
CSCwc40352	Lina Netflow sending permited events to Stealthwatch but they are block by snort afterwards
CSCwc44367	LSP not installed after HA failover. No LSP package found in the active LSP directory
CSCwd04135	Snort3 unexpectedly dropping packets after 4MB when using file inspection with detection mode NAP
CSCwd16850	More information is required on Syslog 202010 messages for troubleshooting
CSCwd31806	ASAv show crashinfo printing in loop continuously
CSCwd34079	FTD: Traceback & reload in process name lina
CSCwd58665	Intel Microcode Update required for FPR1000 products
CSCwd67100	ASA traceback and reload on Datapath process
CSCwd87438	Enhance logging mechanism for syslogs
CSCwe02012	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe03631	Need to provide rate-limit on "logging history <mode>"
CSCwe06562	FPR1K/FPR2K: Increase in failover time in Transparent Mode with high number of Sub-Interfaces
CSCwe11902	FTD: HA crash and interfaces down on FPR4200
CSCwe18472	[FTD Multi-Instance][SNMP] - CPU OIDs return incomplete list of associated CPUs
CSCwe21831	add warning to FTD platform settings when VPN Logging Settings logging level is informational
CSCwe21884	Write wrapper around "kill" command to log who is calling it
CSCwe30359	Traffic drops with huge rule evaluation on snort
CSCwe33282	FTD: The upgrade was unsuccessful because the httpd process was not running
CSCwe34269	DBCheck error is unclear when monetdb is in a 'crashed' state
CSCwe47485	FTD: CLISH slowness due to command execution locking LINA prompt
CSCwe47671	High memory usage on monetDB, FMC does not show connection events

Bug ID	Headline
CSCwe48997	FDM: Cannot create multiple RA-VPN profiles with different SAML servers that have the same SAML IDP
CSCwe56452	BGP IPv6 configuration : route-map association with neighbour not getting deployed
CSCwe58207	Memory leak observed on ASA/FTD when logging history is enabled
CSCwe60267	FXOS fault F0853 and F0855 seen despite keyring certificates reporting renewed
CSCwe65516	show xlate does not display xlate entries for internal interfaces (nlp_int_tap) after enabling ssh.
CSCwe72330	FTD LINA traceback and reload in Datapath thread after adding Static Routing
CSCwe79990	Cisco-Intelligence-Feed - Failed to download due to timeout
CSCwe87134	ASA/FTD: Traceback and reload due to high rate of SCTP traffic
CSCwe90334	Missing Instance ID in unified_events-2.log
CSCwe93137	KP - multimode: ASA traceback observed during HA node break and rejoin.
CSCwe93176	Snort2 rule assignments missing from ngfw.rules (assignment_data table) after FMC upgrade.
CSCwe93736	ASA not updating Timezone despite taking commands
CSCwe97939	ASA/FTD Cluster: Change "cluster replication delay" with max value increase from 15 to 50 sec
CSCwf00736	CSM backup failed within FMC backup due to modification of file while tar was reading it
CSCwf08387	LSP version not updated to latest in LINA Prompt in SSP_CLUSTER with 7.2.4 build.
CSCwf08790	FMC Restore of remote backup fails due to no space left on the device
CSCwf14031	Snort down due to missing lua files because of disabled application detectors (VDB side)
CSCwf17389	ASA accepts replayed SAML assertions for RA VPN authentication
CSCwf20215	admin user should be excluded from CLI shell access filter
CSCwf22045	MYSQL, or any TCP high traffic, getting blocked by snort3, with snort-block as Drop-reason
CSCwf25563	Device list takes longer to load while creating new AC policy
CSCwf36419	ASA/FTD: Traceback and reload with Thread Name 'PTHREAD'
CSCwf39108	Firewall rings may get stuck and cause packet loss when asp load-balance per-packet auto is used

Bug ID	Headline
CSCwf44621	Traceback and reload on Thread DATAPATH-6-21369 and linked to generation of syslog message ID 202010
CSCwf49486	store_*list_history.pl task is created every 5min without getting closed causing FMC slowness.
CSCwf59571	FTD/Lina - ZMQ issue OUT OF MEMORY. due to less Msglyr pool memory on certain platforms
CSCwf63589	FTD snmpd process traceback and restart
CSCwf64590	Units get kicked out of the cluster randomly due to HB miss | ASA 9.16.3.220
CSCwf67337	FMC taking long times to save override objects even if not modified
CSCwf69880	Firewall Traceback and reload due to SNMP thread
CSCwf75695	Duplicate FTD cluster has been created when multiple cluster events comes at same time
CSCwf82447	Editing identity nat rule disables "perform route lookup" silently
CSCwf82970	Snort2 engine is crashing after enabling TLS Server Identity Discovery feature
CSCwf86557	Decrypting engine/ssl connections hang with PKI Interface Error seen
CSCwf89959	ASA: ISA3000 does not respond to entPhySensorValue OID SNMP polls
CSCwf91282	import of .SFO to FMC failed due to included local/custom rules having a blank rule message field
CSCwf92661	ASA|FTD: Traceback & reload due to a free buffer corruption
CSCwf92726	LDAP missing files after upgrade when the Vault token is corrupted
CSCwf94450	FTD Lina traceback Thread Name: DATAPATH due to memory corruption
CSCwf99303	Management UI presents self-signed cert rather than custom CA signed one after upgrade
CSCwh00123	In Multi-manager scenario,cdFMC&Analytics FMC,FTD should only receive identity feeds from Config FMC
CSCwh01673	FTD /ngfw disk space full from Snort3 url db files
CSCwh04231	FMC needs to properly maintain Redis data directory to prevent unbounded disk usage
CSCwh09113	FPR1010 in HA failed to send or receive to GARP/ARP with error "edsa_rcv: out_drop"
CSCwh11411	Snort blacklisting traffic during deployment
CSCwh14352	Lina CiscoSSL upgrade to 1.1.1v and FOM 7.3a
CSCwh14584	Traceback seen on FTD running on Firepower 2100 series

Bug ID	Headline
CSCwh14863	FTD 7.0.4 cluster drops Oracle's sqlnet packets due to tcp-not-syn
CSCwh16759	SNMP is not working on the primary active ASA unit in multi-context environment
CSCwh19475	Intermittently flow is getting white-listed by the snort for the unknow app-id traffic.
CSCwh19613	ASA crashed with Saml scenarios
CSCwh19897	ASA/FTD Cluster: Reuse of TCP Randomized Sequence number on two different conns with same 5 tuple
CSCwh21474	ASA traceback when re-configuring access-list
CSCwh21772	Upgrade FxOS CiscoSSL to version 1.1.1v and FOM 7.3a
CSCwh24901	'Frequent drain of events (not unprocessed events) to be removed from FMC
CSCwh26526	SQL packets involved in large query is drop by SNORT3 with reason snort-block
CSCwh28206	Firewall Blocking packets after failover due to IP <-> SGT mappings
CSCwh30346	ASA/FTD: 1 Second failover delay for each NLP NAT rule
CSCwh36005	Policy deployment failed due to "1 errors seen during populateGlobalSnapshot"
CSCwh40106	FTD hosted on KP incorrectly dropping decoded ESP packets if pre-filter action is analyze
CSCwh40294	ASA traceback due to panic event during SNMP configuration
CSCwh41126	FMC ACP report does not shows all the access control rules
CSCwh42077	Cisco_Firepower_GEODB_FMC_Update* are not included in diskmanager
CSCwh42412	FTD Block 9344 leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwh45450	2100: Interfaces missing from FTD after removing interfaces as members of a port-channel
CSCwh45935	Lina core observed in 6.4.0.17-22 in Kp with scaled traffic
CSCwh47053	ASA/FTD may traceback and reload in Thread Name 'dns_cache_timer'
CSCwh47701	ASA allows same BGP Dynamic routing process for Physical Data and management-only interfaces
CSCwh49244	"show aaa-server" command always shows the Average round trip time 0ms.
CSCwh53745	ASA: unexpected logs for initiating inbound connection for DNS query response
CSCwh57976	Improve CPU utilization in ssl inspection for supported signature algorithm handling
CSCwh58467	ASA does not sent 'warmstart' snmp trap

Bug ID	Headline
CSCwh59199	ASA/FTD traceback and reload with IPSec VPN, possibly involving upgrade
CSCwh60504	LINA would randomly generate a traceback and reload on FPR-1K
CSCwh60604	ASA/FTD may traceback and reload in Thread Name 'lina' while processing DAP data
CSCwh60631	Fragmented UDP packet via MPLS tunnel reassemble fail
CSCwh60783	FTD - Captive portal enabled is still running despite the feature is off
CSCwh62080	additional command outputs needed in FTD troubleshoot for blocks and ssl cache
CSCwh65128	LINA show tech-support fails to generate as part of sf_troubleshoot.pl (Troubleshoot file)
CSCwh66359	ASDM can not see log timestamp after enable logging timestamp on cli
CSCwh68482	FTD: Traceback and Reload in Process Name: lina
CSCwh68878	Diskmanager process terminated unexpectedly
CSCwh69156	FTD-HA does not fail over sometimes when snort3 crashes
CSCwh69346	ASA: Traceback and reload when restore configuration using CLI
CSCwh70323	Timestamp entry missing for some syslog messages sent to syslog server
CSCwh70481	Community string sent from router is not matching ASA
CSCwh71161	ASA|FTD: Traceback & reload in thread Name: update_mem_reference
CSCwh71665	ASA traceback under match_partial_keyword during CPU profiling
CSCwh73727	Snort3 dropping IP protocol 51
CSCwh74586	XTLS: With TSID AC-Policy configured plugin is not disengaging immediately at CH
CSCwh75829	FMC Primary disk degraded error
CSCwh77348	ASA: Traceback and reload when executing the command "show nat pool detail" on a cluster setup
CSCwh79095	Snort generating an excessive number of snort-unified log files with zero bytes
CSCwh83254	ASA/FTD: Traceback and reload on thread name CP Crypto Result Processing
CSCwh84376	In FPR4200/FPR3100-cluster observed core file ?core.lina? observed on device reboot.
CSCwh91065	Lina Traceback : Thread Name: DATAPATH during session terminate
CSCwh91574	FTD: Traceback in threadname cli_xml_request_process
CSCwh92345	crypto_archive file generated after the software upgrade.

Bug ID	Headline
CSCwh92541	Random FTD snort3 traceback
CSCwh93710	Last Rule hit shows a hex value ahead of current time in ASA and ASDM
CSCwh95010	Unexpected traceback on thread name Lina and device experienced reboot
CSCwh95025	GTP connections, under certain circumstances do not get cleared on issuing clear conn.
CSCwh95175	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwh95277	FTD VMWARE 7.0.5 trackbacks due to system memory exhaustion
CSCwh96055	Management DNS Servers may be unreacheable if data interface is used as the gateway
CSCwh99331	syslog not generated "ASA-3-202010: NAT pool exhausted" while passing traffic from iLinux to oLinux
CSCwi01085	FTD VMWare tracebacks at PTHREAD-3587
CSCwi01381	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi02134	FTD sends multiple replicated NetFlow records for the same flow event
CSCwi02754	FTD 1120 standby sudden reboot
CSCwi03407	Traceback on FP2140 without any trigger point.
CSCwi04351	FTD upgrade failling on script 999_finish/999_zz_install_bundle.sh
CSCwi11520	FTD OSPFV3 IPV6 Routing: FTD is sending unsupported extended LSA request to neighbor routers
CSCwi14896	Node kicked out of cluster while enabling or disabling rule profiling
CSCwi15409	ASA/FTD - may traceback and reload in Thread Name 'Unicorn Proxy Thread'
CSCwi15595	ASA traceback and reload during ACL configuration modification
CSCwi16998	CCM Seq 58 - LTS18
CSCwi18581	Firewall traceback and reload due to SSH thread
CSCwi18663	FMC-4600: Pre-Filter policy is showing as none
CSCwi19145	FTD/ASA may traceback and reload in PKI, syslog, during upgrade
CSCwi19485	Fail open snort-down is off in inline pairs despite it being enabled and deployed from FMC
CSCwi19849	VPN load-balancing cluster encryption using Phase 2 deprecated ciphers
CSCwi20045	ASA/FTD may traceback and reload in Thread Name 'lina' due to a watchdog in 9.16.3.23 code

Bug ID	Headline
CSCwi20848	ASA/FTD high memory usage due to SNMP caused by RAVPN OID polling
CSCwi20955	FTD with may traceback in data-path during deployment when enabling TAP mode
CSCwi21625	FailSafe admin password is not properly sync'd with system context enable pw
CSCwi26895	ASA SNMP OID cpmCPUTotalPhysicalIndex returning zero values instead of CPU index values
CSCwi27338	Stale asp entry for TCP 443 remains on standby after changing default port
CSCwi27402	FTD: Update WM firmware to 1023.0207
CSCwi27459	Snort Crash during selection of signature algorithm ECDSA
CSCwi31091	OSPF Redistribution route-map with prefix-list not working after upgrade
CSCwi31558	file-extracts.logs are not recognised by the diskmanager leading to High disk space
CSCwi31966	FTD ADI debugs may show incorrect server_group and/or realm_id for SAML-authenticated sessions
CSCwi32063	ASA/FTD: SSL VPN Second Factor Fields Disappear
CSCwi32759	Username-from-certificate secondary attribute is not extracted if the first attribute is missing
CSCwi33817	ASA/FTD: 'IKEv2 Negotiation aborted due to ERROR: Platform errors' during a rekey
CSCwi34125	ASA: Snmpwalk shows "No Such Instance" for the OID ceSensorExtThresholdValue
CSCwi34719	Unable to SSH into FTD device using External authentication with Radius
CSCwi36311	use kill tree function in SMA instead of SIGTERM
CSCwi38061	ASA/FTD traceback and reload due to file descriptor limit being exceeded
CSCwi40193	Hairpinning of DCE/RPC traffic during the suboptimal lookup
CSCwi40487	FTD HA Failure after SNORT crash.
CSCwi40536	ASA/FTD: Traceback and reload when running show tech and under High Memory utilization condition
CSCwi42962	installing GeoDB country code package update to FMC does not automatically push updates to FTDs
CSCwi42992	ASA/FTD may traceback and reload in Thread Name IKEv2 Daemon
CSCwi43782	GTP inspection dropping packets with IE 152 due to header length being invalid for IE type 152
CSCwi44208	low memory/stress causing traceback in SNMP

Bug ID	Headline
CSCwi46010	ASA/FTD: Cluster incorrectly generating syslog 202010 for invalid packets destined to PAT IP
CSCwi46023	FTD drops double tagged BPDUs.
CSCwi48699	ASA traceback and reload on Thread Name: pix_flash_config_thread
CSCwi49884	TCP MSS is changed back to the default value when a VTI or loopback interface is created
CSCwi50343	Their standalone FTD running 7.2.2 on FPR-4112 experienced a traceback on the SNMP module
CSCwi53150	Service object-group protocol type mismatch error seen while access-list referencing already
CSCwi53431	Unable to Synch more then 100 environment-data with data unit
CSCwi55938	The "show asp drop" command usage requires better updates for cluster-related drops
CSCwi56048	Interface fragment queue may get stuck at 2/3 of fragment database size
CSCwi59525	Multiple lina cores on 7.2.6 KP2110 managed by cdFMC
CSCwi59831	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi60285	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwi63113	Null pointer dereference in SNMP that results in traceback and reload
CSCwi63743	ASA/FTD may traceback and reload in Thread Name "appAgent_monitor_nd_thread" & Rip: _lina_assert.
CSCwi64829	traceback and reload around function HA
CSCwi65116	DHCPv6:ASA traceback on Thread Name: DHCPv6 CLIENT.
CSCwi66103	Lina traceback on RAVPN connection after enabling webvpn debug
CSCwi66676	ASA/FTD may traceback and reload in Thread Name 'webvpn_task'
CSCwi74214	ASA/FTD traceback and reload in Thread Name: IKEv2 Daemon when moving from active to standby HA
CSCwi75198	Standby FTD experiencing periodic traceback and reload
CSCwi75967	CCM ID 62 - LTS18
CSCwi76002	Memory exhaustion due to absence of freeing up mechanism for tmatch
CSCwi76361	Transparent firewall MAC filter does not capture frames with STP-UplinkFast dst MAC consistently
CSCwi76630	FP2100/FP1000: ASA Smart licenses lost after reload

Bug ID	Headline
CSCwi79042	FTD/Lina traceback and reload of HA pairs, in data path, after adding NAT policy
CSCwi79703	Incorrect Timezone Format on FTD When Configured via FXOS
CSCwi80465	CCM ID 63 - LTS18
CSCwi84615	some stdout logs not rotated by logrotate
CSCwi86198	SFData correlator keep terminating on FTDs configured for IDS
CSCwi86503	File sizes larger than 100MB for AnyConnect/Secure Client images cannot be uploaded on FMC
CSCwi87382	Traceback and reload on Primary unit while running debugs over the SSH session
CSCwi90040	Cisco ASA and FTD Software Command Injection Vulnerability
CSCwi90371	ASA:request to add "logging list" option to the "logging history" command.
CSCwi90399	FTD/ASA system clock resets to year 2023
CSCwi90571	Access to website via Clientless SSL VPN Fails
CSCwi95228	"crypto ikev2 limit queue sa_init" resets after reboot
CSCwi95708	FTD: Hostname Missing from Syslog Message
CSCwi95994	Chromium-based browsers have SSL connection conflicts when FIPS CC is enabled on the firewall.
CSCwi97839	FTD traceback assert in vni_idb_get_mode and reloaded
CSCwi98284	Cisco ASA and FTD Software Persistent Local Code Execution Vulnerability
CSCwj02505	ASA Checkheaps traceback while entering same engineID twice
CSCwj09110	Upload files through Clientless portal is not working as expected after the ASA upgrade
CSCwj10955	Cisco ASA and FTD Software Web Services Denial of Service Vulnerability
CSCwj12131	Bailout when lina_io_write fails persistent with EPIPE errno.

Resolved Bugs in Version 7.0.6.1

Table last updated: 2025-02-25

Table 55: Resolved Bugs in Version 7.0.6.1

Bug ID	Headline
CSCvt25221	FTD traceback in Thread Name cli_xml_server when deploying QoS policy
CSCvx04003	Lack of throttling of ARP miss indications to CP leads to oversubscription

Bug ID	Headline
CSCvx54562	High System Overhead memory on FTD
CSCvy81493	traceback and reload with 'CHECKHEAPS HAS DETECTED A MEMORY CORRUPTION'
CSCvz07439	Smart Lic Agent stuck in waiting state after failover and continuously switches from lock and unlock
CSCwa70323	Unable to push extra domains >1024 Character, as part of Custom Attribute under Anyconnect VPN
CSCwc78781	ASA/FTD may traceback and reload during ACL changes linked to PBR config
CSCwc82205	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwd10822	Failover trigger due to Inspection engine in other unit has failed due to disk failure
CSCwd28037	No nameif during traffic causes the device traceback, lina core is generated.
CSCwd38583	ASA/FTD: Command "no snmp-server enable oid mempool" enabled by default or enforced during upgrades
CSCwd83141	CCL/CLU filters are not working correctly
CSCwd89095	Stratix5950 and ISA3000 LACP channel member SFP port suspended after reload
CSCwd98316	Cisco ASA and FTD Software VPN Packet Validation Vulnerability
CSCwe04043	FTD HA upgrade fails due to one unit starting upgrade before the other rejoins HA pair
CSCwe12705	multimode-tmatch_df_hijack_walk traceback observed during shut/unshut on FO connected switch interfa
CSCwe28407	LINA traceback with icmp_thread
CSCwe28912	FPR 4115- primary unit lost all HA config after ftd HA upgrade
CSCwe42061	Deleting a BVI in FTD interfaces is causing packet drops in other BVIs
CSCwe48399	The public API function BIO_new_NDEF is a helper function used for str
CSCwe51443	ASA Evaluation of OpenSSL vulnerability CVE-2022-4450
CSCwe67816	ASA / FTD Traceback and reload when removing isakmp capture
CSCwe74089	ASA/FTD may traceback and reload in Thread Name DATAPATH-1-1656
CSCwe79051	Deployment for eigrp / bgp change may cause temporary outage during policy apply
CSCwe82704	PortChannel sub-interfaces configured as data/data-sharing, in multi-instance HA go into "waiting"
CSCwe83255	ASA/FTD may traceback and reload in Thread Name 'lina'

Bug ID	Headline
CSCwe86225	ASA/FTD traceback and reload due citing thread name: cli_xml_server in tm_job_add
CSCwe90609	Cisco ASA Software and FTD Software SNMP Denial of Service Vulnerability
CSCwe98319	ASAConfig multiple restarts are leaking 16K memory in every Restart leading to ZMQ Out Of Memory.
CSCwf04460	The fxos directory disappears after cancel show tech fprm detail command with Ctr+c is executed .
CSCwf05295	FTD running on FP1000 series might drop packets on TLS flows after the "Client Hello" message.
CSCwf10910	FTD : Traceback in ZMQ running 7.3.0
CSCwf14126	ASA Traceback and reload citing process name 'lina'
CSCwf15902	ASAv in Hyper-V drops packets on management interface
CSCwf16559	getReadinessStatusTaskList pjb request is very frequent when user in Upgrade sensor list page
CSCwf17042	ASDM replaces custom policy-map with default map on class inspect options at backup restore.
CSCwf22005	ASA/FTD : Packet-tracer may displays incorrect ACL rule, though produces correct verdict.
CSCwf22637	Network Object Group overrides not visible or be edited from FMC GUI
CSCwf25144	FMC backup management page showing "Verifying Backup" for FTD sensors.
CSCwf26407	FP2130- Unable to disassociate member from port channel, deployment fails, member is lost on FTD/FMC
CSCwf26534	ASA/FTD: Connection information in SIP-SDP header remains untranslated with destination static Any
CSCwf33904	[IMS_7_4_0] - Virtual FDM Upgrade fails: HA configStatus='OUT_OF_SYNC after UpgradeOnStandby
CSCwf34500	FTD: GRE traffic is not being load balanced between CPU cores
CSCwf35207	ASA: Traceback and reload while updating ACLs on ASA
CSCwf35233	Cisco Adaptive Security Appliance Software and Firepower Threat Defense DoS
CSCwf35573	Traffic may be impacted if TLS Server Identity probe timeout is too long
CSCwf39163	ASAv - High latency is experienced on Azure environment for ICMP ping packets while running snmpwalk
CSCwf43537	Lina crash in thread name: cli_xml_request_process during FTD cluster upgrade

Bug ID	Headline
CSCwf44537	99.20.1.16 lina crash on nat_remove_policy_from_np
CSCwf45094	MariaDB Process in FMC should use jemalloc instead of glibc
CSCwf47227	Remove Priority-queue command from FTD|| Priority-queue command causes silent egress packet drops
CSCwf48599	VPN load-balancing cluster encryption using deprecated ciphers
CSCwf49573	ASA/FTD: Traceback and reload when issuing 'show memory webvpn all objects'
CSCwf50497	DNS cache entry exhaustion leads to traceback
CSCwf52810	ASA SNMP polling not working and showing "Unable to honour this request now" on show commands
CSCwf54418	Reduce time taken to clear stale IKEv2 SAs formed after Duplicate Detection
CSCwf54510	ASA traceback and reload on Thread Name: DHCPRA Monitor
CSCwf56811	ASA Traceback & reload on process name lina due to memory header validation
CSCwf59176	FXOS raises a fault for administratively disabled management interface
CSCwf60311	ASA generating traceback with thread-name: DATAPATH-53-18309 after upgrade to 9.16.4.19
CSCwf60590	"show route all summary" executed on transparent mode FTD is causing CLISH to become Sluggish.
CSCwf62729	Cisco ASA/FTD Firepower 2100 SSL/TLS Denial of Service Vulnerability
CSCwf62820	Failover: standby unit traceback and reload during modifying access-lists
CSCwf63872	FTD taking longer than expected to form OSPF adjacencies after a failover switchover
CSCwf69901	FTD: Traceback and reload during OSPF redistribution process execution
CSCwf72434	Add meaningful logs when the maximums system limit rules are hit
CSCwf73773	Dumping of last 20 rmu request response packets failed
CSCwf77191	ASA appliance mode - 'connect fxos [admin]' will get ERROR: failed to open connection.
CSCwf78321	ASA: Checkheaps traceback and reload due to Clientless WebVPN
CSCwf81058	FTD: Firepower 3100 Dynamic Flow Offload showing as Enabled
CSCwf82247	Policy deployment fails when a route same prefix/metric is configured in a separate VRF.
CSCwf92135	ASA: Traceback and reload on Tread name "fover_FSM_thread" and ha_ntfy_prog_process_timer

Bug ID	Headline
CSCwf92182	Cisco Firepower Management Center Software SQL Injection Vulnerability
CSCwf92646	ECDSA Self-signed certificate using SHA384 for EC521
CSCwf94677	"failover standby config-lock" config is lost after both HA units are reloaded simultaneously
CSCwf95147	OSPFv3 Traffic is Centralized in Transparent Mode
CSCwf95288	FPR1k Switchport passing CDP traffic
CSCwh04365	ASA Traceback & reload on process name lina due to memory header validation - webvpn side fix
CSCwh04395	ASDM application randomly exits/terminates with an alert message on multi-context setup
CSCwh04730	ASA/FTD HA checkheaps crash where memory buffers are corrupted
CSCwh05863	ASA omits port in host field of HTTP header of OCSP request if non-default port begins with 80
CSCwh06452	Interface speed mismatch in SNMP response using OID .1.3.6.1.2.1.2.2
CSCwh08403	FMC HA - Health Policy - Applied count shows "0" appliance
CSCwh08481	ASA traceback on Lina process with FREEB and VPN functions
CSCwh11764	ASA/FTD may traceback and reload in Thread Name "RAND_DRBG_bytes" and CTM function on n5 platforms
CSCwh12987	Large SMB servers result in timeouts returning verdicts between FMC and FTD devices
CSCwh13821	ASA/FTD may traceback and reload in when changing capture buffer size
CSCwh14467	File sizes larger than 100MB for AnyConnect/Secure Client images cannot be uploaded on FMC
CSCwh14597	ASA/FTD residual free
CSCwh15223	Lina crash in snp_fp_tcp_normalizer() when DAQ/Snort sends malformed L3 header
CSCwh16301	Incorrect Hit count statistics on ASA Cluster only for Cluster-wide output
CSCwh20002	Standby FMC is not getting updated with latest GEO DB package
CSCwh21141	The FMC preview deployment shows a wrong information.
CSCwh21772	Upgrade FxOS CiscoSSL to version 1.1.1v and FOM 7.3a
CSCwh23100	Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
CSCwh23567	PAC Key file missing on standby on reload

Bug ID	Headline
CSCwh25668	ASA 55xx devices running 7.0.6 show up as 100% usage on CPU01 [LINA]
CSCwh27230	Connections are not cleared after idle timeout when the interfaces are in inline mode.
CSCwh28144	Specific OID 1.3.6.1.2.1.25 should not be responding
CSCwh30676	Ping to the configured systemIP on management interface getting failed in cluster setup.
CSCwh30891	ASA/FTD may traceback and reload in Thread Name 'ssh' when adding SNMPV3 config
CSCwh31495	FTD - Traceback and reload due to nat rule removed by CPU core
CSCwh32118	ASDM management-sessions quota reached due to HTTP sessions stuck in CLOSE_WAIT
CSCwh37475	Removal of msie-proxy commands during flexconfig rollback
CSCwh41127	ASA/FTD: NAT64 error "overlaps with inside standby interface address" for Standalone ASA
CSCwh45108	Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
CSCwh49483	ASA/FTD may traceback and reload while running show inventory
CSCwh50060	Some TLS1.3 probes test site cases fail due to rst+ack not sent out of FTD during timeout
CSCwh52420	AMP Cloud look up timeout frequently.
CSCwh56945	SFDataCorrelator crashing repeatedly in RNA_DB_InsertServiceInfo
CSCwh64508	Fixing the regression caused while handling web UI is not getting FTDv Variable
CSCwh69209	Prefilter cannot add Tunnel Endpoints in Tunnel Rule on FMC
CSCwh69815	FTDvs through put got changed to 100Kbps after upgrade

Resolved Bugs in Version 7.0.6

Table last updated: 2024-05-22

Table 56: Resolved Bugs in Version 7.0.6

Bug ID	Headline
CSCvo58100	Incorrect validation msg - Invalid value supplied for input parameter : "?"
CSCvq20057	Improve logging of Secure Firewall (Firepower)backups and retry for gzip when using remote storage

Bug ID	Headline
CSCvq25866	Flex config Preview of $SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST throws error
CSCvr45136	Adding details and logs when gzip fails and results in backup failure
CSCvs27336	Traceback on ASA by Smart Call Home process
CSCvs89229	Incorrect rules are highlighted during search in AC rules
CSCvt35116	Cisco Firepower Management Center Software Information Disclosure Vulnerability
CSCvt43334	Cores generated due to expected/graceful shutdown need to be cleaned up
CSCvu22491	FMC fails to connect to SSM with error "Failed to send the message to the server"
CSCvu24703	FTD - Flow-Offload should be able to coexist with Rate-limiting Feature (QoS)
CSCvu96436	Traceback of master and one slave when a particular lock is contended for long
CSCvv59757	FMC event report generation fails if one is already running
CSCvw82067	ASA/FTD 9344 blocks depleted due to high volume of fragmented traffic
CSCvx04436	Forbidden to run multiple SFDaCo processes, but pidfile not successful at blocking second instance
CSCvx21458	FMC shows error when editing prefix-list attached to active route-map within BGP protocol
CSCvx24207	FQDN Object Containing IPv4 and IPv6 Addresses Only Install IPv6 Entries
CSCvx27744	Policy deployment may fail on FTD after 6.6.1 due to failure to get version upgrade information
CSCvx36885	ASA Traceback & reload in thread Name: DATAPATH
CSCvx52042	Upgrade to 6.6.1 got failed at 800_post/1025_vrf_policy_upgrade.pl
CSCvx55978	Performance Degradation in GetGroupDependency API
CSCvx56021	FTD: CTS SGT propagation gets enabled after reload
CSCvx59181	Email/SNMP/Syslog Health Alerts are not sent out of fmc for cpu and mem
CSCvx65032	FMC ACL Search Move arrows do not work
CSCvx67856	Prometheus process doesnt come up when system ungracefully rebooted
CSCvx68173	Observed few snort instances stuck at 100%
CSCvx71936	FXOS: Fault "The password encryption key has not been set." displayed on FPR1000 and FPR2100 devices
CSCvx94744	FMC UI inaccessible due to flood of TSA (version 1.3) REST-API calls to FMC

Bug ID	Headline
CSCvx97723	hmdaemon process restart during automation test
CSCvy12991	Chassis local date and time may drift back to midnight Jan 1 2015 after reboot
CSCvy16537	Some externalization columns do not match any data when used in where clause
CSCvy24435	FMC GUI can be accessed by an expired password when using .cgi with https://FMCIP/login.cgi
CSCvy26511	Tune unmanaged disk alert thresholds for low end platforms
CSCvy26676	"Warning:Update failed/in-progress." Cosmetic after successful update
CSCvy33879	FTD: repair_users.pl creates rogue .firstboot file that causes FTD reboot failure
CSCvy35737	FTD traceback and reload during anyconnect package verification
CSCvy40493	Selective policy deployment of AC Policy does not export to ngfw.rules
CSCvy47786	Deployment preview will show unchanged/unadded comments to ACP rules
CSCvy50598	BGP table not removing connected route when interface goes down
CSCvy50797	Policy deployment may fail if platform settings contain DH group1 for SSL
CSCvy52617	FMC6.7 changes IPSec Profiles on VTI with each deployment resulting in tunnel flap
CSCvy55676	FMC Deployment failed due to internal errors
CSCvy57905	VTI tunnel interface stays down post reload on KP/WM platform in HA
CSCvy63414	Deploy Preview & Rollback not working when config archival is corrupted
CSCvy65178	Need dedicated Rx rings for to the box BGP traffic on Firepower platform
CSCvy65770	ASA/FTD: Traceback and reload during BGP route update
CSCvy67765	FTD VTI reports TUNNEL_SRC_IS_UP false despite source interface is up/up and working
CSCvy73130	FP4100 platform: Active-Standby changed to dual Active after running "show conn" command
CSCvy84336	Add a warning when member interfaces of the port-channel are different between active and standby
CSCvy86817	Cruz ASIC CLU filter has the incorrect src/dst IP subnet when a custom CCL IP subnet is set
CSCvy88023	FP2100 coredumps do not display the original crashing thread
CSCvy90836	ASA Traceback and reload in Thread Name: SNMP ContextThread
CSCvy90949	import of iips sfo with some overriden rules across sibling domains

Bug ID	Headline
CSCvy91668	PAT pool exhaustion with stickiness traffic could lead to new connection drop.
CSCvy98458	FP21xx -traceback "Panic:DATAPATH-10-xxxx -remove_mem_from_head: Error - found a bad header"
CSCvz03407	IPTables.conf file is disappearing resulting in backup and restore failure.
CSCvz07439	Smart Lic Agent stuck in waiting state after failover and continuously switches from lock and unlock
CSCvz07712	Deployment fails with internal_errors - Cannot get fresh id
CSCvz09106	Cisco ASA and FTD Software SSL VPN Denial of Service Vulnerability
CSCvz10428	FMC Health monitoring standby FMC unit does not have data displayed for CPU
CSCvz10481	sfo import fails when "import as new" option is selected
CSCvz20679	FTDv - Lina Traceback and reload
CSCvz22668	FMC backup restoration may fail due to VMS database restoration failure
CSCvz24765	device rebooted with snmpd core
CSCvz28145	Error "Another operation by another user prevented this operation. Please retry after sometime."
CSCvz29656	FMC connection event search causing high memory utilization for index.cgi
CSCvz29976	Malware event processing may misbehave with "already part of another table" error
CSCvz34289	In some cases transition to lightweight proxy doesn't work for Do Not Decrypt flows
CSCvz36903	ASA traceback and reload while allocating a new block for cluster keepalive packet
CSCvz37306	ASDM session is not served for new user after doing multiple context switches in existing user
CSCvz38332	FTD/ASA - Stuck in boot loop after upgrade from 9.14.2.15 to 9.14.3
CSCvz38692	ASAv traceback in snmp_master_callback_thread and reload
CSCvz39646	ASA/AnyConnect - Stale RADIUS sessions
CSCvz40098	FTD HA: Health Monitor page shows "Error in fetching device details Error: validation failed"
CSCvz40245	Firepower bandwidth_analyzer tool calculates results in MBps instead of Mbps
CSCvz41551	FP2100: ASA/FTD with threat-detection statistics may traceback and reload in Thread Name 'lina'
CSCvz42065	IPS policy should be imported when its referred in Access Control policy

Bug ID	Headline
CSCvz42553	Alarm: Health Alert Smart Licensing Agent not running
CSCvz43414	Internal ldap attribute mappings fail after HA failover
CSCvz43455	ASAv observed traceback while upgrading hostscan
CSCvz44339	FTD - Deployment will fail if you try to delete an SNMP host with ngfw-interface and host-group
CSCvz48407	Traceback and reload in Thread Name: DATAPATH-15-18621
CSCvz49163	Observed some time drift in seconds in the output when we execute show rule hits multiple times
CSCvz50712	TLS server discovery uses incorrect source IP address for probes in AnyConnect deployment
CSCvz51175	FTD HA not forming when SNMP adminState is disabled
CSCvz53142	ASA does not use the interface specified in the name-server command to reach IPv6 DNS servers
CSCvz53372	Snort goes into D state after executing "config log-events-to-ramdisk disable"
CSCvz54318	Policy deployment failure: "No LSP package found in the active lsp directory"
CSCvz55302	FTD/ASA Traceback and reload due to SSL null checks under low memory conditions
CSCvz55395	TCP connections are cleared after configured idle-timeout even though traffic is present
CSCvz57710	conf t is converted to disk0:/t under context-config mode
CSCvz58710	ASA traceback due to SCTP traffic.
CSCvz60142	ASA/FTD stops serving SSL connections
CSCvz61160	ASA traceback on DATAPATH when handling ICMP error message
CSCvz61477	RAVPN Authorization fails if same RADIUS server is used as authentication and authorization server
CSCvz62653	ASA memory leak resulting in error messages and causing tracebacks
CSCvz64470	ASA/FTD Traceback and reload due to memory corruption when generating ICMP unreachable message
CSCvz66236	Threshold mis-behavior of "-1" after configuring Type:Both for specific rule
CSCvz67003	ASDM session count and quota management's count mismatch. 'Lost connection firewall' msg in ASDM
CSCvz68713	PLR license reservation for ASAv5 is requesting ASAv10

Bug ID	Headline
CSCvz69571	ASA log shows wrong value of the transferred data after the anyconnect session terminated.
CSCvz69729	Unstable client processes may cause LINA zmqio traceback on FTD
CSCvz70316	LINA may generate traceback and reload
CSCvz70595	Cisco ASA Software and FTD Software Web Services Interface Denial of Service Vulnerability
CSCvz71340	observed snort3 core on xTLSServerKeyExchangeProcessor
CSCvz71542	No messages displayed on the console for any inserted SFP cable after removal.
CSCvz71596	"Number of interfaces on Active and Standby are not consistent" should trigger warning syslog
CSCvz73709	ASA/FTD Standby unit fails to join HA
CSCvz75988	Inconsistent logging timestamp with RFC5424 enabled
CSCvz76652	Proxy URI URL for URL Filtering (beaker service) includes encoded user/password strings
CSCvz77213	FTD: show ntp shows managing DC even though NTP sync is done via FXOS
CSCvz77254	Hotfix patch upgrade doesn't clean old snort3 binaries
CSCvz77662	Crash at data-path from Scaled AC-SSL TVM Profile test.
CSCvz77744	OSPFv3: FTD Wrong "Forwarding address" added in ospfv3 database
CSCvz78548	Unable to load Devices --> Certificates page
CSCvz81480	Cisco ASA Software and FTD Software IPsec IKEv2 VPN Information Disclosure Vulnerability
CSCvz81513	FMC - Backup failing due to "CSM backup failed"
CSCvz84850	ASA/FTD traceback and reload caused by "timer services" function
CSCvz85493	FTD backup.log increased file size causing /ngfw to reach 100% full
CSCvz87401	SNMP Operations Can Be Performed from Any Host to FTD
CSCvz88020	ASAv: coredumpfsys is formatted during bootup
CSCvz91396	FTD: Deployment will fail when AC Policy is huge
CSCvz94322	"adi" core file on FTDv after instance resize - VMware
CSCvz94841	Grammatical errors in failover operating mode mismatch error message
CSCvz97196	Can't create Flexconfig Object with ldap-naming-attribute pager cause pager is block.

Bug ID	Headline
CSCwa03341	Standby's sub interface mac doesn't revert to old mac with no mac-address command
CSCwa04262	Cisco ASA Software SSL VPN Client-Side Request Smuggling Vulnerability via "/"URI
CSCwa08084	FMC hardware appliance restore ends with an error "Unknown Failure Condition"
CSCwa22766	FMC4500/4600 shows virtual license
CSCwa27253	FMC : Device Listing Page Slowness
CSCwa27488	Fail to import with error "is not a table"
CSCwa29934	Interfaces on standalone 2120 and 2110 FTD show as modified after upgrade to 7.0.1-84 from 6.6.5
CSCwa31488	FDM High Availability cannot be created using Etherchannel as failover interface.
CSCwa32956	Connection events are not sent to Firepower Management Center due to deploy race condition
CSCwa35596	Registered devices may miss on standby FMC due to AnyConnect HostScan class files sync failure
CSCwa36535	Standby unit failed to join failover due to large config size.
CSCwa41936	Cisco FTD Bleichenbacher Attack Vulnerability
CSCwa43311	Snort blocking and dropping packet, with bigger size(1G) file download
CSCwa45369	Execution of commands appears to result in a new zombie process
CSCwa47737	ASA/FTD may hit a watchdog traceback related to snmp config writing
CSCwa49480	SNMP OID , stop working after around one hour and a half - FTD
CSCwa56969	FMC Readiness Check failed for 7.0.1 7.1.0 HF: type object ProgressReport has no attribute 'KB_UNIT'
CSCwa59907	LINA observed traceback on thread name "snmp_client_callback_thread"
CSCwa61361	ASAv traceback when SD_WAN ACL enabled, then disabled (or vice-versa) in PBR
CSCwa62025	IPv6: Some of egress interfaces of global and user vrf routes are missing in asp table
CSCwa68004	FMC 7.0 FlexConfig blocked mac-address-table aging-time for transparent FTD without any alternativ
CSCwa68552	All type-8 passwords are lost upon upgrade from ASA 9.12-9.15 to 9.16, failover gets disabled
CSCwa70323	Unable to push extra domains >1024 Character, as part of Custom Attribute under Anyconnect VPN

Bug ID	Headline
CSCwa72481	API key corrupted for FMC with multiple interfaces
CSCwa72528	user-name from certificate feature does not work with SER option
CSCwa72530	FTD: Time gap/mismatch seen when new node joins a Cluster Control node under history
CSCwa72929	SNMPv3 polling may fail using privacy algorithms AES192/AES256
CSCwa73172	ASA reload and traceback in Thread Name: PIX Garbage Collector
CSCwa75966	ASA: Reload and Traceback in Thread Name: Unicorn Proxy Thread with Page fault: Address not mapped
CSCwa79604	Infinitely running jobs in the task list
CSCwa79905	FMC NAT Policy report generation does not record the rules every 51*x
CSCwa82850	ASA Failover does not detect context mismatch before declaring joining node as "Standby ready"
CSCwa87298	ASA conn data-rate: incorrect "current rate" and "data-rate-filter" doesn't work properly
CSCwa89116	Clean up session index handling in IKEv2/SNMP/Session-mgr for MIB usage
CSCwa89560	NAT rule modification after rule search changes rule order
CSCwa94440	syncd process exits due to invalid GID and database synchronization issue
CSCwa95079	ASA/FTD Traceback and reload due to NAT configuration
CSCwa96860	Failover high convergence causes traffic failures
CSCwa96920	ASA/FTD may traceback and reload in process Lina
CSCwa97423	Deployment rollback causes brief traffic drop due to order of operations
CSCwa97917	ISA3000 in boot loop after powercycle
CSCwa99931	ASA/FTD: Tuning of update_mem_reference process
CSCwb00871	ENH: Reduce latency in log_handler_file to reduce watchdog under scale or stress
CSCwb02060	snmp-group host with Invalid host range and subnet causing traceback and reload
CSCwb02955	Modify /800_post/1027_ldap_external_auth_fix.pl to not fail FMC upgrade when objects are corrupt
CSCwb03702	SSH: missing null pointer check leading to snort traceback and reload
CSCwb03704	ASA/FTD datapath threads may run into deadlock and generate traceback
CSCwb04000	ASA/FTD: DF bit is being set on packets routed into VTI

Bug ID	Headline
CSCwb04975	FTD Snort3 traceback in daq-pdts while handling FQDN based traffic
CSCwb05148	Cisco ASA Software and FTD Software SNMP Denial of Service Vulnerability
CSCwb05291	Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability
CSCwb05920	Crash in KP at webVpn free, HTTPCleanUp and mem_mh_free from Scaled AC-IK/IPSec TVM test.
CSCwb06575	Windows 11 OS is not selectable when creating a DAP record via FMC
CSCwb06847	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-9-11543'
CSCwb07908	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
CSCwb07981	Traceback: Standby FTD reboots and generates crashinfo and lina core on thread name cli_xml_server
CSCwb08189	Microsoft update traffic blocked with Snort version 3 Malware inspection
CSCwb08644	ASA/FTD traceback and reload at IKEv2 from Scaled S2S+AC-DTLS+SNMP long duration test
CSCwb09606	FP2100: ASA/FTD high availability is not resilient to unexpected lacp process termination
CSCwb10874	Ensure DB consistency when synchronizing users
CSCwb12476	vm_max size for MonetDB is not set programmatically, which can lead to a setting of zero
CSCwb16037	Unable to replace the anyconnect image when maximum memory used for anyconnect images.
CSCwb16920	CPU profile cannot be reactivated even if previously active memory tracking is disabled
CSCwb17187	SNMP cores are generated every minute while running snmpwalk on HA
CSCwb17963	Unable to identify dynamic rate liming mechanism & not following msg limit per/sec at syslog server.
CSCwb19387	ASA SNMP Poll is failing & show display "Unable to honour this request now.Please try again later."
CSCwb19648	SNMP queries for crasLocalAddress are not returning the assigned IPs for SSL/DTLS tunnels.
CSCwb20206	FTD: Logs and Debugs for SSL/TLS traffic drop due to NAP in Detection Mode
CSCwb22592	SSH Functionalty stopped working after running long duration tests of SCP + Scaled TVM VPN Profiles
CSCwb24039	ASA traceback and reload on routing

Bug ID	Headline
CSCwb24306	duplicate log entry for /mnt/disk0/log/asa_snmp.log
CSCwb25809	Single Pass - Traceback due to stale ifc
CSCwb28123	FTD HA deployment fails with error "Deployment failed due to major version change on device"
CSCwb28427	ssl rule with appid condition may get matched incorrectly, potentially causing connection failure
CSCwb31551	When inbound packet contains SGT header, FPR2100 cannot distribute properly per 5 tuple
CSCwb31699	Primary takes active role after reload
CSCwb32267	Crash on KP Active node while clearing vpnsessiondb with AnyConnect-SSL TVM Profile running
CSCwb32721	Syslog IDs 725021 and 725022 are not listed as valid IDs
CSCwb32790	Replace log4j with slf4j
CSCwb32841	NAT (any,any) statements in-states the failover interface and resulting on Split Brain events
CSCwb38961	Bootstrap After Upgrade failed due to Duplicate Key of Network Object
CSCwb40001	Long delays when executing SNMP commands
CSCwb41739	debug crypto conditional need to be made multi-ctx aware
CSCwb42031	Cisco FTD Software and FMC Software Code Injection Vulnerability
CSCwb43018	Implement SNP API to check ifc and ip belongs to HA LU or CMD interface
CSCwb43433	Jumbo frame performance has degraded up to -45% on Firepower 2100 series
CSCwb43629	License and rule counts telemetry data incorrectly generated for HA managed devices
CSCwb44848	ASA/FTD Traceback and reload in Process Name: lina
CSCwb46293	Memory leak in pub-sub channel in the loggerd process restart scenario's
CSCwb46481	SNMPv3 not working after upgrade of FMC
CSCwb50395	Lina crash and core when creating secondary flow when parent flow is already freed
CSCwb50405	ASA/FTD Traceback in crypto hash function
CSCwb51707	ASA Traceback and reload in process name: lina
CSCwb51821	Disk usage errors on Firepower Azure device due to large backup unified files under ngfw directory

Bug ID	Headline
CSCwb52401	Cisco Firepower Threat Defense Software Privilege Escalation Vulnerability
CSCwb53172	FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated
CSCwb53191	Certificate validation fails post upgrade to 9.17.1
CSCwb53328	ASA/FTD Traceback and reload caused by Smart Call Home process sch_dispatch_to_url
CSCwb54791	ASA DHCP server fails to bind reserved address to Linux devices
CSCwb56905	ASA blocking 0.0.0.0 IP and netmask combination in SSH/TELNET/HTTP config
CSCwb57213	FTD - Unable to resolve DNS when only diagnostic interface is used for DNS lookups
CSCwb57615	Configuring PBR access-list with line number failed
CSCwb58554	Resumed SSL sessions with uncached tickets may fail to complete
CSCwb58817	FMC Deploying negative and positive form of BGP password command across deployments
CSCwb59218	Unable to save DAP Endpoint Criteria as "Disabled"
CSCwb59465	ASA/FTD may traceback (watchdog) and reload when generating a syslog from the VPN Failover subsystem
CSCwb59488	ASA/FTD Traceback in memory allocation failed
CSCwb61402	Unreachable LDAP/AD referrals may cause delays or timeouts in external authentication on FMC
CSCwb61408	FMC: Did not remove unneeded shell external auth users from /etc/passwd
CSCwb63827	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS
CSCwb64551	FMC Backup failure- Monetdb backup failure code 102
CSCwb66761	Cisco Firepower Threat Defense Software Generic Routing Encapsulation DoS Vulnerability
CSCwb67040	FP4112|4115 Traceback & reload on Thread Name: netfs_thread_init
CSCwb68642	ASA traceback in Thread Name: SXP CORE
CSCwb69503	ASA unable to configure aes128-gcm@openssh.com when FIPS enabled
CSCwb71460	ASA traceback in Thread Name: fover_parse and triggered by snmp related functions
CSCwb73248	FW traceback in timer infra / netflow timer
CSCwb74571	PBR not working on ASA routed mode with zone-members

Bug ID	Headline
CSCwb76423	ASA/FTD traceback and reload when checking CRL
CSCwb78323	Update diskmanager to monitor cisco_uridb files in /ngfw/var/sf/cloud_download folder.
CSCwb79812	RIP is advertising all connected Anyconnect users and not matching route-map for redistribution
CSCwb80559	FTD offloads SGT tagged packets although it should not
CSCwb80862	ASA/FTD proxy arps any traffic when using the built-in 'any' object in translated destination
CSCwb82796	ASA/FTD firewall may traceback and reload when tearing down IKE tunnels
CSCwb83388	ASA HA Active/standby tracebacks seen approximately every two months.
CSCwb83691	ASA/FTD traceback and reload due to the initiated capture from FMC
CSCwb84901	CIAM: heimdal 1.0.1
CSCwb85633	Snmpwalk output of memory does not match show memory/show memory detail
CSCwb86118	TPK ASA: Device might get stuck on ftp copy to disk
CSCwb87498	Lina traceback and reload during EIGRP route update processing.
CSCwb87950	Cisco ASA Software and FTD Software Web Services Interface Denial of Service Vulnerability
CSCwb88406	FMC-HA upgrade failure due to presence of this file "update.status"
CSCwb88651	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwb88729	FTD - %FTD-3-199015: port-manager: Error: DOM Block Read failure, port X, st = X log false/positive
CSCwb89963	ASA Traceback & reload in thread name: Datapath
CSCwb90074	ASA: Multiple Context Mixed Mode SFR Redirection Validation
CSCwb90532	ASA/FTD traceback and reload on NAT related function nat_policy_find_location
CSCwb91101	SNMP interface threshold doesn't trigger properly when traffic sent to interface ~4gbps
CSCwb91598	copying FMC backup to remote storage will fail if FMC has never connected via SSH/SCP to remote host
CSCwb92709	We can't monitor the interface via "snmpwalk" once interface is removed from context.
CSCwb93932	ASA/FTD failover pair traceback and reload due to connection replication race condition
CSCwb94190	ASA graceful shut down when applying ACL's with forward reference feature and FIPS enabled.

Bug ID	Headline
CSCwb94312	Unable to apply SSH settings to ASA version 9.16 or later
CSCwb95453	ASA: The timestamp for all logs generated by Admin context are the same
CSCwb95784	cache and dump last 20 rmu request response packets in case failures/delays while reading registers
CSCwb95850	Snort down due to missing lua files because of disabled application detectors (PM side)
CSCwb97251	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCwb97486	FPR3100: 25G optic may show link up on some 1/10G capable only fiber ports
CSCwb99375	Config sync fails for command "quit"
CSCwc00115	FTD registration fails on on-prem FMC
CSCwc02488	ASA/FTD may traceback and reload in Thread Name 'None'
CSCwc02700	Fragmented packets are dropped when unit leaves cluster
CSCwc03069	Interface internal data0/0 is up/up from cli but up/down from SNMP polling
CSCwc03332	FTD on FP2100 can take over as HA active unit during reboot process
CSCwc03507	No-buffer drops on Internal Data interfaces despite little evidence of CPU hog
CSCwc05434	FMC shows 'File Not Stored' after download a file
CSCwc07015	Cisco FTD Software SSL and Snort 3 Detection Engine Bypass and DoS Vulnerability
CSCwc07262	Standby ASA goes to booting loop during configuration replication after upgrade to 9.16(3).
CSCwc08374	Azure ASA NIC MAC address for Gigeth 0/1 and 0/2 become out of order when adding interfaces
CSCwc09414	ASA/FTD may traceback and reload in Thread Name 'ci/console'
CSCwc10483	ASA/FTD - Traceback in Thread Name: appAgent_subscribe_nd_thread
CSCwc10792	ASA/FTD IPSEC debugs missing reason for change of peer address and timer delete
CSCwc11511	FTD: SNMP failures after upgrade to 7.0.2
CSCwc11597	ASA tracebacks after SFR was upgraded to 6.7.0.3
CSCwc11663	ASA traceback and reload when modifying DNS inspection policy via CSM or CLI
CSCwc13017	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
CSCwc13477	FMC | Interface update Failed. Could not find source interface

Bug ID	Headline
CSCwc13994	ASA - Restore not remove the new configuration for an interface setup after backup
CSCwc18285	Conn data-rate command can be enabled or disabled in unprivileged user EXEC mode
CSCwc18312	"show nat pool cluster" commands run within EEM scripts lead to traceback and reload
CSCwc18524	ASA/FTD Voltage information is missing in the command "show environment"
CSCwc18668	Failed user login on FMC does not record entry in audit log when using external authentication
CSCwc19124	FMC Deployment does not start for cluster devices
CSCwc20635	Cisco Firepower Threat Defense ICMPv6 with Snort 2 Denial of Service Vulnerability
CSCwc22170	Issue with snort perfstat parsing / Hmdeamon not starting after disk full reported
CSCwc23356	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-20-7695'
CSCwc23695	ASA/FTD can not parse UPN from SAN field of user's certificate
CSCwc23844	ASAv high CPU and stack memory allocation errors despite over 30% free memory
CSCwc24906	ASA/FTD traceback and reload on Thread id: 1637
CSCwc26648	ASA/FTD Traceback and Reload in Thread name Lina or Datatath
CSCwc27424	Unable to removed not used SAL On-Premise FMC configuration
CSCwc27797	ASA mgmt ip cannot be released
CSCwc27846	Traceback and Reload while HA sync after upgrading and reloading.
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwc28532	9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwc28806	ASA Traceback and Reload on process name Lina
CSCwc28928	ASA: SLA debugs not showing up on VTY sessions
CSCwc30573	Deployment/Tasks Button not seen FMC_UI while doing upgrade tests configured in Light theme
CSCwc32245	FMC: Validation check to prevent exponential expansion of NAT rules
CSCwc32246	NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used
CSCwc33036	Observed Logs at syslog server side as more than configured message limit per/sec.
CSCwc35181	OSPF template adds "default-information-originate" to area <area-id> nssa statement on hitting OK.

Bug ID	Headline
CSCwc35583	Snort leaking file descriptors with each u2 file created
CSCwc36905	ASA traceback and reload due to "Heap memory corrupted at slib_malloc.c
CSCwc37256	SSL AnyConnect access blocked after upgrade
CSCwc38567	ASA/FTD may traceback and reload while executing SCH code
CSCwc39525	FMC HA status alert "degraded - maintenance" seen periodically after upgrade
CSCwc40381	ASA : HTTPS traffic authentication issue with Cut-through Proxy enabled
CSCwc41293	Firepower module show-tech file generation may fail with error "Failed to create archive!"
CSCwc41592	False positives for Ultrasurf
CSCwc42174	CIAM: mariadb - multiple versions CVE-2022-32081
CSCwc42561	Deploy page listing takes 1.5 to 2 mins with 462 HA device
CSCwc43807	FTD is unusable post reboot if manager is deleted and FIPS is enabled
CSCwc44289	FTD - Traceback and reload when performing IPv4 <> IPv6 NAT translations
CSCwc44367	LSP not installed after HA failover. No LSP package found in the active LSP directory
CSCwc44608	Selective deployment of IPS may cause outage due to incorrectly written FTD configuration files
CSCwc45108	ASA/FTD: GTP inspection causing 9344 sized blocks leak
CSCwc45397	ASA HA - Restore in primary not remove new interface configuration done after backup
CSCwc48375	Inbound IPSEC SA stuck inactive - many inbound SPIs for one outbound SPI in "show crypto ipsec sa"
CSCwc48853	SFDataCorrelator Discovery Event bottleneck can cause Connection Event delay and backlog
CSCwc49095	ASA/FTD 2100 platform traceback and reload when fragments are coalesced and sent to PDTS
CSCwc49364	mojo_server processes unnecessarily restarting during log rotation
CSCwc50519	Excessive logging from hm_du.pm may lead to syslog-ng process restarts
CSCwc50846	FTD Upgrade Fail - Readiness Check Successful, but Readiness status never shown
CSCwc50887	FTD - Traceback and reload on NAT IPv4<>IPv6 for UDP flow redirected over CCL link
CSCwc50891	MPLS tagging removed by FTD

Bug ID	Headline
CSCwc51326	FXOS-based Firepower platform showing 'no buffer' drops despite high values for RX ring watermarks
CSCwc51588	Failing to generate FMC Backup/Restore via SMB/SSH
CSCwc52351	ASA/FTD Cluster Split Brain due to NAT with "any" and Global IP/range matching broadcast IP
CSCwc53280	ASA parser accepts incomplete network statement under OSPF process and is present in show run
CSCwc54217	syslog related to failover is not outputted in FPR2140
CSCwc54901	Scheduled tasks may not run on active FMC in HA after switchover or split-brain resolution
CSCwc54984	IKEv2 rekey - Responding Invalid SPI for the new SPI received right after Create_Child_SA response
CSCwc56003	Trigger FTD backup with remote storage option enabled along with retrieval to FMC fails
CSCwc56952	Able to see the SLA debug logs on both console & VTY sessions even if we enable only on VTY session.
CSCwc57575	FMC: Scheduled backups working fine, but FMC email alerts displaying it failed.
CSCwc60037	ASA fails to rekey with IPSEC ERROR: Failed to allocate an outbound hardware context
CSCwc60227	FMC-GUI bypass session timeout while staying in any Event tab if Refresh Interval is enabled
CSCwc60463	FXOS is not rotating log messages files for partition opt_cisco_platform_logs
CSCwc61912	ASA/FTD OSPFv3 does not generate messages Type 8 LSA for IPv6
CSCwc62215	FTD unable to sync HA due to snort validation failed
CSCwc63273	SFDataCorrelator host timeout query can block event processing and cause a deadlock restart
CSCwc64333	FMC GUI timeout and issues with loading http page due to exceeded http connections
CSCwc64923	ASA/FTD may traceback and reload in Thread Name 'lina' ip routing ndbshr
CSCwc66757	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwc67687	ASA HA failover triggers HTTP server restart failure and ASDM outage
CSCwc67886	ASA/FTD may traceback and reload in Thread Name 'lina_inotify_file_monitor_thread'
CSCwc68543	mismatch in the config pushed from FMC and running config on FTD

Bug ID	Headline
CSCwc68656	ASA CLI for TCP Maximum unprocessed segments
CSCwc69583	Portchannel configured from FDM breaks "Use the Data Interfaces as the Gateway" for Mgmt interface
CSCwc70962	FTD/ASA "Write Standby" enables ECDSA ciphers causing AC SSLv3 handshake failure
CSCwc72155	ASA/FTD Traceback and reload on function "snp_cluster_trans_allocb"
CSCwc72284	TACACS Accounting includes an incorrect IPv6 address of the client
CSCwc73224	Call home configuration on standby device is lost after reload
CSCwc74099	FPR2140 ASA Clock Timezone reverts to UTC after appliance restart/reload
CSCwc74103	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-11-32591'
CSCwc74271	Auth-Daemon process is getting restarted continuously when SSO disabled in HA setup
CSCwc74378	FMC UI should disallow simultaneous deactivation of FMC interface management and event channels
CSCwc74841	FMC RSS Feed broken because FeedBurner is no longer active - "Unable to parse feed"
CSCwc74858	FTD - Traceback in Thread Name: DATAPATH
CSCwc76700	Cisco Firepower Management Center Software Stored Cross-Site Scripting Vulnerability
CSCwc77519	FPR1000 ASA/FTD: Primary takes active role after reloading
CSCwc77680	FTD may traceback and reload in Thread Name 'DATAPATH-0-4948'
CSCwc79366	During the deployment time, device got stuck processing the config request.
CSCwc80234	"inspect snmp" config difference between active and standby
CSCwc80357	[Deploy Performance] degrade in deployment page on FMC
CSCwc81184	ASA/FTD traceback and reload caused by SNMP process failure
CSCwc81219	Intrusion events intermittently stop appearing in FMC when using snort3
CSCwc81727	Default Domain in VPN group policy objects cannot be deleted
CSCwc81960	Unable to configure 'match ip address' under route-map when using object-group in access list
CSCwc82188	FTD Traceback and reload when applying long commands from FMC UI or CLISH
CSCwc86330	Vulnerabilities in spring-framework - multiple versions CVE-2022-22970

Bug ID	Headline
CSCwc86391	On slow networks with some packets loss sftunnel may mark connections as STALE
CSCwc87441	for system processes limit the CPUs used to the number of system CPUs
CSCwc88108	Prefilter policy - Available port menu long response time, Prefilter Network Search takes long time
CSCwc88897	ASA traceback and reload due to null pointer in Umbrella after modifying DNS inspection policy
CSCwc89661	FTD misses diagnostic data required for investigation of "Communication with NPU lost" error
CSCwc89796	ASA/FTD may traceback and reload in Thread Name 'appagent_async_client_receive_thread' hog detection
CSCwc89924	FXOS ASA/FTD SNMP OID to poll Internal-data 'no buffer' interface counters
CSCwc90091	ASA 9.12(4)47 with user-statistics, will affects the "policy-server xxxx global" visibility.
CSCwc91451	dvti hub core at ctm_sw_ipsec_cleanup_frags+394
CSCwc92761	7.3 - Message flood by Use of uninitialized value $unix_time in numeric gt
CSCwc93166	Using write standby in a user context leaves secondary firewall license status in an invalid state
CSCwc93687	Error message while editing ACP
CSCwc94085	Unable to establish DTLSv1.2 with FIPS enabled after upgrade from 6.6.5.
CSCwc94148	Deploy page fails to load if any FTD cluster or HA device state is not proper in DB
CSCwc94466	Cisco ASA/FTD Firepower 2100 SSL/TLS Denial of Service Vulnerability
CSCwc94501	ASA/FTD memory leak and tracebacks due to ctm_n5 resets
CSCwc95290	ESP rule missing in vpn-context may cause IPSec traffic drop
CSCwc96016	Captive portal support in cross domain
CSCwc96805	traceback and reload due to tcp intercept stat in thread unicorn
CSCwc99242	ISA3000 LACP channel member SFP port suspended after reload
CSCwd00386	ASA/FTD may traceback and reload when clearing the configration due to "snp_clear_acl_log_flow_all"
CSCwd00778	ifAdminStatus output is abnormal via snmp polling
CSCwd01032	ASA/FTD may traceback and reload when RAVPN with SAML is configured
CSCwd02864	logging/syslog is impacted by SNMP traps and logging history

Bug ID	Headline
CSCwd02925	Cisco Firepower Management Center Software Command Injection Vulnerability
CSCwd03113	FMC local backup fails cause of "Update Task: Database integrity check failed" - Syslog server issue
CSCwd03793	FTD Traceback and reload
CSCwd03810	ASA Custom login page is not working through webvpn after an upgrade
CSCwd04210	ASA: ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT
CSCwd05814	PDTS write from Daq can fail when PDTS buffer is full eventually leads to block depletion
CSCwd06005	ASA/FTD Cluster Traceback and Reload during node leave
CSCwd07059	multiple snort3 crashes after upgrading FTD from 7.2.0 to 7.2.0.1
CSCwd08430	Create a resiliency configuration option for SFTunnel to support HA and FTD connectivity
CSCwd09231	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwd10121	Invalid query seen in MonetDB merovingian.log
CSCwd10497	FTD sensor rules missing from ngfw.rules file after a sensor backup restore execution
CSCwd10760	Firewall_rule_cache may not pruned for many years for some customers
CSCwd10880	critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on FPR 1100/2100/3100
CSCwd11005	Missing fqdns_old.conf file causes FTD HA app sync failure
CSCwd11165	"Move" option is greyed out on Backup-Restore in FMC
CSCwd11303	ASA might generate traceback in ikev2 process and reload
CSCwd11855	ASA/FTD may traceback and reload in Thread Name 'ikev2_fo_event'
CSCwd11963	Error message seen in the log "Error operation timed out getting CriticalStatus from PM."
CSCwd13083	FMC Unable to initiate deployment due to incorrect threat license validation
CSCwd13917	during download from file event on FMC, high CPU use on FMC for 20 minutes before download fails
CSCwd14432	"Inspection Interruption" is seen as YES but snort3 didn't restart
CSCwd14688	FTD upgrade failure due to Syslog files getting generated/deleted rapidly
CSCwd14972	ASA/FTD Traceback and Reload in Thread Name: pix_flash_config_thread

Bug ID	Headline
CSCwd16017	Object edit slowness when it is associated with NAT rules
CSCwd16294	GTP inspection drops packets for optional IE Header Length being too short
CSCwd16517	GTP drops not always logged on buffer and syslog
CSCwd16689	ASA/FTD traceback due to block data corruption
CSCwd16712	Device readiness upgrade check failure - sftunnel sync issue due to time change
CSCwd16902	File events show Action as "Malware Block" for files with correct disposition of unknown
CSCwd17037	SFDataCorrelator RNA-Stop action should not block when database operations are hung
CSCwd17856	ASA goes for traceback/reload with message - snmp_ma_kill_restart: vf is NULL
CSCwd17940	HA did not failover due to misleading status updates from NDClient
CSCwd18744	FPR1K FTD fails to form HA due to reason "Other unit has different set of hwidb index"
CSCwd19053	ASA/FTD may traceback with large number of network objects deployment using distribute-list
CSCwd20627	ASA/FTD: NAT configuration deployment failure
CSCwd20900	HTTP Block Response and Interactive Block response pages not being displayed by Snort3
CSCwd22413	ASA/FTD: Traceback and reload in Thread Name: EIGRP-IPv4
CSCwd22907	ASA/FTD High CPU in SNMP Notify Thread
CSCwd23188	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwd23913	FTD in HA traceback multiple times after adding a BGP neighbour with prefix list.
CSCwd25201	ASA/FTD SNMP traps enqueued when no SNMP trap server configured
CSCwd25256	ASA/FTD Transactional Commit may result in mismatched rules and traffic loss
CSCwd26466	Incorrect Frequent Drain of Connection Events alert
CSCwd26867	Device should not move to Active state once Reboot is triggered
CSCwd28236	standby unit using both active and standby IPs causing duplicate IP issues due to nat "any"
CSCwd29835	log rotate failing to cycle files, resulting in large file sizes
CSCwd30296	Device Metrics Not Working After Upgrade to 7.0.3 from pre -7.0.0 version

Bug ID	Headline
CSCwd30298	FTD: FTPS Data Channel connection impacted by TLS Server Identity and Discovery Probe sent by FTD
CSCwd30774	FMC HA - files in tmp/Sync are left on secondary when synchronisation task fails
CSCwd30856	User with no vpn-filter may get additional access when per-user-override is set
CSCwd30977	FMC deleted some access-rules due to an incorrect delta generated during the policy deployment.
CSCwd31181	Lina traceback and reload - VPN parent channel (SAL) has an invalid underlying channel
CSCwd32952	Active and Standby device details not available in FMC logs during FTD HA break
CSCwd33054	DHCP Relay is looping back the DHCP offer packet causing dhcprelay to fail on the FTD/ASA
CSCwd33811	Cluster registration is failing because DATA_NODE isn't joining the cluster
CSCwd34288	FP1000 - During boot process in LINA mode, broadcasts leaked between interfaces resulting in storm
CSCwd34662	LTS18 and LTS21 commit id update in CCM layer (seq 39)
CSCwd35726	Cisco FXOS Software Arbitrary File Write Vulnerability
CSCwd37238	TLS connections to Exchange 2007 server may fail
CSCwd38526	FMC can allow deployment of NAP in test mode with Decrypt policy
CSCwd38774	ASA: Traceback and reload due to clientless webvpn session closure
CSCwd38775	ASA/FTD may traceback and reload in Thread lina
CSCwd38805	Syslog 106016 is not rate-limited by default
CSCwd39039	FMC - Error message "The server response was not understood. Please contact support." on UI
CSCwd39468	ASA/FTD Traceback and reload when configuring ISAKMP captures on device
CSCwd39506	SSL Policy DND default Rule fails on error unsupported cipher suite and SKE error.
CSCwd40141	Firepower Management Center GUI view for Snort2 Local Intrusion Rules is missing
CSCwd40260	Serviceability Enhancement - Unable to parse payload are silently drop by ASA/FTD
CSCwd41083	ASA traceback and reload due to DNS inspection
CSCwd41224	FMC HA webUI is not getting FTDv Variable tier assigned FTDv - Variable
CSCwd41466	Re-downloaded users from a forest with trusted domains may become unresolved/un-synchronized

Bug ID	Headline
CSCwd41806	deployment failed with OOM (out of memory) for policy_apply.pl process
CSCwd42072	SRU installation failure.
CSCwd42347	FMC not showing any alerts/warnings when deploying changes of prefix list with same seq #
CSCwd43666	Analyze why there is no logrotate for /opt/cisco/config/var/log/ASAconsole.log
CSCwd44326	Object NAT edit is failing
CSCwd46741	fxos log rotate failing to cycle files, resulting in large file sizes
CSCwd46780	ASA/FTD: Traceback and reload in Thread Name: appAgent_reply_processor_thread
CSCwd47340	FXOS: memory leak in svc_sam_envAG process
CSCwd47424	Device name always shows as 'firepower' in CDO event view
CSCwd47442	800_post/1027_ldap_external_auth_fix.pl upgrade error -- reference to missing authentication object
CSCwd47481	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 40)
CSCwd48633	ASA - traceback and reload when Webvpn Portal is used
CSCwd49685	Missing SSL MEMCAP causes deployment failure due timeout waiting for snort detection engines
CSCwd50131	Upgrades are not cleaning up mysql files leading to alert for 'High unmanaged disk usage on /ngfw'
CSCwd50218	ASA restore is not applying vlan configuration
CSCwd51757	Unable to get polling results using snmp GET for connection rate OID\u2019s
CSCwd51964	Add validation in lua detector api to check for empty patterns for service apps
CSCwd53135	ASA/FTD: Object Group Search Syslog for flows exceeding threshold
CSCwd53340	FTD PDTS LINA RX queue can become stuck when snort send messages with 4085-4096 bytes size
CSCwd53863	Data migration from Sybase to MariaDB taking more time due to large data size of POLICY_SNAPSHOT
CSCwd54360	FP2100: FXOS side changes for HA is not resilient to unexpected lacp process termination issue
CSCwd54439	FMC gives an irrelevant error message for Snort2 to Snort3 rules conversion failure
CSCwd55673	Need corrections in log_handler_file watchdog crash fix
CSCwd55853	FDM: Deployment failure with localpool overlap error after upgrade

Bug ID	Headline
CSCwd56254	"show tech-support" generation does not include "show inventory" when run on FTD
CSCwd56296	FTD Lina traceback and reload in Thread Name 'IP Init Thread'
CSCwd56431	Disable asserts in FTD production builds
CSCwd56654	Platform faults related to management interface on FXOS
CSCwd56774	Misleading drop reason in "show asp drop"
CSCwd56995	Clientless Accessing Web Contents using application/octet-stream vs text/plain
CSCwd57698	Recursive panic under lina_duart_write
CSCwd58188	Inline-pair's state could not able to auto recover from hardware-bypass to standby mode.
CSCwd58337	allocate more cgroup memory for policy deployment subgroup
CSCwd58417	HA Periodic sync is failing due to cfg files are missing
CSCwd58430	At times AC Policy save takes longer time, may be around 10 or above mins
CSCwd58528	Memory depletion while running EMIX traffic profile on QP HA active node
CSCwd59736	ASA/FTD: Traceback and reload due to SNMP group configuration during upgrade
CSCwd61016	ASA: Standby may get stuck in "Sync Config" status upon reboot when there is EEM is configured
CSCwd61082	FMC UI Showing inaccurate data in S2S VPN Monitoring page
CSCwd61410	mdbtrace.log can fill storage on FMC
CSCwd62025	FTDv: Policy Deployment failure due to interface setting on failover interface
CSCwd62138	ASA Connections stuck in idle state when DCD is enabled
CSCwd62729	FDM QW/QP: All URL traffic blocked in BAT/BQT test
CSCwd62859	Cisco ASA and FTD AnyConnect SSL/TLS VPN Denial of Service Vulnerability
CSCwd62915	Cross-domain users with non-ASCII characters are not resolved
CSCwd63221	Frequent drain of events alert is not getting triggered
CSCwd63580	FPR2100: Increase in failover convergence time with ASA in Appliance mode
CSCwd63961	AC clients fail to match DAP rules due to attribute value too large
CSCwd64919	FXOS is not rotating PoE logs
CSCwd65239	vFTD Platforms not tracking CPU/Memory metrics for Health Monitoring
CSCwd65327	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 41)

Bug ID	Headline
CSCwd66815	Lina changes to support - Snort3 traceback in daq-pdts while handling FQDN based traffic
CSCwd67101	FPR1150 : Exec format error seen and the device hung until reload when erase secure all is executed
CSCwd68088	ASA|FTD: Implement different TLS diffie-hellman prime based on RFC recommendation
CSCwd69236	FMC Connection Event stop displaying latest event
CSCwd69454	Port-channel interfaces of secondary unit are in waiting status after reload
CSCwd72656	FMC GUI takes long time to load Intrusion Event packet view
CSCwd72680	FXOS: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
CSCwd72915	FMC 7.1.0.1 Doesn't throw warning that S2S VPN Configs contain deprecated MD5 Hash during deployment
CSCwd73981	FMC: Updates page takes more than 5 minutes to load
CSCwd74116	S2S Tunnels do not come up due to DH computation failure caused by DSID Leak
CSCwd74648	External authentication with Radius server fail with error "This account is currently not available"
CSCwd74839	30+ seconds data loss when unit re-join cluster
CSCwd75738	Predefined FlexConfig Text Objects are not exported by Import-Export
CSCwd75912	ASA SFR/FTD is failing registration or not sending events to FMC
CSCwd76634	FMC import takes too long
CSCwd77581	Cisco ASA and FTD ICMPv6 Message Processing Denial of Service Vulnerability
CSCwd78123	ASA/FTD traceback and reload when IPSec/Ikev2 vpn session bringup with dh group 31 in fips mode
CSCwd78624	ASA may traceback and reload with multiple input/output error messages
CSCwd78940	Traps are not getting generated in UUT for config change in multicontext
CSCwd79388	intrusion events fail to migrate from MariaDB to MonetDB following FMC upgrade from 7.0.3 to 7.1.0
CSCwd80343	MI FTD running 7.0.4 is on High disk utilization
CSCwd81384	FMC upgrade fails: 114_DB_table_data_integrity_check.pl, stating Snort2IPSNAPCleanup.pm not be found
CSCwd81538	FTD Traffic failure due to 9344 block depletion in peer_proxy_tx_q

Bug ID	Headline
CSCwd81897	Snort3 crash seen sometimes while processing a future flow connection after appid detectors reload
CSCwd82235	LINA Traceback on FPR-1010 under Thread Name: update_cpu_usage
CSCwd82801	Snort outputs massive volume of packet events - IPS event view may show "No Packet Information"
CSCwd83613	Multiple Cisco Products Snort FTP Inspection Bypass Vulnerability
CSCwd83956	snort2 does not match rules based on application SMTP/SMTPS anymore after a while
CSCwd83990	FTD -Snort match incorrect NAP id for traffic
CSCwd84133	ASA/FTD may traceback and reload in Thread Name 'telnet/ci'
CSCwd84868	Observing some devcmd failures and checkheaps traceback when flow offload is not used.
CSCwd85178	AWS ASAv PAYG Licensing not working in GovCloud regions.
CSCwd85609	FTDs running 6.6.x show as disconnected on new HM (6.7+) but checks are running and updating
CSCwd85927	Traceback and reload when webvpn users match DAP access-list with 36k elements
CSCwd86313	Unable to access Dynamic Access policy
CSCwd86457	Number of objects are not getting updated under policies>>>Security intelligence >>>Block list
CSCwd86929	Cut-Through Proxy does not work with HTTPS traffic
CSCwd88585	ASA/FTD NAT Pool Cluster allocation and reservation discrepancy between units
CSCwd88641	Deployment changes to push VDB lite package based on Device model and snort engine
CSCwd89349	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (seq 42)
CSCwd90112	MariaDB crash (segmentation fault) related to netmap query
CSCwd91013	FMC | Deployment failure in csm_snapshot_error
CSCwd91421	ASA/FTD may traceback and reload in logging_cfg processing
CSCwd92804	FAN LED flashing amber on FPR2100
CSCwd93316	No Inspect Interruption warning when deploy after FMC upgrade
CSCwd93376	Clientless VPN users are unable to download large files through the WebVPN portal
CSCwd93792	SFDataCorrelator performance degradation involving hosts with many discovered MAC addresses

Bug ID	Headline
CSCwd94096	Anyconnect users unable to connect when ASA using different authentication and authorization server
CSCwd94183	Blade not coming up after FXOS update support on multi-instance due to ssp_ntp.log log rotation prob
CSCwd95043	Cisco ASA and FTD VPN Web Client Services Client-Side Request Smuggling Vulnerability
CSCwd95415	The Standby Device going in failed state due to snort heartbeat failure
CSCwd95436	Primary ASA traceback upon rebooting the secondary
CSCwd95908	ASA/FTD traceback and reload, Thread Name: rtcli async executor process
CSCwd96041	FMC SecureX via proxy stops working after upgrade to 7.x
CSCwd96493	Link Up seen for a few seconds on FPR1010 during bootup
CSCwd96755	ASA is unexpected reload when doing backup
CSCwd96766	FPR41xx/9300: Blade does not capture or log a reboot signal
CSCwd96790	High FMC backup file size due to configurations snapshot for all managed devices
CSCwd96845	Cisco ASA and FTD AnyConnect Access Control List Bypass Vulnerability
CSCwd97020	ASA/FTD: External IDP SAML authentication fails with Bad Request message
CSCwd97276	Unified events and connection events pages don't load anymore. DB Cores generated every few minutes
CSCwe00757	Summary status dashboard takes more than 3 mins to load upon login
CSCwe00828	Interactive Block action doesn't work when websites are redirected to https
CSCwe00864	License Commands go missing in Cluster data unit if the Cluster join fails.
CSCwe03529	FTD traceback and reload while deploying PAT POOL
CSCwe03991	FTD/ASA traceback and reload during to tmatch compilation process
CSCwe04043	FTD HA upgrade fails due to one unit starting upgrade before the other rejoins HA pair
CSCwe04437	collection of top.log.gz in troubleshoot can be corrupt due to race condition
CSCwe05913	FTD traceback/reloads - Icmp error packet processing involves snp_nat_xlate_identity
CSCwe06724	Database table optimization not working for some of the tables
CSCwe06826	Email alert incorrectly send for a successful database backup

Bug ID	Headline
CSCwe06828	FMC HA Synchronization can hang forever if no response from SendUserReloadSGTAndEndpointsEvent
CSCwe07103	FMC: Upgrade fails at DB Integrity check due to large number of EO warnings for "rule_comments"
CSCwe07722	Cluster data unit drops non-VPN traffic with ASP reason "VPN reclassify failure
CSCwe07928	On a cloud-delivered FMC there is no way to send events to syslog without sending to SAL/CDO as well
CSCwe08729	FPR1120:connections are getting teardown after switchover in HA
CSCwe08908	Threatgrid integration configuration is not sync'd as part of the FMC HA Synchronisation
CSCwe09074	None option under trustpoint doesn't work when CRL check is failing
CSCwe09811	FTD traceback and reload during policy deployment adding/removing/editing of NAT statements.
CSCwe10670	Identity network filter not removed from FTD
CSCwe11119	ASA: Traceback and reload while processing SNMP packets
CSCwe11189	monetdb log use all of disk spaces on /Volume
CSCwe11263	Cisco Firepower Management Center Software Arbitrary File Download Vulnerability
CSCwe11304	Snort crashing on FTD
CSCwe11727	Purging of Config Archive failed for all the devices if one device has no versions
CSCwe12407	High Lina memory use due to leaked SSL handles
CSCwe13627	FMC Unable to fetch VPN troubleshooting logs.
CSCwe14062	FTD/Lina or ASA traceback and reload related to thread ctm_qat_engine
CSCwe14174	FTD - 'show memory top-usage' providing improper value for memory allocation
CSCwe14514	ASA/FTD Traceback and reload of Standby Unit while removing capture configurations
CSCwe15164	ASA: ASDM cannot display SFR tabs until it's "woken up" through its CLI.
CSCwe15280	Multiple Cisco Products Snort 3 Access Control Policy Bypass Vulnerability
CSCwe16620	FMC Health Monitor does not report alerts for the Interface Status module
CSCwe18090	FMC deployment failure:"Validation failed: This is a slav*/ha standby device, rejecting deployment."
CSCwe18859	After device registration or FMC upgrade, devices sometimes don't send events to the FMC

Bug ID	Headline
CSCwe18974	ASA/FTD may traceback and reload in Thread Name: CTM Daemon
CSCwe20043	256-byte memory block gets depleted on start if jumbo frame is enabled with FTD on ASA5516
CSCwe20634	Cisco Firepower Management Center Software HTML Injection Vulnerability
CSCwe20641	Cisco Firepower Management Center Software HTML Injection Vulnerability
CSCwe20714	Traffic drop when primary device is active
CSCwe20918	Cisco ASA and FTD Software Remote Access SSL VPN Multiple Certificate Auth Bypass
CSCwe21037	Snort mem used alert should be consistent with value from top.log
CSCwe21187	ASA/FTD may drop multicast packets due to no-mcast-intrf ASP drop reason until UDP timeout expires
CSCwe21280	Multicast connection built or teardown syslog messages may not always be generated
CSCwe21831	add warning to FTD platform settings when VPN Logging Settings logging level is informational
CSCwe21959	Snort3: Process in D state resulting in OOM with jemalloc memory manager
CSCwe22176	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 43)
CSCwe22216	Maria DB crashing/holding high CPU and not allowing users to login GUI and CLI
CSCwe22254	After disabling malware analysis, high disk usage on /dev/shm/snort
CSCwe22302	Partition "/opt/cisco/config" gets full due to wtmp file not getting logrotated
CSCwe22492	Slow UI loading for Table View of Hosts
CSCwe22980	Database integrity check takes several minutes to complete
CSCwe23039	NTP polling frequency changed from 5 minutes to 1 second causes large useless log files
CSCwe23139	FTD HA does not break from FMC GUI but HA bootstrap is removed from devices
CSCwe23801	FTD : Numerous snort cores have been noticed on the FPR2100 device
CSCwe24532	Multiple instances of nvram.out log rotated files under /opt/cisco/platform/logs/
CSCwe24880	Using proxy authentication in FMC for smart licensing is failing after upgrading to 7.0.5
CSCwe25025	8x10Gb netmod fails to come online
CSCwe25187	FMC External authentication getting "Internal error"

Bug ID	Headline
CSCwe25342	ASA/FTD - SNMP related memory leak behavior when snmp-server is not configured
CSCwe26612	FTD taking longer than expected to form OSPF adjacencies after a failover switchover
CSCwe28094	ASA/FTD may traceback and reload after executing 'clear counters all' when VPN tunnels are created
CSCwe28726	The command "app-agent heartbeat" is getting removed when deleting any created context
CSCwe29179	CLUSTER: ICMP reply arrives at director earlier than CLU add flow request from flow owner.
CSCwe29381	Sybase arbiter is not up on FMC HA
CSCwe29498	occasional failure to load light-modal-ac-rule-xx.css with a net::ERR_TOO_MANY_RETRIES error
CSCwe29529	FTD MI does not adjust PVID on vlans attached to BVI
CSCwe29583	ASA/FTD may traceback and reload in Thread Name 'None' at lua_getinfo
CSCwe29850	ASA/FTD Show chunkstat top command implementation
CSCwe29952	SFDataCorrelator cores due to stuck database query after 1 hour deadlock timeout
CSCwe30228	ASA/FTD might traceback in funtion "snp_fp_l2_capture_internal" due to cf_reinject_hide flag
CSCwe30653	FTD upgrade failure at "999_finish/999_zz_install_bundle.sh" due to bad key cert
CSCwe30867	Workaround to set hwclock from ntp logs on low end platforms
CSCwe32375	7.0 - Snort3 process in D state and outage due to OOM
CSCwe32448	changing time window settings in FMC GUI event viewers may not work with FMC integrated with SecureX
CSCwe32537	ASDM Managed SFR modules 7.0.5 upgrade failure in 114_Snort_table_data_integrity_check.pl
CSCwe33282	FTD: The upgrade was unsuccessful because the httpd process was not running
CSCwe33819	Snort2 ENH: Use a common pattern matcher list for CN and SNI patterns in apps
CSCwe34269	DBCheck error is unclear when monetdb is in a 'crashed' state
CSCwe36176	ASA/FTD: High failover delay with large number of (sub)interfaces and http server enabled
CSCwe37132	TLS Server Identity may cause certain clients to produce mangled Client Hello
CSCwe37941	v1_message* and abp* files & sxp bookmark are not cleaned in user_enforcement on device registration

Bug ID	Headline
CSCwe38029	Multiple traceback seen on standby unit.
CSCwe38585	FMC + FTD's Upgrade to 7.0.4(5) version from pre -7.0.0 version creates 7.2.0 configurations on FMC
CSCwe38640	EventHandler warnings if syslog facility is CONSOLE
CSCwe39425	2100: Power switch toggle leads to ungraceful shutdowns and "PowerCycleRequest" reset
CSCwe40463	Stale IKEv2 SA formed during simultaneous IKE SA handling when missing delete from the peer
CSCwe41898	ASA: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
CSCwe44311	FP2100:Update LINA asa.log files to avoid recursive messages-<date>.1.gz rotated filenames
CSCwe44620	Question mark in NAT description causes config mismatch on Data members of an FTD cluster
CSCwe44672	Syslog ASA-6-611101 is generated twice for a single ssh connection
CSCwe44766	IMS: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
CSCwe45093	User with no vpn-filter may get additional access when per-user-override is set (IKEv2 RAVPN)
CSCwe45779	ASA/FTD drops traffic to BVI if floating conn is not default value due to no valid adjacency
CSCwe45879	Frequent errors seen regarding failures to load bulkcsv files that don't exist
CSCwe47671	High memory usage on monetDB, FMC does not show connection events
CSCwe48378	FMC WebUI extreme slowness due to heavy disk I/O
CSCwe48432	Unable to save Access Control Policy changes due to Internal error
CSCwe48997	FDM: Cannot create multiple RA-VPN profiles with different SAML servers that have the same SAML IDP\u2028
CSCwe49185	Generate password does not meet requirements while in CC mode
CSCwe50993	SNMPD running on FXOS platform goes down and won't come back up
CSCwe51286	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe51489	Unable to process query error on events; FMC UI; monetdb maximum connections reached
CSCwe51893	Cisco Firepower Management Center Software Log API Denial of Service Vulnerability

Bug ID	Headline
CSCwe52120	SSL decrypted conns fails when tx chksum-offload is enabled with the egress interface a pppoe.
CSCwe52499	NGIPSv syslog-tls.conf.tt needs filters removed when in CC mode
CSCwe52640	Certain containers have extra gray borders and certain containers are styled incorrectly
CSCwe54529	FTD on FPR2140 - Lina traceback and reload by TCP normalization
CSCwe55308	Memory leak in the MessageService
CSCwe55556	logging is getting disabled if ssl rules are reordered
CSCwe56452	BGP IPv6 configuration : route-map association with neighbour not getting deployed
CSCwe58576	FTD:Node not joining cluster with "Health check detected that control left cluster" due to SSL error
CSCwe58620	FMC Connection Events page "Error: Unable to process this query. Please contact support."
CSCwe58881	After FMC upgrade, SecureX ribbon redirects to US cloud region regardless of the set cloud region
CSCwe59380	FTD: "timeout floating-conn" not operating as expected for connections dependent on VRF routing
CSCwe59664	DAP policy created in FMC Gui, to detect a Windows OS with a hotfix, will not work as expected
CSCwe59737	ASA/FTD reboots due to traceback pointing to watchdog timeout on p3_tree_lookup
CSCwe59809	CCM seq 45 - WR6, WR8, LTS18 and LTS21.
CSCwe59919	FTD Traceback and reload on Thread Name "NetSnmp Event mib process"
CSCwe60267	FXOS fault F0853 and F0855 seen despite keyring certificates reporting renewed
CSCwe61599	FTD 2100 -Update daq-ioq mempool to help protect against buffer corruption
CSCwe61928	PIM register packets are not sent to RP after a reload if FTD uses a default gateway to reach the RP
CSCwe61969	ASA Multicontext 'management-only' interface attribute not synced during creation
CSCwe62927	DCCSM session authorization failure cause multiple issues across FMC
CSCwe62997	ASA/FTD traceback in snp_tracer_format_route
CSCwe63067	ASA/FTD may traceback and reload in Thread Name 'lina' due to due to tcp intercept stat
CSCwe63232	ASA/FTD: Ensure flow-offload states within cluster are the same

Bug ID	Headline
CSCwe63316	Pri-Active FMC NOT triggering registration TASK for FTD to configure standby manager
CSCwe64404	ASA/FTD may traceback and reload
CSCwe64542	TID python processes stuck at 100% CPU
CSCwe64557	ASA: Prevent SFR module configuration on unsuported platforms
CSCwe64563	The command "neighbor x.x.x.x ha-mode graceful-restart" removed when deleting any created context
CSCwe65245	FP2100 series devices might use excessive memory if there is a very high SNMP polling rate
CSCwe65634	ASA - Standby device may traceback and reload during synchronization of ACL DAP
CSCwe66132	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe66137	SSO user gets logged in to FMC UI if a valid local user credentials are pre-populated in the browser
CSCwe67751	Last fragment from SIP IPv6 packets has MF equal to 1, flagging that more packets are expected
CSCwe68159	Failover fover_trace.log file is flooding and gets overwritten quickly
CSCwe69388	FMC Incorrectly Pushing AnyConnect Custom attribute "defer" as "Defer" CASE-SENSITIVE
CSCwe69833	Cisco Firepower Threat Defense Software Snort 3 Geolocation IP Filter Bypass Vulnerability
CSCwe70202	Multiple times the failover may be disabled by wrongly seeing a different "Mate operational mode".
CSCwe70378	Connections not replicated to Standby FTD
CSCwe70558	FTD: unable to run any commands on CLISH prompt
CSCwe70721	Deployment is blocked due to Pre-deploy Validation Error - Invalid endpoint
CSCwe71084	IN clause does not work for externalization queries after upgrading to 7.0.x
CSCwe71284	ASA/FTD may traceback and reload in Thread Name DATAPATH-3-21853
CSCwe71672	Selective deployment negating the route configs
CSCwe71673	Selective deployment removing the prefilter-configs
CSCwe72535	Unable to login to FTD using external authentication
CSCwe73240	FMC runs out of space when Snort sends massive numbers of packet logs

Bug ID	Headline
CSCwe74059	logrotate is not compressing files on 9.16 ASA or 7.0 FTD
CSCwe74328	AnyConnect - mobile devices are not able to connect when hostscan is enabled
CSCwe74899	CD App Sync error is App Config Apply Failed on Secondary/Standby after backup restore on RMA device
CSCwe74916	Interface remains DOWN in an Inline-set with propagate link state
CSCwe75124	Upgraded FMC didn't mark FTD's with Hot Fix as light registered - failed FMC HA sync
CSCwe75207	High rate of network map updates can cause large delays and backlogs in event processing
CSCwe76036	ndclientd error message 'Local Disk is full' needs to provide mount details which is full
CSCwe78977	ASA/FTD may traceback and reload in Thread Name 'pix_flash_config_thread'
CSCwe79051	Deployment for eigrp / bgp change may cause temporary outage during policy apply
CSCwe79072	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe79954	LDAP External auth config fails to deploy to FTD if same LDAP server is added as Primary and backup
CSCwe79990	Cisco-Intelligence-Feed - Failed to download due to timeout
CSCwe81684	ASA: Standby failure on parsing of "management-only" not reported to parser/failover subsystem
CSCwe83061	FMC Upgrade from Active-Primary FMC is failed with "Installation failed: Peer Discovery incomplete."
CSCwe83478	Prune target should account for the allocated memory from the thread pruned
CSCwe83775	Incorrect CPU and core metrics collected on 55XX platform
CSCwe83812	SFDataCorrelator log spam when network map is full
CSCwe84079	asa_snmp.log is not rotated, resulting in large file size
CSCwe85432	ASA/FTD traceback and reload on thread DATAPATH-14-11344 when SIP inspection is enabled
CSCwe86687	Apache Commons FileUpload before 1.5 does not limit the number of request
CSCwe86690	In Apache MINA, a specifically crafted, malformed HTTP request may cause
CSCwe86693	An issue in protobuf-java allowed the interleaving of com.google.protobu
CSCwe86923	In Apache MINA, a specifically crafted, malformed HTTP request may cause

Bug ID	Headline
CSCwe86951	Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 throu
CSCwe87591	Cisco FTD Software SSL/TLS URL Category and Snort 3 Detection Engine Bypass and DOS Vulnerability
CSCwe88496	"Failed to convert snort 2 custom rules. Refer /var/sf/htdocs/ips/snort.rej for more details."
CSCwe89024	FTS under AC Policy Listing page with 'obj' gives Error Moving Data error with CTS DB
CSCwe89030	Serial number attribute from the subject DN of certificate should be taken as the username
CSCwe89305	vFMC300 to FMC2600 migration failure with error "migration from R to N is not allowed"
CSCwe89731	Notification Daemon false alarm of Service Down
CSCwe90202	ASA: Standby failure on parsing of "management-only" for dynamic configuraiton changes
CSCwe90334	Missing Instance ID in unified_events-2.log
CSCwe90720	ASA Traceback and reload in parse thread due ha_msg corruption
CSCwe91652	Database backup failed on KVM FMC
CSCwe91674	Mserver restarts frequently
CSCwe91900	FTD - Repeated message in logs from sftunnel processing pub files
CSCwe91958	correlation events based on connection events do not contain Security Intelligence Category content
CSCwe92905	ngfwManager process continuously restarting leading to ZMQ Out of Memory traceback
CSCwe93162	FP1140 7.0.4 Deployment keep failing with error "Can\'t use an undefined value as a HASH reference"
CSCwe93176	Snort2 rule assignments missing from ngfw.rules (assignment_data table) after FMC upgrade.
CSCwe93202	FXOS REST API: Unable to create a keyring with type "ecdsa"
CSCwe93489	Threat-detection does not recognize exception objects with a prefix in IPv6
CSCwe93532	ASA/FTD may traceback and reload in Thread Name 'lina'.
CSCwe93561	Cisco ASA and FTD VPN Web Client Services Client-Side Request Smuggling Vulnerability
CSCwe93566	need to turn off default TLS 1.1 (deprecated) support for the FDM GUI

Bug ID	Headline
CSCwe94287	FTD DHCP Relay drops NACK if multiple DHCP Servers are configured
CSCwe95729	Cisco ASA & FTD SAML Authentication Bypass Vulnerability
CSCwe95757	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwe96023	ASa/FTD: SNMP related traceback and reload immediately after upgrade from 6.6.5 to 7.0.1
CSCwe96068	ASA: Configurable CLU for Large amount of under/overruns on CLU RX/TX queues
CSCwe97277	Observed ASA traceback and reload when performing hitless upgrade while VPN traffic running
CSCwe98146	Snort3 cores seen in certain conditions with traffic
CSCwe98430	AC policy deploy failing on 7.2.4 FMC to 6.7 FTD
CSCwe98435	Selective policy deploy with Identity Policy (captive-portal) and SSL Policy (dp-tcp-proxy) CLI
CSCwe98687	Cisco FTD Software Software for Cisco Firepower 2100 Series Inspection Rules DoS Vulnerability
CSCwe98751	FMC is suddenly not showing stack after creation.
CSCwe99040	traceback and reload thread datapath on process tcpmod_proxy_continue_bp
CSCwe99550	Add knob to pause/resume file specific logging in asa log infra.
CSCwf00736	CSM backup failed within FMC backup due to modification of file while tar was reading it
CSCwf00803	Mode / License mismatch information is not seen in show failover history
CSCwf01051	standby in disabled state after QP-MI HA 7.0.3 to 7.2.4-126, APPLY_APP_CONFIG_APPLICATION_FAILURE
CSCwf02005	ActionQueue task sandbox data update throws SQL Error post 7.2.4 upgrade
CSCwf02363	Snort3 Crash in SslServiceDetector after call from nss_passwd_lookup
CSCwf03490	portmanager.sh outputing continuous bash warnings to log files
CSCwf04831	ASA/FTD may traceback and reload in Thread Name 'ci/console'
CSCwf06261	Health Monitoring exports negative snort swap memory metric value
CSCwf06377	Setting heartbeat timeout to 6sec for Firepower 4100 and 9300
CSCwf06818	Cisco Firepower Threat Defense Software Encrypted Archive File Policy Bypass Vulnerability

Bug ID	Headline
CSCwf07030	Upgrade Device listing page is taking more than 15 mins to load page fully with 25 FTDs registered
CSCwf07791	ASA running out of SNMP PDU and SNMP VAR chunks
CSCwf08043	Lina traceback and reload due to fragmented packets
CSCwf08790	FMC Restore of remote backup fails due to no space left on the device
CSCwf10422	"Security Intelligence feed download failed" displayed even though it succeeded
CSCwf12005	ASA sends OCSP request without user-agent and host
CSCwf12408	ASA: After upgrade to 9.16.4 all type-8 passwords are lost on first reboot
CSCwf14031	Snort down due to missing lua files because of disabled application detectors (VDB side)
CSCwf14735	traceback and reload in Process Name: lina related to Nat/Pat
CSCwf14811	TCP normalizer needs stats that show actions like packet drops
CSCwf15858	LDAP authentication over SSL not working for users that send large authorisation profiles
CSCwf15978	xml2js version 0.4.23 allows an external attacker to edit or add new pro
CSCwf16559	getReadinessStatusTaskList pjb request is very frequent when user in Upgrade sensor list page
CSCwf17814	ASA/FTD may traceback and reload in Thread Name '19', free block checksum failure
CSCwf19562	Changes to lamplighter logs written to /var/log/tid_process.log
CSCwf19761	SFDC cores on FTD-HA setup due to threads stuck in clamav library
CSCwf19853	FATAL errors in DBCheck due to missing columns in eventdb table
CSCwf20215	admin user should be excluded from CLI shell access filter
CSCwf20338	ASA may traceback and reload in Thread Name 'DHCPv6 Relay'
CSCwf21106	ASA/FTD: Traceback on thread name: snmp_master_callback_thread during SNMP and interface changes
CSCwf22241	Security zones are not showing in AC policy UI
CSCwf22568	FTD HA Creation fails resulting in devices showing up in an inconsistent state on the FMC
CSCwf22637	Network Object Group overrides not visible or be edited from FMC GUI
CSCwf23564	Unable to establish BGP when using MD5 authentication over GRE TUNNEL and FTD as passthrough device

Bug ID	Headline
CSCwf24124	SFDataCorrelator process crashing very frequently on the FMC.
CSCwf24773	crashhandler running with test mode snort
CSCwf25144	FMC backup management page showing "Verifying Backup" for FTD sensors.
CSCwf25563	Device list takes longer to load while creating new AC policy
CSCwf26939	FTD may fail to create a NAT rule with error: "IPv4 dst real obj address range is huge"
CSCwf28488	Inconsistent log messages seen when emblem is configured and buffer logging is set to debug
CSCwf28592	In some specific scenarios, object optimizer can cause incorrect rules to be deployed to the device
CSCwf30716	ASA in multi context shows standby device in failed stated even after MIO HB recovery.
CSCwf30727	ASA integration with umbrella does not work without validation-usage ssl-server.
CSCwf31176	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwf31701	ASA traceback and reload with the Thread name: **CP Crypto Result Processing**
CSCwf31820	Firewall may drop packets when routing between global or user VRFs
CSCwf32890	Standby FMC SSH connection getting disconnected frequently.
CSCwf33574	ASA access-list entries have the same hash after upgrade
CSCwf34450	Snort3 crash after the consequent snort restart if duplicate custom apps are present
CSCwf35510	Possible segfault in snort3 when appid tries to delete the app info table
CSCwf36674	Cross site Scripting Vulnerability in FMC
CSCwf39821	FTD: High-Availability unit struck at CD App Sync error due to error ngfwManager restart on peer
CSCwf42144	ASA/FTD may traceback and reload citing process name "lina"
CSCwf43288	Traceback in Thread Name: ssh/client in a clustered setup
CSCwf45094	MariaDB Process in FMC should use jemalloc instead of glibc
CSCwf47924	Cisco ASA and FTD VPN Web Client Services Client-Side Request Smuggling Vulnerability
CSCwf49254	cannot unregister FTD from Cisco Cloud in FDM if already unregistered/unenrolled from cloud side
CSCwf49486	store_*list_history.pl task is created every 5min without getting closed causing FMC slowness.

Bug ID	Headline
CSCwf51933	FTD username with dot fails AAA-RADIUS external authentication login after upgrade
CSCwf56386	vFTD runs out of memory and goes to failed state
CSCwf57261	ASA: Traceback and reload due to clientless webvpn session closure
CSCwf57850	TelemetryApp process keeps exiting every minute after upgrading the FMC
CSCwf58876	KP2140-HA, reloaded primary unit not able to detect the peer unit
CSCwf62729	Cisco ASA/FTD Firepower 2100 SSL/TLS Denial of Service Vulnerability
CSCwf63210	Cisco Firepower Management Center Software Command Injection Vulnerability
CSCwf63215	Cisco Firepower Management Center Software Path Traversal Vulnerability
CSCwf67337	FMC taking long times to save override objects even if not modified
CSCwf70275	FTD: TLS Server Identity does not work if size of client hello more than TCP MSS bytes
CSCwf75695	Duplicate FTD cluster has been created when multiple cluster events comes at same time
CSCwf76945	Packet data is still dropped after upgrade
CSCwf82447	Editing identity nat rule disables "perform route lookup" silently
CSCwf82742	FTD: SNMP not working on management interface
CSCwf82970	Snort2 engine is crashing after enabling TLS Server Identity Discovery feature
CSCwf86557	Decrypting engine/ssl connections hang with PKI Interface Error seen
CSCwf91282	import of .SFO to FMC failed due to included local/custom rules having a blank rule message field
CSCwf92182	Cisco Firepower Management Center Software SQL Injection Vulnerability
CSCwf92726	Some Vault secrets including LDAP missing files after upgrade if the Vault token is corrupted
CSCwf99173	DOC:When using an SLR, it does not properly documented what happens if one of the licenses expires.
CSCwh00123	In Multi-manager scenario,cdFMC&Analytics FMC,FTD should only receive identity feeds from Config FMC
CSCwh04231	FMC needs to properly maintain Redis data directory to prevent unbounded disk usage
CSCwh08403	FMC HA - Health Policy - Applied count shows "0" appliance
CSCwh11411	Snort blacklisting traffic during deployment

Bug ID	Headline
CSCwh12987	Large SMB servers result in timeouts returning verdicts between FMC and FTD devices
CSCwh14467	File sizes larger than 100MB for AnyConnect/Secure Client images cannot be uploaded on FMC
CSCwh14584	Traceback seen on FTD running on Firepower 2100 series
CSCwh19475	Intermittently flow is getting white-listed by the snort for the unknow app-id traffic.
CSCwh20002	Standby FMC is not getting updated with latest GEO DB package
CSCwh21141	The FMC preview deployment shows a wrong information.
CSCwh24901	'Frequent drain of events (not unprocessed events) to be removed from FMC
CSCwh25668	ASA 55xx devices running 7.0.6 show up as 100% usage on CPU01 [LINA]
CSCwh36005	Policy deployment failed due to "1 errors seen during populateGlobalSnapshot"
CSCwh37475	Removal of msie-proxy commands during flexconfig rollback
CSCwh41094	Cisco FTD TCP/IP Traffic Snort 2/3 Denial of Service Vulnerability
CSCwh41126	FMC ACP report does not shows all the access control rules
CSCwh41922	Cisco Firepower Management Center Software HTML Injection Vulnerability
CSCwh41958	Cisco Firepower Management Center Software HTML Injection Vulnerability
CSCwh42077	Cisco_Firepower_GEODB_FMC_Update* are not included in diskmanager
CSCwh49085	Avoid unnecessary DB operations when processing derived fingerprints
CSCwh52420	AMP Cloud look up timeout frequently.
CSCwh56945	SFDataCorrelator crashing repeatedly in RNA_DB_InsertServiceInfo
CSCwh57976	Improve CPU utilization in ssl inspection for supported signature algorithm handling
CSCwh59222	SNORT3 - FTD - TSID high cpu, daq polling when ssl enabled is not pulling enough packets
CSCwh60783	FTD - Captive portal enabled is still running despite the feature is off
CSCwh62080	additional command outputs needed in FTD troubleshoot for blocks and ssl cache
CSCwh64508	Fixing the regression caused while handling web UI is not getting FTDv Variable
CSCwh68878	Diskmanager process terminated unexpectedly
CSCwh69209	Prefilter cannot add Tunnel Endpoints in Tunnel Rule on FMC
CSCwh69787	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwh69815	FTDvs through put got changed to 100Kbps after upgrade

Bug ID	Headline
CSCwh70866	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwh74586	XTLS: With TSID AC-Policy configured plugin is not disengaging immediately at CH
CSCwh75829	FMC Primary disk degraded error
CSCwh75924	A vulnerability was found in MariaDB. An OpenVAS port scan on ports 3306
CSCwh87058	FTD: Internal certificate generation results to certificate and private key mismatch
CSCwh89835	FMC plain-text passwords for radius server and certificate passphrase
CSCwh92541	Random FTD snort3 traceback
CSCwi14896	Node kicked out of cluster while enabling or disabling rule profiling
CSCwi18663	FMC-4600: Pre-Filter policy is showing as none
CSCwi19485	Fail open snort-down is off in inline pairs despite it being enabled and deployed from FMC
CSCwi23477	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwi23613	Cisco Firepower Management Center SQL Injection Vulnerability
CSCwi26709	Cisco Firepower Management Center Software HTML Injection Vulnerability
CSCwi27402	FTD: Update WM firmware to 1023.0207
CSCwi27459	Snort Crash during selection of signature algorithm ECDSA
CSCwi31558	File-extracts.logs are not recognised by the diskmanager leading to high disk space
CSCwi34719	Unable to SSH into FTD device using External authentication with Radius
CSCwi38061	ASA/FTD traceback and reload due to file descriptor limit being exceeded
CSCwi38662	FTD HA should not be created partially on FMC
CSCwi40487	FTD HA Failure after SNORT crash.
CSCwi42962	installing GeoDB country code package update to FMC does not automatically push updates to FTDs
CSCwi61058	Cisco Firepower Management Center Cross Site Scripting Vulnerability
CSCwi78063	Cisco FTD Software and FMC Software Code Injection Vulnerability
CSCwi78588	Cisco Secure Firewall Management Center Software Command Injection Vulnerability
CSCwi78593	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwi78594	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability

Bug ID	Headline
CSCwi78596	Cisco Firepower Management Center SQL Injection Vulnerabilities
CSCwi78941	FDM deployment fails with error "Some interfaces have been added to or removed from the device"
CSCwi82368	Classic licenses needs to be manually added after registering to license during migration/RMA
CSCwi85823	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwi86198	SFData correlator keep terminating on FTDs configured for IDS
CSCwi86503	File sizes larger than 100MB for AnyConnect/Secure Client images cannot be uploaded on FMC
CSCwi93842	Cisco Firepower Management Center Software HTML Injection Vulnerability
CSCwi98147	Tomcat restarts in the middle of the LTP flow due to certificate update
CSCwi99692	Firepower Management Center Access Policies web UI Cross-Site Scripting
CSCwj00956	Snort process spamming syslog-ng messages causing syslog-ng termination
CSCwj03056	FMC username enumeration from API response
CSCwj03112	pmtool restart of monetdb fails to bring up monetdb, too many files in monetdb Volume directory
CSCwj09456	Cisco Firepower Management Center Stored Software Cross-Site Scripting Vulnerability
CSCwj11119	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwj14624	Backup exits with memory allocation error on 4115
CSCwj14798	TSS_Daemon process is exiting every minute
CSCwj17969	rna_ip_os_map can grow very large that causes SFDataCorrelator to stop processing events
CSCwj19632	Cisco Firepower Management Center Stored Software Cross-Site Scripting Vulnerability
CSCwj40597	FTD: Backups fail on Multi-Instance or standalone with error "Backup died unexpectedly"
CSCwj51115	FMC backup remote server copy to Solar Winds remote server failing after upgrading to 7.x versions.
CSCwj61885	File descriptor leak when validating upgrade images
CSCwj68540	Cisco Secure Firewall Management Center Software Command Injection Vulnerability
CSCwj72721	Deployment failure and rollback when BGP communities added or removed in route-map match clause

Bug ID	Headline
CSCwj77284	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwj82713	sf.xml lacks entries for recent Secure Firewall system software updates
CSCwj88414	CVE-2023-48795 is not addressed on FMC 7.0.6.2 version
CSCwk24881	Steps to remove / unregister decommissioned FTD HA devices from FMC
CSCwk25506	Multiple snort binaries are present (Patch or HF) at /var/sf/bin/ making tar command to fail
CSCwk27741	Cisco Firepower Management Center SQL Injection Vulnerability
CSCwk40726	FMC REST API calls to get AC policy data times out, AC policy GUI slowness with larger rule query
CSCwk41806	Need to Protect LINA from getting killed by OOM

Resolved Bugs in Version 7.0.5.1

Table last updated: 2022-04-26

Table 57: Resolved Bugs in Version 7.0.5.1

Bug ID	Headline
CSCwe52499	NGIPSv syslog-tls.conf.tt needs filters removed when in CC mode

Resolved Bugs in Version 7.0.5

Table last updated: 2022-11-17

Table 58: Resolved Bugs in Version 7.0.5

Bug ID	Headline
CSCvo17612	Return error messages when failing to retrieve objects from database
CSCvq70838	Traceback in the output of tail-logs command
CSCvr06065	Snort core due to DAQ IOQ Corruption
CSCvw82067	ASA/FTD 9344 blocks depleted due to high volume of fragmented traffic
CSCvw90399	FMC HA issues with too many open file descriptors for sfipproxy UDP conn
CSCvx24207	FQDN Object Containing IPv4 and IPv6 Addresses Only Install IPv6 Entries
CSCvx68586	Not able to login to UI/SSH on FMC, console login doesn't prompt for password
CSCvx75743	Inconsistent FMC audit log severity

Bug ID	Headline
CSCvx86569	Access Control Rule - Comment disappears if clicked to another tab before saving the comment.
CSCvy24180	Default variable set missing on FMC
CSCvy38070	File/Malware Event Report fails when date is x-axis and count y-axis for table chart
CSCvy38650	Unable to download captured file from FMC Captured files UI
CSCvy45048	Subsystem query parameter not filtering records for "auditrecords" restapi
CSCvy47927	Unable to select multiple policies for scheduled firepower recommended rules
CSCvy50598	BGP table not removing connected route when interface goes down
CSCvy63463	Error deleting users due to special characters
CSCvy65178	Need dedicated Rx rings for to the box BGP traffic on Firepower platform
CSCvy67765	FTD VTI reports TUNNEL_SRC_IS_UP false despite source interface is up/up and working
CSCvy68974	ActionQueue process is killed by OOM killer due to process utilizing more than 3 GB limit for memory
CSCvy73130	FP4100 platform: Active-Standby changed to dual Active after running "show conn" command
CSCvy75131	Occasionally deleted sensor/interfaces are not removed from security zones
CSCvy93607	Health monitor alert indicates QP HA in split brain when one device reboots and re-joins
CSCvy95520	Cisco Firepower Management Center and Firepower Threat Defense Software SSH DoS Vulnerability
CSCvy95809	Crashinfo script is invoked on SFR running snort2 and device fails to upgrade to 7.0
CSCvz07004	SNORT2: FTD is performing Full proxy even when SSL rule has DND action.
CSCvz09106	Cisco ASA and FTD Software SSL VPN Denial of Service Vulnerability
CSCvz13564	Firepower 2100 FTD: ssh-access-list configuration are lost after upgrading
CSCvz19364	FXOS does not send any syslog messages when the duplex changes to "Half Duplex"
CSCvz31184	Validation of unsupported flow-offload using pre-filter in passive/inline interfaces in FPR4100/9300
CSCvz32593	FPR4110 and FPR4115 in disabled state CD App Sync error is Rsync is not enabled on active device
CSCvz35669	KP-2110 Standby disabled upgrade 6.6.4-64 to 7.0.1-30 "CD App Sync error is App Config Apply Failed"

Bug ID	Headline
CSCvz36903	ASA traceback and reload while allocating a new block for cluster keepalive packet
CSCvz40542	FMC : Remote Storage Device's SMB share password does not make it when upgrading from 6.6 to 7
CSCvz40765	FMC CPU graph displays the wrong number of Snort and System cores
CSCvz42823	Bulk Operation of AC Policy REST API taking time
CSCvz43325	Active FMC not deregistering sensors after breaking HA
CSCvz49163	Observed some time drift in seconds in the output when we execute show rule hits multiple times
CSCvz52785	Management interface flaps every 13mins post upgrade from 9.12 to 9.14.2.15
CSCvz57917	High unmanaged disk usage on /ngfw filled with module-xxxx-x86_64.tgz files in packages folder
CSCvz60142	ASA/FTD stops serving SSL connections
CSCvz61456	Software upgrade on ASA application may failure without obvious reasons
CSCvz61463	FP9k SM-44 High CPU on radware vdp Cores after upgrade
CSCvz62517	SRU install should validate files upon completion
CSCvz68713	PLR license reservation for ASAv5 is requesting ASAv10
CSCvz69729	Unstable client processes may cause LINA zmqio traceback on FTD
CSCvz71596	"Number of interfaces on Active and Standby are not consistent" should trigger warning syslog
CSCvz77050	Occasionally policy deployment failure are reported as successful
CSCvz78331	SNMP polling fails after a re-image
CSCvz84733	LACP packets through inline-set are silently dropped
CSCvz85234	Facilities ALERT, AUDIT, CLOCK and KERN do not work in sending Audit Log to syslog from FMC.
CSCvz94841	Grammatical errors in failover operating mode mismatch error message
CSCwa03341	Standby's sub interface mac doesn't revert to old mac with no mac-address command
CSCwa06608	WM 1010 HA Failover is not successful when we give failover active in secondary.
CSCwa07390	Config only FMC: SI feed downloaded file does not match expected checksum
CSCwa15093	Access Policy Control Clear Hit Count throwing Error 403: Forbidden
CSCwa16626	Syslog over TLS accepting wildcard in middle of FQDN

Bug ID	Headline
CSCwa33248	Auto LSP update not getting triggered, missing Talos registration (beakerd)
CSCwa36535	Standby unit failed to join failover due to large config size.
CSCwa38996	Big number of repetitive messages in snmpd.log leading to huge log size
CSCwa41936	Cisco FTD Bleichenbacher Attack Vulnerability
CSCwa42596	ASA with SNMPv3 configuration observes unexpected reloads with snmpd cores
CSCwa43311	Snort blocking and dropping packet, with bigger size(1G) file download
CSCwa47737	ASA/FTD may hit a watchdog traceback related to snmp config writing
CSCwa49480	SNMP OID , stop working after around one hour and a half - FTD
CSCwa55142	SNORT3 / SSL / Definitive DND verdict when there's an extra DND bottom rule, instead of regular DND
CSCwa59907	LINA observed traceback on thread name "snmp_client_callback_thread"
CSCwa61361	ASAv traceback when SD_WAN ACL enabled, then disabled (or vice-versa) in PBR
CSCwa62025	IPv6: Some of egress interfaces of global and user vrf routes are missing in asp table
CSCwa64739	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwa68552	All type-8 passwords are lost upon upgrade from ASA 9.12-9.15 to 9.16, failover gets disabled
CSCwa72528	username form cert feature does not work with SER option
CSCwa72530	FTD: Time gap/mismatch seen when new node joins a Cluster Control node under history
CSCwa72641	URL incorrectly extracted for TLS v1.2 self signed URLs when "Early application detection" enabled
CSCwa72929	SNMPv3 polling may fail using privacy algorithms AES192/AES256
CSCwa73172	ASA reload and traceback in Thread Name: PIX Garbage Collector
CSCwa75966	ASA: Reload and Traceback in Thread Name: Unicorn Proxy Thread with Page fault: Address not mapped
CSCwa77083	Host information is missing when Security Zones are configured in Network Discovery rules
CSCwa78082	FMC intrusion event search produces inconsistent results
CSCwa80040	FMC NFS configuration failling after upgrade from 6.4.0.4 to 7.0.1
CSCwa81143	Unable to save the application policy filter. Save tab is stuck and its continuously loading.

Bug ID	Headline
CSCwa85492	URL lookup responding with two categories
CSCwa85709	Cisco Firepower Management Center Information Disclosure Vulnerability
CSCwa87298	ASA conn data-rate: incorrect "current rate" and "data-rate-filter" doesn't work properly
CSCwa89347	Cannot add object to network group on FMC
CSCwa90735	FTD/FXOS - ASAconsole.log files fail to rotate causing excessive disk space used in /ngfw
CSCwa91070	Cgroup triggering oom-k for backup process
CSCwa92596	Access Control File policy rule message is misleading and unnecessary
CSCwa92822	TLS client in the sftunnel TLS tunnel offers curves in CC mode that are not allowed by CC
CSCwa92883	Deployment Failed at phase-2 with domain snapshot error
CSCwa93499	Cisco Firepower Management Center Stored Cross-Site Scripting Vulnerability
CSCwa95079	ASA/FTD Traceback and reload due to NAT configuration
CSCwa97541	Cisco ASA FirePOWER Module, FMC and NGIPS SNMP Default Credential Vulnerability
CSCwa97917	ISA3000 in boot loop after powercycle
CSCwa98853	Error F0854 FDM Keyring's RSA modulus is invalid
CSCwa98983	Upgrade failed on FPR2100-HA at 800_post/901_reapply_sensor_policy.pl
CSCwa99171	Chassis and application sets the time to Jan 1, 2010 after reboot
CSCwa99931	ASA/FTD: Tuning of update_mem_reference process
CSCwa99932	ASA/FTD stuck after crash and reboot
CSCwb00749	FMC upgrade failure: 114_DB_table_data_integrity_check.pl failed
CSCwb01983	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb01990	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb01995	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb02006	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb02018	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb02026	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb02060	snmp-group host with Invalid host range and subnet causing traceback and reload

Bug ID	Headline
CSCwb03704	ASA/FTD datapath threads may run into deadlock and generate traceback
CSCwb04000	ASA/FTD: DF bit is being set on packets routed into VTI
CSCwb05148	Cisco ASA Software and FTD Software SNMP Denial of Service Vulnerability
CSCwb05291	Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability
CSCwb05920	Crash in KP at webVpn free, HTTPCleanUp and mem_mh_free from Scaled AC-IK/IPSec TVM test.
CSCwb06273	Continuous memory leak in the process hmlsd (SF::Messaging::smartSend)
CSCwb06847	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-9-11543'
CSCwb07908	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
CSCwb07981	Traceback: Standby FTD reboots and generates crashinfo and lina core on thread name cli_xml_server
CSCwb08644	ASA/FTD traceback and reload at IKEv2 from Scaled S2S+AC-DTLS+SNMP long duration test
CSCwb08773	FPR2130 LED is off when power supply module 1 is back
CSCwb08828	FP1010 Switchport access vlan interface in up/up status but not passing traffic
CSCwb12730	Policy deployment failed in FMC however FTD deployment status shows "INPROGRESS"
CSCwb16037	Unable to replace the anyconnect image when maximum memory used for anyconnect images.
CSCwb16663	Unable to configure NAP under Advanced Tab in AC policy
CSCwb16920	CPU profile cannot be reactivated even if previously active memory tracking is disabled
CSCwb17187	SNMP cores are generated every minute while running snmpwalk on HA
CSCwb17963	Unable to identify dynamic rate liming mechanism & not following msg limit per/sec at syslog server.
CSCwb19648	SNMP queries for crasLocalAddress are not returning the assigned IPs for SSL/DTLS tunnels.
CSCwb22592	SSH Functionalty stopped working after running long duration tests of SCP + Scaled TVM VPN Profiles
CSCwb23029	Cisco Firepower Management Center Software Command Injection Vulnerability
CSCwb23048	Cisco Firepower Management Center Software Command Injection Vulnerability
CSCwb24039	ASA traceback and reload on routing

Bug ID	Headline
CSCwb25809	Single Pass - Traceback due to stale ifc
CSCwb28123	FTD HA deployment fails with error "Deployment failed due to major version change on device"
CSCwb29126	Cannot use underscore (_) in FMC's realm AD Primary Domain configuration
CSCwb31551	When inbound packet contains SGT header, FPR2100 cannot distribute properly per 5 tuple
CSCwb31699	Primary takes active role after reload
CSCwb32267	Crash on KP Active node while clearing vpnsessiondb with AnyConnect-SSL TVM Profile running
CSCwb32418	Cisco FirePOWER Software for ASA FirePOWER Module Command Injection Vulnerability
CSCwb32841	NAT (any,any) statements in-states the failover interface and resulting on Split Brain events
CSCwb33184	Memory leak in MessageService causes UI slowness
CSCwb35675	Snort3 is partially in sync with Snort 2 warning alert
CSCwb37077	“show access-control-config” for DNS Reputation Enforcement does not work.
CSCwb37999	Customized Variables name cause Snort3 validation failure
CSCwb38406	GeoDB updates on multi-domain environment requires a manual policy deployment
CSCwb39431	FTD unified logs do not print the log as per rfc5424 standard
CSCwb40001	Long delays when executing SNMP commands
CSCwb41739	debug crypto conditional need to be made multi-ctx aware
CSCwb41854	Cisco FTD Software and Cisco FXOS Software Command Injection Vulnerability
CSCwb42978	ASA accepting invalid netmask in SSH/TELNET/HTTP/TFTP config
CSCwb43018	Implement SNP API to check ifc and ip belongs to HA LU or CMD interface
CSCwb43433	Jumbo frame performance has degraded up to -45% on Firepower 2100 series
CSCwb50405	ASA/FTD Traceback in crypto hash function
CSCwb51707	ASA Traceback and reload in process name: lina
CSCwb52401	Cisco Firepower Threat Defense Software Privilege Escalation Vulnerability
CSCwb53172	FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated
CSCwb53191	Certificate validation fails post upgrade to 9.17.1

Bug ID	Headline
CSCwb53328	ASA/FTD Traceback and reload caused by Smart Call Home process sch_dispatch_to_url
CSCwb53694	Cisco Firepower Management Center Software XML External Entity Injection Vulnerability
CSCwb54791	ASA DHCP server fails to bind reserved address to Linux devices
CSCwb56718	Policy deployment fails with error- Rule update is running but there are no updates in progress.
CSCwb56905	ASA blocking 0.0.0.0 IP and netmask combination in SSH/TELNET/HTTP config
CSCwb57524	FTD upgrade fails - not enough disk space from old FXOS bundles in distributables partition
CSCwb57615	Configuring pbr access-list with line number failed.
CSCwb59465	ASA/FTD may traceback (watchdog) and reload when generating a syslog from the VPN Failover subsystem
CSCwb59488	ASA/FTD Traceback in memory allocation failed
CSCwb59619	PM needs to restart the Disk Manager after creating ramdisk to make DM aware of the ramdisk
CSCwb60993	FDM Need to block the deployment when a Security zone object is not associated with an interface
CSCwb61901	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb61908	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb62059	Unable to login to FTD using external authentication after upgrade
CSCwb64620	CC mode is not properly enabled on NGIPSv impacting syslog over TLS and SSH
CSCwb65447	FTD: AAB cores are not complete and not decoding
CSCwb65718	FMC is stuck on loading SI objects page
CSCwb66761	Cisco Firepower Threat Defense Software Generic Routing Encapsulation DoS Vulnerability
CSCwb67040	FP4112|4115 Traceback & reload on Thread Name: netfs_thread_init
CSCwb68642	ASA traceback in Thread Name: SXP CORE
CSCwb68993	FTD/FDM: SSL connections to sites using RSA certs with 3072 bit keys may fail
CSCwb69503	ASA unable to configure aes128-gcm@openssh.com when FIPS enabled
CSCwb71460	ASA traceback in Thread Name: fover_parse and triggered by snmp related functions

Bug ID	Headline
CSCwb73248	FW traceback in timer infra / netflow timer
CSCwb74571	PBR not working on ASA routed mode with zone-members
CSCwb76129	Some SSL patterns not detected after VDB 356 or higher is installed
CSCwb76423	ASA crashes on fp2100 when checking CRL
CSCwb79812	RIP is advertising all connected Anyconnect users and not matching route-map for redistribution
CSCwb80108	FP2100/FP1000: Built-in RJ45 ports randomly not coming up after portmanager restart events
CSCwb80559	FTD offloads SGT tagged packets although it should not
CSCwb80862	ASA/FTD proxy arps any traffic when using the built-in 'any' object in translated destination
CSCwb82796	ASA/FTD firewall may traceback and reload when tearing down IKE tunnels
CSCwb83388	ASA HA Active/standby tracebacks seen approximately every two months.
CSCwb83691	ASA/FTD traceback and reload due to the initiated capture from FMC
CSCwb84901	CIAM: heimdal 1.0.1
CSCwb85633	Snmpwalk output of memory does not match show memory/show memory detail
CSCwb85822	Deployment failing when collecting policies.
CSCwb86118	TPK ASA: Device might get stuck on ftp copy to disk
CSCwb86565	FMC upgrade fails due Mismatch in number of entries between /etc/passwd and /etc/shadow
CSCwb87498	Lina traceback and reload during EIGRP route update processing.
CSCwb87950	Cisco ASA Software and FTD Software Web Services Interface Denial of Service Vulnerability
CSCwb88587	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb88651	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwb89187	Flex Config allow - "timeout icmp-error hh:mm:ss"
CSCwb90074	ASA: Multiple Context Mixed Mode SFR Redirection Validation
CSCwb90532	ASA/FTD traceback and reload on NAT related function nat_policy_find_location
CSCwb91101	SNMP interface threshold doesn't trigger properly when traffic sent to interface ~4gbps
CSCwb92376	FMC syslog-ng daemon fails to start if log facility is set to ALERT

Bug ID	Headline
CSCwb92709	We can't monitor the interface via "snmpwalk" once interface is removed from context.
CSCwb92937	Error 403: Forbidden when expanding in view group objects
CSCwb93932	ASA/FTD traceback and reload with timer services assertion
CSCwb94170	merovingian.log file extremly big size can fill the disk
CSCwb94190	ASA graceful shut down when applying ACL's with forward reference feature and FIPS enabled.
CSCwb94312	Unable to apply SSH settings to ASA version 9.16 or later
CSCwb95112	Intrusion Policy shows last modified by admin even though changes are made by a different user
CSCwb95787	FPR1010 - No ARP on switchport VLAN interface after portmanager DIED event
CSCwb97251	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCwc02488	ASA/FTD may traceback and reload in Thread Name 'None'
CSCwc02700	Fragmented packets are dropped when unit leaves cluster
CSCwc03069	Interface internal data0/0 is up/up from cli but up/down from SNMP polling
CSCwc03393	Lina traceback and core file size is beyond 40G and compression fails on FTD
CSCwc04959	Disk usage is 100% on secondary FMC .dmp files created utilized all the disk space
CSCwc05132	Unable to disable "Retrieve to Management Center
CSCwc06833	Deployment failure with ERROR Process Manager failed to verify LSP ICDB
CSCwc07262	Standby ASA goes to booting loop during configuration replication after upgrade to 9.16(3).
CSCwc08374	Azure ASA NIC MAC address for Gigeth 0/1 and 0/2 become out of order when adding interfaces
CSCwc09414	ASA/FTD may traceback and reload in Thread Name 'ci/console'
CSCwc10037	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwc10483	ASA/FTD - Traceback in Thread Name: appAgent_subscribe_nd_thread
CSCwc10792	ASA/FTD IPSEC debugs missing reason for change of peer address and timer delete
CSCwc11511	FTD: SNMP failures after upgrade to 7.0.2
CSCwc11597	ASA tracebacks after SFR was upgraded to 6.7.0.3
CSCwc11663	ASA traceback and reload when modifying DNS inspection policy via CSM or CLI

Bug ID	Headline
CSCwc13017	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
CSCwc13994	ASA - Restore not remove the new configuration for an interface setup after backup
CSCwc15530	Syslog facility "ALERT" should be changed on FDM since is not supported anymore by syslog-ng
CSCwc18285	Conn data-rate command can be enabled or disabled in unprivileged user EXEC mode
CSCwc18312	"show nat pool cluster" commands run within EEM scripts lead to traceback and reload
CSCwc18524	ASA/FTD Voltage information is missing in the command "show environment"
CSCwc23075	Upgrade to MariaDB 10.5.16 to get security vulnerability fixes
CSCwc23356	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-20-7695'
CSCwc23695	ASA/FTD can not parse UPN from SAN field of user's certificate
CSCwc24582	Update diskmanager to monitor deploy directories in /ngfw/var/cisco/deploy/db
CSCwc24906	ASA/FTD traceback and reload on Thread id: 1637
CSCwc25207	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 33)
CSCwc26406	FMC: Slowness in Device management page
CSCwc27236	FMC Health Monitoring JSON error
CSCwc27797	ASA mgmt ip cannot be released
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwc28532	9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwc28660	Snort3: NFSv3 mount may fail for traffic through FTD
CSCwc28806	ASA Traceback and Reload on process name Lina
CSCwc28854	Incorrect IF-MIB response when failover is configured on multiple contexts
CSCwc28928	ASA: SLA debugs not showing up on VTY sessions
CSCwc29591	Retrospective file disposition updates fail due to incorrect eventsecond values in fileevent tables
CSCwc30487	High unmanaged disk usage on Firepower 2110 device
CSCwc31163	FPR1010 upgrade failed - Error running script 200_pre/100_get_snort_from_dc.pl
CSCwc32246	NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used

Bug ID	Headline
CSCwc33036	Observed Logs at syslog server side as more than configured message limit per/sec.
CSCwc33076	JOBS_TABLE not getting purged due to foreign Key constraint violation in policy_diff_main
CSCwc33323	FMC 7.0 - Receiving alert "health monitor process: no events received yet" for multiple devices
CSCwc34818	The device is unregistered when Rest API calls script.
CSCwc35969	cannot add IP from event to global lists (block or do-not-block) if similar IP is already on list
CSCwc36905	ASA traceback and reload due to "Heap memory corrupted at slib_malloc.c
CSCwc37061	SNMP: FMC doesn't reply to OID 1.3.6.1.2.1.25.3.3.1.2
CSCwc37695	In addition to the c_rehash shell command injection identified in CVE-2022-1292
CSCwc38567	ASA/FTD may traceback and reload while executing SCH code
CSCwc40381	ASA : HTTPS traffic authentication issue with Cut-through Proxy enabled
CSCwc41661	FTD Multiple log files with zero byte size.
CSCwc44289	FTD - Traceback and reload when performing IPv4 <> IPv6 NAT translations
CSCwc45108	ASA/FTD: GTP inspection causing 9344 sized blocks leak
CSCwc45397	ASA HA - Restore in primary not remove new interface configuration done after backup
CSCwc45759	NTP logs will eventually overwrite all useful octeon kernel logs
CSCwc46569	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 34)
CSCwc46847	FXOS partition opt_cisco_platform_logs on FP1K/FPR2K may go Full due to ucssh_*.log
CSCwc47586	vFMC upgrade 7.0.4-36 > 7.3.0-1553 failed: Error running script 200_pre/007_check_sru_install.sh
CSCwc48375	Inbound IPSEC SA stuck inactive - many inbound SPIs for one outbound SPI in "show crypto ipsec sa"
CSCwc49369	When searching IPv6 rule in the access-control policy, no result will show
CSCwc49952	Selective deploy enables interaction with SRU interdependent-policies due to FMC API timeout
CSCwc50098	show ssl-policy-config does not show the policy when countries are being used in source/dest network

Bug ID	Headline
CSCwc50887	FTD - Traceback and reload on NAT IPv4<>IPv6 for UDP flow redirected over CCL link
CSCwc50891	MPLS tagging removed by FTD
CSCwc52351	ASA/FTD Cluster Split Brain due to NAT with "any" and Global IP/range matching broadcast IP
CSCwc52357	Estreamer page fails to load in ASDM
CSCwc53280	ASA parser accepts incomplete network statement under OSPF process and is present in show run
CSCwc54217	syslog related to failover is not outputted in FPR2140
CSCwc54984	IKEv2 rekey - Responding Invalid SPI for the new SPI received right after Create_Child_SA response
CSCwc56048	AD username with trailing space causes download of users/groups to fail
CSCwc56952	Able to see the SLA debug logs on both console & VTY sessions even if we enable only on VTY session.
CSCwc57088	Limit the number of deployment jobs in deploy history to 50 as default to avoid slowness
CSCwc57975	Snort3 crashes during the deployment - disabling TLS Server identity
CSCwc60037	ASA fails to rekey with IPSEC ERROR: Failed to allocate an outbound hardware context
CSCwc60907	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 35)
CSCwc62144	FMC does not use proxy with authentication when accessing AMP cloud services
CSCwc62384	Vulnerabilities on Cisco FTD Captive Portal on TCP port 885
CSCwc65907	snort3 hangs in Crash handler which can lead to extended outage time during a snort crash
CSCwc66671	FMC ACP PDF report generared in blank/0 bytes using UI
CSCwc67111	Unable to bind to port 51320: Address already in use
CSCwc75061	FMC allows shell access for user name with "." but external authentication will fail
CSCwc76195	Fail-To-Wire interfaces flaps intermittently due to watchdog timeout in KP platform
CSCwc78296	Database may fail to shut down and/or start up properly during upgrade
CSCwc83037	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 36)
CSCwc88425	FMC can download only the first 10000 cross-domain user groups

Bug ID	Headline
CSCwc88583	Deployment fails with error Invalid Snort3IntrusionPolicy mode. Supports only inline and inline-test
CSCwc96136	CCM layer (Seq 38) WR8, LTS18, LTS21
CSCwd07558	Access Control Policy Deployments failing after upgrading to 7.0.4 on SFR Managed by ASDM
CSCwd09093	Access rule policy page takes longer time to load
CSCwd09341	Multiple log files have zero bytes on the FMC
CSCwd24072	rsc_5_min.log store location should move to a different partition

Resolved Bugs in Version 7.0.4

Table last updated: 2022-08-10

Table 59: Resolved Bugs in Version 7.0.4

Bug ID	Headline
CSCvj08826	FMC ibdata1 file might grow large in size
CSCvw82067	ASA/FTD 9344 blocks depleted due to high volume of fragmented traffic
CSCvx59252	FXOS is not rotating log files for management interface
CSCvy16004	Delay in DIFF calculations can cause deployment issues and HA App sync timeout in FTDs
CSCvy50598	BGP table not removing connected route when interface goes down
CSCvy67765	FTD VTI reports TUNNEL_SRC_IS_UP false despite source interface is up/up and working
CSCvy73130	FP4100 platform: Active-Standby changed to dual Active after running "show conn" command
CSCvy99348	Shutdown command reboots instead of shutting the FP1k device down.
CSCvz36903	ASA traceback and reload while allocating a new block for cluster keepalive packet
CSCvz60142	ASA/FTD stops serving SSL connections
CSCvz68713	PLR license reservation for ASAv5 is requesting ASAv10
CSCvz69729	Unstable client processes may cause LINA zmqio traceback on FTD
CSCvz70539	Loggerd process is getting killed due to OOM under high logging rate
CSCwa00038	Disk corruption occurs when /mnt/disk0 partition is full and blade is rebooted

Bug ID	Headline
CSCwa03732	Deployment gets hung at snapshot generation phase during deploy or causes deploy slowness
CSCwa08640	MonetDB crashing due to file size error
CSCwa21061	FTD upgrade fails on 800_post/100_ftd_onbox_data_import.sh
CSCwa32628	SFDataCorrelator crash at AddFileToPendingHash() due to race condition
CSCwa42350	ASA installation/upgrade fails due to internal error "Available resources not updated by module"
CSCwa43311	Snort blocking and dropping packet, with bigger size(1G) file download
CSCwa43475	ASA SNMPd traceback in netsnmp_subtree_split
CSCwa45656	SLR license application failes on manged devices
CSCwa48169	ASA/FTD traceback and reload on netsnmp_handler_check_cache function
CSCwa59907	LINA observed traceback on thread name "snmp_client_callback_thread"
CSCwa61361	ASAv traceback when SD_WAN ACL enabled, then disabled (or vice-versa) in PBR
CSCwa62025	IPv6: Some of egress interfaces of global and user vrf routes are missing in asp table
CSCwa68552	All type-8 passwords are lost upon upgrade from ASA 9.12-9.15 to 9.16, failover gets disabled
CSCwa72530	FTD: Time gap/mismatch seen when new node joins a Cluster Control node under history
CSCwa73172	ASA reload and traceback in Thread Name: PIX Garbage Collector
CSCwa76621	Memory Usage Warnings - System memory leak caused by run_hm.pl
CSCwa85340	Unable to generate the PDF with access policy having large nested objects
CSCwa86210	When PM disables mysqld, sometimes it is taking longer than expected to fully shutdown.
CSCwa90615	WR8 and LTS18 commit id update in CCM layer (seq 24)
CSCwa95079	ASA/FTD Traceback and reload due to NAT configuration
CSCwa95694	Snort cores generated intermittently when SSL policy is enabled on the ASA-SFR module
CSCwa97910	Connection event report displays the same device twice
CSCwa97917	ISA3000 in boot loop after powercycle
CSCwa99931	ASA/FTD: Tuning of update_mem_reference process

Bug ID	Headline
CSCwb01633	FXOS misses logs to diagnose root cause of module show-tech file generation failure
CSCwb02060	snmp-group host with Invalid host range and subnet causing traceback and reload
CSCwb02316	"Non stop forwarding not supported on '1'" error while configuring MAC address
CSCwb05291	Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability
CSCwb06543	Increase logging level to diagnose LACP process unexpected restart events
CSCwb06847	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-9-11543'
CSCwb07319	Entitlement tags contain invalid character.
CSCwb07908	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
CSCwb07981	Traceback: Standby FTD reboots and generates crashinfo and lina core on thread name cli_xml_server
CSCwb08393	SSL policy deploy failing from FMC: Timeout waiting for snort detection engines to process traffic
CSCwb08644	ASA/FTD traceback and reload at IKEv2 from Scaled S2S+AC-DTLS+SNMP long duration test
CSCwb12465	FIPS self-tests must be run when CC mode is enabled - files are missing
CSCwb13294	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 25)
CSCwb16920	CPU profile cannot be reactivated even if previously active memory tracking is disabled
CSCwb17187	SNMP cores are generated every minute while running snmpwalk on HA
CSCwb17963	Unable to identify dynamic rate liming mechanism & not following msg limit per/sec at syslog server.
CSCwb19648	SNMP queries for crasLocalAddress are not returning the assigned IPs for SSL/DTLS tunnels.
CSCwb19664	Malware Block false positives triggered after upgrade to version 7.0.1
CSCwb22359	Portmanager/LACP improvement to avoid false restarts and increase of logging events
CSCwb24039	ASA traceback and reload on routing
CSCwb24101	Loggerd syslog has stray incorrect timestamps, e.g. well before FirstPacketSecond
CSCwb25809	Single Pass - Traceback due to stale ifc
CSCwb28047	FMC - "Receiving thread exited with an exception: stoi" causing pxGrid to flap
CSCwb31699	Primary takes active role after reload

Bug ID	Headline
CSCwb32841	NAT (any,any) statements in-states the failover interface and resulting on Split Brain events
CSCwb40001	Long delays when executing SNMP commands
CSCwb41361	WR8, LTS18 and LTS21 commit id update in CCM layer (seq 26)
CSCwb43018	Implement SNP API to check ifc and ip belongs to HA LU or CMD interface
CSCwb46949	LTS18 commit id update in CCM layer (seq 27)
CSCwb49416	ASA snmpd Traceback & cores on an active unit
CSCwb50405	ASA/FTD Traceback in crypto hash function
CSCwb51707	ASA Traceback and reload in process name: lina
CSCwb53172	FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated
CSCwb53191	Certificate validation fails post upgrade to 9.17.1
CSCwb53328	ASA/FTD Traceback and reload caused by Smart Call Home process sch_dispatch_to_url
CSCwb54791	ASA DHCP server fails to bind reserved address to Linux devices
CSCwb57615	Configuring pbr access-list with line number failed.
CSCwb59465	ASA/FTD may traceback (watchdog) and reload when generating a syslog from the VPN Failover subsystem
CSCwb59488	ASA/FTD Traceback in memory allocation failed
CSCwb67040	FP4112|4115 Traceback & reload on Thread Name: netfs_thread_init
CSCwb68642	ASA traceback in Thread Name: SXP CORE
CSCwb71460	ASA traceback in Thread Name: fover_parse and triggered by snmp related functions
CSCwb73248	FW traceback in timer infra / netflow timer
CSCwb74357	FXOS is not rotating log files for partition opt_cisco_platform_logs
CSCwb74571	PBR not working on ASA routed mode with zone-members
CSCwb79812	RIP is advertising all connected Anyconnect users and not matching route-map for redistribution
CSCwb80559	FTD offloads SGT tagged packets although it should not
CSCwb80862	ASA/FTD proxy arps any traffic when using the built-in 'any' object in translated destination
CSCwb82796	ASA/FTD firewall may traceback and reload when tearing down IKE tunnels

Bug ID	Headline
CSCwb83388	ASA HA Active/standby tracebacks seen approximately every two months.
CSCwb83691	ASA/FTD traceback and reload due to the initiated capture from FMC
CSCwb84638	Portmanager/LACP improvement to capture logging events on external event restarts
CSCwb85633	Snmpwalk output of memory does not match show memory/show memory detail
CSCwb86118	TPK ASA: Device might get stuck on ftp copy to disk
CSCwb87498	Lina traceback and reload during EIGRP route update processing.
CSCwb88651	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwb89004	FMC DBcheck.pl hungs at "Checking mysql.rna_flow_stats_template against the current schema"
CSCwb90074	ASA: Multiple Context Mixed Mode SFR Redirection Validation
CSCwb90532	ASA/FTD traceback and reload on NAT related function nat_policy_find_location
CSCwb92583	upgrade with a large amount of unmonitored disk space used can cause failed upgrade and hung device
CSCwb92709	We can't monitor the interface via "snmpwalk" once interface is removed from context.
CSCwb93932	ASA/FTD traceback and reload with timer services assertion
CSCwb94190	ASA graceful shut down when applying ACL's with forward reference feature and FIPS enabled.
CSCwb94312	Unable to apply SSH settings to ASA version 9.16 or later
CSCwb97251	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCwc02416	Not re-subscribing to ISE topics after certain ISE connectivity issues.
CSCwc02488	ASA/FTD may traceback and reload in Thread Name 'None'
CSCwc02700	Fragmented packets are dropped when unit leaves cluster
CSCwc03069	Interface internal data0/0 is up/up from cli but up/down from SNMP polling
CSCwc08676	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 32)
CSCwc09414	ASA/FTD may traceback and reload in Thread Name 'ci/console'
CSCwc10483	ASA/FTD - Traceback in Thread Name: appAgent_subscribe_nd_thread
CSCwc10792	ASA/FTD IPSEC debugs missing reason for change of peer address and timer delete
CSCwc11597	ASA tracebacks after SFR was upgraded to 6.7.0.3
CSCwc11663	ASA traceback and reload when modifying DNS inspection policy via CSM or CLI

Bug ID	Headline
CSCwc13017	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
CSCwc13382	DCERPC traffic is dropped after upgrade to snort3 due to Parent flow is closed
CSCwc13994	ASA - Restore not remove the new configuration for an interface setup after backup
CSCwc18218	Database files on disk grow larger than expected for some frequently updated tables
CSCwc18312	"show nat pool cluster" commands run within EEM scripts lead to traceback and reload
CSCwc23695	ASA/FTD can not parse UPN from SAN field of user's certificate
CSCwc24906	ASA/FTD traceback and reload on Thread id: 1637
CSCwc27797	ASA mgmt ip cannot be released
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwc28532	9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwc32246	NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used
CSCwc41590	Upgrade fail & App Instance fail to start with err "CSP_OP_ERROR. CSP signature verification error."
CSCwc53680	MonetDB crashing due to file size error (7.2.0-7.4.0)

Resolved Bugs in Version 7.0.3

Table last updated: 2022-06-30

Table 60: Resolved Bugs in Version 7.0.3

Bug ID	Headline
CSCwa65014	Cloud-managed 7.0.3 device support for 7.2 FMC eventing
CSCwa75204	SNORT3 Certsize 16k traffic failing on 2100 with all SSL rules
CSCwa98690	AWS FTDv AutoScale_layer.zip file is using vulnerable pycrypto 2.x toolkit
CSCwb93932	ASA/FTD traceback and reload with timer services assertion

Resolved Bugs in Version 7.0.2.1

Table last updated: 2022-06-27

Table 61: Resolved Bugs in Version 7.0.2.1

Bug ID	Headline
CSCwb93932	ASA/FTD traceback and reload with timer services assertion

Resolved Bugs in Version 7.0.2

Table last updated: 2022-05-05

Table 62: Resolved Bugs in Version 7.0.2

Bug ID	Headline
CSCvt68055	snmpd is respawning frequently on fxos for FP21xx device
CSCvy82668	SSH session not being released
CSCvy64145	WR6 and WR8 commit id update in CCM layer(sprint 113, seq 12)
CSCvt15348	ASA show processes cpu-usage output is misleading on multi-core platforms
CSCvy72841	Firepower 1K FTD sends LLDP packets with internal MAC address of eth2 interface
CSCvz80981	SNMPv3 doesn't work for SFR modules running version 7.0
CSCvy08351	Intrusion and Correlation Email Alerts stop being sent to mail server
CSCvz66474	Snmpd core files generated on FTD
CSCvx75683	The 'show cluster info trace' output is overwhelmed by 'tag does not exist' messages
CSCvz25434	ASA/FTD blackholes traffic due to 1550 block depletion when BVI is configured as DHCP client
CSCwa45799	High CPU on FXOS due to bcm_usd process
CSCwa18889	Clock drift observed between Lina and FXOS on multi-instance
CSCvy99217	IKEv2: SA Error code should be translated to human friendly reason
CSCvz00961	AnyConnect connection failure related to ASA truncated/corrupt config
CSCvz36905	If we add v6 route same as V route , duplicate entry is getting created.
CSCwa58060	LSP download fails if no ICMP reply is received from updates-talos.sco.cisco.com
CSCvz03524	PKI "OCSP revocation check" failing due to sha256 request instead of sha1
CSCwa74900	Traceback and reload after enabling debug webvpn cifs 255

Bug ID	Headline
CSCvz29233	ASA: ARP entries from custom context not removed when an interface flap occurs on system context
CSCvy35416	Deploy failure from global domain when parallel deploy triggered to different child domains
CSCvy99218	VDB Version shouldn't be update if fails
CSCvz81888	NTP will not change to *(synced) status after upgrade to asa-9.15.1/9.16.1.28 from asa-9.14.3
CSCvx66329	FTD Hotfix Cisco_FTD_SSP_FP2K_Hotfix_O installation fails on script 000_start/125_verify_bundle.sh
CSCvz75988	Inconsistent logging timestamp with RFC5424 enabled
CSCvz52199	Increase precision of ASA VPN load-balancing algorithm
CSCvz48407	Traceback and reload in Thread Name: DATAPATH-15-18621
CSCvz05687	Fragmented Certificate request failed for DND flow
CSCwa96759	Lina may traceback and reload on tcpmod_proxy_handle_mixed_mode
CSCvz90722	With object-group in crypto ACL sum of hitcnt mismatches with the individual elements
CSCvz59950	IKEv2 Crash from scaled long duration test on KP-FPR2130
CSCvz38332	FTD/ASA - Stuck in boot loop after upgrade from 9.14.2.15 to 9.14.3
CSCvz55140	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 117, seq 17)
CSCwa58686	ASA/FTD Change in OGS compilation behavior causing boot loop
CSCvz43455	ASAv observed traceback while upgrading hostscan
CSCvz20679	FTDv - Lina Traceback and reload
CSCvz60578	Cluster unit in MASTER_POST_CONFIG state should transition to Disabled state after an interva
CSCvz59464	IPReputation Feed Error Message-Method Not Allowed
CSCvy31424	QP FTD application fails to start due to outdated affinity.conf following FXOS/FTD upgrade
CSCvz79930	Snort3 .dmp and crashinfo files are not managed by diskmanager
CSCvy89144	Cisco ASA and FTD Web Services Denial of Service Vulnerability
CSCwa19713	Traffic dropped by ASA configured with BVI interfaces due to asp drop type "no-adjacency"
CSCvz70958	High Control Plane CPU on StandBy due to dhcpp_add_ipl_stby

Bug ID	Headline
CSCvz61689	Port-channel member interfaces are lost and status is down after software upgrade
CSCvz92016	Cisco ASA and FTD Software Web Services Interface Privilege Escalation Vulnerability
CSCvz34831	If ASA fails to download DACL it will never stop trying
CSCvz90375	Low available DMA memory on ASA 9.14 at boot reduces AnyConnect sessions supported
CSCvy40401	L2L VPN session bringup fails when using NULL encryption in ipsec configuration
CSCwa76822	Tune throttling flow control on syslog-ng destinations
CSCvz33468	ASA/FTD - NAT stops translating source addresses after changes to object-groups in manual NAT Rule
CSCwa11186	Mask sensitive information in aaa ldap debugs
CSCvz00383	FTD lina traceback and reload in thread Name Checkheaps
CSCvy17030	FMC Connection Events page "Error: Unable to process this query. Please contact support."
CSCvx97053	Unable to configure ipv6 address/prefix to same interface and network in different context
CSCvx24470	FTD/FDM: RA VPN sessions disconnected after every deployment if custom port for RA VPN is configured
CSCwa05385	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 19)
CSCvz96440	FMC should not create archival for NGIPS devices
CSCwa68660	FTP inspection stops working properly after upgrading the ASA to 9.12.4.x
CSCvy98027	Application interface down whereas physical interface Up on FXOS
CSCvx95652	ASAv Azure: Some or all interfaces might stop passing traffic after a certain period of run time
CSCvz73146	FTD - Traceback in Thread Name: DATAPATH
CSCwa87597	ASA/FTD Failover: Joining Standby reboots when receiving configuration replication from Active mate
CSCwb01919	FP2140 ASA 9.16.2 HA units traceback and reload at lua_getinfo (getfuncname)
CSCvy96895	ASA disconnects the VTY session using of Active IP address and Standby MAC address after failed over
CSCwa55878	FTD Service Module Failure: False alarm of "ND may have gone down"
CSCwa14725	ASA/FTD traceback and reload on IKE Daemon Thread

Bug ID	Headline
CSCvy35737	FTD traceback and reload during anyconnect package verification
CSCvz91218	Statelink hello messages dropped on Standby unit due to interface ring drops on high rate traffic
CSCwa20758	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 20)
CSCwa67882	Offloaded GRE tunnels may be silently un-offloaded and punted back to CPU
CSCwa67884	Conditional flow-offload debugging produces no output
CSCwa97784	ASA: Jumbo sized packets are not fragmented over the L2TP tunnel
CSCwa29956	"Interface configuration has changed on device" message may be shown after FTD upgrade
CSCwa60574	ASA traceback and reload on snp_ha_trans_alloc_msg_muxbuf_space function
CSCwa89243	SNMP no longer responds to polls after upgrade to 9.15.1.17
CSCvz30582	Cisco Firepower Management Center Cross-site Scripting Vulnerability
CSCwa04461	Cisco ASA Software and FTD Software Remote Access SSL VPN Denial of Service
CSCwa30114	"Error:NAT unable to reserve ports" when using a range of ports in an object service
CSCvy80030	ENH: Addition of "show coredump filesystem" to "show tech" output
CSCwa39680	Snort stops processing packets when SSL decryption debug enabled - Snort2
CSCvy96803	ASA/FTD traceback and reload in Process Name "lina" or "snmp_alarm_thread"
CSCvz34149	Update the new location of /opt/cisco/platfom/logs/var/log/messages
CSCvo77184	VMware ASAv should default to vmxnet3, not e1000
CSCvx92932	Missing events on FMC due to SFDataCorrelator process exiting
CSCwa79980	SNMP get command in FPR does not show interface index.
CSCvz38976	7.1/Firepower Threat Defense device occasionally unable to pass large packets/Fragmentation failures
CSCvz64470	ASA/FTD Traceback and reload due to memory corruption when generating ICMP unreachable message
CSCwb34035	ASA CLI gets hung randomly while configuring SNMP
CSCvz00032	Cisco Firepower Threat Defense Software TCP Proxy Denial of Service Vulnerability
CSCvu23149	Backup generation in FMC fails due to corrupt SID_GID_ORD index in database table rule_opts
CSCwa57115	New access-list are not taking effect after removing non-existance ACL with objects.

Bug ID	Headline
CSCvz37306	ASDM session is not served for new user after doing multiple context switches in existing user
CSCwa53489	Lina Traceback and Reload Due to invalid memory access while accessing Hash Table
CSCvy98458	FP21xx -traceback "Panic:DATAPATH-10-xxxx -remove_mem_from_head: Error - found a bad header"
CSCvy52924	FTD loses OSPF network statements config for all VRF instances upon reboot
CSCvz92932	ASA show tech execution causing spike on CPU and impacting to IKEv2 sessions
CSCvz44339	FTD - Deployment will fail if you try to delete an SNMP host with ngfw-interface and host-group
CSCwa40223	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCvy47108	Remote Access IKEv2 VPN session cannot be established because of stuck Uauth entry
CSCvy86780	Error Could not complete LSP installation. Please try again.
CSCvz57710	conf t is converted to disk0:/t under context-config mode
CSCvz14377	Losing admin and other users from Mysql DB and EO
CSCvz89126	ASDM session/quota count mismatch in ASA when multiple context switchover is done from ASDM
CSCvy78209	Getting Snort High CPU alerts but top.log is not showing high CPU
CSCwa19443	Flow Offload - Compare state values remains in error state for longer periods
CSCvy91668	PAT pool exhaustion with stickiness traffic could lead to new connection drop.
CSCwa70008	Expired certs cause Security Intelligence updates to fail
CSCvz81480	IV in the outbound pkt is not updated on Nitrox V platforms when GCM is used for IPsec
CSCvx70480	403 error when accessing Policies -> Access Control after exporting User Role from FMC(4600) to FMCv
CSCwa18795	Crash at "thread: Unicorn Proxy Thread cpu: 7 watchdog_cycles" from Scaled AC-SSL TVM Profle test
CSCvz67816	IPV6 DNS PTR query getting modified on FTD
CSCvy96698	Resolve spurious status actions checking speed values twice in FXOS portmgr
CSCvs85607	FXOS login breaks when log partition gets full
CSCwb18252	FTD/ASA: Traceback on BFD function causing unexpected reboot

Bug ID	Headline
CSCvz02076	Snort reload times out causing restart
CSCvz44645	FTD may traceback and reload in Thread Name 'lina'
CSCwa79676	FPR1010 in HA Printing Broadcast Storm Alerts for Multiple Interfaces
CSCvy24921	SNMPv3 - SNMP EngineID changes after every configuration change
CSCvz36933	Sensor SNMP process may restart when policy deploy
CSCvz86796	Crash in thread CMP when doing CMPV2 enrollment
CSCvz70316	LINA may generate traceback and reload
CSCwa60300	axios 0.21.1
CSCvy30392	Backup generation on FMC fails due to corrupt int_id index in table ids_event_msg_map
CSCvz55849	FTD Traceback and Reload on process LINA
CSCvz61160	ASA traceback on DATAPATH when handling ICMP error message
CSCvx43150	On the FMC, process of registration of member device post RMA is not successful
CSCwa91090	SSL handshake logging showing unknown session during AnyConnect TLSv1.2 Session establishment
CSCvz43848	TID source stuck at parsing state
CSCvz61767	Policy deployment with SNMPv2 or SNMPv1 configuration fails
CSCvz69571	ASA log shows wrong value of the transferred data after the anyconnect session terminated.
CSCwa51862	LSP downloads fail when using proxy
CSCwa31373	duplicate ACP rules are generated on FMC 6.6.5 after rule copy.
CSCwa65389	ASA traceback and reload in Unicorn Admin Handler when change interface configuration via ASDM
CSCwa32286	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 125, seq 21)
CSCwa08262	AnyConnect users with mapped group-policies take attributes from default GP under the tunnel-group
CSCvy96625	Roll back changes introduced by CSCvr33428 and CSCvy39659
CSCwa36678	Random FTD reloads with the traceback during deployment from FMC
CSCvz50712	TLS server discovery uses incorrect source IP address for probes in AnyConnect deployment

Bug ID	Headline
CSCwa41918	ssl inspection may have unexpected behavior when evicting certificates
CSCwa36672	ASA on FPR4100 traceback and reload when running captures using ASDM
CSCvz64548	SFTunnel on device not processing event messages
CSCvy93480	Cisco ASA and FTD Software IKEv2 Site-to-Site VPN Denial of Service Vulnerability
CSCvy43002	Observed crash while running SNMPWalk + S2S-IKEv2 and AnyConnect TVM Profiles
CSCwa46963	Security: CVE-2021-44228 -> Log4j 2 Vulnerability
CSCvy74984	ASAv on Azure loses connectivity to Metadata server once default outside route is used
CSCvv36788	MsgLayer[PID]: Error : Msglyr::ZMQWrapper::registerSender() : Failed to bind ZeroMQ Socket
CSCvy97080	Snort3 unexpected restart while proccessing SMB traffic
CSCwa67145	Realm download fails if one of the groups is deleted on the AD
CSCvz77744	OSPFv3: FTD Wrong "Forwarding address" added in ospfv3 database
CSCvz17923	Dispatcher doesn't account for asynclock pend q work under some conditions result lower cpu util
CSCvx67851	PLR on FDM for ISA3000
CSCwa56449	ASA traceback in HTTP cli EXEC code
CSCvz77662	Crash at data-path from Scaled AC-SSL TVM Profile test.
CSCwb09219	ASA/FTD: OCSP may fail to work after upgrade due to "signer certificate not found"
CSCvz84850	ASA/FTD traceback and reload caused by "timer services" function
CSCwa42594	ASA: IP Header check validation failure when GTP Header have SEQ and EXT field
CSCwa40312	Standby ASA unit showing wrong IPV6 messages
CSCwa88571	Unable to register FMC with the Smart Portal
CSCvk62945	ASA: Syslog 317007 not found error received
CSCvz38692	ASAv traceback in snmp_master_callback_thread and reload
CSCwa50145	FPR8000 sensor UI login creates shell user with basic privileges
CSCvz08387	ASP drop capture output may display incorrect drop reason
CSCvy35352	Error handling for Suppression settings needed in certain conditions

Bug ID	Headline
CSCvy69453	WM Standby device do not send out coldstart trap after reboot.
CSCwa02929	FTD Blocks Traffic with SSL Flow Error CORRUPT_MESSAGE
CSCvz89545	SSL VPN performance degraded and significant stability issues after upgrade
CSCvz24765	device rebooted with snmpd core
CSCvz07614	ASA: Orphaned SSH session not allowing us to delete a policy-map from CLI
CSCvy40482	9.14MR3: snmpwalk got failed with [Errno 146] Connection refused error.
CSCvz02425	Deployment failing due to NPE while reading policy names
CSCvz28103	FDM: Saving DHCP relay config throws flex-config/smart CLI error
CSCvz01604	ASA High CPU (100%) when testing DDoS under 100K CPS rate despite fix introduced by CSCvx82503
CSCvu96436	Traceback of master and one slave when a particular lock is contended for long
CSCvy79952	ASA/FTD traceback and reload after downgrade
CSCvx80830	VPN conn fails from same user if Radius server sends a dACL and vpn-simultaneous-logins is set to 1
CSCvy39791	Lina traceback and core file size is beyond 40G and compression fails.
CSCvy64911	Debugs for: SNMP MIB value for crasLocalAddress is not showing the IP address
CSCwa68805	FTD Traceback & reload during HA creation
CSCvz71064	Deleting The Context From ASA taking Almost 2 Minutes with ikev2 tunnel
CSCvz40352	ASA traffic dropped by Implicit ACL despite the fact of explicit rules present on Access-list
CSCvz86256	Primary ASA should send GARP as soon as split-brain is detected and peer becomes cold standby
CSCvy34333	When ASA upgrade fails, version status is desynched between platform and application
CSCvz72771	ASA/FTD may traceback and reload. "c_assert_cond_terminate" in stack trace
CSCvw37191	FXOS SNMPv3 Engine ID changes after reboot
CSCwa34287	ASA: Loss of NTP sync following a reload after upgrade
CSCvz83432	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 121, seq 18)
CSCwa31508	Continuous deployment failure on QW-4145 device
CSCvz81342	Diskmanager not pruning AMP File Capture files

Bug ID	Headline
CSCvy60831	ASA/FTD Memory block location not updating for fragmented packets in data-path
CSCvz67003	ASDM session count and quota management's count mismatch. 'Lost connection firewall' msg in ASDM
CSCvz67001	FMC Event backups to remote SSH storage targets fail
CSCvz47709	[IMS_7_1_0] DeployACPolicyPostUpgrade at Upgrade FMC 7.1.0 - 2022
CSCvz23157	SNMP agent restarts when show commands are issued
CSCwa96327	Incorrect ifHighSpeed value for a interfaces that are port channel members
CSCvw29647	FTD: NAS-IP-Address:0.0.0.0 in Radius Request packet as network interface for aaa-server not defined
CSCvz61658	CPU hogs in update_mem_reference
CSCvy78525	VRF route lookup for TCP ping is missing
CSCvz82562	ASA/FTD: site-to-site VPN - traffic incorrectly fragmented
CSCvy56395	ASA traceback and reload due to snmp encrypted community string when key config is present
CSCwa79494	Traffic keep failing on Hub when IPSec tunnel from Spoke flaps
CSCvz88149	Lina traceback and reload during block free causing FTD boot loop
CSCvy89658	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 114, seq 13)
CSCvz38361	BGP packets dropped for non directly connected neighbors
CSCvx14489	snmpwalk fails on ipv6 interface post a failover
CSCwa90408	Crash on SSH SCP from long duration test.
CSCvz58710	ASA traceback due to SCTP traffic.
CSCvy55439	FTDv throughput degredation due to frequent PDTS read/write
CSCvy08972	Event Database runs into utf8 error causing pause in processing of events
CSCwa35200	Some syslogs for AnyConnect SSL are generated in admin context instead of user context
CSCvi58484	Cluster: ping sourced from FTD/ASA to external IPs may if reply lands on different cluster unit
CSCvz30558	Cisco Firepower Management Center Cross-site Scripting Vulnerability
CSCwa69303	ASA running on SSP platform generate critical error "[FSM:FAILED]: sam:dme:MgmtIfSwMgmtOobIfConfig"

Bug ID	Headline
CSCwb42846	Snort instance CPU stuck at 100%
CSCvy73585	FMC should not allow to configure port-channel ID higher than 8 on FPR1010
CSCvz95108	FTD Deployment failure post upgrade due to major version change on device
CSCwa38277	ASA NAT66 with big range as a pool don't works with IPv6
CSCvy33501	FDM failover pair - new configured sVTI IPSEC SA is not synced to standby. FDM shows HA not in sync
CSCvy21334	Active tries to send CoA update to Standby in case of "No Switchover"
CSCvz20544	ASA/FTD may traceback and reload in loop processing Anyconnect profile
CSCvz61431	"Netsnmp_update_ma_config: ERROR Failed to build req"messages seen during cluster configuration sync
CSCvv43190	Crypto engine errors when GRE header protocol field doesn't match protocol field in inner ip header
CSCvy04430	Management Sessions fail to connect after several weeks
CSCvy95329	Incorrect Access rule matching because of ac rule entry missing
CSCvy04343	ASA in PLR mode,"license smart reservation" is failing.
CSCwa25033	Unexpected HTTP/2 data frame causing segfault
CSCvz53884	SNMP OID HOST-RESOURCES-MIB (1.3.6.1.2.1.25) does not exist on FMC
CSCwb01700	ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA
CSCvz55395	TCP connections are cleared after configured idle-timeout even though traffic is present
CSCvx36885	ASA reload and traceback in DATAPATH
CSCvz05468	Multiple SSH host entries in platform settings as first feature enable/deploy will break SSH on LINA
CSCvz95949	FP1120 9.14.3 : temporary split brain happened after active device reboot
CSCvz65181	Cisco Firepower Threat Defense Software Security Intelligence DNS Feed Bypass Vulnerabilit
CSCwa98684	Console has an excessive rate of warnings during policy deployment
CSCvy10789	FTD 2110 ascii characters are disallowed in LDAP password
CSCvz12494	In FPR2100,after power off/on,the fxos version is mismatched with asa version.
CSCvz62578	Cannot edit or move AC rules for SFR module in Administrator rules section in ASDM

Bug ID	Headline
CSCwa26353	snort3 - Policy does not become dirty after updating LSP -when only custom intrusion policies in use
CSCvz55302	FTD/ASA Traceback and reload due to SSL null checks under low memory conditions
CSCwa85043	Traceback: ASA/FTD may traceback and reload in Thread Name 'Logger'
CSCvz39646	ASA/AnyConnect - Stale RADIUS sessions
CSCwa13873	ASA Failover Split Brain caused by delay on state transition after "failover active" command run
CSCvz85437	FTD 25G, 40G and 100G interfaces down after upgrade of FXOS and FTD to 2.10.1.159 and 6.6.4
CSCvv48942	Snmpwalk showing traffic counter as 0 for failover interface
CSCvy74781	The standby device is sending the keep alive messages for ssl traffic after the failover
CSCwa36661	Traffic is not hitting on some egress interfaces of user vrf due to routes missing in asp table
CSCvz69699	Unable to access UI of FMC integrated with ISE using PxGrid
CSCwa33364	FTD misleading OVER_SUBSCRIBED flow flag for mid-stream flow-issue seen on MR branches
CSCwa11052	SNMP Stopped Responding After Upgrading to Version- 9.14(2)15
CSCwa48849	ssl unexpected behavior with resumed sessions
CSCwa56975	DHCP Offer not seen on control plane
CSCvy78573	cloudagent should not send zero-length urls to beaker for lookup
CSCvz58376	Snort down after deploying the policy
CSCvz36862	FMC policy deployment takes more than 15 min on phase 3
CSCvw65324	mserver core on buildout FMC caused by concurrent merge table queries
CSCvy58268	Block 80 and 256 exhaustion snapshots are not created
CSCvx79526	Cisco ASA and FTD Software Resource Exhaustion Denial of Service Vulnerability
CSCvz93407	IPS policy with space in name becomes unusable after upgrade
CSCwa36889	FTD management interface programming is broken in FXOS
CSCvu18510	MonetDB's eventdb crash causes loss of connection events on FMC
CSCvz53993	Random packet block by Snort in SSL flow

Bug ID	Headline
CSCvz53142	ASA does not use the interface specified in the name-server command to reach IPv6 DNS servers
CSCvz00934	Not able to configure VTI with tunnel source as (FMC Access) data-interface
CSCwa40719	Traceback: Secondary firewall reloading in Threadname: fover_parse
CSCvy35948	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 111, seq 11)
CSCwa17918	Unable to uncheck option Always advertise the default route for OSPF
CSCwa55418	multiple db folders current-policy-bundle after deployment with anyconnect package before upgrade
CSCvz35787	FTD misleading OVER_SUBSCRIBED flow flag for mid-stream flow
CSCvz15676	In Firepower 1010 device, after upgrading ASA app, device going for fail safe mode
CSCvz70595	Traceback observed on ASA while handling SAML handler
CSCvy90836	ASA Traceback and reload in Thread Name: SNMP ContextThread
CSCvz78816	ASA disconnects the ssh, https session using of Active IP address and Standby MAC address after FO
CSCvz30933	ASA tracebacks and reload when clear configure snmp-server command is issued
CSCvz96462	IP Address 'in use' though no VPN sessions
CSCvz94573	MIO heartbeat failure caused by heartbeat dropped by delay
CSCwa14485	Cisco Firepower Threat Defense Software Denial of Service Vulnerability
CSCwa33898	Cisco Adaptive Security Appliance Software Clientless SSL VPN Heap Overflow Vulnerability
CSCvy19170	SAML: Memory leaks observed for AnyConnect IKEv2
CSCwa99932	ASA/FTD stuck after crash and reboot
CSCvz89327	OSPFv2 flow missing cluster centralized "c" flag
CSCwa03347	IPv6 PIM packets are dropped in ASP with invalid-ip-length drop reason
CSCvz05541	ASA55XX: Expansion module interfaces not coming up after a software upgrade
CSCwa34110	FMC should support southern hemisphere DST configurations
CSCvy90162	Seen crash related to watchdog bark at Unicorn Proxy Thread from scaled AC-SSL-SAML Auth TVM profile
CSCvz71569	FTD Traceback & reload due to process ZeroMQ out of memory condition
CSCvz25454	ASA: Drop reason is missing from 129 lines of asp-drop capture

Bug ID	Headline
CSCvz68336	SSL decryption not working due to single connection on multiple in-line pairs
CSCvy37484	Entries in device_policy_ref is huge causing slow performance when opening DeviceManagement page
CSCvz41761	FMC Does not allow to create an EIGRP authentication secret key using the $ character
CSCvq29993	FPR2100 ONLY - PERMANENT block leak of size 80, 256, and 1550 memory blocks & blackholes traffic
CSCwa76564	ASDM session/quota count mismatch in ASA when multiple context switch before and after failover
CSCvz05189	FTD reload with Lina traceback during xlate replication in Cluster
CSCwa87315	ASA/FTD may traceback and reload in Thread Name 'IP Address Assign'
CSCvc57575	ISIS:Invalid ISIS debugs displayed while deleting context.
CSCvy32366	After upgrading ASA to 9.15(1)10, ASDM 7.15(1)150 One Time Password (OTP) field does not appear
CSCvw62288	ASA: 256 byte block depletion when syslog rate is high
CSCvy60574	Port dcosAG leak fix CSCvx14602 to KP/WM
CSCvz00699	Traceback in webvpn and reload experienced periodically after ASA upgrade
CSCvz66795	ASA traceback and reload in SSH process when executing the command "show access-list"
CSCvz09109	Cluster CCL interface capture shows full packets although headers-only is configured
CSCwa28822	FTD moving UI management from FDM to FMC causes traffic to fail
CSCvz51258	show tech-support output can be confusing when there crashinfo, need to clean up/make more intuitive
CSCwa26038	ICMP inspection causes packet drops that are not logged appropriately
CSCwb15795	Audit message not generated by: no logging enable from ASAv9.12
CSCvz09106	Cisco ASA and FTD Software SSL VPN Denial of Service Vulnerability
CSCvy41763	Cisco Firepower Threat Defense Software XML Injection Vulnerability
CSCwa41834	ASA/FTD traceback and reload due to pix_startup_thread
CSCvy89648	ma_ctx files with '.backup' extension seen after applying the workaround for CSCvx29429
CSCvz02398	Crypto archive generated with SE ring timeout on 7.0

Bug ID	Headline
CSCvz76746	While implementing management tunnel a user can use open connect to bypass anyconnect.
CSCvz76745	SFDataCorrelator memory growth with cloud-based malware events
CSCvz91618	KP - traceback observed when add and remove snmp host-group
CSCvz99222	Clear and show conn for inline-set is not working
CSCvy53461	RSA keys & Certs get removed post reload on WS-SVC-ASA-SM1-K7 with ASA code 9.12.x
CSCvy75724	ZMQ OOM due to less Msglyr pool memory in low end platforms
CSCvz05767	FP-1010 HA link goes down or New hosts unable to connect to the device
CSCwa28895	FTD SSL Proxy should allow configurable or dynamic maximum TCP window size
CSCvz06652	snmpd corefiles noticed on SNMP longevity setup
CSCvz50922	FPR2100: Unable to form L2L VPN tunnels when using ESP-Null encryption
CSCvz95743	Loss of NTP sync following an upgrade
CSCvz77037	FMC user interface access may fail with SSL errors in mojo-server
CSCvy96325	FTD/ASA: Adding new ACE entries to ACP causes removal and re-add of ACE elements in LINA
CSCwa69376	under stress, getting bus error in snmp_logging.c:1303
CSCwa53088	snort 2 ssl-debug files may not be written
CSCvx81447	The dnsproxy log messages are displayed continuously on the ASA
CSCwa39683	log file flooded by ssl_policy log_error messages when ssl debug is enabled
CSCvy58697	ssl shared cache process can leak memory
CSCvz24238	CiscoÂ Firepower Management Center Cross-site Scripting Vulnerability
CSCwa15185	ASA/FTD: remove unwanted process call from LUA
CSCvw56551	ASA displays cosmetic NAT warning message when making the interface config changes
CSCvz76848	FTD traceback and reload when using DTLS1.2 on RA tunnels
CSCvz76966	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DNS DoS
CSCvz15529	ASA traceback and reload thread name: Datapath
CSCvy57905	VTI tunnel interface stays down post reload on KP/WM platform in HA

Bug ID	Headline
CSCwa27822	Lina process remains in started status after a major FTD upgrade to 6.7 or 7.0
CSCvy33676	UN-NAT created on FTD once a prior dynamic xlate is created
CSCvz30333	FTD/Lina may traceback when "show capture" command is executed
CSCwa21016	Cisco Firepower Threat Defense Software DNS Enforcement Denial of Service Vulnerability
CSCvy82655	REST API - Bulk AC rules creation fails with 422 Unprocessable Entity
CSCwb00595	Mempool_DMA allocation issue / memory leakage
CSCwa85138	Multiple issues with transactional commit diagnostics
CSCwa51241	Switch detected unknown MAC address from FPR1140 Management Interface
CSCwa03275	BGP routes shows unresolved and dropping packet with asp-drop reason "No route to host"
CSCvz73709	ASA/FTD Standby unit fails to join HA
CSCvz21886	Twice nat's un-nat not happening if nat matches a pbr acl that matches a port number instead of IP
CSCvy63464	FTD 1100/ 2100 series reboots with clock set to 2033
CSCvz19634	FTD software upgrade may fail at 200_pre/505_revert_prep.sh
CSCwa94894	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-4-9608'
CSCvx89451	ISA3000 shutdown command reboots system and does not shut system down.
CSCwa61218	Polling OID "1.3.6.1.4.1.9.9.171.1.3.2.1.2" gives negative index value of the associated tunnel
CSCvy02247	Cisco Firepower System Software Rule Editor Non-impactful Buffer Overflow Vulnerability
CSCvy99348	Shutdown command reboots instead of shutting the FP1k device down.
CSCvz71825	MAC algorithms on Firepower 2K devices are not correct for CC and UCAPL mode
CSCwa18858	ASA drops non DNS traffic with reason "label length 164 bytes exceeds protocol limit of 63 bytes"
CSCvz54471	ASA:Failed ASA in HA pair not recovering by itself, after an "HA state progression failed"
CSCvs27336	Traceback on ASA by Smart Call Home process
CSCwa67209	FMC may disable autonegotiation for port-channels with 1Gbps SFP fiber members after FTD upgrade

Bug ID	Headline
CSCwb33334	ASA: crash after sending some traffic over RAVPN tunnel
CSCwa75077	Time-range objects incorrectly populated in prefilter rules
CSCwa40237	Cisco Firepower Management Center File Upload Security Bypass Vulnerability
CSCvz94153	NTP sync on IPV6 will fail if the IPV4 address is not configured
CSCwa55562	Different CG-NAT port-block allocated for same source IP causing per-host PAT port block exhaustion
CSCvz31880	ASA Crashing with 'Unicorn Proxy Thread cpu: 9 watchdog_cycles' after stopping scaled stress test.
CSCwb20940	FMC: Add validation checks for the combination of SSL/Snort3/NAP in Detection mode
CSCwa77073	SNMP is responding to snmpgetbulk with unexpected order of results
CSCwa11088	Access rule-ordering gets automatically changed while trying to edit it before page refresh/load
CSCvz43414	Internal ldap attribute mappings fail after HA failover
CSCvz46879	Fine tune mojo_server configuration on Sourcefire modules
CSCvy90821	Autocomplete for "debug snmp ?" not working on ASA

Resolved Bugs in Version 7.0.1.1

Table last updated: 2022-02-17

Table 63: Resolved Bugs in Version 7.0.1.1

Bug ID	Headline
CSCwa46963	Security: CVE-2021-44228 -> Log4j 2 Vulnerability
CSCwa70008	Expired certs cause Security Intel. and malware file preclassification signature updates to fail
CSCwa88571	Unable to register FMC with the Smart Portal

Resolved Bugs in Version 7.0.1

Table last updated: 2021-10-07

Table 64: Resolved Bugs in Version 7.0.1

Bug ID	Headline
CSCum03297	ENH: ASA should save the timestamp of the MAXHOG in 'show proc cpu-hog'
CSCvf89237	Evaluate unicorn expat for CVE-2017-9233
CSCvg66052	2 CPU Cores continuously spike on firepower appliances
CSCvr11958	AWS FTD: Deployment failure with ERROR: failed to set interface to promiscuous mode
CSCvs50538	Firewall engine should fall back on info from SSL handshake if SSL engine is not returning a verdict
CSCvt62869	SPLIT-BRAIN: Pre allocation of blocks for failover control messages
CSCvv21602	cfprApSmMonitorTable is missing in the FP2K MIB
CSCvv36788	MsgLayer[PID]: Error : Msglyr::ZMQWrapper::registerSender() : Failed to bind ZeroMQ Socket
CSCvv43190	Crypto engine errors when GRE header protocol field doesn't match protocol field in inner ip header
CSCvv48942	Snmpwalk showing traffic counter as 0 for failover interface
CSCvv59676	Snort2: Implement aggressive pruning for certificate cache for TLS to free up memory
CSCvv71097	traceback: ASA reloaded snp_fdb_destroy_fh_callback+104
CSCvv89715	Fastpath rules for 8000 series stack disappear randomly from the FMC
CSCvw46630	FTD: NLP path dropping return ICMP destination unreachable messages
CSCvw62526	ASA traceback and reload on engineering ASA build - 9.12.3.237
CSCvw71405	FPR1120 running ASA traceback and reload in crypto process.
CSCvx11917	FTD active unit might drop interface failover messages with host-move-pkt drop reason
CSCvx20872	ASA/FTD Traceback and reload due to netflow refresh timer
CSCvx21050	Snort3 UDP performance down up to 40% relative to snort2 and Correct CPU utilisation meaningful
CSCvx23833	IKEv2 rekey - Invalid SPI for ESP packet using new SPI received right after Create_Child_SA response
CSCvx26308	ASA traceback and reload due to strcpy_s: source string too long for dest

Bug ID	Headline
CSCvx26927	TLS site not loading when it has segmented and retransmitted CH
CSCvx38124	Core-local block alloc failure on cores where CP is pinned leading to drops
CSCvx48490	SSL Decrypted https flow EOF events showing 'Initiator/Responder' Packets as 0
CSCvx50980	ASA CP CPU wrong calculation leads to high percentage (100% CP CPU)
CSCvx51123	FMC UI ERROR : An error occurred saving domain
CSCvx63788	Edit policy in new window for AC Policy default action IPS policy shows error pop-up
CSCvx65178	SNMP bulkget not working for specific OIDs in firewall mib and device performance degradation
CSCvx66329	FTD Hotfix Cisco_FTD_SSP_FP2K_Hotfix_O installation fails on script 000_start/125_verify_bundle.sh
CSCvx76665	Error messages "Updating Interface Status failed" seen on 2100
CSCvx77768	Traceback and reload due to Umbrella
CSCvx78238	multi context Firepower services on ASA traffic goes to incorrect interfaces
CSCvx79793	Slow file transfer or file upload with SSL policy is applied with Decrypt resign action
CSCvx80830	VPN conn fails from same user if Radius server sends a dACL and vpn-simultaneous-logins is set to 1
CSCvx85922	ASA/FTD may traceback and reload when saving/writitng the configuration to memory
CSCvx87709	FPR 2100 running ASA in HA. Traceback and reload on watchdog during failover
CSCvx90486	In some cases snmpwalk for ifXTable may not return data interfaces
CSCvx91317	A remote code execution issue was discovered in MariaDB 10.2 before 10
CSCvx93254	DHCP relay server "Invalid helper address"
CSCvx94398	Secondary ASA could not get the startup configuration
CSCvx95652	ASAv Azure: Some or all interfaces might stop passing traffic after a certain period of run time
CSCvx95884	High CPU and massive "no buffer" drops during HA bulk sync and during normal conn sync
CSCvx96452	Some HTTP2 TLS traffic ends with TCP RST, not TCP FIN, after complete payload transmission
CSCvx97632	ASA traceback and reload when copying files with long destination filenames using cluster command
CSCvy01482	Realm Sync Results Page Hangs After Upgrade

Bug ID	Headline
CSCvy01752	Traceback on FPR 4115 in Thread - Lic HA Cluster
CSCvy03006	improve debugging capability for uauth
CSCvy03907	Creation/Edit of Access Control Policy fails with error 'Rule Name Already Exists'
CSCvy04343	ASA in PLR mode,"license smart reservation" is failing.
CSCvy05966	Snort 2.9.16.3-3033 traceback (FTD 6.6.3)
CSCvy07113	7.0.0-1459 :FTPs traffic(malware file) is not blocked with file policy config,specifi to QP platform
CSCvy07491	ASA traceback when re-configuring access-list
CSCvy09217	HA goes to active-active state due to cipher mismatch
CSCvy09436	DHCP reservation fails to apply reserved address for some devices
CSCvy10583	ASA Traceback and Reload in Thread Name: DATAPATH
CSCvy10789	FTD 2110 ascii characters are disallowed in LDAP password
CSCvy13229	FDM - GUI Inaccessible - tomcat is opening too many file descriptors
CSCvy14721	ssl traffic dropped by FTD while CH packet has a destination port no greater than source port
CSCvy16179	ASA cluster Traceback with Thread Name: Unicorn Admin Handler even when running fix for CSCuz67596
CSCvy17078	Traceback: ASA on FPR 2110 traceback and reload on process Lina
CSCvy17365	REST API Login Page Issue
CSCvy17470	ASA Traceback and reload on the A/S failover pair at IKEv2
CSCvy18138	PIM Register Sent counter does not increase when encapsulated packets with register flag sent to RP
CSCvy19136	Web portal persistent redirects when certificate authentication is used.
CSCvy19453	SFDataCorrelator performance problems involving redundant new host events with only MAC addresses
CSCvy21334	Active tries to send CoA update to Standby in case of "No Switchover"
CSCvy23349	FTD unnecessarily ACKing TCP flows on inline-pair deployment
CSCvy27261	Inconsistencies in Snort2 and Snort3 Events views
CSCvy29815	NTP AES-CMAC input not compatible with IOS-XE
CSCvy30016	"Max cert cache entries" pruning needs to lock the ssl cache

Bug ID	Headline
CSCvy30101	snort2 memory usage can grow beyond expected limits when using ssl decryption
CSCvy31096	Host rediscovery in case of snort configuration reload
CSCvy31229	No space left disk space is full on /ngfw
CSCvy31400	FPR1K: Fiber SFP Interfaces down due to speed autonegotiation disabled
CSCvy31521	Add syslog-ng monitor to the FMC
CSCvy32154	Flows are offloaded after disable the offload cli on policy-map
CSCvy32366	After upgrading ASA to 9.15(1)10, ASDM 7.15(1)150 One Time Password (OTP) field does not appear
CSCvy33105	Ambiguous command error is shown for 'show route bgp' or 'show route isis' if DNS lookup is enabled
CSCvy33676	UN-NAT created on FTD once a prior dynamic xlate is created
CSCvy34333	When ASA upgrade fails, version status is desynched between platform and application
CSCvy36694	FTDv 6.7 on Azure is unable to set 1000 speed on GigabitEthernet interfaces
CSCvy37835	ssl replace key only action can cause unbounded detection engine memory usage
CSCvy39191	An internal server error 500 in T-ufin when doing API calls to the FMC
CSCvy39621	ASA/FTD sends continuous Radius Access Requests Even After Max Retry Count is Reached
CSCvy39659	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-15-14815'
CSCvy39791	Lina traceback and core file size is beyond 40G and compression fails.
CSCvy40482	9.14MR3: snmpwalk got failed with [Errno 146] Connection refused error.
CSCvy41157	HA formation failing after restore
CSCvy43447	FTD traceback and reload on Lic TMR Thread on Multi Instance FTD
CSCvy47108	Remote Access IKEv2 VPN session cannot be established because of stuck Uauth entry
CSCvy48159	ASA Traceback & reload on process name lina due to memory header validation
CSCvy48730	ASA/FTD may traceback and reload in Thread Name 'Unicorn Proxy Thread'
CSCvy49732	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCvy50011	ASA traceback in IKE Daemon process and reload
CSCvy51659	Long OCSP timeout may cause AnyConnect authentication failure

Bug ID	Headline
CSCvy51814	Firepower flow-offload stops offloading all existing and new flows
CSCvy52074	ASA/FTD may traceback and reload in Thread Name 'webvpn_task'
CSCvy52924	FTD loses OSPF network statements config for all VRF instances upon reboot
CSCvy53301	HA Configuration fails on FDM with 'Internal error during deployment'
CSCvy53461	RSA keys & Certs get removed post reload on WS-SVC-ASA-SM1-K7 with ASA code 9.12.x
CSCvy53798	memory leak when decrypting flows using x25519 curve
CSCvy55356	CPU hogs less than 10 msec are produced contrary to documentation
CSCvy56395	ASA traceback and reload due to snmp encrypted community string when key config is present
CSCvy58268	Block 80 and 256 exhaustion snapshots are not created
CSCvy60100	SNMP v3 configuration lost after reboot for HA
CSCvy60574	Port dcosAG leak fix CSCvx14602 to KP/WM
CSCvy61008	Time out of sync between Lina and FXOS
CSCvy63949	ASA direct authentication timeouts even if direct authentication traffic is passing through the ASA
CSCvy64492	ASAv adding non-identity L2 entries for own addresses on MAC table and dropping HA hellos
CSCvy64911	Debugs for: SNMP MIB value for crasLocalAddress is not showing the IP address
CSCvy66711	Cisco ASA 9.16.1 and FTD 7.0.0 IPsec Denial of Service Vulnerability
CSCvy67756	Firepower Services HTTPS traffic stops working when matching Do not decrypt rule in SSL policy
CSCvy68859	DB Conn not released with LSP and category filter in Intrusion rules
CSCvy69189	FTD HA stuck in bulk state due to stuck vpnfol_sync/Bulk-sync keytab
CSCvy69787	ASAv on AWS TenGigabit interface is learning 1000mbps instead of 10000Mbps
CSCvy72118	High snort cpu usage while copying navl attribute - (Fragmented metadata)
CSCvy72321	Packet-tracer adds "after-auto" option to manual/twice NATs when matching it in the NAT Phases
CSCvy72846	ASA accounting reports incorrect Acct-Session-Time
CSCvy73554	ASA: "deny ip any any" entry in crypto ACL prevents IKEv2 remote AnyConnect access connections

Bug ID	Headline
CSCvy74781	The standby device is sending the keep alive messages for ssl traffic after the failover
CSCvy74984	ASAv on Azure loses connectivity to Metadata server once default outside route is used
CSCvy79023	Device UI down due to idhttpsd access log file exceeding size and log rotation failure
CSCvy79952	ASA/FTD traceback and reload after downgrade
CSCvy82794	ASA/FTD traceback and reload when negating snmp commands
CSCvy83116	WM standby fails to re-join HA with msg "CD App Sync error is SSP Config Generation Failure"
CSCvy84733	SFR Upgrade 6.7 to 7.0: Syslogs stopped working
CSCvy89440	s2sCryptoMap Configuration Loss
CSCvy89648	ma_ctx files with '.backup' extension seen after applying the workaround for CSCvx29429
CSCvy89658	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 114, seq 13)
CSCvy92990	FTD traceback and reload related to SSL after upgrade to 7.0
CSCvy95554	Unable to download LDAP due to database MERGE failure on group_fsp_reference table
CSCvy96625	Revert 'fix' introduced by CSCvr33428 and CSCvy39659
CSCvy96698	Resolve spurious status actions checking speed values twice in FXOS portmgr
CSCvy96803	FTD traceback and reload in Process Name lina related to SNMP functions
CSCvy99373	ADI Session Processing Delays when resolving adSamAccountName with AD
CSCvz00032	FTD tracebacks and reloads on Thread name Lina
CSCvz00254	FDM 6.7.0 to 7.0.0 Upgrade Failed due to invalid state for site to site VPN during upgrade import
CSCvz00383	FTD lina traceback and reload in thread Name Checkheaps
CSCvz00699	Traceback in webvpn and reload experienced periodically after ASA upgrade
CSCvz05189	FTD reload with Lina traceback during xlate replication in Cluster
CSCvz05197	Event pages do not work in IE 11
CSCvz05468	Multiple SSH host entries in platform settings as first feature enable/deploy will break SSH on LINA
CSCvz05767	FP-1010 HA link goes down or New hosts are not not able to connect to the device

Bug ID	Headline
CSCvz06652	snmpd corefiles noticed on SNMP longevity setup
CSCvz06848	FTD/FDM upgrade fails due to snmp-server community validation failure
CSCvz07614	ASA: Orphaned SSH session not allowing us to delete a policy-map from CLI
CSCvz14616	No connection events due to SFDataCor process stuck
CSCvz15529	ASA traceback and reload thread name: Datapath
CSCvz17534	FTD Restore Backup CLI does not restore the VPN configuration
CSCvz20544	ASA/FTD may traceback and reload in loop processing Anyconnect profile
CSCvz21886	Twice nat's un-nat not happening if nat matches a pbr acl that matches a port number instead of IP
CSCvz23157	SNMP agent restarts when show commands are issued
CSCvz25434	ASA/FTD blackholes traffic due to 1550 block depletion when BVI is configured as DHCP client
CSCvz25663	FTD/FDM upgrade error due to snmp-server host community string validation failure
CSCvz26950	[DOC] The Appliance Information Widget missing High Availability information in FMC Documentation
CSCvz29233	ASA: ARP entries from custom context not removed when an interface flap occurs on system context
CSCvz30333	FTD/Lina may traceback when "show capture" command is executed
CSCvz30933	ASA tracebacks and reload when clear configure snmp-server command is issued
CSCvz32386	FTD Deployment error when FMC pushes PFS21 and IKEv1 settings on same crypto map entry
CSCvz34831	If ASA fails to download DACL it will never stop trying
CSCvz35201	Upgrade failure / Stuck on 999_finish/989_update_ngfw_conf_aquila_ssp.sh
CSCvz38361	BGP packets dropped for non directly connected neighbors
CSCvz38811	Deleted files holding disk space under Java process
CSCvz46333	FTD policy deployment failure due to internal socket connection loss
CSCvz66506	Continuous ADI crash is seen on FPR2100 after upgrade to 7.0 registered to FMC HA

Resolved Bugs in Version 7.0.0.1

Table last updated: 2021-07-15

Table 65: Resolved Bugs in Version 7.0.0.1

Bug ID	Headline
CSCvy66711	Cisco ASA 9.16.1 and FTD 7.0.0 IPsec Denial of Service Vulnerability

Resolved Bugs in Version 7.0.0

Table last updated: 2021-05-25

Table 66: Resolved Bugs in Version 7.0.0

Bug ID	Headline
CSCvi96835	No validation err when changing host thats part of a group object used in a routing policy, to Range
CSCvk22190	No connection/intrusion events received on FMC following time synchronisation issues
CSCvm69294	Standby FMC sending Flood of SNMP traps
CSCvm99989	SNMP OID for SystemUpTime show incorrect value
CSCvo57004	Analyze Hit Counts displaying timestamps in UTC instead of the configured user time zone.
CSCvp54996	GNU Wget Buffer Overflow Vulnerability
CSCvp58886	Special characters in Location for SNMP FXOS (FPR2100) causes policy deployment failure
CSCvq55919	Cisco Firepower Management Center Software Stored Cross-Site Scripting Vulnerability
CSCvq89604	Cisco_Firepower_Mgmt_Center_Patch_Uninstaller-6.4.0.3-29.sh.REL.tar fails to run
CSCvr03127	Apache HTTP Server mod_proxy Cross-Site Scripting Vulnerability
CSCvr13762	NGFWHA Missing EO UUID on FMC
CSCvr46901	Analysis Connection Events doesn't show and report all the events in UI
CSCvr74896	Cannot update Security intelligence when AC Policy is imported to FMC with cloud feeds disabled
CSCvs02229	Network Time Protocol Authenticated Mode 6 Packet Processing NULL Poin
CSCvs05066	Snort file mempool corruption leads to performance degradation and process failure.
CSCvs06043	TunnelClient for CSM_CCMservice on ngfwManager not reading ACK sent from CSM_CCM service on FMC

Bug ID	Headline
CSCvs71034	Beaker registration fails with error 400 : Bad Request.
CSCvs71969	Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability
CSCvs74802	AnyConnect/S2S IKEv2 crypto policy occasionally not deployed to device
CSCvs79606	"dns server-group DefaultDNS" cli not getting negated
CSCvs84242	FMC Deployment Failure when removing Auto NAT and correlated network object
CSCvt29771	invalid Response message when we change the security zone from the object management page
CSCvt31292	FTD device might not send events to SSE
CSCvt43136	Multiple Cisco Products Snort TCP Fast Open File Policy Bypass Vulnerability
CSCvt49334	On the 4120 sensor, the task delete is not removing the "task_xx" files from the cron.d directory
CSCvt74194	Error getting unified2 record: Corrupt file
CSCvt74893	FMCv Ethernet driver indicates vmxnet3 TCP performance compromised
CSCvt91258	FDM: None of the NTP Servers can be reached - Using Data interfaces as Management Gateway
CSCvt93177	Disable Full Proxy to Light Weight Proxy by Default. (FP2LWP) on FTD Devices
CSCvt93999	FMC shouldn't allow a second upgrade on same device if upgrade is going on
CSCvu12608	ASA5506/5508/5516 devices not booting up properly / Boot loop
CSCvu18510	MonetDB's eventdb crash causes loss of connection events on FMC 6.6.0 and 6.6.1
CSCvu21953	FMC 6.4.0 is randomly sending "strong-encryption-disable" to FTD
CSCvu22293	FMC scheduled backup of multiple managed devices with remote storage fails
CSCvu29508	FMC manual removal and addition of FTD Cluster member causes dangling stale interfaces
CSCvu30756	User Identity does not correctly handle identical sessions in different netmaps
CSCvu34228	FTD LINA traceback & reload while processing snort return verdict
CSCvu35704	APIKEY mismatch among the FMC, Sensor and ThreatGrid results significant file submission drop
CSCvu44472	FMC System processes are starting
CSCvu54706	Cisco Firepower Management Center CWE-772 - Slow HTTP POST vulnerability
CSCvu75855	stunnel process enabled on managed device when it should not be

Bug ID	Headline
CSCvu77689	FTP to FileZilla miscategorized as SMTP
CSCvu88005	FMC REST API user permission for GET taskstatus
CSCvu88886	Threat data deployment to managed FTD may fail after upgrade.
CSCvv00155	Deleting interface or sub-interface should also delete failover MAC address configuration
CSCvv08244	Firepower module may block trusted HTTPS connections matching 'Do not decrypt' SSL decryption rule
CSCvv12491	cloudagent_urllookup_health file still had old format after upgrading to 6.4
CSCvv14109	new FMC restored from backup file doesn't send down user ip and user group mappings to devices
CSCvv14442	FMC backup restore fails if it contains files/directories with future timestamps
CSCvv17893	Bad uip snapshot and log file causes FTD to repeatedly requests catchup, and exhausts file handlers
CSCvv20780	Policy deploy fails with "Failed to hold the deployment transaction" error
CSCvv21782	6.6.1: Prefilter Policy value shown as Invalid ID for all the traffic in ASA SFR Platform
CSCvv27084	EventHandler syslog via loggerd does not support destination host names
CSCvv27867	FMC classic theme - No scrollbar in object details for group with multiple items
CSCvv29275	FMC OSPF area limits until 49 entries. Upon adding 50th entry, process gets disabled automatically
CSCvv34523	The firewall_target_cache table is not pruned as expected which leads to large database size
CSCvv34851	6.7.0-1992: duplicate connection events with empty SSL info in one of them
CSCvv36915	"Show NTP" command does not work on multi-instance FTD
CSCvv38869	FMC fails to upgrade FTD from 6.3 to 6.7 due to database error
CSCvv40961	http-proxy setting causing upgrade failure
CSCvv43771	Unable to select multiple devices for scheduled backups
CSCvv45106	CSD does not start on 2100 due to missing csd-service.json file
CSCvv46490	Policy Deployment Failure on FMC due to ERROR in SnortAttribConfig
CSCvv50298	FTD management interface to be vulnerable to TLS poodle attack- CVE-2014-3566
CSCvv53042	DBCheck.pl output includes fatal errors that cause upgrade attempt to fail

Bug ID	Headline
CSCvv55066	FPR1010: Internal-Data0/0 and data interfaces are flapping during SMB file transfer
CSCvv56644	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web DoS
CSCvv57476	CSS Styles loading issue in Chrome 85, IE and Edge browsers
CSCvv59036	Static routes deleted from the FMC without user deleting it.
CSCvv60849	Memory cgroup limits should be adjusted to avoid Snort D-state
CSCvv62931	FTD does not send Server Hello & Server Certificate to the client when src.port==dst.port
CSCvv68000	bravado error when getting ra vpn group policy created by FDM UI
CSCvv68078	sybase database corrupted on secondary FMC and was not able to sync
CSCvv69862	FMC backup failed error with "Terminating long running backup" after 45 min FTDHA in leaf
CSCvv70096	Snort 2: Memory Leak in SSL Decrypt & Resign Processing
CSCvv70683	No New Notification in Task tab.
CSCvv73054	Snort libs are deleted during deployment
CSCvv74658	FTD/ASA creates coredump file with "!" character in filename (zmq changes (fxos) for CSCvv40406)
CSCvv74795	syslog-ng has extra instances running on ASA5525-X
CSCvv74816	FDM should not allow removal of local address pool while NAT exemption is in place.
CSCvv74951	Disable memory cgroups when running the system upgrade scripts
CSCvv75148	Rabbitmq queue of VPN Events does not have any size limit to avoid accumulating *.idx files
CSCvv76581	Cisco Firepower product line Evaluation of Racoon attack CVE-2020-1968
CSCvv79459	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 94, seq 1)
CSCvv79897	Block "sensor restart" command for FTD units to prevent Lina crash and system reboot event
CSCvv83841	upgrade - Not enough root disk space available in 600_schema/100_update_database.sh
CSCvv84172	Dangling ref in Clustered_table and EO upon failed registration
CSCvv84385	Disk Manager incorrectly prunes unified files used by FMC e-streamer
CSCvv89715	Fastpath rules for 8000 series stack disappear randomly from the FMC

Bug ID	Headline
CSCvv90079	No router BGP pushed after making chnages on 9300 intra chassis cluster
CSCvv92897	System might hit previously missing memcap limits on upgrade to version 6.6.0
CSCvv94165	FTD 6.6 : High CPU spikes on snmpd process
CSCvv97527	asa config timeout command breaks snort's DAQ configuration
CSCvv97902	Deployment purge doesn't happen due to deployment_info missing at policy_deployment.db
CSCvw03256	FMC dashboard shows "No Data" for intrusion table when 'Message' Field is Selected
CSCvw04171	For Readonly User, Device Summary tab is returning forbidden error page
CSCvw07352	SFDataCorrelator log spam, metadata fails after Sybase connection status 0
CSCvw10877	/var/sf/user_identity should not bring the archive with it in a troubleshoot
CSCvw13395	FMC 6.6.0 "Reset Connection Upon Timeout" Checkbox missing in Light Theme of UI
CSCvw16565	Policy Deployment fails after enabling "SMB Auto-Detect Ports" in DCE/RPC Configuration.
CSCvw21145	Duplicate NAT rule error when saving the policy (caused by duplicate Auto NAT rules)
CSCvw21161	Duplicate NAT rule error when saving the policy (different rules are detected as duplicates)
CSCvw21628	Upgrade from pre-6.6.x to 6.6.x and above breaks Intrusion Event Packet-Drill down
CSCvw27966	Policy deployment fails with object names starts with 'any'
CSCvw28894	SFDataCorrelator slow startup and vuln remap due to duplicate entries in vuln tables
CSCvw28946	When deploying VxLan config the command mtu is sent out of order causing deployment failures
CSCvw29561	FMC SLR license 'shows continuous Smart agent communication with Smart Licensing Cloud' alert
CSCvw29563	repair_users.pl script no longer works
CSCvw29581	VDB upgrade doesn't work when mysql user table is damaged.
CSCvw30252	ASA/FTD may traceback and reload due to memory corruption in SNMP
CSCvw33939	FMC Deployment failure due to VPN split-tunnel standard ACL with Network Group containing IPv6object
CSCvw34692	Not possible to change after the first time the TTL Hops for BGP neighbor

Bug ID	Headline
CSCvw38708	AC policy save, validateActivity not using cache for building blocks
CSCvw38870	FMC upgrade failure to 6.6.0, 6.6.1, 6.6.3, or 6.7.0 at 800_post/1027_ldap_external_auth_fix.pl
CSCvw41901	Deleting System Defined objects via FMC's REST API returns HTTP 500 error code.
CSCvw42497	Error during policy validation while navigating through AC policy
CSCvw45125	Block deployment while secondary nodes are in config or bulk sync
CSCvw47943	Optimization of the query for scan results in Firepower Recommendations
CSCvw51307	ASA/FTD traceback and reload in process name "Lina"
CSCvw60177	Standby/Secondary cluster unit might crash in Thread Name: fover_parse and "cluster config sync"
CSCvw79294	sftunnel logging huge number of logs to messages file
CSCvw85377	URL is not updated in the access policy URL filtering rule
CSCvx19934	Deployment gets failed for snmp settings while deleting snmpv1 and adding snmpv3 at a time in 6.6.3
CSCvx20303	ASA/FTD may traceback in after changing snmp host-group object
CSCvx26221	Traceback into snmp at handle_agentx_packet / snmp takes long time to come up on FP1k and 5508
CSCvy08798	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 110, seq 10)