



## **Cisco Firepower Release Notes, Version 7.0.x**

**First Published:** 2021-05-26

### **Americas Headquarters**

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





## CONTENTS

---

<b>CHAPTER 1</b>	<b>Welcome</b>	<b>1</b>
	Release Highlights	1
	Release Dates	2
	Sharing Data with Cisco	3
	For Assistance	4

---

<b>CHAPTER 2</b>	<b>System Requirements</b>	<b>7</b>
	FMC Platforms	7
	Device Platforms	8
	Device Management	11

---

<b>CHAPTER 3</b>	<b>Features</b>	<b>15</b>
	FMC Features	16
	FMC Features in Version 7.0.6	16
	FMC Features in Version 7.0.5	17
	FMC Features in Version 7.0.4	17
	FMC Features in Version 7.0.3	18
	FMC Features in Version 7.0.2	20
	FMC Features in Version 7.0.1	21
	FMC Features in Version 7.0.0	22
	FDM Features in Version 7.0.x	35

---

<b>CHAPTER 4</b>	<b>Upgrade Guidelines</b>	<b>41</b>
	Planning Your Upgrade	41
	Minimum Version to Upgrade	42
	Upgrade Guidelines for Version 7.0	43

- Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0 44
- Reconnect with Cisco Threat Grid for High Availability FMCs 45
- Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs 45
- FMCv Requires 28 GB RAM for Upgrade 45
- Firepower 1000 Series Devices Require Post-Upgrade Power Cycle 46
- Historical Data Removed During FTD Upgrade with FDM 47
- New URL Categories and Reputations 47
  - Pre-Upgrade Actions for URL Categories and Reputations 48
  - Post-Upgrade Actions for URL Categories and Reputations 49
  - Guidelines for Rules with Merged URL Categories 50
- Upgrade Guidelines for Cloud-delivered Firewall Management Center 53
- Upgrade Guidelines for the Firepower 4100/9300 Chassis 53
- Unresponsive Upgrades 53
- Revert or Uninstall the Upgrade 54
  - Uninstall ASA FirePOWER Patches with ASDM 54
- Traffic Flow and Inspection 56
  - Traffic Flow and Inspection for Chassis Upgrades 57
  - Traffic Flow and Inspection for FTD Upgrades with FMC 57
  - Traffic Flow and Inspection for FTD Upgrades with FDM 59
  - Traffic Flow and Inspection for ASA FirePOWER Upgrades 60
  - Traffic Flow and Inspection for NGIPSv Upgrades with FMC 60
- Time and Disk Space 61

---

**CHAPTER 5**

- Install the Software 63**
  - Installation Guidelines 63
  - Installation Guides 65

---

**CHAPTER 6**

- Bugs 67**
  - Open Bugs 67
    - Open Bugs in Version 7.0.0 67
  - Resolved Bugs 69
    - Resolved Bugs in Version 7.0.6.2 69
    - Resolved Bugs in Version 7.0.6.1 78
    - Resolved Bugs in Version 7.0.6 83

Resolved Bugs in Version 7.0.5.1	115
Resolved Bugs in Version 7.0.5	115
Resolved Bugs in Version 7.0.4	128
Resolved Bugs in Version 7.0.3	133
Resolved Bugs in Version 7.0.2.1	133
Resolved Bugs in Version 7.0.2	134
Resolved Bugs in Version 7.0.1.1	149
Resolved Bugs in Version 7.0.1	149
Resolved Bugs in Version 7.0.0.1	156
Resolved Bugs in Version 7.0.0	156





# CHAPTER 1

## Welcome

---

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

For Cisco Defense Orchestrator (CDO) deployments, see the [Cisco Cloud-Delivered Firewall Management Center Release Notes](#) or [What's New for Cisco Defense Orchestrator](#).

- [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
7.0.6.2	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



Version	Build	Date	Platforms
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 FDM.

### Web Analytics

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

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

# For Assistance

## Upgrade Guides

In management center deployments, the management center must run the same or newer version as its managed devices. Upgrade the management center first, then devices. Note that you always want to use the upgrade guide for the version of management center or device manager that you are *currently* running—not your target version.

**Table 2: Upgrade Guides**

Platform	Upgrade Guide	Link
Management center	Management center version you are <i>currently</i> running.	<a href="https://www.cisco.com/go/fmc-upgrade">https://www.cisco.com/go/fmc-upgrade</a>
Threat defense with management center	Management center version you are <i>currently</i> running.	<a href="https://www.cisco.com/go/ftd-fmc-upgrade">https://www.cisco.com/go/ftd-fmc-upgrade</a>
Threat defense with device manager	Threat defense version you are <i>currently</i> running.	<a href="https://www.cisco.com/go/ftd-fdm-upgrade">https://www.cisco.com/go/ftd-fdm-upgrade</a>
Threat defense with cloud-delivered Firewall Management Center	Cloud-delivered Firewall Management Center.	<a href="https://www.cisco.com/go/ftd-cdfmc-upgrade">https://www.cisco.com/go/ftd-cdfmc-upgrade</a>

## 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 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
Management center hardware	Getting started guide for your management center hardware model.	<a href="https://www.cisco.com/go/fmc-install">https://www.cisco.com/go/fmc-install</a>
Management center virtual	Getting started guide for the management center virtual.	<a href="https://www.cisco.com/go/fmcv-quick">https://www.cisco.com/go/fmcv-quick</a>
Threat defense hardware	Getting started or reimage guide for your device model.	<a href="https://www.cisco.com/go/ftd-quick">https://www.cisco.com/go/ftd-quick</a>
Threat defense virtual	Getting started guide for your threat defense virtual version.	<a href="https://www.cisco.com/go/ftdv-quick">https://www.cisco.com/go/ftdv-quick</a>

Platform	Install Guide	Link
FXOS for the Firepower 4100/9300	Configuration guide for your FXOS version, in the <i>Image Management</i> chapter.	<a href="https://www.cisco.com/go/firepower9300-config">https://www.cisco.com/go/firepower9300-config</a>
FXOS for the Firepower 1000/2100 and Secure Firewall 3100	Troubleshooting guide, in the <i>Reimage Procedures</i> chapter.	<a href="#">Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense</a>

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

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

### Contact Cisco

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

- Email Cisco TAC: [tac@cisco.com](mailto: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.

- [FMC Platforms, on page 7](#)
- [Device Platforms, on page 8](#)
- [Device Management, on page 11](#)

## FMC Platforms

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

### FMC Hardware

Version 7.0 supports the following FMC 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 [Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes](#).

### FMCv

Version 7.0 supports FMCv deployments in both public and private clouds.

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

**Table 4: Version 7.0 FMCv 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	—	—
<b>Private Cloud</b>			
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

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

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

## Device Platforms

Firepower devices monitor network traffic and decide whether to allow or block specific traffic based on a defined set of security rules. For details on device management methods, see [Device Management, on page 11](#). For general compatibility information, see the [Cisco Secure Firewall Threat Defense Compatibility Guide](#) or the [Cisco Firepower Classic Device Compatibility Guide](#).

### FTD Hardware

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

Table 5: Version 7.0 FTD Hardware

Platform	FMC Compatibility		FDM Compatibility		Notes
	Customer Deployed	Cloud Delivered	FDM Only	FDM + 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 2.10.1.159 or later build. We recommend the latest firmware. See the <a href="#">Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide</a> .
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 <a href="#">Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide</a> .
ISA 3000	YES	YES Requires Version 7.0.3+	YES	YES	May require a ROMMON update. See the <a href="#">Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide</a> .

### FTDv

Version 7.0 FTDv 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 FTDv Platforms

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO
<b>Public Cloud</b>				
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+	—	—
<b>Private Cloud</b>				
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 <a href="#">Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide</a> .
ISA 3000	YES	Requires ASDM 7.16(1).	Requires ASA 9.5(2) to 9.16(x). May require a ROMMON update. See the <a href="#">Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide</a> .
NGIPSv	YES	—	Requires VMware vSphere/VMware ESXi 6.5, 6.7, or 7.0. For supported instances, throughputs, and other hosting requirements, see the <a href="#">Cisco Firepower NGIPSv Quick Start Guide for VMware</a> .

## Device Management

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

### Customer-Deployed FMC

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

- You *can* manage older devices with a newer FMC, usually a few major versions back. However, we recommend you always update your entire deployment. New features and resolved issues often require the latest release on both the FMC and its managed devices.
- You *cannot* upgrade a device past the FMC. Even for maintenance (third-digit) releases, you must upgrade the FMC first.

Note that in most cases you can upgrade an older device directly to the FMC's major 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. For release-specific requirements, see [Minimum Version to Upgrade](#), on page 42.

**Table 8: Customer-Deployed FMC-Device Compatibility**

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

### Cloud-delivered Firewall Management Center

The cloud-delivered Firewall Management Center can manage FTD devices running:

- Version 7.2+
- Version 7.0.3 and later maintenance releases

The cloud-delivered Firewall Management Center cannot manage FTD 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 Version 7.2+.

You can add a cloud-managed device to a Version 7.2+ customer-deployed FMC for event logging and analytics purposes only. Or, you can send security events to the Cisco cloud with Security Analytics and Logging (SaaS).

### **FDM**

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

Optionally, add Cisco Defense Orchestrator (CDO) to remotely manage multiple FTD devices, as an alternative to the FMC. Although some configurations still require FDM, CDO allows you to establish and maintain consistent security policies across your FTD 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

---

This document describes the new and deprecated features for Version 7.0.

For 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; for example, if you must change a configuration.

### Snort

Snort 3 is the default inspection engine for FTD. Snort 3 features for FMC deployments also apply to FDM, even if they are not listed as new FDM features. However, keep in mind that the FMC may offer more configurable options than FDM.



---

**Important** If you are still using the Snort 2 inspection engine, switch to Snort 3 now for improved detection and performance. Snort 2 will be deprecated in a future release and will eventually prevent threat defense upgrade.

---

### 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. 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 below include information on deprecated FlexConfigs when appropriate. For a full list of deprecated FlexConfigs, see your configuration guide.



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

- [FMC Features, on page 16](#)
- [FDM Features in Version 7.0.x, on page 35](#)

## FMC Features

### FMC Features in Version 7.0.6

Table 9:

Feature	Details
Updated web analytics provider.	<p><b>Upgrade impact. Your browser connects to new resources.</b></p> <p>While using the FMC, your browser now contacts Amplitude (amplitude.com) instead of Google (google.com) for web analytics.</p> <p>Version restrictions: Amplitude analytics are not supported in management center Version 7.0.0–7.0.5, 7.1.0–7.2.5, 7.3.x, or 7.4.0. Permanent support returns in Version 7.4.1 If you upgrade from a supported version to an unsupported version, your browser resumes contacting Google.</p>
Smaller VDB for lower memory Snort 2 devices.	<p><b>Upgrade impact. Application identification on lower memory devices is affected.</b></p> <p>For VDB 363+, the system now installs a smaller VDB (also called <i>VDB lite</i>) 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.</p> <p>Lower memory devices: ASA 5506-X series, ASA-5508-X, 5512-X, 5515-X, 5516-X, 5525-X, 5545-X</p> <p>Version restrictions: The ability to install a smaller VDB depends on the version of the management center, not managed devices. If you upgrade the 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 <a href="#">CSCwd88641</a>.</p> <p>See: <a href="#">Update the Vulnerability Database</a></p>

#### Deprecated Features

Feature	Details
Deprecated: high unmanaged disk usage alerts.	<p>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).</p> <p><b>Note</b> 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 FMC is running any of these versions, you may also continue to see alerts.</p> <p>For information on the remaining Disk Usage alerts, see <a href="#">Disk Usage and Drain of Events Health Monitor Alerts</a>.</p>

## FMC Features in Version 7.0.5

Table 10:

Feature	Details
ISA 3000 System LED support for shutting down.	<p>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.</p> <p>Version restrictions: Version 7.1 temporarily deprecates support for this feature. Support returns in Version 7.3.</p>
Automatically update CA bundles.	<p><b>Upgrade impact. The system connects to Cisco for something new.</b></p> <p>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.</p> <p>New/modified CLI commands: <b>configure cert-update auto-update</b>, <b>configure cert-update run-now</b>, <b>configure cert-update test</b>, <b>show cert-update</b></p> <p>Version restrictions: This feature is included in Versions 7.0.5+, 7.1.0.3+, and 7.2.4+. It is not supported in earlier 7.0, 7.1, or 7.2 releases. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco.</p> <p>See: <a href="#">Firepower Management Center Command Line Reference</a> and <a href="#">Cisco Secure Firewall Threat Defense Command Reference</a></p>

## FMC Features in Version 7.0.4

This release introduces stability, hardening, and performance enhancements.

## FMC Features in Version 7.0.3

Table 11: FMC Features in Version 7.0.3

Feature	Minimum Management Center	Minimum Threat Defense	Details
FTD support for cloud-delivered Firewall Management Center.	7.2.0 for analytics-only support	7.0.3	



Feature	Minimum Management Center	Minimum Threat Defense	Details
			<p>Version 7.0.3 FTD devices support management by the cloud-delivered Firewall Management Center, which we introduced in spring of 2022. The cloud-delivered Firewall Management Center uses the Cisco Defense Orchestrator (CDO) platform and unites management across multiple Cisco security solutions. We take care of feature updates.</p> <p>You should use Version 7.0.3 FTD with the cloud-delivered Firewall Management Center if:</p> <ul style="list-style-type: none"> <li>• You are currently using a customer-deployed ("on prem") hardware or virtual FMC.</li> <li>• You want to migrate to the cloud-delivered Firewall Management Center right now.</li> <li>• You do not want to upgrade devices to Version 7.2+, which also supports management by the cloud-delivered Firewall Management Center.</li> </ul> <p>If this is your situation, you should:</p> <ol style="list-style-type: none"> <li>1. Upgrade the current FMC to Version 7.2+.                     <p>Although you can technically use a Version 7.0.3 or 7.1 FMC to upgrade FTD to Version 7.0.3, you will not be able to easily migrate devices to the cloud-delivered management center, nor will you be able to leave the devices registered to the on-prem management center for event logging and analytics purposes only ("analytics only").</p> </li> <li>2. Use the upgraded FMC to upgrade devices to Version 7.0.3.</li> <li>3. Enable cloud management on the devices.                     <p>For Version 7.0.x devices only, you must enable cloud management from the device CLI: <b>configure manager-cdo enable</b>. The <b>show manager-cdo</b> command displays whether cloud management is enabled.</p> </li> <li>4. Use CDO's Migrate FTD to Cloud wizard to migrate the devices to the cloud-delivered Firewall Management Center.                     <p>Optionally, leave the devices registered to the on-prem management center as analytics-only devices. Or, you can send security events to the Cisco cloud with Security Analytics and Logging (SaaS).</p> </li> </ol> <p>The cloud-delivered Firewall Management Center cannot manage FTD 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 Version 7.2+.</p> <p>New/modified CLI commands: <b>configure manager add</b>, <b>configure manager delete</b>, <b>configure manager edit</b>, <b>show managers</b></p> <p>For more information, see <a href="#">Managing Firewall Threat Defense with</a></p>

Feature	Minimum Management Center	Minimum Threat Defense	Details
			<a href="#">Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator.</a>

## FMC Features in Version 7.0.2

Table 12:

Feature	Details
ISA 3000 support for shutting down.	You can now shut down the ISA 3000; previously, you could only reboot the device. Version restrictions: Version 7.1 temporarily deprecates support for this feature. Support returns in Version 7.2.
Dynamic object names now support the dash character.	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. Minimum threat defense: 7.0.2
Improved SecureX integration, SecureX orchestration.	<p><b>Upgrade impact. Cannot upgrade Version 7.0.x → 7.1 with feature enabled.</b></p> <p>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 <b>Integration &gt; SecureX</b> page, click <b>Enable SecureX</b>, 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.</p> <p>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.</p> <p>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 <b>System (⚙️) &gt; Integration &gt; Cloud Services</b>. Enabling SecureX does not affect communications with the Secure Network Analytics cloud; you can send events to both.</p> <p>The FMC 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.</p> <p>As part of this feature, you can no longer use the REST API to configure SecureX integration. You must use the FMC web interface.</p> <p>Version restrictions: This feature is included in Versions 7.0.2+ and 7.2+. It is not supported in Version 7.1. 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+.</p> <p>See: <a href="#">Cisco Secure Firewall Management Center (7.0.2 and 7.2) and SecureX Integration Guide</a></p>

Feature	Details																											
Web interface changes: SecureX, threat intelligence, and other integrations.	<p>We changed these FMC menu options.</p> <p><b>Note</b> These changes are temporarily deprecated in Version 7.1, but come back in Version 7.2.</p> <table> <tr> <td><b>AMP &gt; AMP Management</b></td> <td>is now</td> <td><b>Integration &gt; AMP &gt; AMP Management</b></td> </tr> <tr> <td><b>AMP &gt; Dynamic Analysis Connections</b></td> <td>is now</td> <td><b>Integration &gt; AMP &gt; Dynamic Analysis Connections</b></td> </tr> <tr> <td><b>Intelligence &gt; Sources</b></td> <td>is now</td> <td><b>Integration &gt; Intelligence &gt; Sources</b></td> </tr> <tr> <td><b>Intelligence &gt; Elements</b></td> <td>is now</td> <td><b>Integration &gt; Intelligence &gt; Elements</b></td> </tr> <tr> <td><b>Intelligence &gt; Settings</b></td> <td>is now</td> <td><b>Integration &gt; Intelligence &gt; Settings</b></td> </tr> <tr> <td><b>Intelligence &gt; Incidents</b></td> <td>is now</td> <td><b>Integration &gt; Intelligence &gt; Incidents</b></td> </tr> <tr> <td><b>System (⚙️) &gt; Integration</b></td> <td>is now</td> <td><b>Integration &gt; Other Integrations</b></td> </tr> <tr> <td><b>System (⚙️) &gt; Logging &gt; Security Analytics &amp; Logging</b></td> <td>is now</td> <td><b>Integration &gt; Security Analytics &amp; Logging</b></td> </tr> <tr> <td><b>System (⚙️) &gt; SecureX</b></td> <td>is now</td> <td><b>Integration &gt; SecureX</b></td> </tr> </table>	<b>AMP &gt; AMP Management</b>	is now	<b>Integration &gt; AMP &gt; AMP Management</b>	<b>AMP &gt; Dynamic Analysis Connections</b>	is now	<b>Integration &gt; AMP &gt; Dynamic Analysis Connections</b>	<b>Intelligence &gt; Sources</b>	is now	<b>Integration &gt; Intelligence &gt; Sources</b>	<b>Intelligence &gt; Elements</b>	is now	<b>Integration &gt; Intelligence &gt; Elements</b>	<b>Intelligence &gt; Settings</b>	is now	<b>Integration &gt; Intelligence &gt; Settings</b>	<b>Intelligence &gt; Incidents</b>	is now	<b>Integration &gt; Intelligence &gt; Incidents</b>	<b>System (⚙️) &gt; Integration</b>	is now	<b>Integration &gt; Other Integrations</b>	<b>System (⚙️) &gt; Logging &gt; Security Analytics &amp; Logging</b>	is now	<b>Integration &gt; Security Analytics &amp; Logging</b>	<b>System (⚙️) &gt; SecureX</b>	is now	<b>Integration &gt; SecureX</b>
<b>AMP &gt; AMP Management</b>	is now	<b>Integration &gt; AMP &gt; AMP Management</b>																										
<b>AMP &gt; Dynamic Analysis Connections</b>	is now	<b>Integration &gt; AMP &gt; Dynamic Analysis Connections</b>																										
<b>Intelligence &gt; Sources</b>	is now	<b>Integration &gt; Intelligence &gt; Sources</b>																										
<b>Intelligence &gt; Elements</b>	is now	<b>Integration &gt; Intelligence &gt; Elements</b>																										
<b>Intelligence &gt; Settings</b>	is now	<b>Integration &gt; Intelligence &gt; Settings</b>																										
<b>Intelligence &gt; Incidents</b>	is now	<b>Integration &gt; Intelligence &gt; Incidents</b>																										
<b>System (⚙️) &gt; Integration</b>	is now	<b>Integration &gt; Other Integrations</b>																										
<b>System (⚙️) &gt; Logging &gt; Security Analytics &amp; Logging</b>	is now	<b>Integration &gt; Security Analytics &amp; Logging</b>																										
<b>System (⚙️) &gt; SecureX</b>	is now	<b>Integration &gt; SecureX</b>																										

## FMC Features in Version 7.0.1

Table 13: FMC Features in Version 7.0.1

Feature	Details
Snort 3 rate_filter inspector.	<p>We introduced the Snort 3 rate_filter inspector.</p> <p>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 <a href="#">Snort 3 Inspector Reference</a>.</p> <p>New/modified pages: Configure the inspector by editing the Snort 3 version of a custom network analysis policy.</p> <p>Version restrictions: This feature requires Version 7.0.1+ on both the FMC and the device. Additionally, you must be running lsp-rel-20210816-1910 or later. You can check and update the LSP on <b>System (⚙️) &gt; Updates &gt; Rule Updates</b>.</p>
New default password for ISA 3000 with ASA FirePOWER Services.	<p>For new devices, the default password for the admin account is now Adm!n123. Previously, the default admin password was Admin123.</p> <p>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.</p>

## FMC Features in Version 7.0.0

Table 14: FMC Features in Version 7.0.0

Feature	Details
<b>Platform</b>	
VMware vSphere/VMware ESXi 7.0 support.	<p>You can now deploy FMCv, FTDv, and NGIPsv virtual appliances on VMware vSphere/VMware ESXi 7.0.</p> <p>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.</p>
New virtual environments.	<p>We introduced FMCv and FTDv for:</p> <ul style="list-style-type: none"> <li>• Cisco HyperFlex</li> <li>• Nutanix Enterprise Cloud</li> <li>• OpenStack</li> </ul> <p>For FMCv, all these implementations support FMCv2, v10, and v25.</p> <p>FMCv for HyperFlex also supports high availability with FMCv10 and v25. In an FTD deployment, 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.</p>
FTDv performance tiered Smart Licensing.	<p><b>Upgrade impact. Upgrading automatically assigns devices to the FTDv50 tier.</b></p> <p>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).</p> <p>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.</p> <p>Upgrading FTDv to Version 7.0 automatically assigns the device to the FTDv50 tier. To continue using your legacy (non-tiered) license, after upgrade, change the tier to Variable.</p> <p>For more information on supported instances, throughputs, and other hosting requirements, see the appropriate <a href="#">Getting Started Guide</a>.</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> <li>• You can now specify a performance tier when adding or editing an FTDv device on the <b>Device &gt; Device Management</b> page.</li> <li>• You can bulk-edit performance tiers on <b>System (⚙) &gt; Licenses &gt; Smart Licenses &gt;</b> page.</li> </ul>
<b>High Availability/Scalability</b>	

Feature	Details
Improved PAT port block allocation for clustering	<p>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 <b>cluster-member-limit</b> 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.</p> <p>New/modified commands: <b>cluster-member-limit</b> (FlexConfig), <b>show nat pool cluster [summary]</b>, <b>show nat pool ip detail</b></p> <p>Supported platforms: Firepower 4100/9300</p>
FTD CLI <b>show cluster history</b> improvements.	<p>New keywords allow you to customize the output of the <b>show cluster history</b> command.</p> <p>New/modified commands: <b>show cluster history [brief] [latest] [reverse] [time]</b></p> <p>Supported platforms: Firepower 4100/9300</p>
FTD CLI command to permanently leave a cluster.	<p>You can now use the FTD CLI to permanently remove a unit from the cluster, converting its configuration to a standalone device.</p> <p>New/modified commands: <b>cluster reset-interface-mode</b></p> <p>Supported platforms: Firepower 4100/9300</p>
<b>NAT</b>	
Prioritized system-defined NAT rules.	<p>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.</p> <p>You cannot add, edit, or delete Section 0 rules, but you will see them in <b>show nat detail</b> command output.</p> <p>Supported platforms: FTD</p>
<b>Virtual Routing</b>	
Virtual router support for the ISA 3000.	<p>You can now configure up to 10 virtual routers on an ISA 3000 device.</p> <p>Supported platforms: ISA 3000</p>
<b>Site to Site VPN</b>	
Backup virtual tunnel interfaces (VTI) for route-based site-to-site VPN.	<p>When you configure a site-to-site VPN that uses virtual tunnel interfaces, you can select a backup VTI for the tunnel.</p> <p>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.</p> <p>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.</p> <p>Supported platforms: FTD</p>

Feature	Details
<b>Remote Access VPN</b>	
Load balancing.	<p>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.</p> <p>New/modified screens: We added load balancing options to the Advanced settings in an RA VPN policy.</p> <p>Supported platforms: FTD</p>
Local authentication.	<p>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.</p> <ol style="list-style-type: none"> <li>1. Create a local realm. <p>Local usernames and passwords are stored in local realms. When you create a realm (<b>System</b> (⚙) &gt; <b>Integration</b> &gt; <b>Realms</b>) and select the new <b>LOCAL</b> realm type, the system prompts you to add one or more local users.</p> </li> <li>2. Configure RA VPN to use local authentication. <p>Create or edit an RA VPN policy (<b>Devices</b> &gt; <b>VPN</b> &gt; <b>Remote Access</b>), create a connection profile within that policy, then specify <b>LOCAL</b> as the primary, secondary, or fallback authentication server in that connection profile.</p> </li> <li>3. Associate the local realm you created with an RA VPN policy. <p>In the RA VPN policy editor, use the new <b>Local Realm</b> setting. Every connection profile in the RA VPN policy that uses local authentication will use the local realm you specify here.</p> </li> </ol> <p>Supported platforms: FTD</p>
Dynamic access policies.	<p>The new dynamic access policy allows you to configure remote access VPN authorization that automatically adapts to a changing environment:</p> <ol style="list-style-type: none"> <li>1. Configure HostScan by uploading the AnyConnect HostScan package as an AnyConnect file (<b>Objects</b> &gt; <b>Object Management</b> &gt; <b>VPN</b> &gt; <b>AnyConnect File</b>). There is a new <b>HostScan Package</b> option in the <b>File Type</b> drop-down list. <p>This module runs on endpoints and performs a posture assessment that the dynamic access policy will use.</p> </li> <li>2. Create a dynamic access policy (<b>Devices</b> &gt; <b>Dynamic Access Policy</b>). <p>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.</p> </li> <li>3. Associate the dynamic access policy you created with an RA VPN policy. <p>In the remote access VPN policy editor, use the new <b>Dynamic Access Policy</b> setting.</p> </li> </ol> <p>Supported platforms: FTD</p>

Feature	Details
Multi-certificate authentication.	<p>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.</p> <p>Supported platforms: FTD</p>
AnyConnect custom attributes.	<p>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.</p> <p>Supported platforms: FTD</p>

**Access Control**

Feature	Details
Snort 3 for FTD.	<p>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.</p> <p>Advantages to using Snort 3 include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Improved performance.</li> <li>• Improved SMBv2 inspection.</li> <li>• New script detection capabilities.</li> <li>• HTTP/2 inspection.</li> <li>• Custom rule groups.</li> <li>• Syntax that makes custom intrusion rules easier to write.</li> <li>• Reasons for 'would have dropped' inline results in intrusion events.</li> <li>• No Snort restarts when deploying changes to the VDB, SSL policies, custom application detectors, captive portal identity sources, and TLS server identity discovery.</li> <li>• Improved serviceability, due to Snort 3-specific telemetry data sent to Cisco Success Network, and to better troubleshooting logs.</li> </ul> <p>A Snort 3 intrusion rule update is called an <i>LSP</i> (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.</p> <p>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 <i>and</i> its managed devices. For information on the Snort included with each software version, see the <i>Bundled Components</i> section of the <a href="#">Cisco Firepower Compatibility Guide</a>.</p> <p><b>Important</b> Before you switch to Snort 3, we <i>strongly</i> recommend you read and understand the <a href="#">Firepower Management Center Snort 3 Configuration Guide</a>. 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.</p> <p>You can also visit the Snort 3 website: <a href="https://snort.org/snort3">https://snort.org/snort3</a>.</p> <p>Supported platforms: FTD</p>



Feature	Details
Dynamic objects.	<p>You can now use <i>dynamic objects</i> in access control rules.</p> <p>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.</p> <p>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 <a href="#">Cisco Secure Dynamic Attributes Connector Configuration Guide</a>.</p> <p>After you create a dynamic object, you can add it to access control rules on the new <b>Dynamic Attributes</b> tab in the access control rule editor. This tab replaces the narrower-focus <b>SGT/ISE Attributes</b> tab; continue to configure rules with SGT attributes here.</p> <p><b>Note</b> You can also create a dynamic object on the FMC: <b>Objects &gt; Object Management &gt; External Attributes &gt; Dynamic Objects</b>. However, this creates the container only; you must then populate and manage it using the REST API. See the <a href="#">Firepower Management Center REST API Quick Start Guide, Version 7.0</a>.</p> <p>Supported platforms: FMC</p> <p>Supported virtual/cloud workloads for Cisco Secure Dynamic Attributes Connector integration: Microsoft Azure, AWS, VMware</p>
Cross-domain trust for Active Directory domains.	<p>You can now configure user identity rules with users from Microsoft Active Directory forests (groupings of AD domains that trust each other).</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> <li>• You now configure a realm and directories at the same time.</li> <li>• A new Sync Results page (<b>System</b> (⚙️) &gt; <b>Integration</b> &gt; <b>Sync Results</b>) displays any errors related to downloading users and groups in a cross-domain trust relationship.</li> </ul> <p>Supported platforms: FMC</p>
DNS filtering.	<p>DNS filtering, which was introduced as a Beta feature in Version 6.7, is now fully supported and is enabled by default in new access control policies.</p> <p>Supported platforms: Any</p>

## Event Logging and Analysis

Feature	Details
Improved process for storing events in a Secure Network Analytics on-prem deployment.	<p>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:</p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>3. On the FMC, use one of the new wizards on <b>System</b> (⚙️) &gt; <b>Logging</b> &gt; <b>Security Analytics &amp; Logging</b> to connect to your Stealthwatch deployment.</li> </ol> <p>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.</p> <p>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 (<b>Devices &gt; Platform Settings</b>); to disable sending events to syslog, edit your access control rules.</p> <p>For more information, including Stealthwatch hardware and software requirements, see <a href="#">Cisco Security Analytics and Logging (On Premises): Firewall Event Integration Guide</a>.</p> <p>Supported platforms: FMC</p>
Work with events stored remotely in a Secure Network Analytics on-prem deployment.	<p>You can now use the FMC to work with connection events stored remotely in a Secure Network Analytics on-prem deployment.</p> <p>A new <b>Data Source</b> option on the connection events page (<b>Analysis &gt; Connections &gt; Events</b>) and in the unified event viewer (<b>Analysis &gt; Unified Events</b>) 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..</p> <p>We also added a data source option to report templates (<b>Overview &gt; Reporting &gt; Report Templates</b>), so that you can generate reports based on remotely stored connection events.</p> <p><b>Note</b> 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.</p> <p>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.</p> <p>Supported platforms: FMC</p>

Feature	Details
Store all connection events in the Secure Network Analytics cloud.	<p>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.</p> <p>To change the events you send to the cloud, choose <b>System</b> (⚙️) &gt; <b>Integration</b>. On the <b>Cloud Services</b> tab, edit the <b>Cisco Cloud Event Configuration</b>. The old option to send high priority connection events to the cloud has been replaced with a choice of <b>All</b>, <b>None</b>, or <b>Security Events</b>.</p> <p><b>Note</b> 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 <b>Analysis</b> &gt; <b>SecureX</b>.</p> <p>Supported platforms: FMC</p>
Unified event viewer.	<p>The unified event viewer (<b>Analysis</b> &gt; <b>Unified Events</b>) displays connection, Security Intelligence, intrusion, file, and malware events in a single table. This can help you look relationships between events of different types.</p> <p>A single search field allows you to dynamically filter the view based on multiple criteria, and a <b>Go Live</b> option displays events received from managed devices in real time.</p> <p>Supported platforms: FMC</p>
SecureX ribbon.	<p>The SecureX ribbon on the FMC pivots into SecureX for instant visibility into the threat landscape across your Cisco security products.</p> <p>To connect with SecureX and enable the ribbon, use <b>System</b> (⚙️) &gt; <b>SecureX</b>. Note that you must still use <b>System</b> (⚙️) &gt; <b>Integration</b> &gt; <b>Cloud Services</b> to choose your cloud region and to specify which events to send to SecureX.</p> <p>For more information, see the <a href="#">Cisco Secure Firewall Threat Defense and SecureX Integration Guide</a>.</p> <p>Supported platforms: FMC</p>
Exempt all connection events from rate limiting when you turn off local storage.	<p>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.</p> <p>Now, disabling local connection event storage exempts <i>all</i> connection events from rate limiting, not just security events. To do this, set the <b>Maximum Connection Events</b> to zero on <b>System</b> (⚙️) &gt; <b>Configuration</b> &gt; <b>Database</b>.</p> <p><b>Note</b> Other than turning it off by setting it to zero, <b>Maximum Connection Events</b> does not govern connection event rate limiting. Any non-zero number in this field ensures that <i>all</i> lower-priority connection events are rate limited.</p> <p>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.</p> <p>Supported platforms: FMC</p>

Feature	Details
Port and protocol displayed together in file and malware event tables.	<p>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."</p> <p>New/modified pages:</p> <ul style="list-style-type: none"> <li>• <b>Analysis &gt; Files &gt; Malware Events</b></li> <li>• <b>Analysis &gt; Files &gt; File Events</b></li> </ul> <p>Supported platforms: FMC</p>
<b>Upgrade</b>	
Improved FTD upgrade performance and status reporting.	<p>FTD upgrades are now easier faster, more reliable, and take up less disk space. A new <b>Upgrades</b> tab in the Message Center provides further enhancements to upgrade status and error reporting.</p> <p>Supported platforms: FTD</p>
Upgrade wizard for FTD.	<p>A new device upgrade page (<b>Devices &gt; Device Upgrade</b>) 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.</p> <p>To begin, use the new <b>Upgrade Firepower Software</b> action on the Device Management page (<b>Devices &gt; Device Management &gt; Select Action</b>).</p> <p>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.</p> <p>If you navigate away from wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the wizard.</p> <p><b>Note</b> You must still use <b>System</b> (⚙️) &gt; <b>Updates</b> 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.</p> <p><b>Note</b> 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.</p> <p>To avoid possible time-consuming upgrade failures, <i>manually</i> ensure all group members are ready to move on to the next step of the wizard before you click <b>Next</b>.</p> <p>Supported platforms: FTD</p>

Feature	Details
Upgrade more FTD devices at once.	<p>The FTD upgrade wizard lifts the following restrictions:</p> <ul style="list-style-type: none"> <li>• Simultaneous device upgrades.</li> </ul> <p>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.</p> <p><b>Important</b> Only upgrades to FTD Version 6.7+ 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.</p> <ul style="list-style-type: none"> <li>• Grouping upgrades by device model.</li> </ul> <p>You can now queue and invoke upgrades for all FTD models at the same time, as long as the system has access to the appropriate upgrade packages.</p> <p>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 <i>only</i> 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.</p> <p>Supported platforms: FTD</p>
<b>Administration and Troubleshooting</b>	
Zero-touch restore for the ISA 3000 using the SD card.	<p>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.</p> <p>Supported platforms: ISA 3000</p>
Selectively deploy RA and site-to-site VPN policies.	<p>Selective policy deployment, which was introduced in Version 6.6, now supports remote access and site-to-site VPN policies.</p> <p>New/modified pages: We added VPN policy options on the <b>Deploy &gt; Deployment</b> page.</p> <p>Supported platforms: FTD</p>

Feature	Details
New health modules.	<p>We added the following health modules:</p> <ul style="list-style-type: none"> <li>• AMP Connection Status</li> <li>• AMP Threat Grid Status</li> <li>• ASP Drop</li> <li>• Advanced Snort Statistics</li> <li>• Chassis Status FTD</li> <li>• Event Stream Status</li> <li>• FMC Access Configuration Changes</li> <li>• FMC HA Status (replaces HA Status)</li> <li>• FTD HA Status</li> <li>• File System Integrity Check</li> <li>• Flow Offload</li> <li>• Hit Count</li> <li>• MySQL Status</li> <li>• NTP Status FTD</li> <li>• Rabbit MQ Status</li> <li>• Routing Statistics</li> <li>• SSE Connection Status</li> <li>• Sybase Status</li> <li>• Unresolved Groups Monitor</li> <li>• VPN Statistics</li> <li>• xTLS Counters</li> </ul> <p>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.</p> <p>Supported platforms: FMC</p>
<b>Security and Hardening</b>	
New default password for AWS deployments.	<p>The default password for the admin account is now the AWS Instance ID, unless you define a default password with user data (<b>Advanced Details &gt; User Data</b>) during the initial deployment.</p> <p>Previously, the default admin password was Admin123.</p> <p>Supported platforms: FMCv for AWS, FTDv for AWS</p>

Feature	Details
EST for certificate enrollment.	Support for Enrollment over Secure Transport for certificate enrollment was provided. New/modified pages: New enrollment options when configuring <b>Objects &gt; PKI &gt; Cert Enrollment &gt; CA Information</b> tab. Supported platforms: FMC
Support for EdDSA certificate type.	A new certificate key type- EdDSA was added with key size 256. New/modified pages: New certificate key options when configuring <b>Objects &gt; PKI &gt; Cert Enrollment &gt; Key</b> tab. Supported platforms: FMC
AES-128 CMAC authentication for NTP servers.	You can now use AES-128 CMAC keys to secure connections between the FMC and NTP servers. New/modified pages: <b>System (⚙️) &gt; Configuration &gt; Time Synchronization</b> . Supported platforms: FMC
SNMPv3 users can authenticate using a SHA-224 or SHA-384 authorization algorithm.	SNMPv3 users can now authenticate using a SHA-224 or SHA-384 algorithm. New/modified pages: <b>Devices &gt; Platform Settings &gt; SNMP &gt; Users &gt; Auth Algorithm Type</b> Supported platforms: FTD
<b>Usability and Performance</b>	
Global search for policies and objects.	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 <b>Search</b> icon and field on the FMC menu bar, to the left of the <b>Deploy</b> menu. Supported platforms: FMC
Hardware crypto acceleration on FTDv using Intel QuickAssist Technology (QAT).	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. Supported platforms: FTDv for VMware, FTDv for KVM
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: <b>clear local-host</b> (deprecated), <b>show local-host</b> Supported platforms: FTD
How-to location has changed.	<b>Help &gt; How-Tos</b> now invokes walkthroughs. Previously, you clicked <b>How-Tos</b> at the bottom of the browser window.
<b>FMC REST API</b>	

Feature	Details
FMC REST API.	For information on changes to the management center REST API, see the <a href="#">Firepower Management Center REST API Quick Start Guide, Version 7.0</a> ,
<b>Deprecated Features</b>	
End of support: VMware vSphere/VMware ESXi 6.0.	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.	<p><b>Prevents post-upgrade VPN connections through FTD devices.</b></p> <p>We removed support for RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm.</p> <p>Before you upgrade, use the object manager to update your PKI certificate enrollments with stronger options: <b>Objects &gt; PKI &gt; Cert Enrollment</b>. Otherwise, although the upgrade preserves your current settings, VPN connections through the device will fail.</p> <p>To continue managing older FTD devices only (Version 6.4–6.7.x) with these weaker options, select the new <b>Enable Weak-Crypto</b> option for each device on the <b>Devices &gt; Certificates</b> page.</p>
Deprecated: MD5 authentication algorithm and DES encryption for SNMPv3 users.	<p><b>Deletes Users. Prevents post-upgrade deploy.</b></p> <p>We removed support for the MD5 authentication algorithm and DES encryption for SNMPv3 users on FTD devices.</p> <p>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.</p> <p>These options are in the <b>Auth Algorithm Type</b> and <b>Encryption Type</b> drop-downs when creating or editing an SNMPv3 user in a Threat Defense platform settings policy: <b>Devices &gt; Platform Settings</b>.</p>
Deprecated: Port 32137 comms with AMP clouds.	<p><b>Prevents FMC upgrade.</b></p> <p>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.</p> <p>Before you upgrade, disable the <b>Use Legacy Port 32137 for AMP for Networks</b> option on the <b>System (⚙️) &gt; Integration &gt; Cloud Services</b> page. Do not proceed with upgrade until your AMP for Networks deployment is working as expected.</p>
Deprecated: HA Status health module.	We renamed the HA Status health module to the <i>FMC</i> HA Status health module. This is to distinguish it from the new FTD HA Status module.
Deprecated: Legacy API Explorer.	We removed support for the FMC REST API legacy API Explorer.



Feature	Details
Deprecated: Geolocation details.	<p>In May 2022 we split the GeoDB into two packages: a country code package that maps IP addresses to countries/continents, and an IP package that contains additional contextual data associated with routable IP addresses. The contextual data in the IP package can include additional location details, as well as connection information such as ISP, connection type, proxy type, domain name, and so on.</p> <p>The new country code package has the same file name as the old all-in-one package: <code>Cisco_GEODB_Update-date-build</code>. This allows deployments running Version 7.1 and earlier to continue to obtain GeoDB updates. If you manually download GeoDB updates—for example, in an air-gapped deployment—make sure you get the country code package and not the IP package.</p> <p><b>Important</b> This split does not affect geolocation rules or traffic handling in any way—those rules rely only on the data in the country code package. However, because the country code package essentially replaces the all-in-one package, the contextual data is no longer updated and will grow stale. To obtain fresh data, upgrade or reimage the FMC to Version 7.2+ and update the GeoDB.</p>

## FDM Features in Version 7.0.x

Table 15: FDM Features in Version 7.0.x


Feature	Description
<b>Platform Features</b>	
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 FTDv on AWS.	On AWS, the default admin password for the FTDv is the AWS Instance ID, unless you define a default password with user data ( <b>Advanced Details &gt; User Data</b> ) during the initial deployment.
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.
<b>Firewall and IPS Features</b>	

Feature	Description
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 <b>show nat detail</b> command output.
Custom intrusion rules for Snort 3.	<p>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 FDM, but the rules have the same format as uploaded rules. FDM 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.</p> <p>We added support for custom groups and rules to the <b>Policies &gt; Intrusion</b> page, when you edit an intrusion policy.</p>
Snort 3 new features for FDM-managed systems.	<p>You can now configure the following additional features when using Snort 3 as the inspection engine on an FDM-managed system:</p> <ul style="list-style-type: none"> <li>• Time-based access control rules. (FTD API only.)</li> <li>• Multiple virtual routers.</li> <li>• The decryption of TLS 1.1 or lower connections using the SSL Decryption policy.</li> <li>• The decryption of the following protocols using the SSL Decryption policy: FTPS, SMTPS, IMAPS, POP3S.</li> </ul>
DNS request filtering based on URL category and reputation.	<p>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.</p> <p>We added the <b>Reputation Enforcement on DNS Traffic</b> option to the access control policy settings.</p>
Smaller VDB for lower memory devices with Snort 2.	<p><b>Upgrade impact. Application identification on lower memory devices is affected.</b></p> <p>For Version 7.0.6+ devices with Snort 2, for VDB 363+, the system now installs a smaller VDB (also called <i>VDB lite</i>) 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.</p> <p>Lower memory devices: ASA-5508-X, ASA-5516-X</p> <p>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 <a href="#">CSCwd88641</a>.</p>

## VPN Features

Feature	Description
FDM SSL cipher settings for remote access VPN.	<p>You can define the TLS versions and encryption ciphers to use for remote access VPN connections in FDM. Previously, you needed to use the Firepower Threat Defense API to configure SSL settings.</p> <p>We added the following pages: <b>Objects &gt; SSL Ciphers</b>; <b>Device &gt; System Settings &gt; SSL Settings</b>.</p>
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.	<p>You can change the default settings for how long a security association is maintained before it must be re-negotiated.</p> <p>We added the <b>Lifetime Duration</b> and <b>Lifetime Size</b> options to the site-to-site VPN wizard.</p>
<b>Routing Features</b>	
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.	<p>You can configure ECMP traffic zones to contain multiple interfaces, which lets traffic from an existing connection exit or enter the Firepower Threat Defense device on any interface within the zone. This capability allows Equal-Cost Multi-Path (ECMP) routing on the Firepower Threat Defense device as well as external load balancing of traffic to the Firepower Threat Defense device across multiple interfaces.</p> <p>ECMP traffic zones are used for routing only. They are not the same as security zones.</p> <p>We added the <b>ECMP Traffic Zones</b> tab to the Routing pages. In the Firepower Threat Defense API, we added the ECMPZones resources.</p>
<b>Interface Features</b>	
New default inside IP address.	The default IP address for the inside interface is being changed to <b>192.168.95.1</b> 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.
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.	<p>You can now use FDM to configure EtherChannels on the ISA 3000.</p> <p>New/modified screens: <b>Devices &gt; Interfaces &gt; EtherChannels</b></p>
<b>Licensing Features</b>	
Performance-Tiered Licensing for FTDv.	The FTDv now supports performance-tiered Smart Licensing based on throughput requirements and RA VPN session limits. When the FTDv 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.

Feature	Description
<b>Administrative and Troubleshooting Features</b>	
DHCP relay configuration using the Firepower Threat Defense API.	<p><b>Upgrade impact. Can prevent post-upgrade deploy.</b></p> <p>You can use the Firepower 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.</p> <p>Note that if you used FlexConfig in prior releases to configure DHCP relay (the <b>dhcprelay</b> command), you must re-do the configuration using the API, and delete the FlexConfig object, after you upgrade.</p> <p>We added the following model to the Firepower Threat Defense API: <code>dhcprelayservices</code></p>
Faster bootstrap processing and early login to FDM.	<p>The process to initially bootstrap an FDM-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 FDM. 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.</p>
Improved CPU usage and performance for many-to-one and one-to-many connections.	<p>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.</p> <p>We changed the following commands: <b>clear local-host</b> (deprecated), <b>show local-host</b></p>
Upgrade readiness check for FDM-managed devices.	<p>You can run an upgrade readiness check on an uploaded Firepower 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.</p> <p>A link to run the upgrade readiness check was added to the <b>System Upgrade</b> section of the <b>Device &gt; Updates</b> page.</p>
Automatically update CA bundles.	<p><b>Upgrade impact. The system connects to Cisco for something new.</b></p> <p>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.</p> <p>New/modified CLI commands: <b>configure cert-update auto-update</b>, <b>configure cert-update run-now</b>, <b>configure cert-update test</b>, <b>show cert-update</b></p> <p>Version restrictions: This feature is included in Versions 7.0.5+, 7.1.0.3+, and 7.2.4+. It is not supported in earlier 7.0, 7.1, or 7.2 releases. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco.</p> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Command Reference</a></p>

Feature	Description
FTD REST API version 6.1 (v6).	<p>The Firepower 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.</p> <p>Please re-evaluate all existing calls, as changes might have been made to the resource models you are using. To open the API Explorer, where you can view the resources, log into FDM, then click the more options button (  ) and choose <b>API Explorer</b>.</p>





## CHAPTER 4

# Upgrade Guidelines

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

- [Planning Your Upgrade, on page 41](#)
- [Minimum Version to Upgrade, on page 42](#)
- [Upgrade Guidelines for Version 7.0, on page 43](#)
- [Upgrade Guidelines for Cloud-delivered Firewall Management Center, on page 53](#)
- [Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 53](#)
- [Unresponsive Upgrades, on page 53](#)
- [Revert or Uninstall the Upgrade, on page 54](#)
- [Traffic Flow and Inspection, on page 56](#)
- [Time and Disk Space, on page 61](#)

## 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: <http://www.cisco.com/go/threatdefense-70-docs>.

**Table 16: Upgrade Planning Phases**

Planning Phase	Includes
Planning and Feasibility	Assess your deployment. Plan your upgrade path. Read <i>all</i> 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 17: Minimum Version to Upgrade to Version 7.0**

Platform	Minimum Version
FMC	6.4
FTD	6.4 FXOS 2.10.1.159 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 <a href="#">Cisco Firepower 4100/9300 FXOS Release Notes, 2.10(1)</a> .
ASA with FirePOWER Services	6.4 See <a href="#">Device Platforms, on page 8</a> 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 <a href="#">Cisco Secure Firewall ASA Release Notes</a> .
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 18: Upgrade Guidelines for FTD with FMC Version 7.0**

✓	Guideline	Platforms	Upgrading From	Directly To
<b>ALWAYS CHECK</b>				
	<a href="#">Minimum Version to Upgrade, on page 42</a>	Any	Any	Any
	<a href="#">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.</a>	Any	Any	Any
	<a href="#">Bugs, on page 67, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.</a>	Any	Any	Any
	<a href="#">Upgrade Guidelines for Cloud-delivered Firewall Management Center, on page 53</a>	FTD	Any	Any
	<a href="#">Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 53</a>	Firepower 4100/9300	Any	Any
<b>ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS</b>				
	<a href="#">Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0, on page 44</a>	Any	7.0.4+	7.1.0 only
	<a href="#">Reconnect with Cisco Threat Grid for High Availability FMCs, on page 45</a>	FMC	6.4.0 through 6.7.x	7.0+
	<a href="#">Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 45</a>	Firepower 1010	6.4.0 through 6.6.x	6.7+
	<a href="#">FMCv Requires 28 GB RAM for Upgrade, on page 45</a>	FMCv	6.2.3 through 6.5.0.x	6.6+
	<a href="#">Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 46</a>	Firepower 1000 series	6.4.0.x	6.5+

✓	Guideline	Platforms	Upgrading From	Directly To
	<a href="#">New URL Categories and Reputations, on page 47</a>	Any	6.2.3 through 6.4.0.x	6.5+

Table 19: Upgrade Guidelines for FTD with FDM Version 7.0

✓	Guideline	Platforms	Upgrading From	Directly To
<b>ALWAYS CHECK</b>				
	<a href="#">Minimum Version to Upgrade, on page 42</a>	Any	Any	Any
	<a href="#">Cisco Secure Firewall Device Manager New Features by Release</a> , for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	<a href="#">Bugs, on page 67</a> , for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	<a href="#">Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 53</a>	Firepower 4100/9300	Any	Any
<b>ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS</b>				
	<a href="#">Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0, on page 44</a>	Any	7.0.4+	7.1.0 only
	<a href="#">Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 45</a>	Firepower 1010	6.4.0 through 6.6.x	6.7+
	<a href="#">Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 46</a>	Firepower 1000 series	6.4.0.x	6.5+
	<a href="#">Historical Data Removed During FTD Upgrade with FDM, on page 47</a>	Any	6.2.3 through 6.4.0.x	6.5+
	<a href="#">New URL Categories and Reputations, on page 47</a>	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 FMCs

**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 FMC:

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, FTD 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.

## FMCv Requires 28 GB RAM for Upgrade

**Deployments:** FMCv

**Upgrading from:** Version 6.2.3 through 6.5

**Directly to:** Version 6.6+

All FMCv 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 FMCv 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 20: FMCv 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: <ul style="list-style-type: none"> <li>• <b>From</b> c3.xlarge to c3.4xlarge.</li> <li>• <b>From</b> c3.2.xlarge to c3.4xlarge.</li> <li>• <b>From</b> c4.xlarge to c4.4xlarge.</li> <li>• <b>From</b> c4.2xlarge to c4.4xlarge.</li> </ul> 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.
Azure	Resize instances: <ul style="list-style-type: none"> <li>• <b>From</b> Standard_D3_v2 to Standard_D4_v2.</li> </ul>	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 FTD Upgrade with FDM

**Deployments:** FTD with FDM

**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 21: Deployment Changes on Upgrade

Change	Details
Modifies URL rule categories.	<p>The upgrade modifies URL rules to use the nearest equivalents in the new category set, in the following policies:</p> <ul style="list-style-type: none"> <li>• Access control</li> <li>• SSL</li> <li>• QoS (FMC only)</li> <li>• Correlation (FMC only)</li> </ul> <p>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.</p>
Renames URL rule reputations.	<p>The upgrade modifies URL rules to use the new reputation names:</p> <ol style="list-style-type: none"> <li>1. Untrusted (was <i>High Risk</i>)</li> <li>2. Questionable (was <i>Suspicious sites</i>)</li> <li>3. Neutral (was <i>Benign sites with security risks</i>)</li> <li>4. Favorable (was <i>Benign sites</i>)</li> <li>5. Trusted (was <i>Well Known</i>)</li> </ol>
Clears the URL cache.	<p>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.</p>
Labels 'legacy' events.	<p>For already-logged events, the upgrade labels any associated URL category and reputation information as <code>Legacy</code>. These legacy events will age out of the database over time.</p>

## Pre-Upgrade Actions for URL Categories and Reputations

Before upgrade, take the following actions.

Table 22: Pre-Upgrade Actions

Action	Details
<p>Make sure your appliances can reach Talos resources.</p>	<p>The system must be able to communicate with the following Cisco resources after the upgrade:</p> <ul style="list-style-type: none"> <li>• <a href="https://regsvc.sco.cisco.com/">https://regsvc.sco.cisco.com/</a> — Registration</li> <li>• <a href="https://est.sco.cisco.com/">https://est.sco.cisco.com/</a> — Obtain certificates for secure communications</li> <li>• <a href="https://updates-talos.sco.cisco.com/">https://updates-talos.sco.cisco.com/</a> — Obtain client/server manifests</li> <li>• <a href="http://updates.ironport.com/">http://updates.ironport.com/</a> — Download database (note: uses port 80)</li> <li>• <a href="https://v3.sds.cisco.com/">https://v3.sds.cisco.com/</a> — Cloud queries</li> </ul> <p>The cloud query service also uses the following IP address blocks:</p> <ul style="list-style-type: none"> <li>• IPv4 cloud queries: <ul style="list-style-type: none"> <li>• 146.112.62.0/24</li> <li>• 146.112.63.0/24</li> <li>• 146.112.255.0/24</li> <li>• 146.112.59.0/24</li> </ul> </li> <li>• IPv6 cloud queries: <ul style="list-style-type: none"> <li>• 2a04:e4c7:ffff::/48</li> <li>• 2a04:e4c7:ffe::/48</li> </ul> </li> </ul>
<p>Identify potential rule issues.</p>	<p>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).</p> <p><b>Note</b> You may want to modify URL rules that use deprecated categories now. Otherwise, rules that use them will prevent deploy after the upgrade.</p> <p>In FMC deployments, we recommend you generate an <i>access control policy report</i>, 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 <b>Policies &gt; Access Control</b>, then click the report icon () next to the appropriate policy.</p>

## 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 23: Post-Upgrade Actions**

Action	Details
Remove <b>deprecated categories</b> 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 <b>new categories</b> .	Most of the new categories identify threats. We strongly recommend you use them.  On the FMC, these new categories are not marked after <i>this</i> upgrade, but Talos may add additional categories in the future. When that happens, new categories are marked.
Evaluate rules changed as a result of <b>merged categories</b> .	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 <a href="#">Guidelines for Rules with Merged URL Categories, on page 50</a> .  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 <b>split categories</b> .	The upgrade replaces each old, single category in URL rules with <i>all</i> 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 <b>renamed</b> or are <b>unchanged</b> .	Although no action is required, you should be aware of these changes.  These changes are not marked.
Evaluate how you handle <b>uncategorized</b> and <b>reputationless</b> 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 <b>Uncategorized</b> category, or by <b>Any</b> 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 24: 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	<p>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.</p> <p>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.</p>
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 <b>Any reputation</b> and Category B was associated in the same rule with reputation level <b>3 - Benign sites with security risks</b> , then after merge Category AB in that rule will be associated with <b>Any reputation</b> .
Duplicate and Redundant Categories and Rules	<p>After merge, different rules may have the same category associated with different actions and reputation levels.</p> <p>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.</p> <p>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.</p> <p>Caution: Consider all conditions in the rule when determining how to resolve duplicate or redundant categories.</p>
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.

Guideline	Details
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 25: 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.
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 FTD with the cloud-delivered Firewall Management Center, see the [Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center](#).

## Upgrade Guidelines for the Firepower 4100/9300 Chassis

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

*Table 26: Upgrade Guidelines for the Firepower 4100/9300 Chassis*

Guideline	Details
FXOS upgrades.	<p>FXOS 2.10.1.159+ is required to run threat defense Version 7.0 on the Firepower 4100/9300.</p> <p>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 <a href="#">Cisco Firepower 4100/9300 FXOS Release Notes</a>.</p>
Firmware upgrades.	<p>FXOS 2.14.1+ upgrades include firmware. If you are upgrading to an earlier FXOS version, see the <a href="#">Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide</a>.</p>
Time to upgrade.	<p>Chassis upgrade can take up to 45 minutes and can affect traffic flow and inspection. For more information, see <a href="#">Traffic Flow and Inspection for Chassis Upgrades</a>, on page 57.</p>

## 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 FMC 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 FTD Upgrade

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

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

You can also use the FTD CLI.



---

**Note** By default, FTD automatically reverts to its pre-upgrade state upon upgrade failure ("auto-cancel"). To be able to manually cancel or retry a failed upgrade, disable the auto-cancel option when you initiate the upgrade. 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 54](#) 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 27: Uninstall Order for ASA with FirePOWER Services in ASA Failover Pairs/Clusters

Configuration	Uninstall Order
ASA active/standby failover pair, with ASA FirePOWER	<p>Always uninstall from the standby.</p> <ol style="list-style-type: none"> <li>1. Uninstall from the ASA FirePOWER module on the standby ASA device.</li> <li>2. Fail over.</li> <li>3. Uninstall from the ASA FirePOWER module on the new standby ASA device.</li> </ol>
ASA active/active failover pair, with ASA FirePOWER	<p>Make both failover groups active on the unit you are not uninstalling.</p> <ol style="list-style-type: none"> <li>1. Make both failover groups active on the primary ASA device.</li> <li>2. Uninstall from the ASA FirePOWER module on the secondary ASA device.</li> <li>3. Make both failover groups active on the secondary ASA device.</li> <li>4. Uninstall from the ASA FirePOWER module on the primary ASA device.</li> </ol>
ASA cluster, with ASA FirePOWER	<p>Disable clustering on each unit before you uninstall. Uninstall from one unit at a time, leaving the control unit for last.</p> <ol style="list-style-type: none"> <li>1. On a data unit, disable clustering.</li> <li>2. Uninstall from the ASA FirePOWER module on that unit.</li> <li>3. Reenable clustering. Wait for the unit to rejoin the cluster.</li> <li>4. Repeat for each data unit.</li> <li>5. On the control unit, disable clustering. Wait for a new control unit to take over.</li> <li>6. Uninstall from the ASA FirePOWER module on the former control unit.</li> <li>7. Reenable clustering.</li> </ol>



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

#### Before you begin

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

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

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

**Step 2** Access the Firepower CLI on the ASA FirePOWER module. Log in as `admin` or another Firepower CLI user with configuration access.

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

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

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

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

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

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

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

**Caution** The system does *not* ask you to confirm. Entering this command starts the uninstall, which includes a device reboot. Interruptions in traffic flow and inspection during an uninstall are the same as the interruptions that occur during an upgrade. Make sure you are ready. Note that using the `--detach` option ensures the uninstall process is not killed if your SSH session times out, which can leave the device in an unstable state.

**Step 6** Monitor the uninstall until you are logged out.

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

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

Otherwise, monitor progress in the console or terminal.

**Step 7** Verify uninstall success.

After the uninstall completes, confirm that the module has the correct software version. Choose **Configuration > ASA FirePOWER Configurations > Device Management > Device**.

**Step 8** Redeploy configurations.

### What to do next

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

## Traffic Flow and Inspection

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

## Traffic Flow and Inspection for Chassis Upgrades

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

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

**Table 28: Traffic Flow and Inspection: FXOS Upgrades**

FTD Deployment	Traffic Behavior	Method
Standalone	Dropped.	—
High availability	Unaffected.	<b>Best Practice:</b> 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.	<b>Best Practice:</b> 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: <b>Bypass: Standby</b> or <b>Bypass-Force</b> .
	Dropped until at least one module is online.	Hardware bypass disabled: <b>Bypass: Disabled</b> .
	Dropped until at least one module is online.	No hardware bypass module.

## Traffic Flow and Inspection for FTD Upgrades with FMC

### Software Upgrades for Standalone Devices

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

Table 29: 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: <b>Bypass: Force</b>	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: <b>Bypass: Standby</b>	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: <b>Bypass: Disabled</b>	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 30: 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, <b>Failsafe</b> enabled or disabled.	Passed without inspection.  A few packets might drop if <b>Failsafe</b> is disabled and Snort is busy but not down.
	Inline set, <b>Snort Fail Open: Down:</b> disabled.	Dropped.
	Inline set, <b>Snort Fail Open: Down:</b> enabled.	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

## Traffic Flow and Inspection for FTD Upgrades with FDM

### Software Upgrades

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

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

### 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 31: Traffic Flow and Inspection: ASA FirePOWER Upgrades*

Traffic Redirection Policy	Traffic Behavior
Fail open ( <b>sfr fail-open</b> )	Passed without inspection
Fail closed ( <b>sfr fail-close</b> )	Dropped
Monitor only ( <b>sfr {fail-close}{fail-open} monitor-only</b> )	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 32: 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 33: Traffic Flow and Inspection: Deploying Configuration Changes**

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

## Time and Disk Space

**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 34: 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 with management center, you must also have enough space on the 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 35: Checking Disk Space**

Platform	Command
Management center	Choose <b>System</b> (⚙) > <b>Monitoring</b> > <b>Statistics</b> and select the FMC. Under Disk Usage, expand the By Partition details.
Threat defense with management center	Choose <b>System</b> (⚙) > <b>Monitoring</b> > <b>Statistics</b> and select the device you want to check. Under Disk Usage, expand the By Partition details.
Threat defense with device manager	Use the <b>show disk</b> 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 63](#)
- [Installation Guides, on page 65](#)

## 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 FMC deployments, you should also be able to access the FMC's management interface without traversing the device.

## Unregistering from Smart Software Manager

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

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

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

**Table 36: Scenarios for Unregistering from CSSM (Not Restoring from Backup)**

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

## Removing Devices from the FMC

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

**Table 37: Scenarios for Removing Devices from the FMC (Not Restoring from Backup)**

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

## Fully Reimaging FTD Hardware to Downgrade FXOS

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

Table 38: Scenarios for Full Reimages

Model	Details
Firepower 1000 series Firepower 2100 series	If you use the <b>erase configuration</b> 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 FTD does not downgrade FXOS.  For the Firepower 4100/9300, major FTD versions have a specially qualified and recommended companion FXOS version. After you return to the earlier version of FTD, you may be running a non-recommended version of FXOS (too new).  Although newer versions of FXOS are backwards compatible with older FTD versions, we do perform enhanced testing for the recommended combinations. You cannot manually downgrade FXOS, so if you find yourself in this situation and you want to run a recommended combination, you will need a full reimage.

## Installation Guides

Table 39: Installation Guides

Platform	Guide
<b>FMC</b>	
FMC 1600, 2600, 4600	<a href="#">Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide</a>
FMC 1000, 2500, 4500	<a href="#">Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide</a>
FMCv	<a href="#">Cisco Secure Firewall Management Center Virtual Getting Started Guide</a>
<b>FTD</b>	
Firepower 1000/2100 series	<a href="#">Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide</a>  <a href="#">Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense</a>
Firepower 4100/9300	<a href="#">Cisco Firepower 4100/9300 FXOS Configuration Guides: <i>Image Management</i> chapters</a>  <a href="#">Cisco Firepower 4100 Getting Started Guide</a> <a href="#">Cisco Firepower 9300 Getting Started Guide</a>
ASA 5500-X series	<a href="#">Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide</a>

<b>Platform</b>	<b>Guide</b>
ISA 3000	<a href="#">Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide</a>
FTDv	<a href="#">Cisco Secure Firewall Threat Defense Virtual Getting Started Guide</a>
<b>ASA FirePOWER/NGIPSv</b>	
ASA FirePOWER	<a href="#">Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide</a>
	<a href="#">ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide</a>
NGIPSv	<a href="#">Cisco Firepower NGIPSv Quick Start Guide for VMware</a>





# CHAPTER 6

## Bugs

This document lists open and resolved bugs for threat defense and management center Version 7.0. For bugs in earlier releases, see the release notes for those versions. For cloud-delivered Firewall Management Center bugs, see the [Cisco Cloud-Delivered Firewall Management Center Release Notes](#).



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

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 67](#)
- [Resolved Bugs, on page 69](#)

## Open Bugs

### Open Bugs in Version 7.0.0

Table last updated: 2022-11-02

**Table 40: Open Bugs in Version 7.0.0**

Bug ID	Headline
<a href="#">CSCvr74863</a>	CIP-Multiservice shows wrong service Attributes
<a href="#">CSCvx21050</a>	Snort3 UDP performance down up to 50% relative to snort2
<a href="#">CSCvx25425</a>	snort3 ssl - tickets from undecrypted sessions are not cached for subsequent policy decisions
<a href="#">CSCvx30175</a>	Snort3 - SMTP closing TCP flags are not propagated correctly
<a href="#">CSCvx63788</a>	Edit policy in new window for AC Policy default action IPS policy shows error pop-up

Bug ID	Headline
<a href="#">CSCvx64252</a>	Event Search errors out when using FQDN object search for initiator
<a href="#">CSCvx67856</a>	FTD7.0: Promethues process doesnt come up when system ungracefully rebooted
<a href="#">CSCvx89720</a>	User-based access control rules for RA VPN users may not apply as expected after 7.0.0 upgrade
<a href="#">CSCvx96452</a>	Some HTTP2 TLS traffic ends with TCP RST, not TCP FIN, after complete payload transmission
<a href="#">CSCvx96452</a>	Snort3 - Connection events sporadically show Allow action for traffic hitting SSL Block with Reset
<a href="#">CSCvx99179</a>	FDM-VMWARE: nikita-incremen core during upgrade from 6.5 or higher to 7.0/7.1
<a href="#">CSCvy02879</a>	FDM ISA 3000 HA goes into active-active state
<a href="#">CSCvy07113</a>	7.0.0-1459 :FTPs traffic(malware file) is not blocked with file policy config,specifi to QP platform
<a href="#">CSCvy13572</a>	7.0 - Downgrade to LSP version used in 6.7 causes deployment failure
<a href="#">CSCvy19415</a>	After switching FTD HA, (secondary,active) sends primary device name in syslog message
<a href="#">CSCvy26742</a>	Deployment failure when 1k rules are uploaded on 7.0.0-62 KVM vFTD
<a href="#">CSCvy27261</a>	Snort2 and Snort3 Events view need enhancements to provide more clarity
<a href="#">CSCvy31096</a>	Host rediscovery in case of snort configuration reload
<a href="#">CSCvy32550</a>	Correlation filtering on snort3 custom rule message fails because rule is not built with GID 2000
<a href="#">CSCvy35352</a>	Error handling for Suppression settings needed in certain conditions
<a href="#">CSCvy38070</a>	File/Malware Event Report fails when date is x-axis and count y-axis for table chart
<a href="#">CSCvy39840</a>	SI TALOS feed updates are not synced to rule file
<a href="#">CSCvy43483</a>	Snort Toggle sometimes takes longer time to toggle to Snort 2
<a href="#">CSCvy43740</a>	vFDM ISA HA Security Intelligence feed update throws java.lang.NullPoin
<a href="#">CSCvy44701</a>	Version 7.0 FMC online help for the Snort 3 HTTP/2 inspector contains incorrect content.
<a href="#">CSCvy48764</a>	SSH access with public key authentication requires user password
<a href="#">CSCwa16654</a>	Firepower release 7.0.x does not support ssl_state or ssl_version keywords for Snort 3

# Resolved Bugs

## Resolved Bugs in Version 7.0.6.2

Table last updated: 2024-05-17

**Table 41: Resolved Bugs in Version 7.0.6.2**

Bug ID	Headline
<a href="#">CSCvu22491</a>	FMC fails to connect to SSM with error "Failed to send the message to the server"
<a href="#">CSCvx37329</a>	Remove Syslog Messages 852001 and 852002 in Firewall Threat Defense
<a href="#">CSCvx94744</a>	FMC UI inaccessible due to flood of TSA (version 1.3) REST-API calls to FMC
<a href="#">CSCvy47786</a>	Deployment preview will show unchanged/unadded comments to ACP rules
<a href="#">CSCvy90949</a>	import of iips sfo with some overridden rules across sibling domains
<a href="#">CSCvz03407</a>	IPTables.conf file is disappearing resulting in backup and restore failure.
<a href="#">CSCvz10481</a>	sfo import fails when "import as new" option is selected
<a href="#">CSCvz70310</a>	ASA may fail to create NAT rule for SNMP with: "error NAT unable to reserve ports."
<a href="#">CSCvz77254</a>	Hotfix patch upgrade doesn't clean old snort3 binaries
<a href="#">CSCwa08084</a>	FMC hardware appliance restore ends with an error "Unknown Failure Condition"
<a href="#">CSCwa22766</a>	FMC4500/4600 shows virtual license
<a href="#">CSCwb41189</a>	LINA time-sync correction
<a href="#">CSCwb55243</a>	snort3 crashinfo sometimes fails to collect all frames
<a href="#">CSCwb95850</a>	Snort down due to missing lua files because of disabled application detectors (PM side)
<a href="#">CSCwc31953</a>	Prevention of RSA private key leaks regardless of root cause.
<a href="#">CSCwc40352</a>	Lina Netflow sending permitted events to Stealthwatch but they are block by snort afterwards
<a href="#">CSCwc44367</a>	LSP not installed after HA failover. No LSP package found in the active LSP directory
<a href="#">CSCwd04135</a>	Snort3 unexpectedly dropping packets after 4MB when using file inspection with detection mode NAP
<a href="#">CSCwd16850</a>	More information is required on Syslog 202010 messages for troubleshooting
<a href="#">CSCwd31806</a>	ASAv show crashinfo printing in loop continuously

Bug ID	Headline
<a href="#">CSCwd34079</a>	FTD: Traceback & reload in process name lina
<a href="#">CSCwd58665</a>	Intel Microcode Update required for FPR1000 products
<a href="#">CSCwd67100</a>	ASA traceback and reload on Datapath process
<a href="#">CSCwd87438</a>	Enhance logging mechanism for syslogs
<a href="#">CSCwe02012</a>	ASA/FTD may traceback and reload in Thread Name 'lina'
<a href="#">CSCwe03631</a>	Need to provide rate-limit on "logging history & mode;"
<a href="#">CSCwe06562</a>	FPR1K/FPR2K: Increase in failover time in Transparent Mode with high number of Sub-Interfaces
<a href="#">CSCwe11902</a>	FTD: HA crash and interfaces down on FPR4200
<a href="#">CSCwe18472</a>	[FTD Multi-Instance][SNMP] - CPU OIDs return incomplete list of associated CPUs
<a href="#">CSCwe21831</a>	add warning to FTD platform settings when VPN Logging Settings logging level is informational
<a href="#">CSCwe21884</a>	Write wrapper around "kill" command to log who is calling it
<a href="#">CSCwe30359</a>	Traffic drops with huge rule evaluation on snort
<a href="#">CSCwe33282</a>	FTD: The upgrade was unsuccessful because the httpd process was not running
<a href="#">CSCwe34269</a>	DBCheck error is unclear when monetdb is in a 'crashed' state
<a href="#">CSCwe47485</a>	FTD: CLISH slowness due to command execution locking LINA prompt
<a href="#">CSCwe47671</a>	High memory usage on monetDB, FMC does not show connection events
<a href="#">CSCwe48997</a>	FDM: Cannot create multiple RA-VPN profiles with different SAML servers that have the same SAML IDP
<a href="#">CSCwe56452</a>	BGP IPv6 configuration : route-map association with neighbour not getting deployed
<a href="#">CSCwe58207</a>	Memory leak observed on ASA/FTD when logging history is enabled
<a href="#">CSCwe60267</a>	FXOS fault F0853 and F0855 seen despite keyring certificates reporting renewed
<a href="#">CSCwe65516</a>	show xlate does not display xlate entries for internal interfaces (nlp_int_tap) after enabling ssh.
<a href="#">CSCwe72330</a>	FTD LINA traceback and reload in Datapath thread after adding Static Routing
<a href="#">CSCwe79990</a>	Cisco-Intelligence-Feed - Failed to download due to timeout
<a href="#">CSCwe87134</a>	ASA/FTD: Traceback and reload due to high rate of SCTP traffic
<a href="#">CSCwe90334</a>	Missing Instance ID in unified_events-2.log

Bug ID	Headline
<a href="#">CSCwe93137</a>	KP - multimode: ASA traceback observed during HA node break and rejoin.
<a href="#">CSCwe93176</a>	Snort2 rule assignments missing from ngfw.rules (assignment_data table ) after FMC upgrade.
<a href="#">CSCwe93736</a>	ASA not updating Timezone despite taking commands
<a href="#">CSCwe97939</a>	ASA/FTD Cluster: Change "cluster replication delay" with max value increase from 15 to 50 sec
<a href="#">CSCwf00736</a>	CSM backup failed within FMC backup due to modification of file while tar was reading it
<a href="#">CSCwf08387</a>	LSP version not updated to latest in LINA Prompt in SSP_CLUSTER with 7.2.4 build.
<a href="#">CSCwf08790</a>	FMC Restore of remote backup fails due to no space left on the device
<a href="#">CSCwf14031</a>	Snort down due to missing lua files because of disabled application detectors (VDB side)
<a href="#">CSCwf17389</a>	ASA accepts replayed SAML assertions for RA VPN authentication
<a href="#">CSCwf20215</a>	admin user should be excluded from CLI shell access filter
<a href="#">CSCwf22045</a>	MYSQL, or any TCP high traffic, getting blocked by snort3, with snort-block as Drop-reason
<a href="#">CSCwf25563</a>	Device list takes longer to load while creating new AC policy
<a href="#">CSCwf36419</a>	ASA/FTD: Traceback and reload with Thread Name 'PTHREAD'
<a href="#">CSCwf39108</a>	Firewall rings may get stuck and cause packet loss when asp load-balance per-packet auto is used
<a href="#">CSCwf44621</a>	Traceback and reload on Thread DATAPATH-6-21369 and linked to generation of syslog message ID 202010
<a href="#">CSCwf49486</a>	store_*list_history.pl task is created every 5min without getting closed causing FMC slowness.
<a href="#">CSCwf59571</a>	FTD/Lina - ZMQ issue OUT OF MEMORY. due to less Msglyr pool memory on certain platforms
<a href="#">CSCwf63589</a>	FTD snmpd process traceback and restart
<a href="#">CSCwf64590</a>	Units get kicked out of the cluster randomly due to HB miss   ASA 9.16.3.220
<a href="#">CSCwf67337</a>	FMC taking long times to save override objects even if not modified
<a href="#">CSCwf69880</a>	Firewall Traceback and reload due to SNMP thread
<a href="#">CSCwf75695</a>	Duplicate FTD cluster has been created when multiple cluster events comes at same time

Bug ID	Headline
<a href="#">CSCwf82447</a>	Editing identity nat rule disables "perform route lookup" silently
<a href="#">CSCwf82970</a>	Snort2 engine is crashing after enabling TLS Server Identity Discovery feature
<a href="#">CSCwf86557</a>	Decrypting engine/ssl connections hang with PKI Interface Error seen
<a href="#">CSCwf89959</a>	ASA: ISA3000 does not respond to entPhySensorValue OID SNMP polls
<a href="#">CSCwf91282</a>	import of .SFO to FMC failed due to included local/custom rules having a blank rule message field
<a href="#">CSCwf92661</a>	ASA/FTD: Traceback & reload due to a free buffer corruption
<a href="#">CSCwf92726</a>	LDAP missing files after upgrade when the Vault token is corrupted
<a href="#">CSCwf94450</a>	FTD Lina traceback Thread Name: DATAPATH due to memory corruption
<a href="#">CSCwf99303</a>	Management UI presents self-signed cert rather than custom CA signed one after upgrade
<a href="#">CSCwh00123</a>	In Multi-manager scenario,cdFMC&Analytics FMC,FTD should only receive identity feeds from Config FMC
<a href="#">CSCwh01673</a>	FTD /ngfw disk space full from Snort3 url db files
<a href="#">CSCwh04231</a>	FMC needs to properly maintain Redis data directory to prevent unbounded disk usage
<a href="#">CSCwh09113</a>	FPR1010 in HA failed to send or receive to GARP/ARP with error "edsa_rcv: out_drop"
<a href="#">CSCwh11411</a>	Snort blacklisting traffic during deployment
<a href="#">CSCwh14352</a>	Lina CiscoSSL upgrade to 1.1.1v and FOM 7.3a
<a href="#">CSCwh14584</a>	Traceback seen on FTD running on Firepower 2100 series
<a href="#">CSCwh14863</a>	FTD 7.0.4 cluster drops Oracle's sqlnet packets due to tcp-not-syn
<a href="#">CSCwh16759</a>	SNMP is not working on the primary active ASA unit in multi-context environment
<a href="#">CSCwh19475</a>	Intermittently flow is getting white-listed by the snort for the unknow app-id traffic.
<a href="#">CSCwh19613</a>	ASA crashed with Saml scenarios
<a href="#">CSCwh19897</a>	ASA/FTD Cluster: Reuse of TCP Randomized Sequence number on two different conns with same 5 tuple
<a href="#">CSCwh21474</a>	ASA traceback when re-configuring access-list
<a href="#">CSCwh21772</a>	Upgrade FxOS CiscoSSL to version 1.1.1v and FOM 7.3a
<a href="#">CSCwh24901</a>	'Frequent drain of events (not unprocessed events) to be removed from FMC
<a href="#">CSCwh26526</a>	SQL packets involved in large query is drop by SNORT3 with reason snort-block

Bug ID	Headline
<a href="#">CSCwh28206</a>	Firewall Blocking packets after failover due to IP &lt;-&gt; SGT mappings
<a href="#">CSCwh30346</a>	ASA/FTD: 1 Second failover delay for each NLP NAT rule
<a href="#">CSCwh36005</a>	Policy deployment failed due to "1 errors seen during populateGlobalSnapshot"
<a href="#">CSCwh40106</a>	FTD hosted on KP incorrectly dropping decoded ESP packets if pre-filter action is analyze
<a href="#">CSCwh40294</a>	ASA traceback due to panic event during SNMP configuration
<a href="#">CSCwh41126</a>	FMC ACP report does not shows all the access control rules
<a href="#">CSCwh42077</a>	Cisco_Firepower_GEODB_FMC_Update* are not included in diskmanager
<a href="#">CSCwh42412</a>	FTD Block 9344 leak due to fragmented GRE traffic over inline-set interface inner-flow processing
<a href="#">CSCwh45450</a>	2100: Interfaces missing from FTD after removing interfaces as members of a port-channel
<a href="#">CSCwh45935</a>	Lina core observed in 6.4.0.17-22 in Kp with scaled traffic
<a href="#">CSCwh47053</a>	ASA/FTD may traceback and reload in Thread Name 'dns_cache_timer'
<a href="#">CSCwh47701</a>	ASA allows same BGP Dynamic routing process for Physical Data and management-only interfaces
<a href="#">CSCwh49244</a>	"show aaa-server" command always shows the Average round trip time 0ms.
<a href="#">CSCwh53745</a>	ASA: unexpected logs for initiating inbound connection for DNS query response
<a href="#">CSCwh57976</a>	Improve CPU utilization in ssl inspection for supported signature algorithm handling
<a href="#">CSCwh58467</a>	ASA does not sent 'warmstart' snmp trap
<a href="#">CSCwh59199</a>	ASA/FTD traceback and reload with IPSec VPN, possibly involving upgrade
<a href="#">CSCwh60504</a>	LINA would randomly generate a traceback and reload on FPR-1K
<a href="#">CSCwh60604</a>	ASA/FTD may traceback and reload in Thread Name 'lina' while processing DAP data
<a href="#">CSCwh60631</a>	Fragmented UDP packet via MPLS tunnel reassemble fail
<a href="#">CSCwh60783</a>	FTD - Captive portal enabled is still running despite the feature is off
<a href="#">CSCwh62080</a>	additional command outputs needed in FTD troubleshoot for blocks and ssl cache
<a href="#">CSCwh65128</a>	LINA show tech-support fails to generate as part of sf_troubleshoot.pl (Troubleshoot file)
<a href="#">CSCwh66359</a>	ASDM can not see log timestamp after enable logging timestamp on cli
<a href="#">CSCwh68482</a>	FTD: Traceback and Reload in Process Name: lina

Bug ID	Headline
<a href="#">CSCwh68878</a>	Diskmanager process terminated unexpectedly
<a href="#">CSCwh69156</a>	FTD-HA does not fail over sometimes when snort3 crashes
<a href="#">CSCwh69346</a>	ASA: Traceback and reload when restore configuration using CLI
<a href="#">CSCwh70323</a>	Timestamp entry missing for some syslog messages sent to syslog server
<a href="#">CSCwh70481</a>	Community string sent from router is not matching ASA
<a href="#">CSCwh71161</a>	ASA FTD: Traceback & reload in thread Name: update_mem_reference
<a href="#">CSCwh71665</a>	ASA traceback under match_partial_keyword during CPU profiling
<a href="#">CSCwh73727</a>	Snort3 dropping IP protocol 51
<a href="#">CSCwh74586</a>	XTLS: With TSID AC-Policy configured plugin is not disengaging immediately at CH
<a href="#">CSCwh75829</a>	FMC Primary disk degraded error
<a href="#">CSCwh77348</a>	ASA: Traceback and reload when executing the command "show nat pool detail" on a cluster setup
<a href="#">CSCwh79095</a>	Snort generating an excessive number of snort-unified log files with zero bytes
<a href="#">CSCwh83254</a>	ASA/FTD: Traceback and reload on thread name CP Crypto Result Processing
<a href="#">CSCwh84376</a>	In FPR4200/FPR3100-cluster observed core file ?core.lina? observed on device reboot.
<a href="#">CSCwh91065</a>	Lina Traceback : Thread Name: DATAPATH during session terminate
<a href="#">CSCwh91574</a>	FTD: Traceback in threadname cli_xml_request_process
<a href="#">CSCwh92345</a>	crypto_archive file generated after the software upgrade.
<a href="#">CSCwh92541</a>	Random FTD snort3 traceback
<a href="#">CSCwh93710</a>	Last Rule hit shows a hex value ahead of current time in ASA and ASDM
<a href="#">CSCwh95010</a>	Unexpected traceback on thread name Lina and device experienced reboot
<a href="#">CSCwh95025</a>	GTP connections, under certain circumstances do not get cleared on issuing clear conn.
<a href="#">CSCwh95175</a>	ASA/FTD may traceback and reload in Thread Name 'lina'
<a href="#">CSCwh95277</a>	FTD VMWARE 7.0.5 trackbacks due to system memory exhaustion
<a href="#">CSCwh96055</a>	Management DNS Servers may be unreachable if data interface is used as the gateway
<a href="#">CSCwh99331</a>	syslog not generated "ASA-3-202010: NAT pool exhausted" while passing traffic from iLinux to oLinux
<a href="#">CSCwi01085</a>	FTD VMWare tracebacks at PTHREAD-3587



Bug ID	Headline
<a href="#">CSCwi01381</a>	ASA/FTD may traceback and reload in Thread Name 'lina'
<a href="#">CSCwi02134</a>	FTD sends multiple replicated NetFlow records for the same flow event
<a href="#">CSCwi02754</a>	FTD 1120 standby sudden reboot
<a href="#">CSCwi03407</a>	Traceback on FP2140 without any trigger point.
<a href="#">CSCwi04351</a>	FTD upgrade failling on script 999_finish/999_??_install_bundle.sh
<a href="#">CSCwi11520</a>	FTD OSPFV3 IPV6 Routing: FTD is sending unsupported extended LSA request to neighbor routers
<a href="#">CSCwi14896</a>	Node kicked out of cluster while enabling or disabling rule profiling
<a href="#">CSCwi15409</a>	ASA/FTD - may traceback and reload in Thread Name 'Unicorn Proxy Thread'
<a href="#">CSCwi15595</a>	ASA traceback and reload during ACL configuration modification
<a href="#">CSCwi16998</a>	CCM Seq 58 - LTS18
<a href="#">CSCwi18581</a>	Firewall traceback and reload due to SSH thread
<a href="#">CSCwi18663</a>	FMC-4600: Pre-Filter policy is showing as none
<a href="#">CSCwi19145</a>	FTD/ASA may traceback and reload in PKI, syslog, during upgrade
<a href="#">CSCwi19485</a>	Fail open snort-down is off in inline pairs despite it being enabled and deployed from FMC
<a href="#">CSCwi19849</a>	VPN load-balancing cluster encryption using Phase 2 deprecated ciphers
<a href="#">CSCwi20045</a>	ASA/FTD may traceback and reload in Thread Name 'lina' due to a watchdog in 9.16.3.23 code
<a href="#">CSCwi20848</a>	ASA/FTD high memory usage due to SNMP caused by RAVPN OID polling
<a href="#">CSCwi20955</a>	FTD with may traceback in data-path during deployment when enabling TAP mode
<a href="#">CSCwi21625</a>	FailSafe admin password is not properly sync'd with system context enable pw
<a href="#">CSCwi26895</a>	ASA SNMP OID cpmCPUTotalPhysicalIndex returning zero values instead of CPU index values
<a href="#">CSCwi27338</a>	Stale asp entry for TCP 443 remains on standby after changing default port
<a href="#">CSCwi27402</a>	FTD: Update WM firmware to 1023.0207
<a href="#">CSCwi27459</a>	Snort Crash during selection of signature algorithm ECDSA
<a href="#">CSCwi31091</a>	OSPF Redistribution route-map with prefix-list not working after upgrade
<a href="#">CSCwi31558</a>	file-extracts.logs are not recognised by the diskmanager leading to High disk space

Bug ID	Headline
<a href="#">CSCwi31966</a>	FTD ADI debugs may show incorrect server_group and/or realm_id for SAML-authenticated sessions
<a href="#">CSCwi32063</a>	ASA/FTD: SSL VPN Second Factor Fields Disappear
<a href="#">CSCwi32759</a>	Username-from-certificate secondary attribute is not extracted if the first attribute is missing
<a href="#">CSCwi33817</a>	ASA/FTD: 'IKEv2 Negotiation aborted due to ERROR: Platform errors' during a rekey
<a href="#">CSCwi34125</a>	ASA: Snmpwalk shows "No Such Instance" for the OID ceSensorExtThresholdValue
<a href="#">CSCwi34719</a>	Unable to SSH into FTD device using External authentication with Radius
<a href="#">CSCwi36311</a>	use kill tree function in SMA instead of SIGTERM
<a href="#">CSCwi38061</a>	ASA/FTD traceback and reload due to file descriptor limit being exceeded
<a href="#">CSCwi40193</a>	Hairpinning of DCE/RPC traffic during the suboptimal lookup
<a href="#">CSCwi40487</a>	FTD HA Failure after SNORT crash.
<a href="#">CSCwi40536</a>	ASA/FTD: Traceback and reload when running show tech and under High Memory utilization condition
<a href="#">CSCwi42962</a>	installing GeoDB country code package update to FMC does not automatically push updates to FTDs
<a href="#">CSCwi42992</a>	ASA/FTD may traceback and reload in Thread Name IKEv2 Daemon
<a href="#">CSCwi43782</a>	GTP inspection dropping packets with IE 152 due to header length being invalid for IE type 152
<a href="#">CSCwi44208</a>	low memory/stress causing traceback in SNMP
<a href="#">CSCwi46010</a>	ASA/FTD: Cluster incorrectly generating syslog 202010 for invalid packets destined to PAT IP
<a href="#">CSCwi46023</a>	FTD drops double tagged BPDUs.
<a href="#">CSCwi48699</a>	ASA traceback and reload on Thread Name: pix_flash_config_thread
<a href="#">CSCwi49884</a>	TCP MSS is changed back to the default value when a VTI or loopback interface is created
<a href="#">CSCwi50343</a>	Their standalone FTD running 7.2.2 on FPR-4112 experienced a traceback on the SNMP module
<a href="#">CSCwi53150</a>	Service object-group protocol type mismatch error seen while access-list referencing already
<a href="#">CSCwi53431</a>	Unable to Synch more then 100 environment-data with data unit
<a href="#">CSCwi55938</a>	The "show asp drop" command usage requires better updates for cluster-related drops

Bug ID	Headline
<a href="#">CSCwi56048</a>	Interface fragment queue may get stuck at 2/3 of fragment database size
<a href="#">CSCwi59525</a>	Multiple lina cores on 7.2.6 KP2110 managed by cdFMC
<a href="#">CSCwi59831</a>	ASA/FTD may traceback and reload in Thread Name 'lina'
<a href="#">CSCwi60285</a>	ASA/FTD may traceback and reload in Thread Name 'lina'
<a href="#">CSCwi63113</a>	Null pointer dereference in SNMP that results in traceback and reload
<a href="#">CSCwi63743</a>	ASA/FTD may traceback and reload in Thread Name "appAgent_monitor_nd_thread" & Rip: _lina_assert.
<a href="#">CSCwi64829</a>	traceback and reload around function HA
<a href="#">CSCwi65116</a>	DHCPv6:ASA traceback on Thread Name: DHCPv6 CLIENT.
<a href="#">CSCwi66103</a>	Lina traceback on RAVPN connection after enabling webvpn debug
<a href="#">CSCwi66676</a>	ASA/FTD may traceback and reload in Thread Name 'webvpn_task'
<a href="#">CSCwi74214</a>	ASA/FTD traceback and reload in Thread Name: IKEv2 Daemon when moving from active to standby HA
<a href="#">CSCwi75198</a>	Standby FTD experiencing periodic traceback and reload
<a href="#">CSCwi75967</a>	CCM ID 62 - LTS18
<a href="#">CSCwi76002</a>	Memory exhaustion due to absence of freeing up mechanism for tmatch
<a href="#">CSCwi76361</a>	Transparent firewall MAC filter does not capture frames with STP-UplinkFast dst MAC consistently
<a href="#">CSCwi76630</a>	FP2100/FP1000: ASA Smart licenses lost after reload
<a href="#">CSCwi79042</a>	FTD/Lina traceback and reload of HA pairs, in data path, after adding NAT policy
<a href="#">CSCwi79703</a>	Incorrect Timezone Format on FTD When Configured via FXOS
<a href="#">CSCwi80465</a>	CCM ID 63 - LTS18
<a href="#">CSCwi84615</a>	some stdout logs not rotated by logrotate
<a href="#">CSCwi86198</a>	SFData correlator keep terminating on FTDs configured for IDS
<a href="#">CSCwi86503</a>	File sizes larger than 100MB for AnyConnect/Secure Client images cannot be uploaded on FMC
<a href="#">CSCwi87382</a>	Traceback and reload on Primary unit while running debugs over the SSH session
<a href="#">CSCwi90040</a>	Cisco ASA and FTD Software Command Injection Vulnerability
<a href="#">CSCwi90371</a>	ASA:request to add "logging list" option to the "logging history" command.

Bug ID	Headline
<a href="#">CSCwi90399</a>	FTD/ASA system clock resets to year 2023
<a href="#">CSCwi90571</a>	Access to website via Clientless SSL VPN Fails
<a href="#">CSCwi95228</a>	"crypto ikev2 limit queue sa_init" resets after reboot
<a href="#">CSCwi95708</a>	FTD: Hostname Missing from Syslog Message
<a href="#">CSCwi95994</a>	Chromium-based browsers have SSL connection conflicts when FIPS CC is enabled on the firewall.
<a href="#">CSCwi97839</a>	FTD traceback assert in vni_idb_get_mode and reloaded
<a href="#">CSCwi98284</a>	Cisco ASA and FTD Software Persistent Local Code Execution Vulnerability
<a href="#">CSCwj02505</a>	ASA Checkheaps traceback while entering same engineID twice
<a href="#">CSCwj09110</a>	Upload files through Clientless portal is not working as expected after the ASA upgrade
<a href="#">CSCwj10955</a>	Cisco ASA and FTD Software Web Services Denial of Service Vulnerability
<a href="#">CSCwj12131</a>	Bailout when lina_io_write fails persistent with EPIPE errno.

## Resolved Bugs in Version 7.0.6.1

Table last updated: 2024-05-22

*Table 42: Resolved Bugs in Version 7.0.6.1*

Bug ID	Headline
<a href="#">CSCvt25221</a>	FTD traceback in Thread Name cli_xml_server when deploying QoS policy
<a href="#">CSCvx04003</a>	Lack of throttling of ARP miss indications to CP leads to oversubscription
<a href="#">CSCvx54562</a>	High System Overhead memory on FTD
<a href="#">CSCvy81493</a>	traceback and reload with 'CHECKHEAPS HAS DETECTED A MEMORY CORRUPTION'
<a href="#">CSCvz07439</a>	Smart Lic Agent stuck in waiting state after failover and continuously switches from lock and unlock
<a href="#">CSCwa70323</a>	Unable to push extra domains >1024 Character, as part of Custom Attribute under Anyconnect VPN
<a href="#">CSCwc78781</a>	ASA/FTD may traceback and reload during ACL changes linked to PBR config
<a href="#">CSCwc82205</a>	ASA/FTD may traceback and reload in Thread Name 'lina'
<a href="#">CSCwd10822</a>	Failover trigger due to Inspection engine in other unit has failed due to disk failure

Bug ID	Headline
<a href="#">CSCwd28037</a>	TPK: No nameif during traffic causes the device traceback, lina core is generated.
<a href="#">CSCwd38583</a>	ASA/FTD: Command "no snmp-server enable oid mempool" enabled by default or enforced during upgrades
<a href="#">CSCwd66820</a>	Cisco Firepower Management Center Object Group Access Control List Bypass Vulnerability
<a href="#">CSCwd83141</a>	CCL/CLU filters are not working correctly
<a href="#">CSCwd89095</a>	Stratix5950 and ISA3000 LACP channel member SFP port suspended after reload
<a href="#">CSCwe04043</a>	FTD-HA upgrade failed
<a href="#">CSCwe12705</a>	multimode-tmatch_df_hijack_walk traceback observed during shut/unshut on FO connected switch interfa
<a href="#">CSCwe28407</a>	LINA traceback with icmp_thread
<a href="#">CSCwe28912</a>	FPR 4115- primary unit lost all HA config after ftd HA upgrade
<a href="#">CSCwe42061</a>	Deleting a BVI in FTD interfaces is causing packet drops in other BVIs
<a href="#">CSCwe51443</a>	ASA Evaluation of OpenSSL vulnerability CVE-2022-4450
<a href="#">CSCwe67816</a>	ASA / FTD Traceback and reload when removing isakmp capture
<a href="#">CSCwe74089</a>	ASA/FTD may traceback and reload in Thread Name DATAPATH-1-1656
<a href="#">CSCwe79051</a>	Deployment for eigrp / bgp change may cause temporary outage during policy apply
<a href="#">CSCwe82704</a>	PortChannel sub-interfaces configured as data/data-sharing, in multi-instance HA go into "waiting"
<a href="#">CSCwe83255</a>	ASA/FTD may traceback and reload in Thread Name 'lina'
<a href="#">CSCwe86225</a>	ASA/FTD traceback and reload due citing thread name: cli_xml_server in tm_job_add
<a href="#">CSCwf04460</a>	The fxos directory disappears after cancel show tech fprm detail command with Ctr+c is executed .
<a href="#">CSCwf05295</a>	FTD running on FP1000 series might drop packets on TLS flows after the "Client Hello" message.
<a href="#">CSCwf10910</a>	FTD : Traceback in ZMQ running 7.3.0
<a href="#">CSCwf14126</a>	ASA Traceback and reload citing process name 'lina'
<a href="#">CSCwf15902</a>	ASAv in Hyper-V drops packets on management interface
<a href="#">CSCwf16559</a>	getReadinessStatusTaskList pjb request is very frequent when user in Upgrade sensor list page

Bug ID	Headline
<a href="#">CSCwf17042</a>	ASDM replaces custom policy-map with default map on class inspect options at backup restore.
<a href="#">CSCwf22005</a>	ASA Packet-tracer displays the first ACL rule always, though matches the right ACL
<a href="#">CSCwf22637</a>	Network Object Group overrides not visible or be edited from FMC GUI
<a href="#">CSCwf25144</a>	FMC backup management page showing "Verifying Backup" for FTD sensors.
<a href="#">CSCwf26407</a>	FP2130- Unable to disassociate member from port channel, deployment fails, member is lost on FTD/FMC
<a href="#">CSCwf26534</a>	ASA/FTD: Connection information in SIP-SDP header remains untranslated with destination static Any
<a href="#">CSCwf33904</a>	[IMS_7_4_0] - Virtual FDM Upgrade fails: HA configStatus='OUT_OF_SYNC after UpgradeOnStandby
<a href="#">CSCwf34500</a>	FTD: GRE traffic is load balanced between CPU cores
<a href="#">CSCwf35207</a>	ASA: Traceback and reload while updating ACLs on ASA
<a href="#">CSCwf35233</a>	Cisco Adaptive Security Appliance Software and Firepower Threat Defense DoS
<a href="#">CSCwf35573</a>	Traffic may be impacted if TLS Server Identity probe timeout is too long
<a href="#">CSCwf39163</a>	ASAv - High latency is experienced on Azure environment for ICMP ping packets while running snmpwalk
<a href="#">CSCwf43537</a>	Lina crash in thread name: cli_xml_request_process during FTD cluster upgrade
<a href="#">CSCwf44537</a>	99.20.1.16 lina crash on nat_remove_policy_from_np
<a href="#">CSCwf47227</a>	Priority-queue command causes silent egress packet drops on all port-channel interfaces
<a href="#">CSCwf48599</a>	VPN load-balancing cluster encryption using deprecated ciphers
<a href="#">CSCwf49573</a>	ASA/FTD: Traceback and reload when issuing 'show memory webvpn all objects'
<a href="#">CSCwf50497</a>	DNS cache entry exhaustion leads to traceback
<a href="#">CSCwf52810</a>	ASA SNMP polling not working and showing "Unable to honour this request now" on show commands
<a href="#">CSCwf54418</a>	Reduce time taken to clear stale IKEv2 SAs formed after Duplicate Detection
<a href="#">CSCwf54510</a>	ASA traceback and reload on Thread Name: DHCPRA Monitor
<a href="#">CSCwf56811</a>	ASA Traceback & reload on process name lina due to memory header validation
<a href="#">CSCwf59176</a>	FXOS raises a fault for administratively disabled management interface
<a href="#">CSCwf60311</a>	ASA generating traceback with thread-name: DATAPATH-53-18309 after upgrade to 9.16.4.19

Bug ID	Headline
<a href="#">CSCwf60590</a>	"show route all summary" executed on transparent mode FTD is causing CLISH to become Sluggish.
<a href="#">CSCwf62729</a>	7.0.6 - Lina Crash in RAVPN interface with anomaly traffic in both non-FIPS and FIPS mode
<a href="#">CSCwf63872</a>	FTD taking longer than expected to form OSPF adjacencies after a failover switchover
<a href="#">CSCwf69901</a>	FTD: Traceback and reload during OSPF redistribution process execution
<a href="#">CSCwf72434</a>	Add meaningful logs when the maximums system limit rules are hit
<a href="#">CSCwf73773</a>	Dumping of last 20 rmu request response packets failed
<a href="#">CSCwf77191</a>	ASA appliance mode - 'connect fxos [admin]' will get ERROR: failed to open connection.
<a href="#">CSCwf78321</a>	ASA: Checkheaps traceback and reload due to Clientless WebVPN
<a href="#">CSCwf81058</a>	FTD: Firepower 3100 Dynamic Flow Offload showing as Enabled
<a href="#">CSCwf82247</a>	Policy deployment fails when a route same prefix/metric is configured in a separate VRF.
<a href="#">CSCwf92135</a>	ASA: Traceback and reload on Tread name "fover_FSM_thread" and ha_ntfy_prog_process_timer
<a href="#">CSCwf92182</a>	Cisco Firepower Management Center Software SQL Injection Vulnerability
<a href="#">CSCwf92646</a>	ECDSA Self-signed certificate using SHA384 for EC521
<a href="#">CSCwf94677</a>	"failover standby config-lock" config is lost after both HA units are reloaded simultaneously
<a href="#">CSCwf95147</a>	OSPFv3 Traffic is Centralized in Transparent Mode
<a href="#">CSCwf95288</a>	FPR1k Switchport passing CDP traffic
<a href="#">CSCwh04365</a>	ASA Traceback & reload on process name lina due to memory header validation - webvpn side fix
<a href="#">CSCwh04395</a>	ASDM application randomly exits/terminates with an alert message on multi-context setup
<a href="#">CSCwh04730</a>	ASA/FTD HA checkheaps crash where memory buffers are corrupted
<a href="#">CSCwh06452</a>	Interface speed mismatch in SNMP response using OID .1.3.6.1.2.1.2.2
<a href="#">CSCwh08403</a>	FMC HA - Health Policy - Applied count shows "0" appliance
<a href="#">CSCwh08481</a>	ASA traceback on Lina process with FREEB and VPN functions
<a href="#">CSCwh11764</a>	ASA/FTD may traceback and reload in Thread Name "RAND_DRBG_bytes" and CTM function on n5 platforms

Bug ID	Headline
<a href="#">CSCwh12987</a>	Large SMB servers result in timeouts returning verdicts between FMC and FTD devices
<a href="#">CSCwh13821</a>	ASA/FTD may traceback and reload in when changing capture buffer size
<a href="#">CSCwh14467</a>	File sizes bigger than 100MB for AnyConnect/Secure Client images cannot be uploaded on FMC
<a href="#">CSCwh14597</a>	ASA/FTD residual free
<a href="#">CSCwh16301</a>	Incorrect Hit count statistics on ASA Cluster only for Cluster-wide output
<a href="#">CSCwh20002</a>	Standby FMC is not getting updated with latest GEO DB package
<a href="#">CSCwh21141</a>	The FMC preview deployment shows a wrong information.
<a href="#">CSCwh23100</a>	Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
<a href="#">CSCwh23567</a>	PAC Key file missing on standby on reload
<a href="#">CSCwh25668</a>	ASA 55xx devices running 7.0.6 show up as 100% usage on CPU01 [LINA]
<a href="#">CSCwh27230</a>	Connections are not cleared after idle timeout when the interfaces are in inline mode.
<a href="#">CSCwh28144</a>	Specific OID 1.3.6.1.2.1.25 should not be responding
<a href="#">CSCwh30891</a>	ASA/FTD may traceback and reload in Thread Name 'ssh' when adding SNMPV3 config
<a href="#">CSCwh31495</a>	FTD - Traceback and reload due to nat rule removed by CPU core
<a href="#">CSCwh32118</a>	ASDM management-sessions quota reached due to HTTP sessions stuck in CLOSE_WAIT
<a href="#">CSCwh37475</a>	Removal of msie-proxy commands during flexconfig rollback
<a href="#">CSCwh41127</a>	ASA/FTD: NAT64 error "overlaps with inside standby interface address" for Standalone ASA
<a href="#">CSCwh45108</a>	Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
<a href="#">CSCwh49483</a>	ASA/FTD may traceback and reload while running show inventory all
<a href="#">CSCwh50060</a>	Some TLS1.3 probes test site cases fail due to rst+ack not sent out of FTD during timeout
<a href="#">CSCwh52420</a>	AMP Cloud look up timeout frequently.
<a href="#">CSCwh56945</a>	SFDataCorrelator crashing repeatedly in RNA_DB_InsertServiceInfo
<a href="#">CSCwh64508</a>	Fixing the regression caused while handling web UI is not getting FTDv Variable
<a href="#">CSCwh69209</a>	Prefilter cannot add Tunnel Endpoints in Tunnel Rule on FMC
<a href="#">CSCwh69815</a>	FTDvs through put got changed to 100Kbps after upgrade



## Resolved Bugs in Version 7.0.6

Table last updated: 2024-05-22

**Table 43: Resolved Bugs in Version 7.0.6**

Bug ID	Headline
<a href="#">CSCvo58100</a>	Incorrect validation msg - Invalid value supplied for input parameter : "?"
<a href="#">CSCvq20057</a>	Improve logging of Secure Firewall (Firepower)backups and retry for gzip when using remote storage
<a href="#">CSCvq25866</a>	Flex config Preview of \$SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST throws error
<a href="#">CSCvr45136</a>	Adding details and logs when gzip fails and results in backup failure
<a href="#">CSCvs27336</a>	Traceback on ASA by Smart Call Home process
<a href="#">CSCvt35116</a>	Cisco Firepower Management Center Software Information Disclosure Vulnerability
<a href="#">CSCvu24703</a>	FTD - Flow-Offload should be able to coexist with Rate-limiting Feature (QoS)
<a href="#">CSCvu96436</a>	Traceback of master and one slave when a particular lock is contended for long
<a href="#">CSCvv59757</a>	FMC event report generation fails if one is already running
<a href="#">CSCvw82067</a>	ASA/FTD 9344 blocks depleted due to high volume of fragmented traffic
<a href="#">CSCvx04436</a>	Forbidden to run multiple SFDaCo processes, but pidfile not successful at blocking second instance
<a href="#">CSCvx21458</a>	FMC shows error when editing prefix-list attached to active route-map within BGP protocol
<a href="#">CSCvx24207</a>	FQDN Object Containing IPv4 and IPv6 Addresses Only Install IPv6 Entries
<a href="#">CSCvx27744</a>	Policy deployment may fail on FTD after 6.6.1 due to failure to get version upgrade information
<a href="#">CSCvx36885</a>	ASA Traceback & reload in thread Name: DATAPATH
<a href="#">CSCvx52042</a>	Upgrade to 6.6.1 got failed at 800_post/1025_vrf_policy_upgrade.pl
<a href="#">CSCvx55978</a>	Performance Degradation in GetGroupDependency API
<a href="#">CSCvx56021</a>	FTD: CTS SGT propagation gets enabled after reload
<a href="#">CSCvx59181</a>	Email/SNMP/Syslog Health Alerts are not sent out of fmc for cpu and mem
<a href="#">CSCvx65032</a>	FMC ACL Search Move arrows do not work
<a href="#">CSCvx67856</a>	Prometheus process doesnt come up when system ungracefully rebooted

Bug ID	Headline
<a href="#">CSCvx71936</a>	FXOS: Fault "The password encryption key has not been set." displayed on FPR1000 and FPR2100 devices
<a href="#">CSCvx97723</a>	hmdaemon process restart during automation test
<a href="#">CSCvy12991</a>	Chassis local date and time may drift back to midnight Jan 1 2015 after reboot
<a href="#">CSCvy16537</a>	Some externalization columns do not match any data when used in where clause
<a href="#">CSCvy24435</a>	FMC GUI can be accessed by an expired password when using .cgi with https://FMCIP/login.cgi
<a href="#">CSCvy26511</a>	Tune unmanaged disk alert thresholds for low end platforms
<a href="#">CSCvy26676</a>	"Warning:Update failed/in-progress." Cosmetic after successful update
<a href="#">CSCvy33879</a>	FTD: repair_users.pl creates rogue .firstboot file that causes FTD reboot failure
<a href="#">CSCvy35737</a>	FTD traceback and reload during anyconnect package verification
<a href="#">CSCvy40493</a>	Selective policy deployment of AC Policy does not export to ngfw.rules
<a href="#">CSCvy50598</a>	BGP table not removing connected route when interface goes down
<a href="#">CSCvy50797</a>	Policy deployment may fail if platform settings contain DH group1 for SSL
<a href="#">CSCvy52617</a>	FMC6.7 changes IPSec Profiles on VTI with each deployment resulting in tunnel flap
<a href="#">CSCvy55676</a>	FMC Deployment failed due to internal errors
<a href="#">CSCvy57905</a>	VTI tunnel interface stays down post reload on KP/WM platform in HA
<a href="#">CSCvy63414</a>	Deploy Preview & Rollback not working when config archival is corrupted
<a href="#">CSCvy65178</a>	Need dedicated Rx rings for to the box BGP traffic on Firepower platform
<a href="#">CSCvy65770</a>	ASA/FTD: Traceback and reload during BGP route update
<a href="#">CSCvy67765</a>	FTD VTI reports TUNNEL_SRC_IS_UP false despite source interface is up/up and working
<a href="#">CSCvy73130</a>	FP4100 platform: Active-Standby changed to dual Active after running "show conn" command
<a href="#">CSCvy84336</a>	Add a warning when member interfaces of the port-channel are different between active and standby
<a href="#">CSCvy86817</a>	Cruz ASIC CLU filter has the incorrect src/dst IP subnet when a custom CCL IP subnet is set
<a href="#">CSCvy88023</a>	FP2100 coredumps do not display the original crashing thread
<a href="#">CSCvy90836</a>	ASA Traceback and reload in Thread Name: SNMP ContextThread

Bug ID	Headline
<a href="#">CSCvy91668</a>	PAT pool exhaustion with stickiness traffic could lead to new connection drop.
<a href="#">CSCvy98458</a>	FP21xx -traceback "Panic:DATAPATH-10-xxxx -remove_mem_from_head: Error - found a bad header"
<a href="#">CSCvz07712</a>	Deployment fails with internal_errors - Cannot get fresh id
<a href="#">CSCvz09106</a>	Cisco ASA and FTD Software SSL VPN Denial of Service Vulnerability
<a href="#">CSCvz10428</a>	FMC Health monitoring standby FMC unit does not have data displayed for CPU
<a href="#">CSCvz20679</a>	FTDv - Lina Traceback and reload
<a href="#">CSCvz22668</a>	FMC backup restoration may fail due to VMS database restoration failure
<a href="#">CSCvz24765</a>	device rebooted with snmpd core
<a href="#">CSCvz28145</a>	Error "Another operation by another user prevented this operation. Please retry after sometime."
<a href="#">CSCvz29656</a>	FMC connection event search causing high memory utilization for index.cgi
<a href="#">CSCvz29976</a>	Malware event processing may misbehave with "already part of another table" error
<a href="#">CSCvz34289</a>	In some cases transition to lightweight proxy doesn't work for Do Not Decrypt flows
<a href="#">CSCvz36903</a>	ASA traceback and reload while allocating a new block for cluster keepalive packet
<a href="#">CSCvz37306</a>	ASDM session is not served for new user after doing multiple context switches in existing user
<a href="#">CSCvz38332</a>	FTD/ASA - Stuck in boot loop after upgrade from 9.14.2.15 to 9.14.3
<a href="#">CSCvz38692</a>	ASAv traceback in snmp_master_callback_thread and reload
<a href="#">CSCvz39646</a>	ASA/AnyConnect - Stale RADIUS sessions
<a href="#">CSCvz40098</a>	FTD HA: Health Monitor page shows "Error in fetching device details Error: validation failed"
<a href="#">CSCvz40245</a>	Firepower bandwidth_analyzer tool calculates results in MBps instead of Mbps
<a href="#">CSCvz41551</a>	FP2100: ASA/FTD with threat-detection statistics may traceback and reload in Thread Name 'lina'
<a href="#">CSCvz42065</a>	IPS policy should be imported when its referred in Access Control policy
<a href="#">CSCvz42553</a>	Alarm: Health Alert Smart Licensing Agent not running
<a href="#">CSCvz43414</a>	Internal ldap attribute mappings fail after HA failover
<a href="#">CSCvz43455</a>	ASAv observed traceback while upgrading hostscan

Bug ID	Headline
<a href="#">CSCvz44339</a>	FTD - Deployment will fail if you try to delete an SNMP host with ngfw-interface and host-group
<a href="#">CSCvz48407</a>	Traceback and reload in Thread Name: DATAPATH-15-18621
<a href="#">CSCvz49163</a>	Observed some time drift in seconds in the output when we execute show rule hits multiple times
<a href="#">CSCvz50712</a>	TLS server discovery uses incorrect source IP address for probes in AnyConnect deployment
<a href="#">CSCvz51175</a>	FTD HA not forming when SNMP adminState is disabled
<a href="#">CSCvz53142</a>	ASA does not use the interface specified in the name-server command to reach IPv6 DNS servers
<a href="#">CSCvz53372</a>	Snort goes into D state after executing "config log-events-to-ramdisk disable"
<a href="#">CSCvz54318</a>	Policy deployment failure: "No LSP package found in the active lsp directory"
<a href="#">CSCvz55302</a>	FTD/ASA Traceback and reload due to SSL null checks under low memory conditions
<a href="#">CSCvz55395</a>	TCP connections are cleared after configured idle-timeout even though traffic is present
<a href="#">CSCvz57710</a>	conf t is converted to disk0:/t under context-config mode
<a href="#">CSCvz58710</a>	ASA traceback due to SCTP traffic.
<a href="#">CSCvz60142</a>	ASA/FTD stops serving SSL connections
<a href="#">CSCvz61160</a>	ASA traceback on DATAPATH when handling ICMP error message
<a href="#">CSCvz61477</a>	RAVPN Authorization fails if same RADIUS server is used as authentication and authorization server
<a href="#">CSCvz62653</a>	ASA memory leak resulting in error messages and causing tracebacks
<a href="#">CSCvz64470</a>	ASA/FTD Traceback and reload due to memory corruption when generating ICMP unreachable message
<a href="#">CSCvz66236</a>	Threshold mis-behavior of "-1" after configuring Type:Both for specific rule
<a href="#">CSCvz67003</a>	ASDM session count and quota management's count mismatch. 'Lost connection firewall' msg in ASDM
<a href="#">CSCvz68713</a>	PLR license reservation for ASAv5 is requesting ASAv10
<a href="#">CSCvz69571</a>	ASA log shows wrong value of the transferred data after the anyconnect session terminated.
<a href="#">CSCvz69729</a>	Unstable client processes may cause LINA zmqio traceback on FTD
<a href="#">CSCvz70316</a>	LINA may generate traceback and reload

Bug ID	Headline
<a href="#">CSCvz70595</a>	Cisco ASA Software and FTD Software Web Services Interface Denial of Service Vulnerability
<a href="#">CSCvz71340</a>	observed snort3 core on xTLSServerKeyExchangeProcessor
<a href="#">CSCvz71542</a>	No messages displayed on the console for any inserted SFP cable after removal.
<a href="#">CSCvz71596</a>	"Number of interfaces on Active and Standby are not consistent" should trigger warning syslog
<a href="#">CSCvz73709</a>	ASA/FTD Standby unit fails to join HA
<a href="#">CSCvz75988</a>	Inconsistent logging timestamp with RFC5424 enabled
<a href="#">CSCvz76652</a>	Proxy URI URL for URL Filtering (beaker service) includes encoded user/password strings
<a href="#">CSCvz77213</a>	FTD: show ntp shows managing DC even though NTP sync is done via FXOS
<a href="#">CSCvz77662</a>	Crash at data-path from Scaled AC-SSL TVM Profile test.
<a href="#">CSCvz77744</a>	OSPFv3: FTD Wrong "Forwarding address" added in ospfv3 database
<a href="#">CSCvz78548</a>	Unable to load Devices --> Certificates page
<a href="#">CSCvz81480</a>	Cisco ASA Software and FTD Software IPsec IKEv2 VPN Information Disclosure Vulnerability
<a href="#">CSCvz81513</a>	FMC - Backup failing due to "CSM backup failed"
<a href="#">CSCvz84850</a>	ASA/FTD traceback and reload caused by "timer services" function
<a href="#">CSCvz85493</a>	FTD backup.log increased size out of control to 50GB or more causing /ngfw to 100% full
<a href="#">CSCvz88020</a>	ASAv: coredumpfsys is formatted during bootup
<a href="#">CSCvz91396</a>	FTD: Deployment will fail when AC Policy is huge
<a href="#">CSCvz94841</a>	Grammatical errors in failover operating mode mismatch error message
<a href="#">CSCvz97196</a>	Can't create Flexconfig Object with ldap-naming-attribute pager cause pager is block.
<a href="#">CSCwa03341</a>	Standby's sub interface mac doesn't revert to old mac with no mac-address command
<a href="#">CSCwa04262</a>	Cisco ASA Software SSL VPN Client-Side Request Smuggling Vulnerability via "/"URI
<a href="#">CSCwa27253</a>	FMC : Device Listing Page Slowness
<a href="#">CSCwa27488</a>	Fail to import with error "is not a table"
<a href="#">CSCwa31488</a>	FDM High Availability cannot be created using Etherchannel as failover interface.

Bug ID	Headline
<a href="#">CSCwa32956</a>	Connection events are not sent to Firepower Management Center due to deploy race condition
<a href="#">CSCwa35596</a>	Registered devices may miss on standby FMC due to AnyConnect HostScan class files sync failure
<a href="#">CSCwa36535</a>	Standby unit failed to join failover due to large config size.
<a href="#">CSCwa41936</a>	Cisco FTD Bleichenbacher Attack Vulnerability
<a href="#">CSCwa43311</a>	Snort blocking and dropping packet, with bigger size(1G) file download
<a href="#">CSCwa45369</a>	Execution of commands appears to result in a new zombie process
<a href="#">CSCwa47737</a>	ASA/FTD may hit a watchdog traceback related to snmp config writing
<a href="#">CSCwa49480</a>	SNMP OID , stop working after around one hour and a half - FTD
<a href="#">CSCwa59907</a>	LINA observed traceback on thread name "snmp_client_callback_thread"
<a href="#">CSCwa61361</a>	ASAv traceback when SD_WAN ACL enabled, then disabled (or vice-versa) in PBR
<a href="#">CSCwa62025</a>	IPv6: Some of egress interfaces of global and user vrf routes are missing in asp table
<a href="#">CSCwa68004</a>	FMC 7.0 FlexConfig blocked mac-address-table aging-time for transparent FTD without any alternativ
<a href="#">CSCwa68552</a>	All type-8 passwords are lost upon upgrade from ASA 9.12-9.15 to 9.16, failover gets disabled
<a href="#">CSCwa72481</a>	API key corrupted for FMC with multiple interfaces
<a href="#">CSCwa72528</a>	user-name from certificate feature does not work with SER option
<a href="#">CSCwa72530</a>	FTD: Time gap/mismatch seen when new node joins a Cluster Control node under history
<a href="#">CSCwa72929</a>	SNMPv3 polling may fail using privacy algorithms AES192/AES256
<a href="#">CSCwa73172</a>	ASA reload and traceback in Thread Name: PIX Garbage Collector
<a href="#">CSCwa75966</a>	ASA: Reload and Traceback in Thread Name: Unicorn Proxy Thread with Page fault: Address not mapped
<a href="#">CSCwa79604</a>	Infinitely running jobs in the task list
<a href="#">CSCwa79905</a>	FMC NAT Policy report generation does not record the rules every 51*x
<a href="#">CSCwa82850</a>	ASA Failover does not detect context mismatch before declaring joining node as "Standby ready"
<a href="#">CSCwa87298</a>	ASA conn data-rate: incorrect "current rate" and "data-rate-filter" doesn't work properly
<a href="#">CSCwa89116</a>	Clean up session index handling in IKEv2/SNMP/Session-mgr for MIB usage

Bug ID	Headline
<a href="#">CSCwa89560</a>	NAT rule modification after rule search changes rule order
<a href="#">CSCwa94440</a>	syncd process exits due to invalid GID and database synchronization issue
<a href="#">CSCwa95079</a>	ASA/FTD Traceback and reload due to NAT configuration
<a href="#">CSCwa96860</a>	Failover high convergence causes traffic failures
<a href="#">CSCwa96920</a>	ASA/FTD may traceback and reload in process Lina
<a href="#">CSCwa97423</a>	Deployment rollback causes brief traffic drop due to order of operations
<a href="#">CSCwa97917</a>	ISA3000 in boot loop after powercycle
<a href="#">CSCwa99931</a>	ASA/FTD: Tuning of update_mem_reference process
<a href="#">CSCwb00871</a>	ENH: Reduce latency in log_handler_file to reduce watchdog under scale or stress
<a href="#">CSCwb02060</a>	snmp-group host with Invalid host range and subnet causing traceback and reload
<a href="#">CSCwb02955</a>	Modify /800_post/1027_ldap_external_auth_fix.pl to not fail FMC upgrade when objects are corrupt
<a href="#">CSCwb03702</a>	SSH: missing null pointer check leading to snort traceback and reload
<a href="#">CSCwb03704</a>	ASA/FTD datapath threads may run into deadlock and generate traceback
<a href="#">CSCwb04000</a>	ASA/FTD: DF bit is being set on packets routed into VTI
<a href="#">CSCwb04975</a>	FTD Snort3 traceback in daq-pdts while handling FQDN based traffic
<a href="#">CSCwb05148</a>	Cisco ASA Software and FTD Software SNMP Denial of Service Vulnerability
<a href="#">CSCwb05291</a>	Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability
<a href="#">CSCwb05920</a>	Crash in KP at webVpn free, HTTPCleanUp and mem_mh_free from Scaled AC-IK/IPSec TVM test.
<a href="#">CSCwb06575</a>	Windows 11 OS is not selectable when creating a DAP record via FMC
<a href="#">CSCwb06847</a>	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-9-11543'
<a href="#">CSCwb07908</a>	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
<a href="#">CSCwb07981</a>	Traceback: Standby FTD reboots and generates crashinfo and lina core on thread name cli_xml_server
<a href="#">CSCwb08189</a>	Microsoft update traffic blocked with Snort version 3 Malware inspection
<a href="#">CSCwb08644</a>	ASA/FTD traceback and reload at IKEv2 from Scaled S2S+AC-DTLS+SNMP long duration test
<a href="#">CSCwb09606</a>	FP2100: ASA/FTD high availability is not resilient to unexpected lacp process termination

Bug ID	Headline
<a href="#">CSCwb10874</a>	Ensure DB consistency when synchronizing users
<a href="#">CSCwb12476</a>	vm_max size for MonetDB is not set programmatically, which can lead to a setting of zero
<a href="#">CSCwb16037</a>	Unable to replace the anyconnect image when maximum memory used for anyconnect images.
<a href="#">CSCwb16920</a>	CPU profile cannot be reactivated even if previously active memory tracking is disabled
<a href="#">CSCwb17187</a>	SNMP cores are generated every minute while running snmpwalk on HA
<a href="#">CSCwb17963</a>	Unable to identify dynamic rate limiting mechanism & not following msg limit per/sec at syslog server.
<a href="#">CSCwb19387</a>	ASA SNMP Poll is failing & show display "Unable to honour this request now.Please try again later."
<a href="#">CSCwb19648</a>	SNMP queries for crasLocalAddress are not returning the assigned IPs for SSL/DTLS tunnels.
<a href="#">CSCwb20206</a>	FTD: Logs and Debugs for SSL/TLS traffic drop due to NAP in Detection Mode
<a href="#">CSCwb22592</a>	SSH Functionalty stopped working after running long duration tests of SCP + Scaled TVM VPN Profiles
<a href="#">CSCwb24039</a>	ASA traceback and reload on routing
<a href="#">CSCwb24306</a>	duplicate log entry for /mnt/disk0/log/asa_snmp.log
<a href="#">CSCwb25809</a>	Single Pass - Traceback due to stale ifc
<a href="#">CSCwb28123</a>	FTD HA deployment fails with error "Deployment failed due to major version change on device"
<a href="#">CSCwb28427</a>	ssl rule with appid condition may get matched incorrectly, potentially causing connection failure
<a href="#">CSCwb31551</a>	When inbound packet contains SGT header, FPR2100 cannot distribute properly per 5 tuple
<a href="#">CSCwb31699</a>	Primary takes active role after reload
<a href="#">CSCwb32267</a>	Crash on KP Active node while clearing vpnsessiondb with AnyConnect-SSL TVM Profile running
<a href="#">CSCwb32721</a>	Syslog IDs 725021 and 725022 are not listed as valid IDs
<a href="#">CSCwb32790</a>	Replace log4j with slf4j
<a href="#">CSCwb32841</a>	NAT (any,any) statements in-states the failover interface and resulting on Split Brain events
<a href="#">CSCwb38961</a>	Bootstrap After Upgrade failed due to Duplicate Key of Network Object



Bug ID	Headline
<a href="#">CSCwb40001</a>	Long delays when executing SNMP commands
<a href="#">CSCwb41739</a>	debug crypto conditional need to be made multi-ctx aware
<a href="#">CSCwb43018</a>	Implement SNP API to check ifc and ip belongs to HA LU or CMD interface
<a href="#">CSCwb43433</a>	Jumbo frame performance has degraded up to -45% on Firepower 2100 series
<a href="#">CSCwb43629</a>	License and rule counts telemetry data incorrectly generated for HA managed devices
<a href="#">CSCwb44848</a>	ASA/FTD Traceback and reload in Process Name: lina
<a href="#">CSCwb46481</a>	SNMPv3 not working after upgrade of FMC
<a href="#">CSCwb50405</a>	ASA/FTD Traceback in crypto hash function
<a href="#">CSCwb51707</a>	ASA Traceback and reload in process name: lina
<a href="#">CSCwb51821</a>	Disk usage errors on Firepower Azure device due to large backup unified files under ngfw directory
<a href="#">CSCwb52401</a>	Cisco Firepower Threat Defense Software Privilege Escalation Vulnerability
<a href="#">CSCwb53172</a>	FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated
<a href="#">CSCwb53191</a>	Certificate validation fails post upgrade to 9.17.1
<a href="#">CSCwb53328</a>	ASA/FTD Traceback and reload caused by Smart Call Home process sch_dispatch_to_url
<a href="#">CSCwb54791</a>	ASA DHCP server fails to bind reserved address to Linux devices
<a href="#">CSCwb56905</a>	ASA blocking 0.0.0.0 IP and netmask combination in SSH/TELNET/HTTP config
<a href="#">CSCwb57213</a>	FTD - Unable to resolve DNS when only diagnostic interface is used for DNS lookups
<a href="#">CSCwb57615</a>	Configuring pbr access-list with line number failed.
<a href="#">CSCwb58554</a>	Resumed SSL sessions with uncached tickets may fail to complete
<a href="#">CSCwb58817</a>	FMC Deploying negative and positive form of BGP password command across deployments
<a href="#">CSCwb59218</a>	Unable to save DAP Endpoint Criteria as "Disabled"
<a href="#">CSCwb59465</a>	ASA/FTD may traceback (watchdog) and reload when generating a syslog from the VPN Failover subsystem
<a href="#">CSCwb59488</a>	ASA/FTD Traceback in memory allocation failed
<a href="#">CSCwb61402</a>	FMC: LDAP shell login may fail if LDAP server is slow to query the DNS servers for users
<a href="#">CSCwb64551</a>	FMC Backup failure- Monetdb backup failure code 102

Bug ID	Headline
<a href="#">CSCwb66761</a>	Cisco Firepower Threat Defense Software Generic Routing Encapsulation DoS Vulnerability
<a href="#">CSCwb67040</a>	FP4112 4115 Traceback & reload on Thread Name: netfs_thread_init
<a href="#">CSCwb68642</a>	ASA traceback in Thread Name: SXP CORE
<a href="#">CSCwb69503</a>	ASA unable to configure aes128-gcm@openssh.com when FIPS enabled
<a href="#">CSCwb71460</a>	ASA traceback in Thread Name: fover_parse and triggered by snmp related functions
<a href="#">CSCwb73248</a>	FW traceback in timer infra / netflow timer
<a href="#">CSCwb74571</a>	PBR not working on ASA routed mode with zone-members
<a href="#">CSCwb76423</a>	ASA/FTD traceback and reload when checking CRL
<a href="#">CSCwb78323</a>	Update diskmanager to monitor cisco_uridb files in /ngfw/var/sf/cloud_download folder.
<a href="#">CSCwb79812</a>	RIP is advertising all connected Anyconnect users and not matching route-map for redistribution
<a href="#">CSCwb80559</a>	FTD offloads SGT tagged packets although it should not
<a href="#">CSCwb80862</a>	ASA/FTD proxy arps any traffic when using the built-in 'any' object in translated destination
<a href="#">CSCwb82796</a>	ASA/FTD firewall may traceback and reload when tearing down IKE tunnels
<a href="#">CSCwb83388</a>	ASA HA Active/standby tracebacks seen approximately every two months.
<a href="#">CSCwb83691</a>	ASA/FTD traceback and reload due to the initiated capture from FMC
<a href="#">CSCwb84901</a>	CIAM: heimdal 1.0.1
<a href="#">CSCwb85633</a>	Snmpwalk output of memory does not match show memory/show memory detail
<a href="#">CSCwb86118</a>	TPK ASA: Device might get stuck on ftp copy to disk
<a href="#">CSCwb87498</a>	Lina traceback and reload during EIGRP route update processing.
<a href="#">CSCwb87950</a>	Cisco ASA Software and FTD Software Web Services Interface Denial of Service Vulnerability
<a href="#">CSCwb88406</a>	FMC-HA upgrade failure due to presence of this file "update.status"
<a href="#">CSCwb88651</a>	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
<a href="#">CSCwb88729</a>	FTD - %FTD-3-199015: port-manager: Error: DOM Block Read failure, port X, st = X log false/positive
<a href="#">CSCwb89963</a>	ASA Traceback & reload in thread name: Datapath

Bug ID	Headline
<a href="#">CSCwb90074</a>	ASA: Multiple Context Mixed Mode SFR Redirection Validation
<a href="#">CSCwb90532</a>	ASA/FTD traceback and reload on NAT related function nat_policy_find_location
<a href="#">CSCwb91101</a>	SNMP interface threshold doesn't trigger properly when traffic sent to interface ~4gbps
<a href="#">CSCwb91598</a>	copying FMC backup to remote storage will fail if FMC has never connected via SSH/SCP to remote host
<a href="#">CSCwb92709</a>	We can't monitor the interface via "snmpwalk" once interface is removed from context.
<a href="#">CSCwb93932</a>	ASA/FTD failover pair traceback and reload due to connection replication race condition
<a href="#">CSCwb94190</a>	ASA graceful shut down when applying ACL's with forward reference feature and FIPS enabled.
<a href="#">CSCwb94312</a>	Unable to apply SSH settings to ASA version 9.16 or later
<a href="#">CSCwb95453</a>	ASA: The timestamp for all logs generated by Admin context are the same
<a href="#">CSCwb97251</a>	ASA/FTD may traceback and reload in Thread Name 'ssh'
<a href="#">CSCwb97486</a>	FPR3100: 25G optic may show link up on some 1/10G capable only fiber ports
<a href="#">CSCwb99375</a>	Config sync fails for command "quit"
<a href="#">CSCwc00115</a>	FTD registration fails on on-prem FMC
<a href="#">CSCwc02488</a>	ASA/FTD may traceback and reload in Thread Name 'None'
<a href="#">CSCwc02700</a>	Fragmented packets are dropped when unit leaves cluster
<a href="#">CSCwc03069</a>	Interface internal data0/0 is up/up from cli but up/down from SNMP polling
<a href="#">CSCwc03332</a>	FTD on FP2100 can take over as HA active unit during reboot process
<a href="#">CSCwc03507</a>	No-buffer drops on Internal Data interfaces despite little evidence of CPU hog
<a href="#">CSCwc05434</a>	FMC shows 'File Not Stored' after download a file
<a href="#">CSCwc07015</a>	snort3 crash due to NULL pointer in TLS Client Hello Evaluation
<a href="#">CSCwc07262</a>	Standby ASA goes to booting loop during configuration replication after upgrade to 9.16(3).
<a href="#">CSCwc08374</a>	Azure ASA NIC MAC address for Gigeth 0/1 and 0/2 become out of order when adding interfaces
<a href="#">CSCwc09414</a>	ASA/FTD may traceback and reload in Thread Name 'ci/console'
<a href="#">CSCwc10483</a>	ASA/FTD - Traceback in Thread Name: appAgent_subscribe_nd_thread
<a href="#">CSCwc10792</a>	ASA/FTD IPSEC debugs missing reason for change of peer address and timer delete

Bug ID	Headline
<a href="#">CSCwc11511</a>	FTD: SNMP failures after upgrade to 7.0.2
<a href="#">CSCwc11597</a>	ASA tracebacks after SFR was upgraded to 6.7.0.3
<a href="#">CSCwc11663</a>	ASA traceback and reload when modifying DNS inspection policy via CSM or CLI
<a href="#">CSCwc13017</a>	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
<a href="#">CSCwc13477</a>	FMC   Interface update Failed. Could not find source interface
<a href="#">CSCwc13994</a>	ASA - Restore not remove the new configuration for an interface setup after backup
<a href="#">CSCwc18285</a>	Conn data-rate command can be enabled or disabled in unprivileged user EXEC mode
<a href="#">CSCwc18312</a>	"show nat pool cluster" commands run within EEM scripts lead to traceback and reload
<a href="#">CSCwc18524</a>	ASA/FTD Voltage information is missing in the command "show environment"
<a href="#">CSCwc18668</a>	Failed user login on FMC does not record entry in audit log when using external authentication
<a href="#">CSCwc19124</a>	FMC Deployment does not start for cluster devices
<a href="#">CSCwc22170</a>	Issue with snort perfstat parsing / Hmdeamon not starting after disk full reported
<a href="#">CSCwc23356</a>	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-20-7695'
<a href="#">CSCwc23695</a>	ASA/FTD can not parse UPN from SAN field of user's certificate
<a href="#">CSCwc23844</a>	ASAv high CPU and stack memory allocation errors despite over 30% free memory
<a href="#">CSCwc24906</a>	ASA/FTD traceback and reload on Thread id: 1637
<a href="#">CSCwc26648</a>	ASA/FTD Traceback and Reload in Thread name Lina or Datatath
<a href="#">CSCwc27424</a>	Unable to removed not used SAL On-Premise FMC configuration
<a href="#">CSCwc27797</a>	ASA mgmt ip cannot be released
<a href="#">CSCwc27846</a>	Traceback and Reload while HA sync after upgrading and reloading.
<a href="#">CSCwc28334</a>	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
<a href="#">CSCwc28532</a>	9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing
<a href="#">CSCwc28806</a>	ASA Traceback and Reload on process name Lina
<a href="#">CSCwc28928</a>	ASA: SLA debugs not showing up on VTY sessions
<a href="#">CSCwc30573</a>	Deployment/Tasks Button not seen FMC_UI while doing upgrade tests configured in Light theme
<a href="#">CSCwc32245</a>	FMC: Validation check to prevent exponential expansion of NAT rules

Bug ID	Headline
<a href="#">CSCwc32246</a>	NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used
<a href="#">CSCwc33036</a>	Observed Logs at syslog server side as more than configured message limit per/sec.
<a href="#">CSCwc35181</a>	OSPF template adds "default-information-originate" to area <area-id> nssa statement on hitting OK.
<a href="#">CSCwc36905</a>	ASA traceback and reload due to "Heap memory corrupted at slib_malloc.c
<a href="#">CSCwc37256</a>	SSL AnyConnect access blocked after upgrade
<a href="#">CSCwc38567</a>	ASA/FTD may traceback and reload while executing SCH code
<a href="#">CSCwc39525</a>	FMC HA status alert "degraded - maintenance" seen periodically after upgrade
<a href="#">CSCwc40381</a>	ASA : HTTPS traffic authentication issue with Cut-through Proxy enabled
<a href="#">CSCwc41293</a>	Firepower module show-tech file generation may fail with error "Failed to create archive!"
<a href="#">CSCwc41592</a>	False positives for Ultrasurf
<a href="#">CSCwc42174</a>	CIAM: mariadb - multiple versions CVE-2022-32081
<a href="#">CSCwc42561</a>	Deploy page listing takes 1.5 to 2 mins with 462 HA device
<a href="#">CSCwc43807</a>	FTD is unusable post reboot if manager is deleted and FIPS is enabled
<a href="#">CSCwc44289</a>	FTD - Traceback and reload when performing IPv4 <math>\leftrightarrow</math> IPv6 NAT translations
<a href="#">CSCwc44608</a>	Selective deployment of IPS may cause outage due to incorrectly written FTD configuration files
<a href="#">CSCwc45108</a>	ASA/FTD: GTP inspection causing 9344 sized blocks leak
<a href="#">CSCwc45397</a>	ASA HA - Restore in primary not remove new interface configuration done after backup
<a href="#">CSCwc48375</a>	Inbound IPSEC SA stuck inactive - many inbound SPIs for one outbound SPI in "show crypto ipsec sa"
<a href="#">CSCwc48853</a>	SFDataCorrelator Discovery Event bottleneck can cause Connection Event delay and backlog
<a href="#">CSCwc49095</a>	ASA/FTD 2100 platform traceback and reload when fragments are coalesced and sent to PDTS
<a href="#">CSCwc49364</a>	mojo_server processes unnecessarily restarting during log rotation
<a href="#">CSCwc50519</a>	Excessive logging from hm_du.pm may lead to syslog-ng process restarts
<a href="#">CSCwc50846</a>	FTD Upgrade Fail - Readiness Check Successful, but Readiness status never shown

Bug ID	Headline
<a href="#">CSCwc50887</a>	FTD - Traceback and reload on NAT IPv4<->IPv6 for UDP flow redirected over CCL link
<a href="#">CSCwc50891</a>	MPLS tagging removed by FTD
<a href="#">CSCwc51326</a>	FXOS-based Firepower platform showing 'no buffer' drops despite high values for RX ring watermarks
<a href="#">CSCwc51588</a>	Failing to generate FMC Backup/Restore via SMB/SSH
<a href="#">CSCwc52351</a>	ASA/FTD Cluster Split Brain due to NAT with "any" and Global IP/range matching broadcast IP
<a href="#">CSCwc53280</a>	ASA parser accepts incomplete network statement under OSPF process and is present in show run
<a href="#">CSCwc54217</a>	syslog related to failover is not outputted in FPR2140
<a href="#">CSCwc54901</a>	Scheduled tasks may not run on active FMC in HA after switchover or split-brain resolution
<a href="#">CSCwc54984</a>	IKEv2 rekey - Responding Invalid SPI for the new SPI received right after Create_Child_SA response
<a href="#">CSCwc56003</a>	Trigger FTD backup with remote storage option enabled along with retrieval to FMC fails
<a href="#">CSCwc56952</a>	Able to see the SLA debug logs on both console & VTY sessions even if we enable only on VTY session.
<a href="#">CSCwc57575</a>	FMC: Scheduled backups working fine, but FMC email alerts displaying it failed.
<a href="#">CSCwc60037</a>	ASA fails to rekey with IPSEC ERROR: Failed to allocate an outbound hardware context
<a href="#">CSCwc60227</a>	FMC-GUI bypass session timeout while staying in any Event tab if Refresh Interval is enabled
<a href="#">CSCwc61912</a>	ASA/FTD OSPFv3 does not generate messages Type 8 LSA for IPv6
<a href="#">CSCwc62215</a>	FTD unable to sync HA due to snort validation failed
<a href="#">CSCwc63273</a>	SFDataCorrelator host timeout query can block event processing and cause a deadlock restart
<a href="#">CSCwc64333</a>	FMC GUI timeout and issues with loading http page due to exceeded http connections
<a href="#">CSCwc64923</a>	ASA/FTD may traceback and reload in Thread Name 'lina' ip routing ndbshr
<a href="#">CSCwc66757</a>	ASA/FTD may traceback and reload in Thread Name 'lina'
<a href="#">CSCwc67687</a>	ASA HA failover triggers HTTP server restart failure and ASDM outage
<a href="#">CSCwc67886</a>	ASA/FTD may traceback and reload in Thread Name 'lina_notify_file_monitor_thread'

Bug ID	Headline
<a href="#">CSCwc68543</a>	mismatch in the config pushed from FMC and running config on FTD
<a href="#">CSCwc68656</a>	ASA CLI for TCP Maximum unprocessed segments
<a href="#">CSCwc69583</a>	Portchannel configured from FDM breaks "Use the Data Interfaces as the Gateway" for Mgmt interface
<a href="#">CSCwc70962</a>	FTD/ASA "Write Standby" enables ECDSA ciphers causing AC SSLv3 handshake failure
<a href="#">CSCwc72155</a>	ASA/FTD Traceback and reload on function "snp_cluster_trans_allocb"
<a href="#">CSCwc72284</a>	TACACS Accounting includes an incorrect IPv6 address of the client
<a href="#">CSCwc73224</a>	Call home configuration on standby device is lost after reload
<a href="#">CSCwc74099</a>	FPR2140 ASA Clock Timezone reverts to UTC after appliance restart/reload
<a href="#">CSCwc74103</a>	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-11-32591'
<a href="#">CSCwc74271</a>	Auth-Daemon process is getting restarted continuously when SSO disabled
<a href="#">CSCwc74378</a>	FMC UI should disallow simultaneous deactivation of FMC interface management and event channels
<a href="#">CSCwc74841</a>	FMC RSS Feed broken because FeedBurner is no longer active - "Unable to parse feed"
<a href="#">CSCwc74858</a>	FTD - Traceback in Thread Name: DATAPATH
<a href="#">CSCwc77519</a>	FPR1000 ASA/FTD: Primary takes active role after reloading
<a href="#">CSCwc77680</a>	FTD may traceback and reload in Thread Name 'DATAPATH-0-4948'
<a href="#">CSCwc79366</a>	During the deployment time, device got stuck processing the config request.
<a href="#">CSCwc80234</a>	"inspect snmp" config difference between active and standby
<a href="#">CSCwc80357</a>	[Deploy Performance] degrade in deployment page on FMC
<a href="#">CSCwc81184</a>	ASA/FTD traceback and reload caused by SNMP process failure
<a href="#">CSCwc81219</a>	Intrusion events intermittently stop appearing in FMC when using snort3
<a href="#">CSCwc81727</a>	Default Domain in VPN group policy objects cannot be deleted
<a href="#">CSCwc81960</a>	Unable to configure 'match ip address' under route-map when using object-group in access list
<a href="#">CSCwc82188</a>	FTD Traceback and reload when applying long commands from FMC UI or CLISH
<a href="#">CSCwc86330</a>	Vulnerabilities in spring-framework - multiple versions CVE-2022-22970
<a href="#">CSCwc86391</a>	On slow networks with some packets loss sftunnel may mark connections as STALE

Bug ID	Headline
<a href="#">CSCwc87441</a>	for system processes limit the CPUs used to the number of system CPUs
<a href="#">CSCwc88108</a>	Prefilter policy - Available port menu long response time, Prefilter Network Search takes long time
<a href="#">CSCwc88897</a>	ASA traceback and reload due to null pointer in Umbrella after modifying DNS inspection policy
<a href="#">CSCwc89661</a>	FTD reboots due to heartbeat loss and "Communication with NPU lost"
<a href="#">CSCwc89796</a>	ASA/FTD may traceback and reload in Thread Name 'appagent_async_client_receive_thread' hog detection
<a href="#">CSCwc89924</a>	FXOS ASA/FTD SNMP OID to poll Internal-data 'no buffer' interface counters
<a href="#">CSCwc90091</a>	ASA 9.12(4)47 with user-statistics, will affects the "policy-server xxxx global" visibility.
<a href="#">CSCwc92761</a>	7.3 - Message flood by Use of uninitialized value \$unix_time in numeric gt
<a href="#">CSCwc93166</a>	Using write standby in a user context leaves secondary firewall license status in an invalid state
<a href="#">CSCwc93687</a>	Error message while editing ACP
<a href="#">CSCwc94085</a>	Unable to establish DTLSv1.2 with FIPS enabled after upgrade from 6.6.5.
<a href="#">CSCwc94466</a>	Cisco ASA/FTD Firepower 2100 SSL/TLS Denial of Service Vulnerability
<a href="#">CSCwc94501</a>	ASA/FTD memory leak and tracebacks due to ctm_n5 resets
<a href="#">CSCwc95290</a>	ESP rule missing in vpn-context may cause IPSec traffic drop
<a href="#">CSCwc96016</a>	Captive portal support in cross domain
<a href="#">CSCwc96805</a>	traceback and reload due to tcp intercept stat in thread unicorn
<a href="#">CSCwc99242</a>	ISA3000 LACP channel member SFP port suspended after reload
<a href="#">CSCwd00386</a>	ASA/FTD may traceback and reload when clearing the configuration due to "snp_clear_acl_log_flow_all"
<a href="#">CSCwd00778</a>	ifAdminStatus output is abnormal via snmp polling
<a href="#">CSCwd01032</a>	ASA/FTD may traceback and reload when RAVPN with SAML is configured
<a href="#">CSCwd02864</a>	logging/syslog is impacted by SNMP traps and logging history
<a href="#">CSCwd03113</a>	FMC local backup fails cause of "Update Task: Database integrity check failed" - Syslog server issue
<a href="#">CSCwd03793</a>	FTD Traceback and reload
<a href="#">CSCwd03810</a>	ASA Custom login page is not working through webvpn after an upgrade



Bug ID	Headline
<a href="#">CSCwd04210</a>	ASA: ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT
<a href="#">CSCwd05814</a>	PDTS write from Daq can fail when PDTS buffer is full eventually leads to block depletion
<a href="#">CSCwd06005</a>	ASA/FTD Cluster Traceback and Reload during node leave
<a href="#">CSCwd07059</a>	multiple snort3 crashes after upgrading FTD from 7.2.0 to 7.2.0.1
<a href="#">CSCwd08430</a>	Create a resiliency configuration option for SFTunnel to support HA and FTD connectivity
<a href="#">CSCwd10121</a>	Invalid query seen in MonetDB merovingian.log
<a href="#">CSCwd10497</a>	FTD sensor rules missing from ngfw.rules file after a sensor backup restore execution
<a href="#">CSCwd10760</a>	Firewall_rule_cache may not pruned for many years for some customers
<a href="#">CSCwd10880</a>	critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on 2100/3100 devices
<a href="#">CSCwd11005</a>	Missing fqdns_old.conf file causes FTD HA app sync failure
<a href="#">CSCwd11165</a>	"Move" option is greyed out on Backup-Restore in FMC
<a href="#">CSCwd11303</a>	ASA might generate traceback in ikev2 process and reload
<a href="#">CSCwd11855</a>	ASA/FTD may traceback and reload in Thread Name 'ikev2_fo_event'
<a href="#">CSCwd11963</a>	Error message seen in the log "Error operation timed out getting CriticalStatus from PM."
<a href="#">CSCwd13083</a>	FMC - Unable to initiate deployment due to incorrect threat license validation
<a href="#">CSCwd13917</a>	during download from file event on FMC, high CPU use on FMC for 20 minutes before download fails
<a href="#">CSCwd14432</a>	"Inspection Interruption" is seen as YES but snort3 didn't restart
<a href="#">CSCwd14688</a>	FTD upgrade failure due to Syslog files getting generated/deleted rapidly
<a href="#">CSCwd14972</a>	ASA/FTD Traceback and Reload in Thread Name: pix_flash_config_thread
<a href="#">CSCwd16017</a>	Object edit slowness when it is associated with NAT rules
<a href="#">CSCwd16294</a>	GTP inspection drops packets for optional IE Header Length being too short
<a href="#">CSCwd16517</a>	GTP drops not always logged on buffer and syslog
<a href="#">CSCwd16689</a>	ASA/FTD traceback due to block data corruption
<a href="#">CSCwd16712</a>	Device readiness upgrade check failure - sftunnel sync issue due to time change

Bug ID	Headline
<a href="#">CSCwd16902</a>	File events show Action as "Malware Block" for files with correct disposition of unknown
<a href="#">CSCwd17037</a>	SFDataCorrelator RNA-Stop action should not block when database operations are hung
<a href="#">CSCwd17856</a>	ASA goes for traceback/reload with message - snmp_ma_kill_restart: vf is NULL
<a href="#">CSCwd17940</a>	HA did not failover due to misleading status updates from NDClient
<a href="#">CSCwd18744</a>	FPR1K FTD fails to form HA due to reason "Other unit has different set of hwidb index"
<a href="#">CSCwd19053</a>	ASA/FTD may traceback with large number of network objects deployment using distribute-list
<a href="#">CSCwd20627</a>	ASA/FTD: NAT configuration deployment failure
<a href="#">CSCwd20900</a>	HTTP Block Response and Interactive Block response pages not being displayed by Snort3
<a href="#">CSCwd22413</a>	EIGRPv6 - Crashed with "mem_lock: Assertion mem_refcount' failed" on LINA.
<a href="#">CSCwd22907</a>	ASA/FTD High CPU in SNMP Notify Thread
<a href="#">CSCwd23188</a>	ASA/FTD may traceback and reload in Thread Name 'lina'
<a href="#">CSCwd23913</a>	FTD in HA traceback multiple times after adding a BGP neighbour with prefix list.
<a href="#">CSCwd25201</a>	ASA/FTD SNMP traps enqueued when no SNMP trap server configured
<a href="#">CSCwd25256</a>	ASA/FTD Transactional Commit may result in mismatched rules and traffic loss
<a href="#">CSCwd26466</a>	Incorrect Frequent Drain of Connection Events alert
<a href="#">CSCwd26867</a>	Device should not move to Active state once Reboot is triggered
<a href="#">CSCwd28236</a>	standby unit using both active and standby IPs causing duplicate IP issues due to nat "any"
<a href="#">CSCwd29835</a>	log rotate failing to cycle files, resulting in large file sizes
<a href="#">CSCwd30296</a>	Device Metrics Not Working After Upgrade to 7.0.3 from pre -7.0.0 version
<a href="#">CSCwd30298</a>	FTD: FTPS Data Channel connection impacted by TLS Server Identity and Discovery Probe sent by FTD
<a href="#">CSCwd30774</a>	FMC HA - files in tmp/Sync are left on secondary when synchronisation task fails
<a href="#">CSCwd30977</a>	FMC deleted some access-rules due to an incorrect delta generated during the policy deployment.
<a href="#">CSCwd31181</a>	Lina traceback and reload - VPN parent channel (SAL) has an invalid underlying channel

Bug ID	Headline
<a href="#">CSCwd32952</a>	Active and Standby device details not available in FMC logs during FTD HA break
<a href="#">CSCwd33054</a>	DHCP Relay is looping back the DHCP offer packet causing dhcprelay to fail on the FTD/ASA
<a href="#">CSCwd33811</a>	Cluster registration is failing because DATA_NODE isn't joining the cluster
<a href="#">CSCwd34288</a>	FP1000 - During boot process in LINA mode, broadcasts leaked between interfaces resulting in storm
<a href="#">CSCwd34662</a>	LTS18 and LTS21 commit id update in CCM layer (seq 39)
<a href="#">CSCwd37238</a>	TLS connections to Exchange 2007 server may fail
<a href="#">CSCwd38526</a>	FMC can allow deployment of NAP in test mode with Decrypt policy
<a href="#">CSCwd38774</a>	ASA: Traceback and reload due to clientless webvpn session closure
<a href="#">CSCwd38775</a>	ASA/FTD may traceback and reload in Thread lina
<a href="#">CSCwd38805</a>	Syslog 106016 is not rate-limited by default
<a href="#">CSCwd39039</a>	FMC - Error message "The server response was not understood. Please contact support." on UI
<a href="#">CSCwd39468</a>	ASA/FTD Traceback and reload when configuring ISAKMP captures on device
<a href="#">CSCwd39506</a>	SSL Policy DND default Rule fails on error unsupported cipher suite and SKE error.
<a href="#">CSCwd40141</a>	Firepower Management Center GUI view for Snort2 Local Intrusion Rules is missing
<a href="#">CSCwd40260</a>	Serviceability Enhancement - Unable to parse payload are silently drop by ASA/FTD
<a href="#">CSCwd41083</a>	ASA traceback and reload due to DNS inspection
<a href="#">CSCwd41224</a>	FMC HA webUI is not getting FTDv Variable tier assigned FTDv - Variable
<a href="#">CSCwd41466</a>	Re-downloaded users from a forest with trusted domains may become unresolved/un-synchronized
<a href="#">CSCwd41806</a>	deployment failed with OOM (out of memory) for policy_apply.pl process
<a href="#">CSCwd42072</a>	SRU installation failure.
<a href="#">CSCwd42347</a>	FMC not showing any alerts/warnings when deploying changes of prefix list with same seq #
<a href="#">CSCwd43666</a>	Analyze why there is no logrotate for /opt/cisco/config/var/log/ASAconsole.log
<a href="#">CSCwd44326</a>	Object NAT edit is failing
<a href="#">CSCwd46741</a>	fxos log rotate failing to cycle files, resulting in large file sizes
<a href="#">CSCwd46780</a>	ASA/FTD: Traceback and reload in Thread Name: appAgent_reply_processor_thread

Bug ID	Headline
<a href="#">CSCwd47340</a>	FXOS: memory leak in svc_sam_envAG process
<a href="#">CSCwd47424</a>	Device name always shows as 'firepower' in CDO event view
<a href="#">CSCwd47442</a>	800_post/1027_ldap_external_auth_fix.pl upgrade error -- reference to missing authentication object
<a href="#">CSCwd47481</a>	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 40)
<a href="#">CSCwd48633</a>	ASA - traceback and reload when Webvpn Portal is used
<a href="#">CSCwd49685</a>	Missing SSL MEMCAP causes deployment failure due timeout waiting for snort detection engines
<a href="#">CSCwd50131</a>	Upgrades are not cleaning up mysql files leading to alert for 'High unmanaged disk usage on /ngfw'
<a href="#">CSCwd50218</a>	ASA restore is not applying vlan configuration
<a href="#">CSCwd51757</a>	Unable to get polling results using snmp GET for connection rate OID's
<a href="#">CSCwd51964</a>	Add validation in lua detector api to check for empty patterns for service apps
<a href="#">CSCwd53135</a>	ASA/FTD: Object Group Search Syslog for flows exceeding threshold
<a href="#">CSCwd53340</a>	FTD PDTS LINA RX queue can become stuck when snort send messages with 4085-4096 bytes size
<a href="#">CSCwd53863</a>	Data migration from Sybase to MariaDB taking more time due to large data size of POLICY_SNAPSHOT
<a href="#">CSCwd54439</a>	FMC gives an irrelevant error message for Snort2 to Snort3 rules conversion failure
<a href="#">CSCwd55673</a>	Need corrections in log_handler_file watchdog crash fix
<a href="#">CSCwd55853</a>	Deployment failure with localpool overlap error after upgrade
<a href="#">CSCwd56254</a>	"show tech-support" generation does not include "show inventory" when run on FTD
<a href="#">CSCwd56296</a>	FTD Lina traceback and reload in Thread Name 'IP Init Thread'
<a href="#">CSCwd56431</a>	Disable asserts in FTD production builds
<a href="#">CSCwd56774</a>	Misleading drop reason in "show asp drop"
<a href="#">CSCwd56995</a>	Clientless Accessing Web Contents using application/octet-stream vs text/plain
<a href="#">CSCwd57698</a>	Recursive panic under lina_duart_write
<a href="#">CSCwd58188</a>	Inline-pair's state could not able to auto recover from hardware-bypass to standby mode.
<a href="#">CSCwd58337</a>	allocate more cgroup memory for policy deployment subgroup

Bug ID	Headline
<a href="#">CSCwd58417</a>	HA Periodic sync is failing due to cfg files are missing
<a href="#">CSCwd58430</a>	At times AC Policy save takes longer time, may be around 10 or above mins
<a href="#">CSCwd58528</a>	Memory depletion while running EMIX traffic profile on QP HA active node
<a href="#">CSCwd59736</a>	ASA/FTD: Traceback and reload due to SNMP group configuration during upgrade
<a href="#">CSCwd61016</a>	ASA: Standby may get stuck in "Sync Config" status upon reboot when there is EEM is configured
<a href="#">CSCwd61082</a>	FMC UI Showing inaccurate data in S2S VPN Monitoring page
<a href="#">CSCwd61410</a>	mdbtrace.log can fill storage on FMC
<a href="#">CSCwd62025</a>	FTDv: Policy Deployment failure due to interface setting on failover interface
<a href="#">CSCwd62138</a>	ASA Connections stuck in idle state when DCD is enabled
<a href="#">CSCwd62729</a>	FDM QW/QP: All URL traffic blocked in BAT/BQT test
<a href="#">CSCwd62915</a>	Cross-domain users with non-ASCII characters are not resolved
<a href="#">CSCwd63580</a>	FPR2100: Increase in failover convergence time with ASA in Appliance mode
<a href="#">CSCwd63961</a>	AC clients fail to match DAP rules due to attribute value too large
<a href="#">CSCwd64919</a>	FXOS is not rotating PoE logs
<a href="#">CSCwd65327</a>	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 41)
<a href="#">CSCwd66815</a>	Lina changes to support - Snort3 traceback in daq-pdts while handling FQDN based traffic
<a href="#">CSCwd67101</a>	FPR1150 : Exec format error seen and the device hung until reload when erase secure all is executed
<a href="#">CSCwd68088</a>	ASA FTD: Implement different TLS diffie-hellman prime based on RFC recommendation
<a href="#">CSCwd69236</a>	FMC Connection Event stop displaying latest event
<a href="#">CSCwd69454</a>	Port-channel interfaces of secondary unit are in waiting status after reload
<a href="#">CSCwd72656</a>	FMC GUI takes long time to load Intrusion Event packet view
<a href="#">CSCwd72680</a>	FXOS: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
<a href="#">CSCwd72915</a>	FMC 7.1.0.1 Doesn't throw warning that S2S VPN Configs contain deprecated MD5 Hash during deployment
<a href="#">CSCwd73981</a>	FMC: Updates page takes more than 5 minutes to load

Bug ID	Headline
<a href="#">CSCwd74116</a>	S2S Tunnels do not come up due to DH computation failure caused by DSID Leak
<a href="#">CSCwd74648</a>	External authentication with Radius server fail with error "This account is currently not available"
<a href="#">CSCwd74839</a>	30+ seconds data loss when unit re-join cluster
<a href="#">CSCwd75738</a>	Predefined FlexConfig Text Objects are not exported by Import-Export
<a href="#">CSCwd75912</a>	ASA SFR is failing registration or not sending events to FMC
<a href="#">CSCwd76634</a>	FMC import takes too long
<a href="#">CSCwd78123</a>	ASA/FTD traceback and reload when IPSec/Ikev2 vpn session bringup with dh group 31 in fips mode
<a href="#">CSCwd78624</a>	ASA configured with HA may traceback and reload with multiple input/output error messages
<a href="#">CSCwd78940</a>	Traps are not getting generated in UUT for config change in multicontext
<a href="#">CSCwd79388</a>	intrusion events fail to migrate from MariaDB to MonetDB following FMC upgrade from 7.0.3 to 7.1.0
<a href="#">CSCwd80343</a>	MI FTD running 7.0.4 is on High disk utilization
<a href="#">CSCwd81384</a>	FMC upgrade fails: 114_DB_table_data_integrity_check.pl, stating Snort2IPSNAPCleanup.pm not be found
<a href="#">CSCwd81538</a>	FTD Traffic failure due to 9344 block depletion in peer_proxy_tx_q
<a href="#">CSCwd81897</a>	Snort3 crash seen sometimes while processing a future flow connection after appid detectors reload
<a href="#">CSCwd82235</a>	LINA Traceback on FPR-1010 under Thread Name: update_cpu_usage
<a href="#">CSCwd82801</a>	Snort outputs massive volume of packet events - IPS event view may show "No Packet Information"
<a href="#">CSCwd83956</a>	snort2 does not match rules based on application SMTP/SMTPS anymore after a while
<a href="#">CSCwd83990</a>	FTD -Snort match incorrect NAP id for traffic
<a href="#">CSCwd84133</a>	ASA/FTD may traceback and reload in Thread Name 'telnet/ci'
<a href="#">CSCwd84868</a>	Observing some devcmd failures and checkheaps traceback when flow offload is not used.
<a href="#">CSCwd85178</a>	AWS ASAv PAYG Licensing not working in GovCloud regions.
<a href="#">CSCwd85609</a>	FTDs running 6.6.x show as disconnected on new HM (6.7+) but checks are running and updating
<a href="#">CSCwd85927</a>	Traceback and reload when webvpn users match DAP access-list with 36k elements

Bug ID	Headline
<a href="#">CSCwd86313</a>	Unable to access Dynamic Access policy
<a href="#">CSCwd86457</a>	Number of objects are not getting updated under policies>>>Security intelligence >>>Block list
<a href="#">CSCwd86929</a>	Cut-Through Proxy does not work with HTTPS traffic
<a href="#">CSCwd88585</a>	ASA/FTD NAT Pool Cluster allocation and reservation discrepancy between units
<a href="#">CSCwd88641</a>	Deployment changes to push VDB package based on Device model and snort engine
<a href="#">CSCwd89349</a>	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (seq 42)
<a href="#">CSCwd90112</a>	MariaDB crash (segmentation fault) related to netmap query
<a href="#">CSCwd91013</a>	FMC   Deployment failure in csm_snapshot_error
<a href="#">CSCwd91421</a>	ASA/FTD may traceback and reload in logging_cfg processing
<a href="#">CSCwd92804</a>	FAN LED flashing amber on FPR2100
<a href="#">CSCwd93316</a>	No Inspect Interruption warning when deploy after FMC upgrade
<a href="#">CSCwd93376</a>	Clientless VPN users are unable to download large files through the WebVPN portal
<a href="#">CSCwd93792</a>	SFDataCorrelator performance degradation involving hosts with many discovered MAC addresses
<a href="#">CSCwd94096</a>	Anyconnect users unable to connect when ASA using different authentication and authorization server
<a href="#">CSCwd94183</a>	Blade not coming up after FXOS update support on multi-instance due to ssp_ntp.log log rotation prob
<a href="#">CSCwd95415</a>	The Standby Device going in failed state due to snort heartbeat failure
<a href="#">CSCwd95436</a>	Primary ASA traceback upon rebooting the secondary
<a href="#">CSCwd95908</a>	ASA/FTD traceback and reload, Thread Name: rtcli async executor process
<a href="#">CSCwd96041</a>	FMC SecureX via proxy stops working after upgrade to 7.x
<a href="#">CSCwd96493</a>	Link Up seen for a few seconds on FPR1010 during bootup
<a href="#">CSCwd96755</a>	ASA is unexpected reload when doing backup
<a href="#">CSCwd96766</a>	41xx: Blade does not capture or log a reboot signal
<a href="#">CSCwd96790</a>	High FMC backup file size due to configurations snapshot for all managed devices
<a href="#">CSCwd97020</a>	ASA/FTD: External IDP SAML authentication fails with Bad Request message
<a href="#">CSCwd97276</a>	Unified events and connection events pages don't load anymore. DB Cores generated every few minutes

Bug ID	Headline
<a href="#">CSCwe00757</a>	Summary status dashboard takes more than 3 mins to load upon login
<a href="#">CSCwe00828</a>	Interactive Block action doesn't work when websites are redirected to https
<a href="#">CSCwe00864</a>	License Commands go missing in Cluster data unit if the Cluster join fails.
<a href="#">CSCwe03529</a>	FTD traceback and reload while deploying PAT POOL
<a href="#">CSCwe03991</a>	FTD/ASA traceback and reload during to tmatch compilation process
<a href="#">CSCwe04437</a>	collection of top.log.gz in troubleshoot can be corrupt due to race condition
<a href="#">CSCwe05913</a>	FTD traceback/reloads - Icmp error packet processing involves snp_nat_xlate_identity
<a href="#">CSCwe06724</a>	Database table optimization not working for some of the tables
<a href="#">CSCwe06826</a>	Email alert incorrectly send for a successful database backup
<a href="#">CSCwe06828</a>	FMC HA Synchronization can hang forever if no response from SendUserReloadSGTAndEndpointsEvent
<a href="#">CSCwe07103</a>	FMC: Upgrade fails at DB Integrity check due to large number of EO warnings for "rule_comments"
<a href="#">CSCwe07722</a>	Cluster data unit drops non-VPN traffic with ASP reason "VPN reclassify failure
<a href="#">CSCwe07928</a>	On a cloud-delivered FMC there is no way to send events to syslog without sending to SAL/CDO as well
<a href="#">CSCwe08729</a>	FPR1120:connections are getting teardown after switchover in HA
<a href="#">CSCwe08908</a>	Threatgrid integration configuration is not sync'd as part of the FMC HA Synchronisation
<a href="#">CSCwe09074</a>	None option under trustpoint doesn't work when CRL check is failing
<a href="#">CSCwe09811</a>	FTD traceback and reload during policy deployment adding/removing/editing of NAT statements.
<a href="#">CSCwe11119</a>	ASA: Traceback and reload while processing SNMP packets
<a href="#">CSCwe11189</a>	monetdb log use all of disk spaces on /Volume
<a href="#">CSCwe11304</a>	Snort crashing on FTD
<a href="#">CSCwe11727</a>	Purging of Config Archive failed for all the devices if one device has no versions
<a href="#">CSCwe12407</a>	High Lina memory use due to leaked SSL handles
<a href="#">CSCwe13627</a>	FMC Unable to fetch VPN troubleshooting logs.
<a href="#">CSCwe14062</a>	FTD/Lina or ASA traceback and reload related to thread ctm_qat_engine
<a href="#">CSCwe14174</a>	FTD - 'show memory top-usage' providing improper value for memory allocation



Bug ID	Headline
<a href="#">CSCwe14514</a>	ASA/FTD Traceback and reload of Standby Unit while removing capture configurations
<a href="#">CSCwe15164</a>	ASA: ASDM cannot display SFR tabs until it's "woken up" through its CLI.
<a href="#">CSCwe16620</a>	FMC Health Monitor does not report alerts for the Interface Status module
<a href="#">CSCwe18090</a>	FMC deployment failure:"Validation failed: This is a slav*/ha standby device, rejecting deployment."
<a href="#">CSCwe18859</a>	After device registration or FMC upgrade, devices sometimes don't send events to the FMC
<a href="#">CSCwe18974</a>	ASA/FTD may traceback and reload in Thread Name: CTM Daemon
<a href="#">CSCwe20043</a>	256-byte memory block gets depleted on start if jumbo frame is enabled with FTD on ASA5516
<a href="#">CSCwe20714</a>	Traffic drop when primary device is active
<a href="#">CSCwe21037</a>	Snort mem used alert should be consistent with value from top.log
<a href="#">CSCwe21187</a>	ASA/FTD may drop multicast packets due to no-mcast-intrf ASP drop reason until UDP timeout expires
<a href="#">CSCwe21280</a>	Multicast connection built or teardown syslog messages may not always be generated
<a href="#">CSCwe21959</a>	Snort3: Process in D state resulting in OOM with jemalloc memory manager
<a href="#">CSCwe22216</a>	Maria DB crashing/holding high CPU and not allowing users to login GUI and CLI
<a href="#">CSCwe22254</a>	After disabling malware analysis, high disk usage on /dev/shm/snort
<a href="#">CSCwe22302</a>	Partition "/opt/cisco/config" gets full due to wtmp file not getting logrotated
<a href="#">CSCwe22492</a>	Slow UI loading for Table View of Hosts
<a href="#">CSCwe22980</a>	Database integrity check takes several minutes to complete
<a href="#">CSCwe23039</a>	NTP polling frequency changed from 5 minutes to 1 second causes large useless log files
<a href="#">CSCwe23139</a>	FTD HA does not break from FMC GUI but HA bootstrap is removed from devices
<a href="#">CSCwe23801</a>	FPR2100: Multiple snort3 & snort2 cores got generated and sensor goes down in KP platform
<a href="#">CSCwe24532</a>	Multiple instances of nvram.out log rotated files under /opt/cisco/platform/logs/
<a href="#">CSCwe24880</a>	Using proxy authentication in FMC for smart licensing is failing after upgrading to 7.0.5
<a href="#">CSCwe25187</a>	FMC External authentication getting "Internal error"

Bug ID	Headline
<a href="#">CSCwe28094</a>	ASA/FTD may traceback and reload after executing 'clear counters all' when VPN tunnels are created
<a href="#">CSCwe28726</a>	The command "app-agent heartbeat" is getting removed when deleting any created context
<a href="#">CSCwe29179</a>	CLUSTER: ICMP reply arrives at director earlier than CLU add flow request from flow owner.
<a href="#">CSCwe29381</a>	Sybase arbiter is not up on FMC HA
<a href="#">CSCwe29498</a>	occasional failure to load light-modal-ac-rule-xx.css with a net::ERR_TOO_MANY_RETRIES error
<a href="#">CSCwe29529</a>	FTD MI does not adjust PVID on vlans attached to BVI
<a href="#">CSCwe29583</a>	ASA/FTD may traceback and reload in Thread Name 'None' at lua_getinfo
<a href="#">CSCwe29850</a>	ASA/FTD Show chunkstat top command implementation
<a href="#">CSCwe29952</a>	SFDataCorrelator cores due to stuck database query after 1 hour deadlock timeout
<a href="#">CSCwe30228</a>	ASA/FTD might traceback in funtion "snp_fp_l2_capture_internal" due to cf_reinject_hide flag
<a href="#">CSCwe30653</a>	FTD upgrade failure at "999_finish/999_zz_install_bundle.sh" due to bad key cert
<a href="#">CSCwe30867</a>	Workaroud to set hwclock from ntp logs on low end platforms
<a href="#">CSCwe32375</a>	7.0 - Snort3 process in D state and outage due to OOM
<a href="#">CSCwe32448</a>	changing time window settings in FMC GUI event viewers may not work with FMC integrated with SecureX
<a href="#">CSCwe32537</a>	ASDM Managed SFR modules 7.0.5 upgrade failure in 114_Snort_table_data_integrity_check.pl
<a href="#">CSCwe36176</a>	ASA/FTD: High failover delay with large number of (sub)interfaces and http server enabled
<a href="#">CSCwe38029</a>	Multiple traceback seen on standby unit.
<a href="#">CSCwe38585</a>	FMC + FTD's Upgrade to 7.0.4(5) version from pre -7.0.0 version creates 7.2.0 configurations on FMC
<a href="#">CSCwe38640</a>	EventHandler warnings if syslog facility is CONSOLE
<a href="#">CSCwe39425</a>	2100: Power switch toggle leads to ungraceful shutdowns and "PowerCycleRequest" reset
<a href="#">CSCwe40463</a>	Stale IKEv2 SA formed during simultaneous IKE SA handling when missing delete from the peer

Bug ID	Headline
<a href="#">CSCwe41898</a>	ASA: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
<a href="#">CSCwe44311</a>	FP2100:Update LINA asa.log files to avoid recursive messages-<date>.1.gz rotated filenames
<a href="#">CSCwe44620</a>	Question mark in NAT description causes config mismatch on Data members of an FTD cluster
<a href="#">CSCwe44672</a>	Syslog ASA-6-611101 is generated twice for a single ssh connection
<a href="#">CSCwe44766</a>	IMS: FP2100 FTW timeout triggered by high CPU usage during FTD Access Control Policy deploy.
<a href="#">CSCwe45779</a>	ASA/FTD drops traffic to BVI if floating conn is not default value due to no valid adjacency
<a href="#">CSCwe45879</a>	Frequent errors seen regarding failures to load bulkcsv files that don't exist
<a href="#">CSCwe48378</a>	Remove FMC drop_cache trigger to prevent Disk I/O increase due to file cache thrashing
<a href="#">CSCwe48432</a>	Unable to save Access Control Policy changes due to Internal error
<a href="#">CSCwe49185</a>	Generate password does not meet requirements while in CC mode
<a href="#">CSCwe50993</a>	SNMP on SFR module goes down and won't come back up
<a href="#">CSCwe51286</a>	ASA/FTD may traceback and reload in Thread Name 'lina'
<a href="#">CSCwe51489</a>	Unable to process query error on events; FMC UI; monetdb maximum connections reached
<a href="#">CSCwe52120</a>	SSL decrypted conns fails when tx chksum-offload is enabled with the egress interface a pppoe.
<a href="#">CSCwe52499</a>	NGIPsv syslog-tls.conf.tt needs filters removed when in CC mode
<a href="#">CSCwe52640</a>	Certain containers have extra gray borders and certain containers are styled incorrectly
<a href="#">CSCwe54529</a>	FTD on FPR2140 - Lina traceback and reload by TCP normalization
<a href="#">CSCwe55556</a>	logging is getting disabled if ssl rules are reordered
<a href="#">CSCwe58576</a>	FTD:Node not joining cluster with "Health check detected that control left cluster" due to SSL error
<a href="#">CSCwe58620</a>	FMC 7.3 Connection Events page "Error: Unable to process this query. Please contact support."
<a href="#">CSCwe58881</a>	After FMC upgrade, SecureX ribbon redirects to US cloud region regardless of the set cloud region

Bug ID	Headline
<a href="#">CSCwe59380</a>	FTD: "timeout floating-conn" not operating as expected for connections dependent on VRF routing
<a href="#">CSCwe59664</a>	DAP policy created in FMC Gui, to detect a Windows OS with a hotfix, will not work as expected
<a href="#">CSCwe59737</a>	ASA/FTD reboots due to traceback pointing to watchdog timeout on p3_tree_lookup
<a href="#">CSCwe59809</a>	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (seq 45)
<a href="#">CSCwe59919</a>	FTD Traceback and reload on Thread Name "NetSnmp Event mib process"
<a href="#">CSCwe61599</a>	FTD 2100 -Update daq-ioq mempool to help protect against buffer corruption
<a href="#">CSCwe61928</a>	PIM register packets are not sent to RP after a reload if FTD uses a default gateway to reach the RP
<a href="#">CSCwe61969</a>	ASA Multicontext 'management-only' interface attribute not synced during creation
<a href="#">CSCwe62927</a>	DCCSM session authorization failure cause multiple issues across FMC
<a href="#">CSCwe62997</a>	ASA/FTD traceback in snp_tracer_format_route
<a href="#">CSCwe63067</a>	ASA/FTD may traceback and reload in Thread Name 'lina' due to due to tcp intercept stat
<a href="#">CSCwe63232</a>	ASA/FTD: Ensure flow-offload states within cluster are the same
<a href="#">CSCwe63316</a>	Pri-Active FMC NOT triggering registration TASK for FTD to configure standby manager
<a href="#">CSCwe64404</a>	ASA/FTD may traceback and reload after changing IP of authentication server
<a href="#">CSCwe64542</a>	TID python processes stuck at 100% CPU
<a href="#">CSCwe64557</a>	ASA: Prevent SFR module configuration on unsupported platforms
<a href="#">CSCwe64563</a>	The command "neighbor x.x.x.x ha-mode graceful-restart" removed when deleting any created context
<a href="#">CSCwe65245</a>	FP2100 series devices might use excessive memory if there is a very high SNMP polling rate
<a href="#">CSCwe65634</a>	ASA - Standby device may traceback and reload during synchronization of ACL DAP
<a href="#">CSCwe66132</a>	ASA/FTD may traceback and reload in Thread Name 'lina'
<a href="#">CSCwe66137</a>	SSO user gets logged in to FMC UI if a valid local user credentials are pre-populated in the browser
<a href="#">CSCwe67751</a>	Last fragment from SIP IPv6 packets has MF equal to 1, flagging that more packets are expected
<a href="#">CSCwe68159</a>	Failover fover_trace.log file is flooding and gets overwritten quickly

Bug ID	Headline
<a href="#">CSCwe69388</a>	FMC should push the AnyConnect Custom attribute defer keyword as lowercase instead of capitalized
<a href="#">CSCwe69833</a>	IP addresses are susceptible to be skipped by geolocation rules when using snort 3
<a href="#">CSCwe70202</a>	Multiple times the failover may be disabled by wrongly seeing a different "Mate operational mode".
<a href="#">CSCwe70558</a>	FTD: unable to run any commands on CLISH prompt
<a href="#">CSCwe70721</a>	Deployment is blocked due to Pre-deploy Validation Error - Invalid endpoint
<a href="#">CSCwe71284</a>	ASA/FTD may traceback and reload in Thread Name DATAPATH-3-21853
<a href="#">CSCwe71672</a>	Selective deployment negating the route configs
<a href="#">CSCwe71673</a>	Selective deployment removing the prefilter-configs
<a href="#">CSCwe72535</a>	Unable to login to FTD using external authentication
<a href="#">CSCwe73240</a>	FMC runs out of space when Snort sends massive numbers of packet logs
<a href="#">CSCwe74059</a>	logrotate is not compressing files on 9.16 ASA or 7.0 FTD
<a href="#">CSCwe74328</a>	AnyConnect - mobile devices are not able to connect when hostscan is enabled
<a href="#">CSCwe74899</a>	CD App Sync error is App Config Apply Failed on Secondary/Standby after backup restore on RMA device
<a href="#">CSCwe74916</a>	Interface remains DOWN in an Inline-set with propagate link state
<a href="#">CSCwe75124</a>	Upgraded FMC didn't mark FTD's with Hot Fix as light registered - failed FMC HA sync
<a href="#">CSCwe75207</a>	High rate of network map updates can cause large delays and backlogs in event processing
<a href="#">CSCwe76036</a>	ndclientd error message 'Local Disk is full' needs to provide mount details which is full
<a href="#">CSCwe78977</a>	ASA/FTD may traceback and reload in Thread Name 'pix_flash_config_thread'
<a href="#">CSCwe79072</a>	ASA/FTD may traceback and reload in Thread Name 'lina'
<a href="#">CSCwe79954</a>	LDAP External auth config fails to deploy to FTD if same LDAP server is added as Primary and backup
<a href="#">CSCwe81684</a>	ASA: Standby failure on parsing of "management-only" not reported to parser/failover subsystem
<a href="#">CSCwe83061</a>	FMC Upgrade from Active-Primary FMC is failed with "Installation failed: Peer Discovery incomplete."
<a href="#">CSCwe83478</a>	Prune target should account for the allocated memory from the thread pruned

Bug ID	Headline
<a href="#">CSCwe83775</a>	Incorrect CPU and core metrics collected on 55XX platform
<a href="#">CSCwe83812</a>	SFDataCorrelator log spam when network map is full
<a href="#">CSCwe84079</a>	asa_snmp.log is not rotated, resulting in large file size, QP-HA MI 7.2.4-97
<a href="#">CSCwe85432</a>	ASA/FTD traceback and reload on thread DATAPATH-14-11344 when SIP inspection is enabled
<a href="#">CSCwe86687</a>	Apache Commons FileUpload before 1.5 does not limit the number of reques
<a href="#">CSCwe86690</a>	In Apache MINA, a specifically crafted, malformed HTTP request may cause
<a href="#">CSCwe86693</a>	An issue in protobuf-java allowed the interleaving of com.google.protobuf
<a href="#">CSCwe88496</a>	"Failed to convert snort 2 custom rules. Refer /var/sf/htdocs/ips/snort.rej for more details."
<a href="#">CSCwe89024</a>	FTS under AC Policy Listing page with 'obj' gives Error Moving Data error with CTS DB
<a href="#">CSCwe89030</a>	Serial number attribute from the subject DN of certificate should be taken as the username
<a href="#">CSCwe89305</a>	vFMC300 to FMC2600 migration failure with error "migration from R to N is not allowed"
<a href="#">CSCwe89731</a>	Notification Daemon false alarm of Service Down
<a href="#">CSCwe90202</a>	ASA: Standby failure on parsing of "management-only" for dynamic configuraiton changes
<a href="#">CSCwe90720</a>	ASA Traceback and reload in parse thread due ha_msg corruption
<a href="#">CSCwe91652</a>	Database backup failed on KVM FMC
<a href="#">CSCwe91674</a>	Mserver restarts frequently
<a href="#">CSCwe91958</a>	correlation events based on connection events do not contain Security Intelligence Category content
<a href="#">CSCwe92905</a>	ngfwManager process continuously restarting leading to ZMQ Out of Memory traceback
<a href="#">CSCwe93162</a>	FP1140 7.0.4 Deployment keep failing with error "Can't use an undefined value as a HASH reference"
<a href="#">CSCwe93202</a>	FXOS REST API: Unable to create a keyring with type "ecdsa"
<a href="#">CSCwe93489</a>	Threat-detection does not recognize exception objects with a prefix in IPv6
<a href="#">CSCwe93532</a>	ASA/FTD may traceback and reload in Thread Name 'lina'.
<a href="#">CSCwe93566</a>	need to turn off default TLS 1.1 (deprecated) support for the FDM GUI

Bug ID	Headline
<a href="#">CSCwe94287</a>	FTD DHCP Relay drops NACK if multiple DHCP Servers are configured
<a href="#">CSCwe95757</a>	ASA/FTD may traceback and reload in Thread Name 'lina'
<a href="#">CSCwe96023</a>	ASa/FTD: SNMP related traceback and reload immediately after upgrade from 6.6.5 to 7.0.1
<a href="#">CSCwe96068</a>	ASA: Configurable CLU for Large amount of under/overruns on CLU RX/TX queues
<a href="#">CSCwe98430</a>	AC policy deploy failing on 7.2.4 FMC to 6.7 FTD
<a href="#">CSCwe98435</a>	Selective policy deploy with Identity Policy (captive-portal) and SSL Policy (dp-tcp-proxy) CLI
<a href="#">CSCwe98751</a>	FMC is suddenly not showing stack after creation.
<a href="#">CSCwe99040</a>	traceback and reload thread datapath on process tcpmod_proxy_continue_bp
<a href="#">CSCwe99550</a>	Add knob to pause/resume file specific logging in asa log infra.
<a href="#">CSCwf00803</a>	Mode / License mismatch information is not seen in show failover history
<a href="#">CSCwf02005</a>	ActionQueue task sandbox data update throws SQL Error post 7.2.4 upgrade
<a href="#">CSCwf02363</a>	Snort3 Crash in SslServiceDetector after call from nss_passwd_lookup
<a href="#">CSCwf03490</a>	portmanager.sh outputting continuous bash warnings to log files
<a href="#">CSCwf04831</a>	ASA/FTD may traceback and reload in Thread Name 'ci/console'
<a href="#">CSCwf06261</a>	Health Monitoring exports negative snort swap memory metric value
<a href="#">CSCwf06818</a>	Cisco Firepower Threat Defense Software Encrypted Archive File Policy Bypass Vulnerability
<a href="#">CSCwf07030</a>	Upgrade Device listing page is taking more than 15 mins to load page fully with 25 FTDs registered
<a href="#">CSCwf07791</a>	ASA running out of SNMP PDU and SNMP VAR chunks
<a href="#">CSCwf08043</a>	Lina traceback and reload due to fragmented packets
<a href="#">CSCwf10422</a>	"Security Intelligence feed download failed" displayed even though it succeeded
<a href="#">CSCwf12005</a>	ASA sends OCSP request without user-agent and host
<a href="#">CSCwf12408</a>	ASA: After upgrade to 9.16.4 all type-8 passwords are lost on first reboot
<a href="#">CSCwf14735</a>	traceback and reload in Process Name: lina related to Nat/Pat
<a href="#">CSCwf14811</a>	TCP normalizer needs stats that show actions like packet drops
<a href="#">CSCwf15858</a>	LDAP authentication over SSL not working for users that send large authorisation profiles

Bug ID	Headline
<a href="#">CSCwf15978</a>	xml2js version 0.4.23 allows an external attacker to edit or add new pro
<a href="#">CSCwf17814</a>	ASA/FTD may traceback and reload in Thread Name '19', free block checksum failure
<a href="#">CSCwf19562</a>	Changes to lamplighter logs written to /var/log/tid_process.log
<a href="#">CSCwf19853</a>	FATAL errors in DBCheck due to missing columns in eventdb table
<a href="#">CSCwf20338</a>	ASA may traceback and reload in Thread Name 'DHCPv6 Relay'
<a href="#">CSCwf21106</a>	ASA/FTD: Traceback on thread name: snmp_master_callback_thread during SNMP and interface changes
<a href="#">CSCwf22568</a>	FTD HA Creation fails resulting in devices showing up in an inconsistent state on the FMC
<a href="#">CSCwf23564</a>	Unable to establish BGP when using MD5 authentication over GRE TUNNEL and FTD as passthrough device
<a href="#">CSCwf24124</a>	SFDataCorrelator process crashing very frequently on the FMC.
<a href="#">CSCwf24773</a>	crashhandler running with test mode snort
<a href="#">CSCwf26939</a>	FTD may fail to create a NAT rule with error: "IPv4 dst real obj address range is huge"
<a href="#">CSCwf28488</a>	Inconsistent log messages seen when emblem is configured and buffer logging is set to debug
<a href="#">CSCwf28592</a>	In some specific scenarios, object optimizer can cause incorrect rules to be deployed to the device
<a href="#">CSCwf30716</a>	ASA in multi context shows standby device in failed stated even after MIO HB recovery.
<a href="#">CSCwf30727</a>	ASA integration with umbrella does not work without validation-usage ssl-server.
<a href="#">CSCwf31701</a>	ASA traceback and reload with the Thread name: **CP Crypto Result Processing**
<a href="#">CSCwf31820</a>	Firewall may drop packets when routing between global or user VRFs
<a href="#">CSCwf32890</a>	Standby FMC SSH connection getting disconnected frequently.
<a href="#">CSCwf33574</a>	ASA access-list entries have the same hash after upgrade
<a href="#">CSCwf34450</a>	Snort3 crash after the consequent snort restart if duplicate custom apps are present
<a href="#">CSCwf35510</a>	Possible segfault in snort3 when appid tries to delete the app info table
<a href="#">CSCwf42144</a>	ASA/FTD may traceback and reload citing process name "lina"
<a href="#">CSCwf43288</a>	Traceback in Thread Name: ssh/client in a clustered setup
<a href="#">CSCwf51933</a>	FTD username with dot fails AAA-RADIUS external authentication login after upgrade



Bug ID	Headline
<a href="#">CSCwf57261</a>	ASA: Traceback and reload due to clientless webvpn session closure
<a href="#">CSCwf57850</a>	TelemetryApp process keeps exiting every minute after upgrading the FMC
<a href="#">CSCwf58876</a>	KP2140-HA, reloaded primary unit not able to detect the peer unit
<a href="#">CSCwf76945</a>	Packet data is still dropped after upgrade

## Resolved Bugs in Version 7.0.5.1

Table last updated: 2022-04-26

*Table 44: Resolved Bugs in Version 7.0.5.1*

Bug ID	Headline
<a href="#">CSCwe52499</a>	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 45: Resolved Bugs in Version 7.0.5*

Bug ID	Headline
<a href="#">CSCvo17612</a>	Return error messages when failing to retrieve objects from database
<a href="#">CSCvq70838</a>	Traceback in the output of tail-logs command
<a href="#">CSCvr06065</a>	Snort core due to DAQ IOQ Corruption
<a href="#">CSCvw82067</a>	ASA/FTD 9344 blocks depleted due to high volume of fragmented traffic
<a href="#">CSCvw90399</a>	FMC HA issues with too many open file descriptors for sfiproxy UDP conn
<a href="#">CSCvx24207</a>	FQDN Object Containing IPv4 and IPv6 Addresses Only Install IPv6 Entries
<a href="#">CSCvx68586</a>	Not able to login to UI/SSH on FMC, console login doesn't prompt for password
<a href="#">CSCvx75743</a>	Inconsistent FMC audit log severity
<a href="#">CSCvx86569</a>	Access Control Rule - Comment disappears if clicked to another tab before saving the comment.
<a href="#">CSCvy24180</a>	Default variable set missing on FMC
<a href="#">CSCvy38070</a>	File/Malware Event Report fails when date is x-axis and count y-axis for table chart
<a href="#">CSCvy38650</a>	Unable to download captured file from FMC Captured files UI

Bug ID	Headline
<a href="#">CSCvy45048</a>	Subsystem query parameter not filtering records for "auditrecords" restapi
<a href="#">CSCvy47927</a>	Unable to select multiple policies for scheduled firepower recommended rules
<a href="#">CSCvy50598</a>	BGP table not removing connected route when interface goes down
<a href="#">CSCvy63463</a>	Error deleting users due to special characters
<a href="#">CSCvy65178</a>	Need dedicated Rx rings for to the box BGP traffic on Firepower platform
<a href="#">CSCvy67765</a>	FTD VTI reports TUNNEL_SRC_IS_UP false despite source interface is up/up and working
<a href="#">CSCvy68974</a>	ActionQueue process is killed by OOM killer due to process utilizing more than 3 GB limit for memory
<a href="#">CSCvy73130</a>	FP4100 platform: Active-Standby changed to dual Active after running "show conn" command
<a href="#">CSCvy75131</a>	Occasionally deleted sensor/interfaces are not removed from security zones
<a href="#">CSCvy93607</a>	Health monitor alert indicates QP HA in split brain when one device reboots and re-joins
<a href="#">CSCvy95520</a>	Cisco Firepower Management Center and Firepower Threat Defense Software SSH DoS Vulnerability
<a href="#">CSCvy95809</a>	Crashinfo script is invoked on SFR running snort2 and device fails to upgrade to 7.0
<a href="#">CSCvz07004</a>	SNORT2: FTD is performing Full proxy even when SSL rule has DND action.
<a href="#">CSCvz09106</a>	Cisco ASA and FTD Software SSL VPN Denial of Service Vulnerability
<a href="#">CSCvz13564</a>	Firepower 2100 FTD: ssh-access-list configuration are lost after upgrading
<a href="#">CSCvz19364</a>	FXOS does not send any syslog messages when the duplex changes to "Half Duplex"
<a href="#">CSCvz31184</a>	Validation of unsupported flow-offload using pre-filter in passive/inline interfaces in FPR4100/9300
<a href="#">CSCvz32593</a>	FPR4110 and FPR4115 in disabled state CD App Sync error is Rsync is not enabled on active device
<a href="#">CSCvz35669</a>	KP-2110 Standby disabled upgrade 6.6.4-64 to 7.0.1-30 "CD App Sync error is App Config Apply Failed"
<a href="#">CSCvz36903</a>	ASA traceback and reload while allocating a new block for cluster keepalive packet
<a href="#">CSCvz40542</a>	FMC : Remote Storage Device's SMB share password does not make it when upgrading from 6.6 to 7
<a href="#">CSCvz40765</a>	FMC CPU graph displays the wrong number of Snort and System cores
<a href="#">CSCvz42823</a>	Bulk Operation of AC Policy REST API taking time

Bug ID	Headline
<a href="#">CSCvz43325</a>	Active FMC not deregistering sensors after breaking HA
<a href="#">CSCvz49163</a>	Observed some time drift in seconds in the output when we execute show rule hits multiple times
<a href="#">CSCvz52785</a>	Management interface flaps every 13mins post upgrade from 9.12 to 9.14.2.15
<a href="#">CSCvz57917</a>	High unmanaged disk usage on /ngfw filled with module-xxxx-x86_64.tgz files in packages folder
<a href="#">CSCvz60142</a>	ASA/FTD stops serving SSL connections
<a href="#">CSCvz61456</a>	Software upgrade on ASA application may failure without obvious reasons
<a href="#">CSCvz61463</a>	FP9k SM-44 High CPU on radware vdp Cores after upgrade
<a href="#">CSCvz62517</a>	SRU install should validate files upon completion
<a href="#">CSCvz68713</a>	PLR license reservation for ASAv5 is requesting ASAv10
<a href="#">CSCvz69729</a>	Unstable client processes may cause LINA zmqio traceback on FTD
<a href="#">CSCvz71596</a>	"Number of interfaces on Active and Standby are not consistent" should trigger warning syslog
<a href="#">CSCvz77050</a>	Occasionally policy deployment failure are reported as successful
<a href="#">CSCvz78331</a>	SNMP polling fails after a re-image
<a href="#">CSCvz84733</a>	LACP packets through inline-set are silently dropped
<a href="#">CSCvz85234</a>	Facilities ALERT, AUDIT, CLOCK and KERN do not work in sending Audit Log to syslog from FMC.
<a href="#">CSCvz94841</a>	Grammatical errors in failover operating mode mismatch error message
<a href="#">CSCwa03341</a>	Standby's sub interface mac doesn't revert to old mac with no mac-address command
<a href="#">CSCwa06608</a>	WM 1010 HA Failover is not successful when we give failover active in secondary.
<a href="#">CSCwa07390</a>	Config only FMC: SI feed downloaded file does not match expected checksum
<a href="#">CSCwa15093</a>	Access Policy Control Clear Hit Count throwing Error 403: Forbidden
<a href="#">CSCwa16626</a>	Syslog over TLS accepting wildcard in middle of FQDN
<a href="#">CSCwa33248</a>	Auto LSP update not getting triggered, missing Talos registration (beakerd)
<a href="#">CSCwa36535</a>	Standby unit failed to join failover due to large config size.
<a href="#">CSCwa38996</a>	Big number of repetitive messages in snmpd.log leading to huge log size
<a href="#">CSCwa41936</a>	Cisco FTD Bleichenbacher Attack Vulnerability

Bug ID	Headline
<a href="#">CSCwa42596</a>	ASA with SNMPv3 configuration observes unexpected reloads with snmpd cores
<a href="#">CSCwa43311</a>	Snort blocking and dropping packet, with bigger size(1G) file download
<a href="#">CSCwa47737</a>	ASA/FTD may hit a watchdog traceback related to snmp config writing
<a href="#">CSCwa49480</a>	SNMP OID , stop working after around one hour and a half - FTD
<a href="#">CSCwa55142</a>	SNORT3 / SSL / Definitive DND verdict when there's an extra DND bottom rule, instead of regular DND
<a href="#">CSCwa59907</a>	LINA observed traceback on thread name "snmp_client_callback_thread"
<a href="#">CSCwa61361</a>	ASAv traceback when SD_WAN ACL enabled, then disabled (or vice-versa) in PBR
<a href="#">CSCwa62025</a>	IPv6: Some of egress interfaces of global and user vrf routes are missing in asp table
<a href="#">CSCwa64739</a>	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
<a href="#">CSCwa68552</a>	All type-8 passwords are lost upon upgrade from ASA 9.12-9.15 to 9.16, failover gets disabled
<a href="#">CSCwa72528</a>	username form cert feature does not work with SER option
<a href="#">CSCwa72530</a>	FTD: Time gap/mismatch seen when new node joins a Cluster Control node under history
<a href="#">CSCwa72641</a>	URL incorrectly extracted for TLS v1.2 self signed URLs when "Early application detection" enabled
<a href="#">CSCwa72929</a>	SNMPv3 polling may fail using privacy algorithms AES192/AES256
<a href="#">CSCwa73172</a>	ASA reload and traceback in Thread Name: PIX Garbage Collector
<a href="#">CSCwa75966</a>	ASA: Reload and Traceback in Thread Name: Unicorn Proxy Thread with Page fault: Address not mapped
<a href="#">CSCwa77083</a>	Host information is missing when Security Zones are configured in Network Discovery rules
<a href="#">CSCwa78082</a>	FMC intrusion event search produces inconsistent results
<a href="#">CSCwa80040</a>	FMC NFS configuration failing after upgrade from 6.4.0.4 to 7.0.1
<a href="#">CSCwa81143</a>	Unable to save the application policy filter. Save tab is stuck and its continuously loading.
<a href="#">CSCwa85492</a>	URL lookup responding with two categories
<a href="#">CSCwa85709</a>	Cisco Firepower Management Center Information Disclosure Vulnerability
<a href="#">CSCwa87298</a>	ASA conn data-rate: incorrect "current rate" and "data-rate-filter" doesn't work properly
<a href="#">CSCwa89347</a>	Cannot add object to network group on FMC

Bug ID	Headline
<a href="#">CSCwa90735</a>	FTD/FXOS - ASAconsole.log files fail to rotate causing excessive disk space used in /ngfw
<a href="#">CSCwa91070</a>	Cgroup triggering oom-k for backup process
<a href="#">CSCwa92596</a>	Access Control File policy rule message is misleading and unnecessary
<a href="#">CSCwa92822</a>	TLS client in the sftunnel TLS tunnel offers curves in CC mode that are not allowed by CC
<a href="#">CSCwa92883</a>	Deployment Failed at phase-2 with domain snapshot error
<a href="#">CSCwa93499</a>	Cisco Firepower Management Center Stored Cross-Site Scripting Vulnerability
<a href="#">CSCwa95079</a>	ASA/FTD Traceback and reload due to NAT configuration
<a href="#">CSCwa97541</a>	Cisco ASA FirePOWER Module, FMC and NGIPS SNMP Default Credential Vulnerability
<a href="#">CSCwa97917</a>	ISA3000 in boot loop after powercycle
<a href="#">CSCwa98853</a>	Error F0854 FDM Keyring's RSA modulus is invalid
<a href="#">CSCwa98983</a>	Upgrade failed on FPR2100-HA at 800_post/901_reapply_sensor_policy.pl
<a href="#">CSCwa99171</a>	Chassis and application sets the time to Jan 1, 2010 after reboot
<a href="#">CSCwa99931</a>	ASA/FTD: Tuning of update_mem_reference process
<a href="#">CSCwa99932</a>	ASA/FTD stuck after crash and reboot
<a href="#">CSCwb00749</a>	FMC upgrade failure: 114_DB_table_data_integrity_check.pl failed
<a href="#">CSCwb01983</a>	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
<a href="#">CSCwb01990</a>	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
<a href="#">CSCwb01995</a>	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
<a href="#">CSCwb02006</a>	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
<a href="#">CSCwb02018</a>	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
<a href="#">CSCwb02026</a>	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
<a href="#">CSCwb02060</a>	snmp-group host with Invalid host range and subnet causing traceback and reload
<a href="#">CSCwb03704</a>	ASA/FTD datapath threads may run into deadlock and generate traceback
<a href="#">CSCwb04000</a>	ASA/FTD: DF bit is being set on packets routed into VTI
<a href="#">CSCwb05148</a>	Cisco ASA Software and FTD Software SNMP Denial of Service Vulnerability
<a href="#">CSCwb05291</a>	Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability

Bug ID	Headline
<a href="#">CSCwb05920</a>	Crash in KP at webVpn free, HTTPCleanUp and mem_mh_free from Scaled AC-IK/IPSec TVM test.
<a href="#">CSCwb06273</a>	Continuous memory leak in the process hmlsd (SF::Messaging::smartSend)
<a href="#">CSCwb06847</a>	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-9-11543'
<a href="#">CSCwb07908</a>	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
<a href="#">CSCwb07981</a>	Traceback: Standby FTD reboots and generates crashinfo and lina core on thread name cli_xml_server
<a href="#">CSCwb08644</a>	ASA/FTD traceback and reload at IKEv2 from Scaled S2S+AC-DTLS+SNMP long duration test
<a href="#">CSCwb08773</a>	FPR2130 LED is off when power supply module 1 is back
<a href="#">CSCwb08828</a>	FP1010 Switchport access vlan interface in up/up status but not passing traffic
<a href="#">CSCwb12730</a>	Policy deployment failed in FMC however FTD deployment status shows "INPROGRESS"
<a href="#">CSCwb16037</a>	Unable to replace the anyconnect image when maximum memory used for anyconnect images.
<a href="#">CSCwb16663</a>	Unable to configure NAP under Advanced Tab in AC policy
<a href="#">CSCwb16920</a>	CPU profile cannot be reactivated even if previously active memory tracking is disabled
<a href="#">CSCwb17187</a>	SNMP cores are generated every minute while running snmpwalk on HA
<a href="#">CSCwb17963</a>	Unable to identify dynamic rate limiting mechanism & not following msg limit per/sec at syslog server.
<a href="#">CSCwb19648</a>	SNMP queries for crasLocalAddress are not returning the assigned IPs for SSL/DTLS tunnels.
<a href="#">CSCwb22592</a>	SSH Functionalty stopped working after running long duration tests of SCP + Scaled TVM VPN Profiles
<a href="#">CSCwb23029</a>	Cisco Firepower Management Center Software Command Injection Vulnerability
<a href="#">CSCwb23048</a>	Cisco Firepower Management Center Software Command Injection Vulnerability
<a href="#">CSCwb24039</a>	ASA traceback and reload on routing
<a href="#">CSCwb25809</a>	Single Pass - Traceback due to stale ifc
<a href="#">CSCwb28123</a>	FTD HA deployment fails with error "Deployment failed due to major version change on device"
<a href="#">CSCwb29126</a>	Cannot use underscore ( _ ) in FMC's realm AD Primary Domain configuration

Bug ID	Headline
<a href="#">CSCwb31551</a>	When inbound packet contains SGT header, FPR2100 cannot distribute properly per 5 tuple
<a href="#">CSCwb31699</a>	Primary takes active role after reload
<a href="#">CSCwb32267</a>	Crash on KP Active node while clearing vpnsessiondb with AnyConnect-SSL TVM Profile running
<a href="#">CSCwb32418</a>	Cisco FirePOWER Software for ASA FirePOWER Module Command Injection Vulnerability
<a href="#">CSCwb32841</a>	NAT (any,any) statements in-states the failover interface and resulting on Split Brain events
<a href="#">CSCwb33184</a>	Memory leak in MessageService causes UI slowness
<a href="#">CSCwb35675</a>	Snort3 is partially in sync with Snort 2 warning alert
<a href="#">CSCwb37077</a>	“show access-control-config” for DNS Reputation Enforcement does not work.
<a href="#">CSCwb37999</a>	Customized Variables name cause Snort3 validation failure
<a href="#">CSCwb38406</a>	GeoDB updates on multi-domain environment requires a manual policy deployment
<a href="#">CSCwb39431</a>	FTD unified logs do not print the log as per rfc5424 standard
<a href="#">CSCwb40001</a>	Long delays when executing SNMP commands
<a href="#">CSCwb41739</a>	debug crypto conditional need to be made multi-ctx aware
<a href="#">CSCwb41854</a>	Cisco FTD Software and Cisco FXOS Software Command Injection Vulnerability
<a href="#">CSCwb42978</a>	ASA accepting invalid netmask in SSH/TELNET/HTTP/TFTP config
<a href="#">CSCwb43018</a>	Implement SNP API to check ifc and ip belongs to HA LU or CMD interface
<a href="#">CSCwb43433</a>	Jumbo frame performance has degraded up to -45% on Firepower 2100 series
<a href="#">CSCwb50405</a>	ASA/FTD Traceback in crypto hash function
<a href="#">CSCwb51707</a>	ASA Traceback and reload in process name: lina
<a href="#">CSCwb52401</a>	Cisco Firepower Threat Defense Software Privilege Escalation Vulnerability
<a href="#">CSCwb53172</a>	FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated
<a href="#">CSCwb53191</a>	Certificate validation fails post upgrade to 9.17.1
<a href="#">CSCwb53328</a>	ASA/FTD Traceback and reload caused by Smart Call Home process sch_dispatch_to_url
<a href="#">CSCwb53694</a>	Cisco Firepower Management Center Software XML External Entity Injection Vulnerability

Bug ID	Headline
<a href="#">CSCwb54791</a>	ASA DHCP server fails to bind reserved address to Linux devices
<a href="#">CSCwb56718</a>	Policy deployment fails with error- Rule update is running but there are no updates in progress.
<a href="#">CSCwb56905</a>	ASA blocking 0.0.0.0 IP and netmask combination in SSH/TELNET/HTTP config
<a href="#">CSCwb57524</a>	FTD upgrade fails - not enough disk space from old FXOS bundles in distributables partition
<a href="#">CSCwb57615</a>	Configuring pbr access-list with line number failed.
<a href="#">CSCwb59465</a>	ASA/FTD may traceback (watchdog) and reload when generating a syslog from the VPN Failover subsystem
<a href="#">CSCwb59488</a>	ASA/FTD Traceback in memory allocation failed
<a href="#">CSCwb59619</a>	PM needs to restart the Disk Manager after creating ramdisk to make DM aware of the ramdisk
<a href="#">CSCwb60993</a>	FDM Need to block the deployment when a Security zone object is not associated with an interface
<a href="#">CSCwb61901</a>	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
<a href="#">CSCwb61908</a>	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
<a href="#">CSCwb62059</a>	Unable to login to FTD using external authentication after upgrade
<a href="#">CSCwb64620</a>	CC mode is not properly enabled on NGIPsv impacting syslog over TLS and SSH
<a href="#">CSCwb65447</a>	FTD: AAB cores are not complete and not decoding
<a href="#">CSCwb65718</a>	FMC is stuck on loading SI objects page
<a href="#">CSCwb66761</a>	Cisco Firepower Threat Defense Software Generic Routing Encapsulation DoS Vulnerability
<a href="#">CSCwb67040</a>	FP4112 4115 Traceback & reload on Thread Name: netfs_thread_init
<a href="#">CSCwb68642</a>	ASA traceback in Thread Name: SXP CORE
<a href="#">CSCwb68993</a>	FTD/FDM: SSL connections to sites using RSA certs with 3072 bit keys may fail
<a href="#">CSCwb69503</a>	ASA unable to configure aes128-gcm@openssh.com when FIPS enabled
<a href="#">CSCwb71460</a>	ASA traceback in Thread Name: fover_parse and triggered by snmp related functions
<a href="#">CSCwb73248</a>	FW traceback in timer infra / netflow timer
<a href="#">CSCwb74571</a>	PBR not working on ASA routed mode with zone-members
<a href="#">CSCwb76129</a>	Some SSL patterns not detected after VDB 356 or higher is installed



Bug ID	Headline
<a href="#">CSCwb76423</a>	ASA crashes on fp2100 when checking CRL
<a href="#">CSCwb79812</a>	RIP is advertising all connected Anyconnect users and not matching route-map for redistribution
<a href="#">CSCwb80108</a>	FP2100/FP1000: Built-in RJ45 ports randomly not coming up after portmanager restart events
<a href="#">CSCwb80559</a>	FTD offloads SGT tagged packets although it should not
<a href="#">CSCwb80862</a>	ASA/FTD proxy arps any traffic when using the built-in 'any' object in translated destination
<a href="#">CSCwb82796</a>	ASA/FTD firewall may traceback and reload when tearing down IKE tunnels
<a href="#">CSCwb83388</a>	ASA HA Active/standby tracebacks seen approximately every two months.
<a href="#">CSCwb83691</a>	ASA/FTD traceback and reload due to the initiated capture from FMC
<a href="#">CSCwb84901</a>	CIAM: heimdal 1.0.1
<a href="#">CSCwb85633</a>	Snmpwalk output of memory does not match show memory/show memory detail
<a href="#">CSCwb85822</a>	Deployment failing when collecting policies.
<a href="#">CSCwb86118</a>	TPK ASA: Device might get stuck on ftp copy to disk
<a href="#">CSCwb86565</a>	FMC upgrade fails due Mismatch in number of entries between /etc/passwd and /etc/shadow
<a href="#">CSCwb87498</a>	Lina traceback and reload during EIGRP route update processing.
<a href="#">CSCwb87950</a>	Cisco ASA Software and FTD Software Web Services Interface Denial of Service Vulnerability
<a href="#">CSCwb88587</a>	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
<a href="#">CSCwb88651</a>	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
<a href="#">CSCwb89187</a>	Flex Config allow - "timeout icmp-error hh:mm:ss"
<a href="#">CSCwb90074</a>	ASA: Multiple Context Mixed Mode SFR Redirection Validation
<a href="#">CSCwb90532</a>	ASA/FTD traceback and reload on NAT related function nat_policy_find_location
<a href="#">CSCwb91101</a>	SNMP interface threshold doesn't trigger properly when traffic sent to interface ~4gbps
<a href="#">CSCwb92376</a>	FMC syslog-ng daemon fails to start if log facility is set to ALERT
<a href="#">CSCwb92709</a>	We can't monitor the interface via "snmpwalk" once interface is removed from context.
<a href="#">CSCwb92937</a>	Error 403: Forbidden when expanding in view group objects
<a href="#">CSCwb93932</a>	ASA/FTD traceback and reload with timer services assertion

Bug ID	Headline
<a href="#">CSCwb94170</a>	merovingian.log file extremely big size can fill the disk
<a href="#">CSCwb94190</a>	ASA graceful shut down when applying ACL's with forward reference feature and FIPS enabled.
<a href="#">CSCwb94312</a>	Unable to apply SSH settings to ASA version 9.16 or later
<a href="#">CSCwb95112</a>	Intrusion Policy shows last modified by admin even though changes are made by a different user
<a href="#">CSCwb95787</a>	FPR1010 - No ARP on switchport VLAN interface after portmanager DIED event
<a href="#">CSCwb97251</a>	ASA/FTD may traceback and reload in Thread Name 'ssh'
<a href="#">CSCwc02488</a>	ASA/FTD may traceback and reload in Thread Name 'None'
<a href="#">CSCwc02700</a>	Fragmented packets are dropped when unit leaves cluster
<a href="#">CSCwc03069</a>	Interface internal data0/0 is up/up from cli but up/down from SNMP polling
<a href="#">CSCwc03393</a>	Lina traceback and core file size is beyond 40G and compression fails on FTD
<a href="#">CSCwc04959</a>	Disk usage is 100% on secondary FMC .dmp files created utilized all the disk space
<a href="#">CSCwc05132</a>	Unable to disable "Retrieve to Management Center
<a href="#">CSCwc06833</a>	Deployment failure with ERROR Process Manager failed to verify LSP ICDB
<a href="#">CSCwc07262</a>	Standby ASA goes to booting loop during configuration replication after upgrade to 9.16(3).
<a href="#">CSCwc08374</a>	Azure ASA NIC MAC address for Gigeth 0/1 and 0/2 become out of order when adding interfaces
<a href="#">CSCwc09414</a>	ASA/FTD may traceback and reload in Thread Name 'ci/console'
<a href="#">CSCwc10037</a>	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
<a href="#">CSCwc10483</a>	ASA/FTD - Traceback in Thread Name: appAgent_subscribe_nd_thread
<a href="#">CSCwc10792</a>	ASA/FTD IPSEC debugs missing reason for change of peer address and timer delete
<a href="#">CSCwc11511</a>	FTD: SNMP failures after upgrade to 7.0.2
<a href="#">CSCwc11597</a>	ASA tracebacks after SFR was upgraded to 6.7.0.3
<a href="#">CSCwc11663</a>	ASA traceback and reload when modifying DNS inspection policy via CSM or CLI
<a href="#">CSCwc13017</a>	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
<a href="#">CSCwc13994</a>	ASA - Restore not remove the new configuration for an interface setup after backup
<a href="#">CSCwc15530</a>	Syslog facility "ALERT" should be changed on FDM since is not supported anymore by syslog-ng

Bug ID	Headline
<a href="#">CSCwc18285</a>	Conn data-rate command can be enabled or disabled in unprivileged user EXEC mode
<a href="#">CSCwc18312</a>	"show nat pool cluster" commands run within EEM scripts lead to traceback and reload
<a href="#">CSCwc18524</a>	ASA/FTD Voltage information is missing in the command "show environment"
<a href="#">CSCwc23075</a>	Upgrade to MariaDB 10.5.16 to get security vulnerability fixes
<a href="#">CSCwc23356</a>	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-20-7695'
<a href="#">CSCwc23695</a>	ASA/FTD can not parse UPN from SAN field of user's certificate
<a href="#">CSCwc24582</a>	Update diskmanager to monitor deploy directories in /ngfw/var/cisco/deploy/db
<a href="#">CSCwc24906</a>	ASA/FTD traceback and reload on Thread id: 1637
<a href="#">CSCwc25207</a>	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 33)
<a href="#">CSCwc26406</a>	FMC: Slowness in Device management page
<a href="#">CSCwc27236</a>	FMC Health Monitoring JSON error
<a href="#">CSCwc27797</a>	ASA mgmt ip cannot be released
<a href="#">CSCwc28334</a>	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
<a href="#">CSCwc28532</a>	9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing
<a href="#">CSCwc28660</a>	Snort3: NFSv3 mount may fail for traffic through FTD
<a href="#">CSCwc28806</a>	ASA Traceback and Reload on process name Lina
<a href="#">CSCwc28854</a>	Incorrect IF-MIB response when failover is configured on multiple contexts
<a href="#">CSCwc28928</a>	ASA: SLA debugs not showing up on VTY sessions
<a href="#">CSCwc29591</a>	Retrospective file disposition updates fail due to incorrect eventsecond values in fileevent tables
<a href="#">CSCwc30487</a>	High unmanaged disk usage on Firepower 2110 device
<a href="#">CSCwc31163</a>	FPR1010 upgrade failed - Error running script 200_pre/100_get_snort_from_dc.pl
<a href="#">CSCwc32246</a>	NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used
<a href="#">CSCwc33036</a>	Observed Logs at syslog server side as more than configured message limit per/sec.
<a href="#">CSCwc33076</a>	JOBS_TABLE not getting purged due to foreign Key constraint violation in policy_diff_main
<a href="#">CSCwc33323</a>	FMC 7.0 - Receiving alert "health monitor process: no events received yet" for multiple devices

Bug ID	Headline
<a href="#">CSCwc34818</a>	The device is unregistered when Rest API calls script.
<a href="#">CSCwc35969</a>	cannot add IP from event to global lists (block or do-not-block) if similar IP is already on list
<a href="#">CSCwc36905</a>	ASA traceback and reload due to "Heap memory corrupted at slib_malloc.c
<a href="#">CSCwc37061</a>	SNMP: FMC doesn't reply to OID 1.3.6.1.2.1.25.3.3.1.2
<a href="#">CSCwc37695</a>	In addition to the c_rehash shell command injection identified in CVE-2022-1292
<a href="#">CSCwc38567</a>	ASA/FTD may traceback and reload while executing SCH code
<a href="#">CSCwc40381</a>	ASA : HTTPS traffic authentication issue with Cut-through Proxy enabled
<a href="#">CSCwc41661</a>	FTD Multiple log files with zero byte size.
<a href="#">CSCwc44289</a>	FTD - Traceback and reload when performing IPv4 && IPv6 NAT translations
<a href="#">CSCwc45108</a>	ASA/FTD: GTP inspection causing 9344 sized blocks leak
<a href="#">CSCwc45397</a>	ASA HA - Restore in primary not remove new interface configuration done after backup
<a href="#">CSCwc45759</a>	NTP logs will eventually overwrite all useful octeon kernel logs
<a href="#">CSCwc46569</a>	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 34)
<a href="#">CSCwc46847</a>	FXOS partition opt_cisco_platform_logs on FP1K/FPR2K may go Full due to ucssh_*.log
<a href="#">CSCwc47586</a>	vFMC upgrade 7.0.4-36 & 7.3.0-1553 failed: Error running script 200_pre/007_check_sru_install.sh
<a href="#">CSCwc48375</a>	Inbound IPSEC SA stuck inactive - many inbound SPIs for one outbound SPI in "show crypto ipsec sa"
<a href="#">CSCwc49369</a>	When searching IPv6 rule in the access-control policy, no result will show
<a href="#">CSCwc49952</a>	Selective deploy enables interaction with SRU interdependent-policies due to FMC API timeout
<a href="#">CSCwc50098</a>	show ssl-policy-config does not show the policy when countries are being used in source/dest network
<a href="#">CSCwc50887</a>	FTD - Traceback and reload on NAT IPv4&&IPv6 for UDP flow redirected over CCL link
<a href="#">CSCwc50891</a>	MPLS tagging removed by FTD
<a href="#">CSCwc52351</a>	ASA/FTD Cluster Split Brain due to NAT with "any" and Global IP/range matching broadcast IP
<a href="#">CSCwc52357</a>	Estreamer page fails to load in ASDM

Bug ID	Headline
<a href="#">CSCwc53280</a>	ASA parser accepts incomplete network statement under OSPF process and is present in show run
<a href="#">CSCwc54217</a>	syslog related to failover is not outputted in FPR2140
<a href="#">CSCwc54984</a>	IKEv2 rekey - Responding Invalid SPI for the new SPI received right after Create_Child_SA response
<a href="#">CSCwc56048</a>	AD username with trailing space causes download of users/groups to fail
<a href="#">CSCwc56952</a>	Able to see the SLA debug logs on both console & VTY sessions even if we enable only on VTY session.
<a href="#">CSCwc57088</a>	Limit the number of deployment jobs in deploy history to 50 as default to avoid slowness
<a href="#">CSCwc57975</a>	Snort3 crashes during the deployment - disabling TLS Server identity
<a href="#">CSCwc60037</a>	ASA fails to rekey with IPSEC ERROR: Failed to allocate an outbound hardware context
<a href="#">CSCwc60907</a>	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 35)
<a href="#">CSCwc62144</a>	FMC does not use proxy with authentication when accessing AMP cloud services
<a href="#">CSCwc62384</a>	Vulnerabilities on Cisco FTD Captive Portal on TCP port 885
<a href="#">CSCwc65907</a>	snort3 hangs in Crash handler which can lead to extended outage time during a snort crash
<a href="#">CSCwc66671</a>	FMC ACP PDF report generated in blank/0 bytes using UI
<a href="#">CSCwc67111</a>	Unable to bind to port 51320: Address already in use
<a href="#">CSCwc75061</a>	FMC allows shell access for user name with "." but external authentication will fail
<a href="#">CSCwc76195</a>	Fail-To-Wire interfaces flaps intermittently due to watchdog timeout in KP platform
<a href="#">CSCwc78296</a>	Database may fail to shut down and/or start up properly during upgrade
<a href="#">CSCwc83037</a>	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 36)
<a href="#">CSCwc88425</a>	FMC can download only the first 10000 cross-domain user groups
<a href="#">CSCwc88583</a>	Deployment fails with error Invalid Snort3IntrusionPolicy mode. Supports only inline and inline-test
<a href="#">CSCwc96136</a>	CCM layer (Seq 38) WR8, LTS18, LTS21
<a href="#">CSCwd07558</a>	Access Control Policy Deployments failing after upgrading to 7.0.4 on SFR Managed by ASDM
<a href="#">CSCwd09093</a>	Access rule policy page takes longer time to load

Bug ID	Headline
<a href="#">CSCwd09341</a>	Multiple log files have zero bytes on the FMC
<a href="#">CSCwd24072</a>	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 46: Resolved Bugs in Version 7.0.4**

Bug ID	Headline
<a href="#">CSCvj08826</a>	FMC ibdata1 file might grow large in size
<a href="#">CSCvw82067</a>	ASA/FTD 9344 blocks depleted due to high volume of fragmented traffic
<a href="#">CSCvx59252</a>	FXOS is not rotating log files for management interface
<a href="#">CSCvy16004</a>	Delay in DIFF calculations can cause deployment issues and HA App sync timeout in FTDs
<a href="#">CSCvy50598</a>	BGP table not removing connected route when interface goes down
<a href="#">CSCvy67765</a>	FTD VTI reports TUNNEL_SRC_IS_UP false despite source interface is up/up and working
<a href="#">CSCvy73130</a>	FP4100 platform: Active-Standby changed to dual Active after running "show conn" command
<a href="#">CSCvy99348</a>	Shutdown command reboots instead of shutting the FP1k device down.
<a href="#">CSCvz36903</a>	ASA traceback and reload while allocating a new block for cluster keepalive packet
<a href="#">CSCvz60142</a>	ASA/FTD stops serving SSL connections
<a href="#">CSCvz68713</a>	PLR license reservation for ASAv5 is requesting ASAv10
<a href="#">CSCvz69729</a>	Unstable client processes may cause LINA zmqio traceback on FTD
<a href="#">CSCvz70539</a>	Loggerd process is getting killed due to OOM under high logging rate
<a href="#">CSCwa00038</a>	Disk corruption occurs when /mnt/disk0 partition is full and blade is rebooted
<a href="#">CSCwa03732</a>	Deployment gets hung at snapshot generation phase during deploy or causes deploy slowness
<a href="#">CSCwa08640</a>	MonetDB crashing due to file size error
<a href="#">CSCwa21061</a>	FTD upgrade fails on 800_post/100_ftd_onbox_data_import.sh
<a href="#">CSCwa32628</a>	SFDataCorrelator crash at AddFileToPendingHash() due to race condition

Bug ID	Headline
<a href="#">CSCwa42350</a>	ASA installation/upgrade fails due to internal error "Available resources not updated by module"
<a href="#">CSCwa43311</a>	Snort blocking and dropping packet, with bigger size(1G) file download
<a href="#">CSCwa43475</a>	ASA SNMPd traceback in netsnmp_subtree_split
<a href="#">CSCwa45656</a>	SLR license application failes on manged devices
<a href="#">CSCwa48169</a>	ASA/FTD traceback and reload on netsnmp_handler_check_cache function
<a href="#">CSCwa59907</a>	LINA observed traceback on thread name "snmp_client_callback_thread"
<a href="#">CSCwa61361</a>	ASAv traceback when SD_WAN ACL enabled, then disabled (or vice-versa) in PBR
<a href="#">CSCwa62025</a>	IPv6: Some of egress interfaces of global and user vrf routes are missing in asp table
<a href="#">CSCwa68552</a>	All type-8 passwords are lost upon upgrade from ASA 9.12-9.15 to 9.16, failover gets disabled
<a href="#">CSCwa72530</a>	FTD: Time gap/mismatch seen when new node joins a Cluster Control node under history
<a href="#">CSCwa73172</a>	ASA reload and traceback in Thread Name: PIX Garbage Collector
<a href="#">CSCwa76621</a>	Memory Usage Warnings - System memory leak caused by run_hm.pl
<a href="#">CSCwa85340</a>	Unable to generate the PDF with access policy having large nested objects
<a href="#">CSCwa86210</a>	When PM disables mysqld, sometimes it is taking longer than expected to fully shutdown.
<a href="#">CSCwa90615</a>	WR8 and LTS18 commit id update in CCM layer (seq 24)
<a href="#">CSCwa95079</a>	ASA/FTD Traceback and reload due to NAT configuration
<a href="#">CSCwa95694</a>	Snort cores generated intermittently when SSL policy is enabled on the ASA-SFR module
<a href="#">CSCwa97910</a>	Connection event report displays the same device twice
<a href="#">CSCwa97917</a>	ISA3000 in boot loop after powercycle
<a href="#">CSCwa99931</a>	ASA/FTD: Tuning of update_mem_reference process
<a href="#">CSCwb01633</a>	FXOS misses logs to diagnose root cause of module show-tech file generation failure
<a href="#">CSCwb02060</a>	snmp-group host with Invalid host range and subnet causing traceback and reload
<a href="#">CSCwb02316</a>	"Non stop forwarding not supported on '1'" error while configuring MAC address
<a href="#">CSCwb05291</a>	Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability
<a href="#">CSCwb06543</a>	Increase logging level to diagnose LACP process unexpected restart events

Bug ID	Headline
<a href="#">CSCwb06847</a>	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-9-11543'
<a href="#">CSCwb07319</a>	Entitlement tags contain invalid character.
<a href="#">CSCwb07908</a>	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
<a href="#">CSCwb07981</a>	Traceback: Standby FTD reboots and generates crashinfo and lina core on thread name cli_xml_server
<a href="#">CSCwb08393</a>	SSL policy deploy failing from FMC: Timeout waiting for snort detection engines to process traffic
<a href="#">CSCwb08644</a>	ASA/FTD traceback and reload at IKEv2 from Scaled S2S+AC-DTLS+SNMP long duration test
<a href="#">CSCwb12465</a>	FIPS self-tests must be run when CC mode is enabled - files are missing
<a href="#">CSCwb13294</a>	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 25)
<a href="#">CSCwb16920</a>	CPU profile cannot be reactivated even if previously active memory tracking is disabled
<a href="#">CSCwb17187</a>	SNMP cores are generated every minute while running snmpwalk on HA
<a href="#">CSCwb17963</a>	Unable to identify dynamic rate limiting mechanism & not following msg limit per/sec at syslog server.
<a href="#">CSCwb19648</a>	SNMP queries for crasLocalAddress are not returning the assigned IPs for SSL/DTLS tunnels.
<a href="#">CSCwb19664</a>	Malware Block false positives triggered after upgrade to version 7.0.1
<a href="#">CSCwb22359</a>	Portmanager/LACP improvement to avoid false restarts and increase of logging events
<a href="#">CSCwb24039</a>	ASA traceback and reload on routing
<a href="#">CSCwb24101</a>	Loggerd syslog has stray incorrect timestamps, e.g. well before FirstPacketSecond
<a href="#">CSCwb25809</a>	Single Pass - Traceback due to stale ifc
<a href="#">CSCwb28047</a>	FMC - "Receiving thread exited with an exception: stoi" causing pxGrid to flap
<a href="#">CSCwb31699</a>	Primary takes active role after reload
<a href="#">CSCwb32841</a>	NAT (any,any) statements in-states the failover interface and resulting on Split Brain events
<a href="#">CSCwb40001</a>	Long delays when executing SNMP commands
<a href="#">CSCwb41361</a>	WR8, LTS18 and LTS21 commit id update in CCM layer (seq 26)
<a href="#">CSCwb43018</a>	Implement SNP API to check ifc and ip belongs to HA LU or CMD interface
<a href="#">CSCwb46949</a>	LTS18 commit id update in CCM layer (seq 27)



Bug ID	Headline
<a href="#">CSCwb49416</a>	ASA snmpd Traceback & cores on an active unit
<a href="#">CSCwb50405</a>	ASA/FTD Traceback in crypto hash function
<a href="#">CSCwb51707</a>	ASA Traceback and reload in process name: lina
<a href="#">CSCwb53172</a>	FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated
<a href="#">CSCwb53191</a>	Certificate validation fails post upgrade to 9.17.1
<a href="#">CSCwb53328</a>	ASA/FTD Traceback and reload caused by Smart Call Home process sch_dispatch_to_url
<a href="#">CSCwb54791</a>	ASA DHCP server fails to bind reserved address to Linux devices
<a href="#">CSCwb57615</a>	Configuring pbr access-list with line number failed.
<a href="#">CSCwb59465</a>	ASA/FTD may traceback (watchdog) and reload when generating a syslog from the VPN Failover subsystem
<a href="#">CSCwb59488</a>	ASA/FTD Traceback in memory allocation failed
<a href="#">CSCwb67040</a>	FP4112 4115 Traceback & reload on Thread Name: netfs_thread_init
<a href="#">CSCwb68642</a>	ASA traceback in Thread Name: SXP CORE
<a href="#">CSCwb71460</a>	ASA traceback in Thread Name: fover_parse and triggered by snmp related functions
<a href="#">CSCwb73248</a>	FW traceback in timer infra / netflow timer
<a href="#">CSCwb74357</a>	FXOS is not rotating log files for partition opt_cisco_platform_logs
<a href="#">CSCwb74571</a>	PBR not working on ASA routed mode with zone-members
<a href="#">CSCwb79812</a>	RIP is advertising all connected Anyconnect users and not matching route-map for redistribution
<a href="#">CSCwb80559</a>	FTD offloads SGT tagged packets although it should not
<a href="#">CSCwb80862</a>	ASA/FTD proxy arps any traffic when using the built-in 'any' object in translated destination
<a href="#">CSCwb82796</a>	ASA/FTD firewall may traceback and reload when tearing down IKE tunnels
<a href="#">CSCwb83388</a>	ASA HA Active/standby tracebacks seen approximately every two months.
<a href="#">CSCwb83691</a>	ASA/FTD traceback and reload due to the initiated capture from FMC
<a href="#">CSCwb84638</a>	Portmanager/LACP improvement to capture logging events on external event restarts
<a href="#">CSCwb85633</a>	Snmpwalk output of memory does not match show memory/show memory detail
<a href="#">CSCwb86118</a>	TPK ASA: Device might get stuck on ftp copy to disk

Bug ID	Headline
<a href="#">CSCwb87498</a>	Lina traceback and reload during EIGRP route update processing.
<a href="#">CSCwb88651</a>	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
<a href="#">CSCwb89004</a>	FMC DBcheck.pl hungs at "Checking mysql.rna_flow_stats_template against the current schema"
<a href="#">CSCwb90074</a>	ASA: Multiple Context Mixed Mode SFR Redirection Validation
<a href="#">CSCwb90532</a>	ASA/FTD traceback and reload on NAT related function nat_policy_find_location
<a href="#">CSCwb92583</a>	upgrade with a large amount of unmonitored disk space used can cause failed upgrade and hung device
<a href="#">CSCwb92709</a>	We can't monitor the interface via "snmpwalk" once interface is removed from context.
<a href="#">CSCwb93932</a>	ASA/FTD traceback and reload with timer services assertion
<a href="#">CSCwb94190</a>	ASA graceful shut down when applying ACL's with forward reference feature and FIPS enabled.
<a href="#">CSCwb94312</a>	Unable to apply SSH settings to ASA version 9.16 or later
<a href="#">CSCwb97251</a>	ASA/FTD may traceback and reload in Thread Name 'ssh'
<a href="#">CSCwc02416</a>	Not re-subscribing to ISE topics after certain ISE connectivity issues.
<a href="#">CSCwc02488</a>	ASA/FTD may traceback and reload in Thread Name 'None'
<a href="#">CSCwc02700</a>	Fragmented packets are dropped when unit leaves cluster
<a href="#">CSCwc03069</a>	Interface internal data0/0 is up/up from cli but up/down from SNMP polling
<a href="#">CSCwc08676</a>	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 32)
<a href="#">CSCwc09414</a>	ASA/FTD may traceback and reload in Thread Name 'ci/console'
<a href="#">CSCwc10483</a>	ASA/FTD - Traceback in Thread Name: appAgent_subscribe_nd_thread
<a href="#">CSCwc10792</a>	ASA/FTD IPSEC debugs missing reason for change of peer address and timer delete
<a href="#">CSCwc11597</a>	ASA tracebacks after SFR was upgraded to 6.7.0.3
<a href="#">CSCwc11663</a>	ASA traceback and reload when modifying DNS inspection policy via CSM or CLI
<a href="#">CSCwc13017</a>	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
<a href="#">CSCwc13382</a>	DCERPC traffic is dropped after upgrade to snort3 due to Parent flow is closed
<a href="#">CSCwc13994</a>	ASA - Restore not remove the new configuration for an interface setup after backup
<a href="#">CSCwc18218</a>	Database files on disk grow larger than expected for some frequently updated tables
<a href="#">CSCwc18312</a>	"show nat pool cluster" commands run within EEM scripts lead to traceback and reload

Bug ID	Headline
<a href="#">CSCwc23695</a>	ASA/FTD can not parse UPN from SAN field of user's certificate
<a href="#">CSCwc24906</a>	ASA/FTD traceback and reload on Thread id: 1637
<a href="#">CSCwc27797</a>	ASA mgmt ip cannot be released
<a href="#">CSCwc28334</a>	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
<a href="#">CSCwc28532</a>	9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing
<a href="#">CSCwc32246</a>	NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used
<a href="#">CSCwc41590</a>	Upgrade fail & App Instance fail to start with err "CSP_OP_ERROR. CSP signature verification error."
<a href="#">CSCwc53680</a>	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 47: Resolved Bugs in Version 7.0.3**

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

## Resolved Bugs in Version 7.0.2.1

Table last updated: 2022-06-27

**Table 48: Resolved Bugs in Version 7.0.2.1**

Bug ID	Headline
<a href="#">CSCwb93932</a>	ASA/FTD traceback and reload with timer services assertion

## Resolved Bugs in Version 7.0.2

Table last updated: 2022-05-05

**Table 49: Resolved Bugs in Version 7.0.2**

Bug ID	Headline
<a href="#">CSCvt68055</a>	snmpd is respawning frequently on fxos for FP21xx device
<a href="#">CSCvy82668</a>	SSH session not being released
<a href="#">CSCvy64145</a>	WR6 and WR8 commit id update in CCM layer(sprint 113, seq 12)
<a href="#">CSCvt15348</a>	ASA show processes cpu-usage output is misleading on multi-core platforms
<a href="#">CSCvy72841</a>	Firepower 1K FTD sends LLDP packets with internal MAC address of eth2 interface
<a href="#">CSCvz80981</a>	SNMPv3 doesn't work for SFR modules running version 7.0
<a href="#">CSCvy08351</a>	Intrusion and Correlation Email Alerts stop being sent to mail server
<a href="#">CSCvz66474</a>	Snmpd core files generated on FTD
<a href="#">CSCvx75683</a>	The 'show cluster info trace' output is overwhelmed by 'tag does not exist' messages
<a href="#">CSCvz25434</a>	ASA/FTD blackholes traffic due to 1550 block depletion when BVI is configured as DHCP client
<a href="#">CSCwa45799</a>	High CPU on FXOS due to bcm_usd process
<a href="#">CSCwa18889</a>	Clock drift observed between Lina and FXOS on multi-instance
<a href="#">CSCvy99217</a>	IKEv2: SA Error code should be translated to human friendly reason
<a href="#">CSCvz00961</a>	AnyConnect connection failure related to ASA truncated/corrupt config
<a href="#">CSCvz36905</a>	If we add v6 route same as V route , duplicate entry is getting created.
<a href="#">CSCwa58060</a>	LSP download fails if no ICMP reply is received from updates-talos.sco.cisco.com
<a href="#">CSCvz03524</a>	PKI "OCSP revocation check" failing due to sha256 request instead of sha1
<a href="#">CSCwa74900</a>	Traceback and reload after enabling debug webvpn cifs 255
<a href="#">CSCvz29233</a>	ASA: ARP entries from custom context not removed when an interface flap occurs on system context
<a href="#">CSCvy35416</a>	Deploy failure from global domain when parallel deploy triggered to different child domains
<a href="#">CSCvy99218</a>	VDB Version shouldn't be update if fails
<a href="#">CSCvz81888</a>	NTP will not change to *(synced) status after upgrade to asa-9.15.1/9.16.1.28 from asa-9.14.3

Bug ID	Headline
<a href="#">CSCvx66329</a>	FTD Hotfix Cisco_FTD_SSP_FP2K_Hotfix_O installation fails on script 000_start/125_verify_bundle.sh
<a href="#">CSCvz75988</a>	Inconsistent logging timestamp with RFC5424 enabled
<a href="#">CSCvz52199</a>	Increase precision of ASA VPN load-balancing algorithm
<a href="#">CSCvz48407</a>	Traceback and reload in Thread Name: DATAPATH-15-18621
<a href="#">CSCvz05687</a>	Fragmented Certificate request failed for DND flow
<a href="#">CSCwa96759</a>	Lina may traceback and reload on tcpmod_proxy_handle_mixed_mode
<a href="#">CSCvz90722</a>	With object-group in crypto ACL sum of hitcnt mismatches with the individual elements
<a href="#">CSCvz59950</a>	IKEv2 Crash from scaled long duration test on KP-FPR2130
<a href="#">CSCvz38332</a>	FTD/ASA - Stuck in boot loop after upgrade from 9.14.2.15 to 9.14.3
<a href="#">CSCvz55140</a>	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 117, seq 17)
<a href="#">CSCwa58686</a>	ASA/FTD Change in OGS compilation behavior causing boot loop
<a href="#">CSCvz43455</a>	ASAv observed traceback while upgrading hostscan
<a href="#">CSCvz20679</a>	FTDv - Lina Traceback and reload
<a href="#">CSCvz60578</a>	Cluster unit in MASTER_POST_CONFIG state should transition to Disabled state after an interval
<a href="#">CSCvz59464</a>	IPReputation Feed Error Message-Method Not Allowed
<a href="#">CSCvy31424</a>	QP FTD application fails to start due to outdated affinity.conf following FXOS/FTD upgrade
<a href="#">CSCvz79930</a>	Snort3 .dmp and crashinfo files are not managed by diskmanager
<a href="#">CSCvy89144</a>	Cisco ASA and FTD Web Services Denial of Service Vulnerability
<a href="#">CSCwa19713</a>	Traffic dropped by ASA configured with BVI interfaces due to asp drop type "no-adjacency"
<a href="#">CSCvz70958</a>	High Control Plane CPU on StandBy due to dhcpp_add_ip_l_stby
<a href="#">CSCvz61689</a>	Port-channel member interfaces are lost and status is down after software upgrade
<a href="#">CSCvz92016</a>	Cisco ASA and FTD Software Web Services Interface Privilege Escalation Vulnerability
<a href="#">CSCvz34831</a>	If ASA fails to download DACL it will never stop trying
<a href="#">CSCvz90375</a>	Low available DMA memory on ASA 9.14 at boot reduces AnyConnect sessions supported
<a href="#">CSCvy40401</a>	L2L VPN session bringup fails when using NULL encryption in ipsec configuration

Bug ID	Headline
<a href="#">CSCwa76822</a>	Tune throttling flow control on syslog-ng destinations
<a href="#">CSCvz33468</a>	ASA/FTD - NAT stops translating source addresses after changes to object-groups in manual NAT Rule
<a href="#">CSCwa11186</a>	Mask sensitive information in aaa ldap debugs
<a href="#">CSCvz00383</a>	FTD lina traceback and reload in thread Name Checkheaps
<a href="#">CSCvy17030</a>	FMC Connection Events page "Error: Unable to process this query. Please contact support."
<a href="#">CSCvx97053</a>	Unable to configure ipv6 address/prefix to same interface and network in different context
<a href="#">CSCvx24470</a>	FTD/FDM: RA VPN sessions disconnected after every deployment if custom port for RA VPN is configured
<a href="#">CSCwa05385</a>	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 19)
<a href="#">CSCvz96440</a>	FMC should not create archival for NGIPS devices
<a href="#">CSCwa68660</a>	FTP inspection stops working properly after upgrading the ASA to 9.12.4.x
<a href="#">CSCvy98027</a>	Application interface down whereas physical interface Up on FXOS
<a href="#">CSCvx95652</a>	ASAv Azure: Some or all interfaces might stop passing traffic after a certain period of run time
<a href="#">CSCvz73146</a>	FTD - Traceback in Thread Name: DATAPATH
<a href="#">CSCwa87597</a>	ASA/FTD Failover: Joining Standby reboots when receiving configuration replication from Active mate
<a href="#">CSCwb01919</a>	FP2140 ASA 9.16.2 HA units traceback and reload at lua_getinfo (getfuncname)
<a href="#">CSCvy96895</a>	ASA disconnects the VTY session using of Active IP address and Standby MAC address after failed over
<a href="#">CSCwa55878</a>	FTD Service Module Failure: False alarm of "ND may have gone down"
<a href="#">CSCwa14725</a>	ASA/FTD traceback and reload on IKE Daemon Thread
<a href="#">CSCvy35737</a>	FTD traceback and reload during anyconnect package verification
<a href="#">CSCvz91218</a>	Statelink hello messages dropped on Standby unit due to interface ring drops on high rate traffic
<a href="#">CSCwa20758</a>	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 20)
<a href="#">CSCwa67882</a>	Offloaded GRE tunnels may be silently un-offloaded and punted back to CPU
<a href="#">CSCwa67884</a>	Conditional flow-offload debugging produces no output

Bug ID	Headline
<a href="#">CSCwa97784</a>	ASA: Jumbo sized packets are not fragmented over the L2TP tunnel
<a href="#">CSCwa29956</a>	"Interface configuration has changed on device" message may be shown after FTD upgrade
<a href="#">CSCwa60574</a>	ASA traceback and reload on snp_ha_trans_alloc_msg_muxbuf_space function
<a href="#">CSCwa89243</a>	SNMP no longer responds to polls after upgrade to 9.15.1.17
<a href="#">CSCvz30582</a>	Cisco Firepower Management Center Cross-site Scripting Vulnerability
<a href="#">CSCwa04461</a>	Cisco ASA Software and FTD Software Remote Access SSL VPN Denial of Service
<a href="#">CSCwa30114</a>	"Error:NAT unable to reserve ports" when using a range of ports in an object service
<a href="#">CSCvy80030</a>	ENH: Addition of "show coredump filesystem" to "show tech" output
<a href="#">CSCwa39680</a>	Snort stops processing packets when SSL decryption debug enabled - Snort2
<a href="#">CSCvy96803</a>	ASA/FTD traceback and reload in Process Name "lina" or "snmp_alarm_thread"
<a href="#">CSCvz34149</a>	Update the new location of /opt/cisco/platfom/logs/var/log/messages
<a href="#">CSCvo77184</a>	VMware ASAv should default to vmxnet3, not e1000
<a href="#">CSCvx92932</a>	Missing events on FMC due to SFDataCorrelator process exiting
<a href="#">CSCwa79980</a>	SNMP get command in FPR does not show interface index.
<a href="#">CSCvz38976</a>	7.1/Firepower Threat Defense device occasionally unable to pass large packets/Fragmentation failures
<a href="#">CSCvz64470</a>	ASA/FTD Traceback and reload due to memory corruption when generating ICMP unreachable message
<a href="#">CSCwb34035</a>	ASA CLI gets hung randomly while configuring SNMP
<a href="#">CSCvz00032</a>	Cisco Firepower Threat Defense Software TCP Proxy Denial of Service Vulnerability
<a href="#">CSCvu23149</a>	Backup generation in FMC fails due to corrupt SID_GID_ORD index in database table rule_opts
<a href="#">CSCwa57115</a>	New access-list are not taking effect after removing non-existence ACL with objects.
<a href="#">CSCvz37306</a>	ASDM session is not served for new user after doing multiple context switches in existing user
<a href="#">CSCwa53489</a>	Lina Traceback and Reload Due to invalid memory access while accessing Hash Table
<a href="#">CSCvy98458</a>	FP21xx -traceback "Panic:DATAPATH-10-xxxx -remove_mem_from_head: Error - found a bad header"
<a href="#">CSCvy52924</a>	FTD loses OSPF network statements config for all VRF instances upon reboot

Bug ID	Headline
<a href="#">CSCvz92932</a>	ASA show tech execution causing spike on CPU and impacting to IKEv2 sessions
<a href="#">CSCvz44339</a>	FTD - Deployment will fail if you try to delete an SNMP host with ngfw-interface and host-group
<a href="#">CSCwa40223</a>	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
<a href="#">CSCvy47108</a>	Remote Access IKEv2 VPN session cannot be established because of stuck Uauth entry
<a href="#">CSCvy86780</a>	Error Could not complete LSP installation. Please try again.
<a href="#">CSCvz57710</a>	conf t is converted to disk0:/t under context-config mode
<a href="#">CSCvz14377</a>	Losing admin and other users from Mysql DB and EO
<a href="#">CSCvz89126</a>	ASDM session/quota count mismatch in ASA when multiple context switchover is done from ASDM
<a href="#">CSCvy78209</a>	Getting Snort High CPU alerts but top.log is not showing high CPU
<a href="#">CSCwa19443</a>	Flow Offload - Compare state values remains in error state for longer periods
<a href="#">CSCvy91668</a>	PAT pool exhaustion with stickiness traffic could lead to new connection drop.
<a href="#">CSCwa70008</a>	Expired certs cause Security Intelligence updates to fail
<a href="#">CSCvz81480</a>	IV in the outbound pkt is not updated on Nitrox V platforms when GCM is used for IPsec
<a href="#">CSCvx70480</a>	403 error when accessing Policies -&gt; Access Control after exporting User Role from FMC(4600) to FMCv
<a href="#">CSCwa18795</a>	Crash at "thread: Unicorn Proxy Thread cpu: 7 watchdog_cycles" from Scaled AC-SSL TVM Profile test
<a href="#">CSCvz67816</a>	IPV6 DNS PTR query getting modified on FTD
<a href="#">CSCvy96698</a>	Resolve spurious status actions checking speed values twice in FXOS portmgr
<a href="#">CSCvs85607</a>	FXOS login breaks when log partition gets full
<a href="#">CSCwb18252</a>	FTD/ASA: Traceback on BFD function causing unexpected reboot
<a href="#">CSCvz02076</a>	Snort reload times out causing restart
<a href="#">CSCvz44645</a>	FTD may traceback and reload in Thread Name 'lina'
<a href="#">CSCwa79676</a>	FPR1010 in HA Printing Broadcast Storm Alerts for Multiple Interfaces
<a href="#">CSCvy24921</a>	SNMPv3 - SNMP EngineID changes after every configuration change
<a href="#">CSCvz36933</a>	Sensor SNMP process may restart when policy deploy



Bug ID	Headline
<a href="#">CSCvz86796</a>	Crash in thread CMP when doing CMPV2 enrollment
<a href="#">CSCvz70316</a>	LINA may generate traceback and reload
<a href="#">CSCwa60300</a>	axios 0.21.1
<a href="#">CSCvy30392</a>	Backup generation on FMC fails due to corrupt int_id index in table ids_event_msg_map
<a href="#">CSCvz55849</a>	FTD Traceback and Reload on process LINA
<a href="#">CSCvz61160</a>	ASA traceback on DATAPATH when handling ICMP error message
<a href="#">CSCvx43150</a>	On the FMC, process of registration of member device post RMA is not successful
<a href="#">CSCwa91090</a>	SSL handshake logging showing unknown session during AnyConnect TLSv1.2 Session establishment
<a href="#">CSCvz43848</a>	TID source stuck at parsing state
<a href="#">CSCvz61767</a>	Policy deployment with SNMPv2 or SNMPv1 configuration fails
<a href="#">CSCvz69571</a>	ASA log shows wrong value of the transferred data after the anyconnect session terminated.
<a href="#">CSCwa51862</a>	LSP downloads fail when using proxy
<a href="#">CSCwa31373</a>	duplicate ACP rules are generated on FMC 6.6.5 after rule copy.
<a href="#">CSCwa65389</a>	ASA traceback and reload in Unicorn Admin Handler when change interface configuration via ASDM
<a href="#">CSCwa32286</a>	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 125, seq 21)
<a href="#">CSCwa08262</a>	AnyConnect users with mapped group-policies take attributes from default GP under the tunnel-group
<a href="#">CSCvy96625</a>	Roll back changes introduced by CSCvr33428 and CSCvy39659
<a href="#">CSCwa36678</a>	Random FTD reloads with the traceback during deployment from FMC
<a href="#">CSCvz50712</a>	TLS server discovery uses incorrect source IP address for probes in AnyConnect deployment
<a href="#">CSCwa41918</a>	ssl inspection may have unexpected behavior when evicting certificates
<a href="#">CSCwa36672</a>	ASA on FPR4100 traceback and reload when running captures using ASDM
<a href="#">CSCvz64548</a>	SFTunnel on device not processing event messages
<a href="#">CSCvy93480</a>	Cisco ASA and FTD Software IKEv2 Site-to-Site VPN Denial of Service Vulnerability
<a href="#">CSCvy43002</a>	Observed crash while running SNMPWalk + S2S-IKEv2 and AnyConnect TVM Profiles

Bug ID	Headline
<a href="#">CSCwa46963</a>	Security: CVE-2021-44228 -&gt; Log4j 2 Vulnerability
<a href="#">CSCvy74984</a>	ASAv on Azure loses connectivity to Metadata server once default outside route is used
<a href="#">CSCvv36788</a>	MsgLayer[PID]: Error : Msglyr::ZMQWrapper::registerSender() : Failed to bind ZeroMQ Socket
<a href="#">CSCvy97080</a>	Snort3 unexpected restart while processing SMB traffic
<a href="#">CSCwa67145</a>	Realm download fails if one of the groups is deleted on the AD
<a href="#">CSCvz77744</a>	OSPFv3: FTD Wrong "Forwarding address" added in ospfv3 database
<a href="#">CSCvz17923</a>	Dispatcher doesn't account for asynclock pend q work under some conditions result lower cpu util
<a href="#">CSCvx67851</a>	PLR on FDM for ISA3000
<a href="#">CSCwa56449</a>	ASA traceback in HTTP cli EXEC code
<a href="#">CSCvz77662</a>	Crash at data-path from Scaled AC-SSL TVM Profile test.
<a href="#">CSCwb09219</a>	ASA/FTD: OCSP may fail to work after upgrade due to "signer certificate not found"
<a href="#">CSCvz84850</a>	ASA/FTD traceback and reload caused by "timer services" function
<a href="#">CSCwa42594</a>	ASA: IP Header check validation failure when GTP Header have SEQ and EXT field
<a href="#">CSCwa40312</a>	Standby ASA unit showing wrong IPV6 messages
<a href="#">CSCwa88571</a>	Unable to register FMC with the Smart Portal
<a href="#">CSCvk62945</a>	ASA: Syslog 317007 not found error received
<a href="#">CSCvz38692</a>	ASAv traceback in snmp_master_callback_thread and reload
<a href="#">CSCwa50145</a>	FPR8000 sensor UI login creates shell user with basic privileges
<a href="#">CSCvz08387</a>	ASP drop capture output may display incorrect drop reason
<a href="#">CSCvy35352</a>	Error handling for Suppression settings needed in certain conditions
<a href="#">CSCvy69453</a>	WM Standby device do not send out coldstart trap after reboot.
<a href="#">CSCwa02929</a>	FTD Blocks Traffic with SSL Flow Error CORRUPT_MESSAGE
<a href="#">CSCvz89545</a>	SSL VPN performance degraded and significant stability issues after upgrade
<a href="#">CSCvz24765</a>	device rebooted with snmpd core
<a href="#">CSCvz07614</a>	ASA: Orphaned SSH session not allowing us to delete a policy-map from CLI
<a href="#">CSCvy40482</a>	9.14MR3: snmpwalk got failed with [Errno 146] Connection refused error.

Bug ID	Headline
<a href="#">CSCvz02425</a>	Deployment failing due to NPE while reading policy names
<a href="#">CSCvz28103</a>	FDM: Saving DHCP relay config throws flex-config/smart CLI error
<a href="#">CSCvz01604</a>	ASA High CPU (100%) when testing DDoS under 100K CPS rate despite fix introduced by CSCvx82503
<a href="#">CSCvu96436</a>	Traceback of master and one slave when a particular lock is contended for long
<a href="#">CSCvy79952</a>	ASA/FTD traceback and reload after downgrade
<a href="#">CSCvx80830</a>	VPN conn fails from same user if Radius server sends a dACL and vpn-simultaneous-logins is set to 1
<a href="#">CSCvy39791</a>	Lina traceback and core file size is beyond 40G and compression fails.
<a href="#">CSCvy64911</a>	Debugs for: SNMP MIB value for crasLocalAddress is not showing the IP address
<a href="#">CSCwa68805</a>	FTD Traceback & reload during HA creation
<a href="#">CSCvz71064</a>	Deleting The Context From ASA taking Almost 2 Minutes with ikev2 tunnel
<a href="#">CSCvz40352</a>	ASA traffic dropped by Implicit ACL despite the fact of explicit rules present on Access-list
<a href="#">CSCvz86256</a>	Primary ASA should send GARP as soon as split-brain is detected and peer becomes cold standby
<a href="#">CSCvy34333</a>	When ASA upgrade fails, version status is desynched between platform and application
<a href="#">CSCvz72771</a>	ASA/FTD may traceback and reload. "c_assert_cond_terminate" in stack trace
<a href="#">CSCvw37191</a>	FXOS SNMPv3 Engine ID changes after reboot
<a href="#">CSCwa34287</a>	ASA: Loss of NTP sync following a reload after upgrade
<a href="#">CSCvz83432</a>	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 121, seq 18)
<a href="#">CSCwa31508</a>	Continuous deployment failure on QW-4145 device
<a href="#">CSCvz81342</a>	Diskmanager not pruning AMP File Capture files
<a href="#">CSCvy60831</a>	ASA/FTD Memory block location not updating for fragmented packets in data-path
<a href="#">CSCvz67003</a>	ASDM session count and quota management's count mismatch. 'Lost connection firewall' msg in ASDM
<a href="#">CSCvz67001</a>	FMC Event backups to remote SSH storage targets fail
<a href="#">CSCvz47709</a>	[IMS_7_1_0] DeployACPolicyPostUpgrade at Upgrade FMC 7.1.0 - 2022
<a href="#">CSCvz23157</a>	SNMP agent restarts when show commands are issued
<a href="#">CSCwa96327</a>	Incorrect ifHighSpeed value for a interfaces that are port channel members

Bug ID	Headline
<a href="#">CSCvw29647</a>	FTD: NAS-IP-Address:0.0.0.0 in Radius Request packet as network interface for aaa-server not defined
<a href="#">CSCvz61658</a>	CPU hogs in update_mem_reference
<a href="#">CSCvy78525</a>	VRF route lookup for TCP ping is missing
<a href="#">CSCvz82562</a>	ASA/FTD: site-to-site VPN - traffic incorrectly fragmented
<a href="#">CSCvy56395</a>	ASA traceback and reload due to snmp encrypted community string when key config is present
<a href="#">CSCwa79494</a>	Traffic keep failing on Hub when IPsec tunnel from Spoke flaps
<a href="#">CSCvz88149</a>	Lina traceback and reload during block free causing FTD boot loop
<a href="#">CSCvy89658</a>	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 114, seq 13)
<a href="#">CSCvz38361</a>	BGP packets dropped for non directly connected neighbors
<a href="#">CSCvx14489</a>	snmpwalk fails on ipv6 interface post a failover
<a href="#">CSCwa90408</a>	Crash on SSH SCP from long duration test.
<a href="#">CSCvz58710</a>	ASA traceback due to SCTP traffic.
<a href="#">CSCvy55439</a>	FTDv throughput degradation due to frequent PDTS read/write
<a href="#">CSCvy08972</a>	Event Database runs into utf8 error causing pause in processing of events
<a href="#">CSCwa35200</a>	Some syslogs for AnyConnect SSL are generated in admin context instead of user context
<a href="#">CSCvi58484</a>	Cluster: ping sourced from FTD/ASA to external IPs may if reply lands on different cluster unit
<a href="#">CSCvz30558</a>	Cisco Firepower Management Center Cross-site Scripting Vulnerability
<a href="#">CSCwa69303</a>	ASA running on SSP platform generate critical error "[FSM:FAILED]: sam:dme:MgmtIfSwMgmtOobIfConfig"
<a href="#">CSCwb42846</a>	Snort instance CPU stuck at 100%
<a href="#">CSCvy73585</a>	FMC should not allow to configure port-channel ID higher than 8 on FPR1010
<a href="#">CSCvz95108</a>	FTD Deployment failure post upgrade due to major version change on device
<a href="#">CSCwa38277</a>	ASA NAT66 with big range as a pool don't works with IPv6
<a href="#">CSCvy33501</a>	FDM failover pair - new configured sVTI IPSEC SA is not synced to standby. FDM shows HA not in sync
<a href="#">CSCvy21334</a>	Active tries to send CoA update to Standby in case of "No Switchover"

Bug ID	Headline
<a href="#">CSCvz20544</a>	ASA/FTD may traceback and reload in loop processing Anyconnect profile
<a href="#">CSCvz61431</a>	"Netsnmp_update_ma_config: ERROR Failed to build req" messages seen during cluster configuration sync
<a href="#">CSCvv43190</a>	Crypto engine errors when GRE header protocol field doesn't match protocol field in inner ip header
<a href="#">CSCvy04430</a>	Management Sessions fail to connect after several weeks
<a href="#">CSCvy95329</a>	Incorrect Access rule matching because of ac rule entry missing
<a href="#">CSCvy04343</a>	ASA in PLR mode,"license smart reservation" is failing.
<a href="#">CSCwa25033</a>	Unexpected HTTP/2 data frame causing segfault
<a href="#">CSCvz53884</a>	SNMP OID HOST-RESOURCES-MIB (1.3.6.1.2.1.25) does not exist on FMC
<a href="#">CSCwb01700</a>	ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA
<a href="#">CSCvz55395</a>	TCP connections are cleared after configured idle-timeout even though traffic is present
<a href="#">CSCvx36885</a>	ASA reload and traceback in DATAPATH
<a href="#">CSCvz05468</a>	Multiple SSH host entries in platform settings as first feature enable/deploy will break SSH on LINA
<a href="#">CSCvz95949</a>	FP1120 9.14.3 : temporary split brain happened after active device reboot
<a href="#">CSCvz65181</a>	Cisco Firepower Threat Defense Software Security Intelligence DNS Feed Bypass Vulnerabilit
<a href="#">CSCwa98684</a>	Console has an excessive rate of warnings during policy deployment
<a href="#">CSCvy10789</a>	FTD 2110 ascii characters are disallowed in LDAP password
<a href="#">CSCvz12494</a>	In FPR2100,after power off/on,the fxos version is mismatched with asa version.
<a href="#">CSCvz62578</a>	Cannot edit or move AC rules for SFR module in Administrator rules section in ASDM
<a href="#">CSCwa26353</a>	snort3 - Policy does not become dirty after updating LSP -when only custom intrusion policies in use
<a href="#">CSCvz55302</a>	FTD/ASA Traceback and reload due to SSL null checks under low memory conditions
<a href="#">CSCwa85043</a>	Traceback: ASA/FTD may traceback and reload in Thread Name 'Logger'
<a href="#">CSCvz39646</a>	ASA/AnyConnect - Stale RADIUS sessions
<a href="#">CSCwa13873</a>	ASA Failover Split Brain caused by delay on state transition after "failover active" command run

Bug ID	Headline
<a href="#">CSCvz85437</a>	FTD 25G, 40G and 100G interfaces down after upgrade of FXOS and FTD to 2.10.1.159 and 6.6.4
<a href="#">CSCvv48942</a>	Snmpwalk showing traffic counter as 0 for failover interface
<a href="#">CSCvy74781</a>	The standby device is sending the keep alive messages for ssl traffic after the failover
<a href="#">CSCwa36661</a>	Traffic is not hitting on some egress interfaces of user vrf due to routes missing in asp table
<a href="#">CSCvz69699</a>	Unable to access UI of FMC integrated with ISE using PxGrid
<a href="#">CSCwa33364</a>	FTD misleading OVER_SUBSCRIBED flow flag for mid-stream flow-issue seen on MR branches
<a href="#">CSCwa11052</a>	SNMP Stopped Responding After Upgrading to Version- 9.14(2)15
<a href="#">CSCwa48849</a>	ssl unexpected behavior with resumed sessions
<a href="#">CSCwa56975</a>	DHCP Offer not seen on control plane
<a href="#">CSCvy78573</a>	cloudagent should not send zero-length urls to beaker for lookup
<a href="#">CSCvz58376</a>	Snort down after deploying the policy
<a href="#">CSCvz36862</a>	FMC policy deployment takes more than 15 min on phase 3
<a href="#">CSCvw65324</a>	mserver core on buildout FMC caused by concurrent merge table queries
<a href="#">CSCvy58268</a>	Block 80 and 256 exhaustion snapshots are not created
<a href="#">CSCvx79526</a>	Cisco ASA and FTD Software Resource Exhaustion Denial of Service Vulnerability
<a href="#">CSCvz93407</a>	IPS policy with space in name becomes unusable after upgrade
<a href="#">CSCwa36889</a>	FTD management interface programming is broken in FXOS
<a href="#">CSCvu18510</a>	MonetDB's eventdb crash causes loss of connection events on FMC
<a href="#">CSCvz53993</a>	Random packet block by Snort in SSL flow
<a href="#">CSCvz53142</a>	ASA does not use the interface specified in the name-server command to reach IPv6 DNS servers
<a href="#">CSCvz00934</a>	Not able to configure VTI with tunnel source as (FMC Access) data-interface
<a href="#">CSCwa40719</a>	Traceback: Secondary firewall reloading in Threadname: fover_parse
<a href="#">CSCvy35948</a>	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 111, seq 11)
<a href="#">CSCwa17918</a>	Unable to uncheck option Always advertise the default route for OSPF
<a href="#">CSCwa55418</a>	multiple db folders current-policy-bundle after deployment with anyconnect package before upgrade

Bug ID	Headline
<a href="#">CSCvz35787</a>	FTD misleading OVER_SUBSCRIBED flow flag for mid-stream flow
<a href="#">CSCvz15676</a>	In Firepower 1010 device, after upgrading ASA app, device going for fail safe mode
<a href="#">CSCvz70595</a>	Traceback observed on ASA while handling SAML handler
<a href="#">CSCvy90836</a>	ASA Traceback and reload in Thread Name: SNMP ContextThread
<a href="#">CSCvz78816</a>	ASA disconnects the ssh, https session using of Active IP address and Standby MAC address after FO
<a href="#">CSCvz30933</a>	ASA tracebacks and reload when clear configure snmp-server command is issued
<a href="#">CSCvz96462</a>	IP Address 'in use' though no VPN sessions
<a href="#">CSCvz94573</a>	MIO heartbeat failure caused by heartbeat dropped by delay
<a href="#">CSCwa14485</a>	Cisco Firepower Threat Defense Software Denial of Service Vulnerability
<a href="#">CSCwa33898</a>	Cisco Adaptive Security Appliance Software Clientless SSL VPN Heap Overflow Vulnerability
<a href="#">CSCvy19170</a>	SAML: Memory leaks observed for AnyConnect IKEv2
<a href="#">CSCwa99932</a>	ASA/FTD stuck after crash and reboot
<a href="#">CSCvz89327</a>	OSPFv2 flow missing cluster centralized "c" flag
<a href="#">CSCwa03347</a>	IPv6 PIM packets are dropped in ASP with invalid-ip-length drop reason
<a href="#">CSCvz05541</a>	ASA55XX: Expansion module interfaces not coming up after a software upgrade
<a href="#">CSCwa34110</a>	FMC should support southern hemisphere DST configurations
<a href="#">CSCvy90162</a>	Seen crash related to watchdog bark at Unicorn Proxy Thread from scaled AC-SSL-SAML Auth TVM profile
<a href="#">CSCvz71569</a>	FTD Traceback & reload due to process ZeroMQ out of memory condition
<a href="#">CSCvz25454</a>	ASA: Drop reason is missing from 129 lines of asp-drop capture
<a href="#">CSCvz68336</a>	SSL decryption not working due to single connection on multiple in-line pairs
<a href="#">CSCvy37484</a>	Entries in device_policy_ref is huge causing slow performance when opening DeviceManagement page
<a href="#">CSCvz41761</a>	FMC Does not allow to create an EIGRP authentication secret key using the \$ character
<a href="#">CSCvq29993</a>	FPR2100 ONLY - PERMANENT block leak of size 80, 256, and 1550 memory blocks & blackholes traffic
<a href="#">CSCwa76564</a>	ASDM session/quota count mismatch in ASA when multiple context switch before and after failover

Bug ID	Headline
<a href="#">CSCvz05189</a>	FTD reload with Lina traceback during xlate replication in Cluster
<a href="#">CSCwa87315</a>	ASA/FTD may traceback and reload in Thread Name 'IP Address Assign'
<a href="#">CSCvc57575</a>	ISIS:Invalid ISIS debugs displayed while deleting context.
<a href="#">CSCvy32366</a>	After upgrading ASA to 9.15(1)10, ASDM 7.15(1)150 One Time Password (OTP) field does not appear
<a href="#">CSCvw62288</a>	ASA: 256 byte block depletion when syslog rate is high
<a href="#">CSCvy60574</a>	Port dcosAG leak fix CSCvx14602 to KP/WM
<a href="#">CSCvz00699</a>	Traceback in webvpn and reload experienced periodically after ASA upgrade
<a href="#">CSCvz66795</a>	ASA traceback and reload in SSH process when executing the command "show access-list"
<a href="#">CSCvz09109</a>	Cluster CCL interface capture shows full packets although headers-only is configured
<a href="#">CSCwa28822</a>	FTD moving UI management from FDM to FMC causes traffic to fail
<a href="#">CSCvz51258</a>	show tech-support output can be confusing when there crashinfo, need to clean up/make more intuitive
<a href="#">CSCwa26038</a>	ICMP inspection causes packet drops that are not logged appropriately
<a href="#">CSCwb15795</a>	Audit message not generated by: no logging enable from ASAv9.12
<a href="#">CSCvz09106</a>	Cisco ASA and FTD Software SSL VPN Denial of Service Vulnerability
<a href="#">CSCvy41763</a>	Cisco Firepower Threat Defense Software XML Injection Vulnerability
<a href="#">CSCwa41834</a>	ASA/FTD traceback and reload due to pix_startup_thread
<a href="#">CSCvy89648</a>	ma_ctx files with '.backup' extension seen after applying the workaround for CSCvx29429
<a href="#">CSCvz02398</a>	Crypto archive generated with SE ring timeout on 7.0
<a href="#">CSCvz76746</a>	While implementing management tunnel a user can use open connect to bypass anyconnect.
<a href="#">CSCvz76745</a>	SFDataCorrelator memory growth with cloud-based malware events
<a href="#">CSCvz91618</a>	KP - traceback observed when add and remove snmp host-group
<a href="#">CSCvz99222</a>	Clear and show conn for inline-set is not working
<a href="#">CSCvy53461</a>	RSA keys & Certs get removed post reload on WS-SVC-ASA-SM1-K7 with ASA code 9.12.x
<a href="#">CSCvy75724</a>	ZMQ OOM due to less Msglyr pool memory in low end platforms



Bug ID	Headline
<a href="#">CSCvz05767</a>	FP-1010 HA link goes down or New hosts unable to connect to the device
<a href="#">CSCwa28895</a>	FTD SSL Proxy should allow configurable or dynamic maximum TCP window size
<a href="#">CSCvz06652</a>	snmpd corefiles noticed on SNMP longevity setup
<a href="#">CSCvz50922</a>	FPR2100: Unable to form L2L VPN tunnels when using ESP-Null encryption
<a href="#">CSCvz95743</a>	Loss of NTP sync following an upgrade
<a href="#">CSCvz77037</a>	FMC user interface access may fail with SSL errors in mojo-server
<a href="#">CSCvy96325</a>	FTD/ASA: Adding new ACE entries to ACP causes removal and re-add of ACE elements in LINA
<a href="#">CSCwa69376</a>	under stress, getting bus error in snmp_logging.c:1303
<a href="#">CSCwa53088</a>	snort 2 ssl-debug files may not be written
<a href="#">CSCvx81447</a>	The dnsproxy log messages are displayed continuously on the ASA
<a href="#">CSCwa39683</a>	log file flooded by ssl_policy log_error messages when ssl debug is enabled
<a href="#">CSCvy58697</a>	ssl shared cache process can leak memory
<a href="#">CSCvz24238</a>	Cisco Firepower Management Center Cross-site Scripting Vulnerability
<a href="#">CSCwa15185</a>	ASA/FTD: remove unwanted process call from LUA
<a href="#">CSCvw56551</a>	ASA displays cosmetic NAT warning message when making the interface config changes
<a href="#">CSCvz76848</a>	FTD traceback and reload when using DTLS1.2 on RA tunnels
<a href="#">CSCvz76966</a>	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DNS DoS
<a href="#">CSCvz15529</a>	ASA traceback and reload thread name: Datapath
<a href="#">CSCvy57905</a>	VTI tunnel interface stays down post reload on KP/WM platform in HA
<a href="#">CSCwa27822</a>	Lina process remains in started status after a major FTD upgrade to 6.7 or 7.0
<a href="#">CSCvy33676</a>	UN-NAT created on FTD once a prior dynamic xlate is created
<a href="#">CSCvz30333</a>	FTD/Lina may traceback when "show capture" command is executed
<a href="#">CSCwa21016</a>	Cisco Firepower Threat Defense Software DNS Enforcement Denial of Service Vulnerability
<a href="#">CSCvy82655</a>	REST API - Bulk AC rules creation fails with 422 Unprocessable Entity
<a href="#">CSCwb00595</a>	Mempool_DMA allocation issue / memory leakage

Bug ID	Headline
<a href="#">CSCwa85138</a>	Multiple issues with transactional commit diagnostics
<a href="#">CSCwa51241</a>	Switch detected unknown MAC address from FPR1140 Management Interface
<a href="#">CSCwa03275</a>	BGP routes shows unresolved and dropping packet with asp-drop reason "No route to host"
<a href="#">CSCvz73709</a>	ASA/FTD Standby unit fails to join HA
<a href="#">CSCvz21886</a>	Twice nat's un-nat not happening if nat matches a pbr acl that matches a port number instead of IP
<a href="#">CSCvy63464</a>	FTD 1100/ 2100 series reboots with clock set to 2033
<a href="#">CSCvz19634</a>	FTD software upgrade may fail at 200_pre/505_revert_prep.sh
<a href="#">CSCwa94894</a>	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-4-9608'
<a href="#">CSCvx89451</a>	ISA3000 shutdown command reboots system and does not shut system down.
<a href="#">CSCwa61218</a>	Polling OID "1.3.6.1.4.1.9.9.171.1.3.2.1.2" gives negative index value of the associated tunnel
<a href="#">CSCvy02247</a>	Cisco Firepower System Software Rule Editor Non-impactful Buffer Overflow Vulnerability
<a href="#">CSCvy99348</a>	Shutdown command reboots instead of shutting the FPIk device down.
<a href="#">CSCvz71825</a>	MAC algorithms on Firepower 2K devices are not correct for CC and UCAPL mode
<a href="#">CSCwa18858</a>	ASA drops non DNS traffic with reason "label length 164 bytes exceeds protocol limit of 63 bytes"
<a href="#">CSCvz54471</a>	ASA:Failed ASA in HA pair not recovering by itself, after an "HA state progression failed"
<a href="#">CSCvs27336</a>	Traceback on ASA by Smart Call Home process
<a href="#">CSCwa67209</a>	FMC may disable autonegotiation for port-channels with 1Gbps SFP fiber members after FTD upgrade
<a href="#">CSCwb33334</a>	ASA: crash after sending some traffic over RAVPN tunnel
<a href="#">CSCwa75077</a>	Time-range objects incorrectly populated in prefilter rules
<a href="#">CSCwa40237</a>	Cisco Firepower Management Center File Upload Security Bypass Vulnerability
<a href="#">CSCvz94153</a>	NTP sync on IPV6 will fail if the IPV4 address is not configured
<a href="#">CSCwa55562</a>	Different CG-NAT port-block allocated for same source IP causing per-host PAT port block exhaustion
<a href="#">CSCvz31880</a>	ASA Crashing with 'Unicorn Proxy Thread cpu: 9 watchdog_cycles' after stopping scaled stress test.

Bug ID	Headline
<a href="#">CSCwb20940</a>	FMC: Add validation checks for the combination of SSL/Snort3/NAP in Detection mode
<a href="#">CSCwa77073</a>	SNMP is responding to snmpgetbulk with unexpected order of results
<a href="#">CSCwa11088</a>	Access rule-ordering gets automatically changed while trying to edit it before page refresh/load
<a href="#">CSCvz43414</a>	Internal ldap attribute mappings fail after HA failover
<a href="#">CSCvz46879</a>	Fine tune mojo_server configuration on Sourcefire modules
<a href="#">CSCvy90821</a>	Autocomplete for "debug snmp ?" not working on ASA

## Resolved Bugs in Version 7.0.1.1

Table last updated: 2022-02-17

*Table 50: Resolved Bugs in Version 7.0.1.1*

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

## Resolved Bugs in Version 7.0.1

Table last updated: 2021-10-07

*Table 51: Resolved Bugs in Version 7.0.1*

Bug ID	Headline
<a href="#">CSCum03297</a>	ENH: ASA should save the timestamp of the MAXHOG in 'show proc cpu-hog'
<a href="#">CSCvf89237</a>	Evaluate unicorn expat for CVE-2017-9233
<a href="#">CSCvg66052</a>	2 CPU Cores continuously spike on firepower appliances
<a href="#">CSCvr11958</a>	AWS FTD: Deployment failure with ERROR: failed to set interface to promiscuous mode
<a href="#">CSCvs50538</a>	Firewall engine should fall back on info from SSL handshake if SSL engine is not returning a verdict
<a href="#">CSCvt62869</a>	SPLIT-BRAIN: Pre allocation of blocks for failover control messages

Bug ID	Headline
<a href="#">CSCvv21602</a>	cfprApSmMonitorTable is missing in the FP2K MIB
<a href="#">CSCvv36788</a>	MsgLayer[PID]: Error : Msglyr::ZMQWrapper::registerSender() : Failed to bind ZeroMQ Socket
<a href="#">CSCvv43190</a>	Crypto engine errors when GRE header protocol field doesn't match protocol field in inner ip header
<a href="#">CSCvv48942</a>	Snmpwalk showing traffic counter as 0 for failover interface
<a href="#">CSCvv59676</a>	Snort2: Implement aggressive pruning for certificate cache for TLS to free up memory
<a href="#">CSCvv71097</a>	traceback: ASA reloaded snp_fdb_destroy_fh_callback+104
<a href="#">CSCvv89715</a>	Fastpath rules for 8000 series stack disappear randomly from the FMC
<a href="#">CSCvw46630</a>	FTD: NLP path dropping return ICMP destination unreachable messages
<a href="#">CSCvw62526</a>	ASA traceback and reload on engineering ASA build - 9.12.3.237
<a href="#">CSCvw71405</a>	FPR1120 running ASA traceback and reload in crypto process.
<a href="#">CSCvx11917</a>	FTD active unit might drop interface failover messages with host-move-pkt drop reason
<a href="#">CSCvx20872</a>	ASA/FTD Traceback and reload due to netflow refresh timer
<a href="#">CSCvx21050</a>	Snort3 UDP performance down up to 40% relative to snort2 and Correct CPU utilisation meaningful
<a href="#">CSCvx23833</a>	IKEv2 rekey - Invalid SPI for ESP packet using new SPI received right after Create_Child_SA response
<a href="#">CSCvx26308</a>	ASA traceback and reload due to strepy_s: source string too long for dest
<a href="#">CSCvx26927</a>	TLS site not loading when it has segmented and retransmitted CH
<a href="#">CSCvx38124</a>	Core-local block alloc failure on cores where CP is pinned leading to drops
<a href="#">CSCvx48490</a>	SSL Decrypted https flow EOF events showing 'Initiator/Responder' Packets as 0
<a href="#">CSCvx50980</a>	ASA CP CPU wrong calculation leads to high percentage (100% CP CPU)
<a href="#">CSCvx51123</a>	FMC UI ERROR : An error occurred saving domain
<a href="#">CSCvx63788</a>	Edit policy in new window for AC Policy default action IPS policy shows error pop-up
<a href="#">CSCvx65178</a>	SNMP bulkget not working for specific OIDs in firewall mib and device performance degradation
<a href="#">CSCvx66329</a>	FTD Hotfix Cisco_FTD_SSP_FP2K_Hotfix_O installation fails on script 000_start/125_verify_bundle.sh
<a href="#">CSCvx76665</a>	Error messages "Updating Interface Status failed" seen on 2100

Bug ID	Headline
<a href="#">CSCvx77768</a>	Traceback and reload due to Umbrella
<a href="#">CSCvx78238</a>	multi context Firepower services on ASA traffic goes to incorrect interfaces
<a href="#">CSCvx79793</a>	Slow file transfer or file upload with SSL policy is applied with Decrypt resign action
<a href="#">CSCvx80830</a>	VPN conn fails from same user if Radius server sends a dACL and vpn-simultaneous-logins is set to 1
<a href="#">CSCvx85922</a>	ASA/FTD may traceback and reload when saving/writing the configuration to memory
<a href="#">CSCvx87709</a>	FPR 2100 running ASA in HA. Traceback and reload on watchdog during failover
<a href="#">CSCvx90486</a>	In some cases snmpwalk for ifXTable may not return data interfaces
<a href="#">CSCvx91317</a>	A remote code execution issue was discovered in MariaDB 10.2 before 10
<a href="#">CSCvx93254</a>	DHCP relay server "Invalid helper address"
<a href="#">CSCvx94398</a>	Secondary ASA could not get the startup configuration
<a href="#">CSCvx95652</a>	ASAv Azure: Some or all interfaces might stop passing traffic after a certain period of run time
<a href="#">CSCvx95884</a>	High CPU and massive "no buffer" drops during HA bulk sync and during normal conn sync
<a href="#">CSCvx96452</a>	Some HTTP2 TLS traffic ends with TCP RST, not TCP FIN, after complete payload transmission
<a href="#">CSCvx97632</a>	ASA traceback and reload when copying files with long destination filenames using cluster command
<a href="#">CSCvy01482</a>	Realm Sync Results Page Hangs After Upgrade
<a href="#">CSCvy01752</a>	Traceback on FPR 4115 in Thread - Lic HA Cluster
<a href="#">CSCvy03006</a>	improve debugging capability for uauth
<a href="#">CSCvy03907</a>	Creation/Edit of Access Control Policy fails with error 'Rule Name Already Exists'
<a href="#">CSCvy04343</a>	ASA in PLR mode,"license smart reservation" is failing.
<a href="#">CSCvy05966</a>	Snort 2.9.16.3-3033 traceback (FTD 6.6.3)
<a href="#">CSCvy07113</a>	7.0.0-1459 :FTPs traffic(malware file) is not blocked with file policy config,specifi to QP platform
<a href="#">CSCvy07491</a>	ASA traceback when re-configuring access-list
<a href="#">CSCvy09217</a>	HA goes to active-active state due to cipher mismatch
<a href="#">CSCvy09436</a>	DHCP reservation fails to apply reserved address for some devices

Bug ID	Headline
<a href="#">CSCvy10583</a>	ASA Traceback and Reload in Thread Name: DATAPATH
<a href="#">CSCvy10789</a>	FTD 2110 ascii characters are disallowed in LDAP password
<a href="#">CSCvy13229</a>	FDM - GUI Inaccessible - tomcat is opening too many file descriptors
<a href="#">CSCvy14721</a>	ssl traffic dropped by FTD while CH packet has a destination port no greater than source port
<a href="#">CSCvy16179</a>	ASA cluster Traceback with Thread Name: Unicorn Admin Handler even when running fix for CSCuz67596
<a href="#">CSCvy17078</a>	Traceback: ASA on FPR 2110 traceback and reload on process Lina
<a href="#">CSCvy17365</a>	REST API Login Page Issue
<a href="#">CSCvy17470</a>	ASA Traceback and reload on the A/S failover pair at IKEv2
<a href="#">CSCvy18138</a>	PIM Register Sent counter does not increase when encapsulated packets with register flag sent to RP
<a href="#">CSCvy19136</a>	Web portal persistent redirects when certificate authentication is used.
<a href="#">CSCvy19453</a>	SFDataCorrelator performance problems involving redundant new host events with only MAC addresses
<a href="#">CSCvy21334</a>	Active tries to send CoA update to Standby in case of "No Switchover"
<a href="#">CSCvy23349</a>	FTD unnecessarily ACKing TCP flows on inline-pair deployment
<a href="#">CSCvy27261</a>	Inconsistencies in Snort2 and Snort3 Events views
<a href="#">CSCvy29815</a>	NTP AES-CMAC input not compatible with IOS-XE
<a href="#">CSCvy30016</a>	"Max cert cache entries" pruning needs to lock the ssl cache
<a href="#">CSCvy30101</a>	snort2 memory usage can grow beyond expected limits when using ssl decryption
<a href="#">CSCvy31096</a>	Host rediscovery in case of snort configuration reload
<a href="#">CSCvy31229</a>	No space left disk space is full on /ngfw
<a href="#">CSCvy31400</a>	FPR1K: Fiber SFP Interfaces down due to speed autonegotiation disabled
<a href="#">CSCvy31521</a>	Add syslog-ng monitor to the FMC
<a href="#">CSCvy32154</a>	Flows are offloaded after disable the offload cli on policy-map
<a href="#">CSCvy32366</a>	After upgrading ASA to 9.15(1)10, ASDM 7.15(1)150 One Time Password (OTP) field does not appear
<a href="#">CSCvy33105</a>	Ambiguous command error is shown for 'show route bgp' or 'show route isis' if DNS lookup is enabled

Bug ID	Headline
<a href="#">CSCvy33676</a>	UN-NAT created on FTD once a prior dynamic xlate is created
<a href="#">CSCvy34333</a>	When ASA upgrade fails, version status is desynched between platform and application
<a href="#">CSCvy36694</a>	FTDv 6.7 on Azure is unable to set 1000 speed on GigabitEthernet interfaces
<a href="#">CSCvy37835</a>	ssl replace key only action can cause unbounded detection engine memory usage
<a href="#">CSCvy39191</a>	An internal server error 500 in T-ufin when doing API calls to the FMC
<a href="#">CSCvy39621</a>	ASA/FTD sends continuous Radius Access Requests Even After Max Retry Count is Reached
<a href="#">CSCvy39659</a>	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-15-14815'
<a href="#">CSCvy39791</a>	Lina traceback and core file size is beyond 40G and compression fails.
<a href="#">CSCvy40482</a>	9.14MR3: snmpwalk got failed with [Errno 146] Connection refused error.
<a href="#">CSCvy41157</a>	HA formation failing after restore
<a href="#">CSCvy43447</a>	FTD traceback and reload on Lic TMR Thread on Multi Instance FTD
<a href="#">CSCvy47108</a>	Remote Access IKEv2 VPN session cannot be established because of stuck Uauth entry
<a href="#">CSCvy48159</a>	ASA Traceback & reload on process name lina due to memory header validation
<a href="#">CSCvy48730</a>	ASA/FTD may traceback and reload in Thread Name 'Unicorn Proxy Thread'
<a href="#">CSCvy49732</a>	ASA/FTD may traceback and reload in Thread Name 'ssh'
<a href="#">CSCvy50011</a>	ASA traceback in IKE Daemon process and reload
<a href="#">CSCvy51659</a>	Long OCSP timeout may cause AnyConnect authentication failure
<a href="#">CSCvy51814</a>	Firepower flow-offload stops offloading all existing and new flows
<a href="#">CSCvy52074</a>	ASA/FTD may traceback and reload in Thread Name 'webvpn_task'
<a href="#">CSCvy52924</a>	FTD loses OSPF network statements config for all VRF instances upon reboot
<a href="#">CSCvy53301</a>	HA Configuration fails on FDM with 'Internal error during deployment'
<a href="#">CSCvy53461</a>	RSA keys & Certs get removed post reload on WS-SVC-ASA-SM1-K7 with ASA code 9.12.x
<a href="#">CSCvy53798</a>	memory leak when decrypting flows using x25519 curve
<a href="#">CSCvy55356</a>	CPU hogs less than 10 msec are produced contrary to documentation
<a href="#">CSCvy56395</a>	ASA traceback and reload due to snmp encrypted community string when key config is present

Bug ID	Headline
<a href="#">CSCvy58268</a>	Block 80 and 256 exhaustion snapshots are not created
<a href="#">CSCvy60100</a>	SNMP v3 configuration lost after reboot for HA
<a href="#">CSCvy60574</a>	Port dcosAG leak fix CSCvx14602 to KP/WM
<a href="#">CSCvy61008</a>	Time out of sync between Lina and FXOS
<a href="#">CSCvy63949</a>	ASA direct authentication timeouts even if direct authentication traffic is passing through the ASA
<a href="#">CSCvy64492</a>	ASAv adding non-identity L2 entries for own addresses on MAC table and dropping HA hellos
<a href="#">CSCvy64911</a>	Debugs for: SNMP MIB value for crasLocalAddress is not showing the IP address
<a href="#">CSCvy66711</a>	Cisco ASA 9.16.1 and FTD 7.0.0 IPsec Denial of Service Vulnerability
<a href="#">CSCvy67756</a>	Firepower Services HTTPS traffic stops working when matching Do not decrypt rule in SSL policy
<a href="#">CSCvy68859</a>	DB Conn not released with LSP and category filter in Intrusion rules
<a href="#">CSCvy69189</a>	FTD HA stuck in bulk state due to stuck vpnfol_sync/Bulk-sync keytab
<a href="#">CSCvy69787</a>	ASAv on AWS TenGigabit interface is learning 1000mbps instead of 10000Mbps
<a href="#">CSCvy72118</a>	High snort cpu usage while copying navl attribute - ( Fragmented metadata )
<a href="#">CSCvy72321</a>	Packet-tracer adds "after-auto" option to manual/twice NATs when matching it in the NAT Phases
<a href="#">CSCvy72846</a>	ASA accounting reports incorrect Acct-Session-Time
<a href="#">CSCvy73554</a>	ASA: "deny ip any any" entry in crypto ACL prevents IKEv2 remote AnyConnect access connections
<a href="#">CSCvy74781</a>	The standby device is sending the keep alive messages for ssl traffic after the failover
<a href="#">CSCvy74984</a>	ASAv on Azure loses connectivity to Metadata server once default outside route is used
<a href="#">CSCvy79023</a>	Device UI down due to idhttpsd access log file exceeding size and log rotation failure
<a href="#">CSCvy79952</a>	ASA/FTD traceback and reload after downgrade
<a href="#">CSCvy82794</a>	ASA/FTD traceback and reload when negating snmp commands
<a href="#">CSCvy83116</a>	WM standby fails to re-join HA with msg "CD App Sync error is SSP Config Generation Failure"
<a href="#">CSCvy84733</a>	SFR Upgrade 6.7 to 7.0: Syslogs stopped working
<a href="#">CSCvy89440</a>	s2sCryptoMap Configuration Loss



Bug ID	Headline
<a href="#">CSCvy89648</a>	ma_ctx files with '.backup' extension seen after applying the workaround for CSCvx29429
<a href="#">CSCvy89658</a>	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 114, seq 13)
<a href="#">CSCvy92990</a>	FTD traceback and reload related to SSL after upgrade to 7.0
<a href="#">CSCvy95554</a>	Unable to download LDAP due to database MERGE failure on group_fsp_reference table
<a href="#">CSCvy96625</a>	Revert 'fix' introduced by CSCvr33428 and CSCvy39659
<a href="#">CSCvy96698</a>	Resolve spurious status actions checking speed values twice in FXOS portmgr
<a href="#">CSCvy96803</a>	FTD traceback and reload in Process Name lina related to SNMP functions
<a href="#">CSCvy99373</a>	ADI Session Processing Delays when resolving adSamAccountName with AD
<a href="#">CSCvz00032</a>	FTD tracebacks and reloads on Thread name Lina
<a href="#">CSCvz00254</a>	FDM 6.7.0 to 7.0.0 Upgrade Failed due to invalid state for site to site VPN during upgrade import
<a href="#">CSCvz00383</a>	FTD lina traceback and reload in thread Name Checkheaps
<a href="#">CSCvz00699</a>	Traceback in webvpn and reload experienced periodically after ASA upgrade
<a href="#">CSCvz05189</a>	FTD reload with Lina traceback during xlate replication in Cluster
<a href="#">CSCvz05197</a>	Event pages do not work in IE 11
<a href="#">CSCvz05468</a>	Multiple SSH host entries in platform settings as first feature enable/deploy will break SSH on LINA
<a href="#">CSCvz05767</a>	FP-1010 HA link goes down or New hosts are not not able to connect to the device
<a href="#">CSCvz06652</a>	snmpd corefiles noticed on SNMP longevity setup
<a href="#">CSCvz06848</a>	FTD/FDM upgrade fails due to snmp-server community validation failure
<a href="#">CSCvz07614</a>	ASA: Orphaned SSH session not allowing us to delete a policy-map from CLI
<a href="#">CSCvz14616</a>	No connection events due to SFDataCor process stuck
<a href="#">CSCvz15529</a>	ASA traceback and reload thread name: Datapath
<a href="#">CSCvz17534</a>	FTD Restore Backup CLI does not restore the VPN configuration
<a href="#">CSCvz20544</a>	ASA/FTD may traceback and reload in loop processing Anyconnect profile
<a href="#">CSCvz21886</a>	Twice nat's un-nat not happening if nat matches a pbr acl that matches a port number instead of IP
<a href="#">CSCvz23157</a>	SNMP agent restarts when show commands are issued

Bug ID	Headline
<a href="#">CSCvz25434</a>	ASA/FTD blackholes traffic due to 1550 block depletion when BVI is configured as DHCP client
<a href="#">CSCvz25663</a>	FTD/FDM upgrade error due to snmp-server host community string validation failure
<a href="#">CSCvz26950</a>	[DOC] The Appliance Information Widget missing High Availability information in FMC Documentation
<a href="#">CSCvz29233</a>	ASA: ARP entries from custom context not removed when an interface flap occurs on system context
<a href="#">CSCvz30333</a>	FTD/Lina may traceback when "show capture" command is executed
<a href="#">CSCvz30933</a>	ASA tracebacks and reload when clear configure snmp-server command is issued
<a href="#">CSCvz32386</a>	FTD Deployment error when FMC pushes PFS21 and IKEv1 settings on same crypto map entry
<a href="#">CSCvz34831</a>	If ASA fails to download DACL it will never stop trying
<a href="#">CSCvz35201</a>	Upgrade failure / Stuck on 999_finish/989_update_ngfw_conf_aquila_ssp.sh
<a href="#">CSCvz38361</a>	BGP packets dropped for non directly connected neighbors
<a href="#">CSCvz38811</a>	Deleted files holding disk space under Java process
<a href="#">CSCvz46333</a>	FTD policy deployment failure due to internal socket connection loss
<a href="#">CSCvz66506</a>	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 52: Resolved Bugs in Version 7.0.0.1*

Bug ID	Headline
<a href="#">CSCvy66711</a>	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 53: Resolved Bugs in Version 7.0.0*

Bug ID	Headline
<a href="#">CSCvi96835</a>	No validation err when changing host thats part of a group object used in a routing policy, to Range

Bug ID	Headline
<a href="#">CSCvk22190</a>	No connection/intrusion events received on FMC following time synchronisation issues
<a href="#">CSCvm69294</a>	Standby FMC sending Flood of SNMP traps
<a href="#">CSCvm99989</a>	SNMP OID for SystemUpTime show incorrect value
<a href="#">CSCvo57004</a>	Analyze Hit Counts displaying timestamps in UTC instead of the configured user time zone.
<a href="#">CSCvp54996</a>	GNU Wget Buffer Overflow Vulnerability
<a href="#">CSCvp58886</a>	Special characters in Location for SNMP FXOS (FPR2100) causes policy deployment failure
<a href="#">CSCvq55919</a>	Cisco Firepower Management Center Software Stored Cross-Site Scripting Vulnerability
<a href="#">CSCvq89604</a>	Cisco_Firepower_Mgmt_Center_Patch_Uninstaller-6.4.0.3-29.sh.REL.tar fails to run
<a href="#">CSCvr03127</a>	Apache HTTP Server mod_proxy Cross-Site Scripting Vulnerability
<a href="#">CSCvr13762</a>	NGFWHA Missing EO UUID on FMC
<a href="#">CSCvr46901</a>	Analysis Connection Events doesn't show and report all the events in UI
<a href="#">CSCvr74896</a>	Cannot update Security intelligence when AC Policy is imported to FMC with cloud feeds disabled
<a href="#">CSCvs02229</a>	Network Time Protocol Authenticated Mode 6 Packet Processing NULL Poin
<a href="#">CSCvs05066</a>	Snort file mempool corruption leads to performance degradation and process failure.
<a href="#">CSCvs06043</a>	TunnelClient for CSM_CCMservice on ngfwManager not reading ACK sent from CSM_CCM service on FMC
<a href="#">CSCvs71034</a>	Beaker registration fails with error 400 : Bad Request.
<a href="#">CSCvs71969</a>	Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability
<a href="#">CSCvs74802</a>	AnyConnect/S2S IKEv2 crypto policy occasionally not deployed to device
<a href="#">CSCvs79606</a>	"dns server-group DefaultDNS" cli not getting negated
<a href="#">CSCvs84242</a>	FMC Deployment Failure when removing Auto NAT and correlated network object
<a href="#">CSCvt29771</a>	invalid Response message when we change the security zone from the object management page
<a href="#">CSCvt31292</a>	FTD device might not send events to SSE
<a href="#">CSCvt43136</a>	Multiple Cisco Products Snort TCP Fast Open File Policy Bypass Vulnerability
<a href="#">CSCvt49334</a>	On the 4120 sensor, the task delete is not removing the "task_xx" files from the cron.d directory

Bug ID	Headline
<a href="#">CSCvt74194</a>	Error getting unified2 record: Corrupt file
<a href="#">CSCvt74893</a>	FMCv Ethernet driver indicates vmxnet3 TCP performance compromised
<a href="#">CSCvt91258</a>	FDM: None of the NTP Servers can be reached - Using Data interfaces as Management Gateway
<a href="#">CSCvt93177</a>	Disable Full Proxy to Light Weight Proxy by Default. (FP2LWP) on FTD Devices
<a href="#">CSCvt93999</a>	FMC shouldn't allow a second upgrade on same device if upgrade is going on
<a href="#">CSCvu12608</a>	ASA5506/5508/5516 devices not booting up properly / Boot loop
<a href="#">CSCvu18510</a>	MonetDB's eventdb crash causes loss of connection events on FMC 6.6.0 and 6.6.1
<a href="#">CSCvu21953</a>	FMC 6.4.0 is randomly sending "strong-encryption-disable" to FTD
<a href="#">CSCvu22293</a>	FMC scheduled backup of multiple managed devices with remote storage fails
<a href="#">CSCvu29508</a>	FMC manual removal and addition of FTD Cluster member causes dangling stale interfaces
<a href="#">CSCvu30756</a>	User Identity does not correctly handle identical sessions in different netmaps
<a href="#">CSCvu34228</a>	FTD LINA traceback & reload while processing snort return verdict
<a href="#">CSCvu35704</a>	APIKEY mismatch among the FMC, Sensor and ThreatGrid results significant file submission drop
<a href="#">CSCvu44472</a>	FMC System processes are starting
<a href="#">CSCvu54706</a>	Cisco Firepower Management Center CWE-772 - Slow HTTP POST vulnerability
<a href="#">CSCvu75855</a>	stunnel process enabled on managed device when it should not be
<a href="#">CSCvu77689</a>	FTP to FileZilla miscategorized as SMTP
<a href="#">CSCvu88005</a>	FMC REST API user permission for GET taskstatus
<a href="#">CSCvu88886</a>	Threat data deployment to managed FTD may fail after upgrade.
<a href="#">CSCvv00155</a>	Deleting interface or sub-interface should also delete failover MAC address configuration
<a href="#">CSCvv08244</a>	Firepower module may block trusted HTTPS connections matching 'Do not decrypt' SSL decryption rule
<a href="#">CSCvv12491</a>	cloudagent_urllookup_health file still had old format after upgrading to 6.4
<a href="#">CSCvv14109</a>	new FMC restored from backup file doesn't send down user ip and user group mappings to devices
<a href="#">CSCvv14442</a>	FMC backup restore fails if it contains files/directories with future timestamps

Bug ID	Headline
<a href="#">CSCvv17893</a>	Bad uip snapshot and log file causes FTD to repeatedly requests catchup, and exhausts file handlers
<a href="#">CSCvv20780</a>	Policy deploy fails with "Failed to hold the deployment transaction" error
<a href="#">CSCvv21782</a>	6.6.1: Prefilter Policy value shown as Invalid ID for all the traffic in ASA SFR Platform
<a href="#">CSCvv27084</a>	EventHandler syslog via loggerd does not support destination host names
<a href="#">CSCvv27867</a>	FMC classic theme - No scrollbar in object details for group with multiple items
<a href="#">CSCvv29275</a>	FMC OSPF area limits until 49 entries. Upon adding 50th entry, process gets disabled automatically
<a href="#">CSCvv34523</a>	The firewall_target_cache table is not pruned as expected which leads to large database size
<a href="#">CSCvv34851</a>	6.7.0-1992: duplicate connection events with empty SSL info in one of them
<a href="#">CSCvv36915</a>	"Show NTP" command does not work on multi-instance FTD
<a href="#">CSCvv38869</a>	FMC fails to upgrade FTD from 6.3 to 6.7 due to database error
<a href="#">CSCvv40961</a>	http-proxy setting causing upgrade failure
<a href="#">CSCvv43771</a>	Unable to select multiple devices for scheduled backups
<a href="#">CSCvv45106</a>	CSD does not start on 2100 due to missing csd-service.json file
<a href="#">CSCvv46490</a>	Policy Deployment Failure on FMC due to ERROR in SnortAttribConfig
<a href="#">CSCvv50298</a>	FTD management interface to be vulnerable to TLS poodle attack- CVE-2014-3566
<a href="#">CSCvv53042</a>	DBCheck.pl output includes fatal errors that cause upgrade attempt to fail
<a href="#">CSCvv55066</a>	FPR1010: Internal-Data0/0 and data interfaces are flapping during SMB file transfer
<a href="#">CSCvv56644</a>	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web DoS
<a href="#">CSCvv57476</a>	CSS Styles loading issue in Chrome 85, IE and Edge browsers
<a href="#">CSCvv59036</a>	Static routes deleted from the FMC without user deleting it.
<a href="#">CSCvv60849</a>	Memory cgroup limits should be adjusted to avoid Snort D-state
<a href="#">CSCvv62931</a>	FTD does not send Server Hello & Server Certificate to the client when src.port==dst.port
<a href="#">CSCvv68000</a>	bravado error when getting ra vpn group policy created by FDM UI
<a href="#">CSCvv68078</a>	sybase database corrupted on secondary FMC and was not able to sync

Bug ID	Headline
<a href="#">CSCvv69862</a>	FMC backup failed error with "Terminating long running backup" after 45 min FTDHA in leaf
<a href="#">CSCvv70096</a>	Snort 2: Memory Leak in SSL Decrypt & Resign Processing
<a href="#">CSCvv70683</a>	No New Notification in Task tab.
<a href="#">CSCvv73054</a>	Snort libs are deleted during deployment
<a href="#">CSCvv74658</a>	FTD/ASA creates coredump file with "!" character in filename (zmq changes (fxos) for CSCvv40406 )
<a href="#">CSCvv74795</a>	syslog-ng has extra instances running on ASA5525-X
<a href="#">CSCvv74816</a>	FDM should not allow removal of local address pool while NAT exemption is in place.
<a href="#">CSCvv74951</a>	Disable memory cgroups when running the system upgrade scripts
<a href="#">CSCvv75148</a>	Rabbitmq queue of VPN Events does not have any size limit to avoid accumulating *.idx files
<a href="#">CSCvv76581</a>	Cisco Firepower product line Evaluation of Racocon attack CVE-2020-1968
<a href="#">CSCvv79459</a>	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 94, seq 1)
<a href="#">CSCvv79897</a>	Block "sensor restart" command for FTD units to prevent Lina crash and system reboot event
<a href="#">CSCvv83841</a>	upgrade - Not enough root disk space available in 600_schema/100_update_database.sh
<a href="#">CSCvv84172</a>	Dangling ref in Clustered_table and EO upon failed registration
<a href="#">CSCvv84385</a>	Disk Manager incorrectly prunes unified files used by FMC e-streamer
<a href="#">CSCvv89715</a>	Fastpath rules for 8000 series stack disappear randomly from the FMC
<a href="#">CSCvv90079</a>	No router BGP pushed after making chnages on 9300 intra chassis cluster
<a href="#">CSCvv92897</a>	System might hit previously missing memcap limits on upgrade to version 6.6.0
<a href="#">CSCvv94165</a>	FTD 6.6 : High CPU spikes on snmpd process
<a href="#">CSCvv97527</a>	asa config timeout command breaks snort's DAQ configuration
<a href="#">CSCvv97902</a>	Deployment purge doesn't happen due to deployment_info missing at policy_deployment.db
<a href="#">CSCvw03256</a>	FMC dashboard shows "No Data" for intrusion table when 'Message' Field is Selected
<a href="#">CSCvw04171</a>	For Readonly User, Device Summary tab is returning forbidden error page
<a href="#">CSCvw07352</a>	SFDataCorrelator log spam, metadata fails after Sybase connection status 0
<a href="#">CSCvw10877</a>	/var/sf/user_identity should not bring the archive with it in a troubleshoot

Bug ID	Headline
<a href="#">CSCvw13395</a>	FMC 6.6.0 "Reset Connection Upon Timeout" Checkbox missing in Light Theme of UI
<a href="#">CSCvw16565</a>	Policy Deployment fails after enabling "SMB Auto-Detect Ports" in DCE/RPC Configuration.
<a href="#">CSCvw21145</a>	Duplicate NAT rule error when saving the policy (caused by duplicate Auto NAT rules)
<a href="#">CSCvw21161</a>	Duplicate NAT rule error when saving the policy (different rules are detected as duplicates)
<a href="#">CSCvw21628</a>	Upgrade from pre-6.6.x to 6.6.x and above breaks Intrusion Event Packet-Drill down
<a href="#">CSCvw27966</a>	Policy deployment fails with object names starts with 'any'
<a href="#">CSCvw28894</a>	SFDataCorrelator slow startup and vuln remap due to duplicate entries in vuln tables
<a href="#">CSCvw28946</a>	When deploying VxLan config the command mtu is sent out of order causing deployment failures
<a href="#">CSCvw29561</a>	FMC SLR license 'shows continuous Smart agent communication with Smart Licensing Cloud' alert
<a href="#">CSCvw29563</a>	repair_users.pl script no longer works
<a href="#">CSCvw29581</a>	VDB upgrade doesn't work when mysql user table is damaged.
<a href="#">CSCvw30252</a>	ASA/FTD may traceback and reload due to memory corruption in SNMP
<a href="#">CSCvw33939</a>	FMC Deployment failure due to VPN split-tunnel standard ACL with Network Group containing IPv6object
<a href="#">CSCvw34692</a>	Not possible to change after the first time the TTL Hops for BGP neighbor
<a href="#">CSCvw38708</a>	AC policy save, validateActivity not using cache for building blocks
<a href="#">CSCvw38870</a>	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
<a href="#">CSCvw41901</a>	Deleting System Defined objects via FMC's REST API returns HTTP 500 error code.
<a href="#">CSCvw42497</a>	Error during policy validation while navigating through AC policy
<a href="#">CSCvw45125</a>	Block deployment while secondary nodes are in config or bulk sync
<a href="#">CSCvw47943</a>	Optimization of the query for scan results in Firepower Recommendations
<a href="#">CSCvw51307</a>	ASA/FTD traceback and reload in process name "Lina"
<a href="#">CSCvw60177</a>	Standby/Secondary cluster unit might crash in Thread Name: fover_parse and "cluster config sync"
<a href="#">CSCvw79294</a>	sftunnel logging huge number of logs to messages file

Bug ID	Headline
<a href="#">CSCvw85377</a>	URL is not updated in the access policy URL filtering rule
<a href="#">CSCvx19934</a>	Deployment gets failed for snmp settings while deleting snmpv1 and adding snmpv3 at a time in 6.6.3
<a href="#">CSCvx20303</a>	ASA/FTD may traceback in after changing snmp host-group object
<a href="#">CSCvx26221</a>	Traceback into snmp at handle_agentx_packet / snmp takes long time to come up on FP1k and 5508
<a href="#">CSCvy08798</a>	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 110, seq 10)