



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

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

**Last Modified:** 2022-11-21

### **Americas Headquarters**

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





## CONTENTS

---

### CHAPTER 1

#### Welcome 1

- Release Highlights 1
- Release Dates 2
- Suggested Release 3
- Sharing Data with Cisco 3
- For Assistance 4

---

### CHAPTER 2

#### System Requirements 5

- FMC Platforms 5
- Device Platforms 6
- Device Management 9
- Browser Requirements 11

---

### CHAPTER 3

#### Features and Functionality 13

- New Features 13
  - New Features in FMC Version 7.0 13
  - New Features in FDM Version 7.0 33
  - New Hardware and Virtual Platforms in Version 7.0 37
  - New Intrusion Rules and Keywords 38
- Deprecated Features 39
  - Deprecated Features in FMC Version 7.0 39
  - Deprecated Features in FDM Version 7.0 41
  - Deprecated Hardware and Virtual Platforms in Version 7.0 41
  - Deprecated FlexConfig Commands 41

---

### CHAPTER 4

#### Upgrade Guidelines 43

Planning Your Upgrade	43
Minimum Version to Upgrade	44
Upgrade Guidelines for Version 7.0	45
Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0	46
Reconnect with Cisco Threat Grid for High Availability FMCs	47
Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs	47
FMCv Requires 28 GB RAM for Upgrade	47
Firepower 1000 Series Devices Require Post-Upgrade Power Cycle	48
Historical Data Removed During FTD Upgrade with FDM	48
New URL Categories and Reputations	49
Pre-Upgrade Actions for URL Categories and Reputations	50
Post-Upgrade Actions for URL Categories and Reputations	51
Guidelines for Rules with Merged URL Categories	52
Upgrade Guidelines for FXOS	55
Unresponsive Upgrades	55
Traffic Flow and Inspection	56
Traffic Flow and Inspection for FXOS Upgrades	56
Traffic Flow and Inspection for FTD Upgrades with FMC	57
Traffic Flow and Inspection for FTD Upgrades with FDM	58
Traffic Flow and Inspection for ASA FirePOWER Upgrades	59
Traffic Flow and Inspection for NGIPSv Upgrades with FMC	59
Time and Disk Space Tests	60
Time and Disk Space for Version 7.0.5	62
Time and Disk Space for Version 7.0.4	63
Time and Disk Space for Version 7.0.3	64
Time and Disk Space for Version 7.0.2.1	64
Time and Disk Space for Version 7.0.2	65
Time and Disk Space for Version 7.0.1.1	66
Time and Disk Space for Version 7.0.1	66
Time and Disk Space for Version 7.0.0.1	67
Time and Disk Space for Version 7.0.0	68

---

**CHAPTER 5****Install the Software 69**

## Installation Guidelines 69

---

Installation Guides 71

---

**CHAPTER 6**

**Revert or Uninstall the Software 73**

Revert FTD with FDM 73

Uninstall a Patch in FMC and ASDM Deployments 73

Patches That Support Uninstall 73

Uninstall Order for High Availability/Scalability 74

Uninstall Standalone FMC Patches 76

Uninstall High Availability FMC Patches 76

Uninstall Device Patches with FMC 77

Uninstall ASA FirePOWER Patches with ASDM 79

---

**CHAPTER 7**

**Open and Resolved Bugs 81**

Open Bugs in Version 7.0 81

Open Bugs in Version 7.0.0 81

Resolved Bugs in Version 7.0 83

Resolved Bugs in Version 7.0.5 83

Resolved Bugs in Version 7.0.4 95

Resolved Bugs in Version 7.0.3 101

Resolved Bugs in Version 7.0.2.1 101

Resolved Bugs in Version 7.0.2 101

Resolved Bugs in Version 7.0.1.1 116

Resolved Bugs in Version 7.0.1 117

Resolved Bugs in Version 7.0.0.1 124

Resolved Bugs in Version 7.0.0 124





# CHAPTER 1

## Welcome

---

This document contains release information for Version 7.0 of:

- Cisco Firepower Threat Defense
- Cisco Firepower Management Center
- Cisco Firepower Device Manager
- Cisco Firepower Classic devices: Firepower 7000/8000 series, NGIPSv, and ASA with FirePOWER Services

For the Cisco Cloud-Delivered Firewall Management Center, features closely parallel the most recent customer-deployed (or *on-prem*) FMC release. You should also see [What's New for Cisco Defense Orchestrator](#).

- [Release Highlights, on page 1](#)
- [Release Dates, on page 2](#)
- [Suggested Release, on page 3](#)
- [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
7.0.5	72	2022-11-17	All
7.0.4	55	2022-08-10	All
7.0.3	37	2022-06-30	All
7.0.2.1	10	2022-06-27	All



Version	Build	Date	Platforms
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

## Suggested Release

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

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

- [Cisco Secure Firewall Management Center New Features by Release](#)
- [Cisco Secure Firewall Device Manager New Features by Release](#)

### Suggested Releases for Older Appliances

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

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

## 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 Tracking

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

You are enrolled by default but you can change your enrollment at any time after you complete initial setup.

## For Assistance

### Online Resources

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

- Documentation: <http://www.cisco.com/go/threatdefense-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 5](#)
- [Device Platforms, on page 6](#)
- [Device Management, on page 9](#)
- [Browser Requirements, on page 11](#)

## FMC Platforms

This section lists the FMCs supported in Version 7.0.

For device compatibility with the FMC, see [Device Management, on page 9](#). For general compatibility information, see the [Cisco Secure Firewall Management Center Compatibility Guide](#).

### FMC Hardware

Version 7.0 supports the following FMC hardware:

- FMC 1600, 2600, 4600
- FMC 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/on-prem clouds.

With the FMCv, you can purchase licenses that enable you to manage 2, 10, 25, or 300 devices; note that only select platforms support FMCv300. Additionally, FMCv2 does not support high availability. For full details on supported instances, see the [Cisco Secure Firewall Management Center Virtual Getting Started Guide](#).

**Table 2: Version 7.0 FMCv Platforms**

Platform	FMCv2, 10, 25	FMCv300	High Availability
Public Cloud			

Platform	FMCv2, 10, 25	FMCv300	High Availability
Amazon Web Services (AWS)	YES	—	—
Google Cloud Platform (GCP)	YES	—	—
Microsoft Azure	YES	—	—
Oracle Cloud Infrastructure (OCI)	YES	—	—
<b>On-Prem/Private Cloud</b>			
Cisco HyperFlex	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 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. The cloud-delivered management center does not have a version, and its features closely parallel the most recent customer-deployed FMC release.

Note that the customer-deployed management center is often referred to as the *on-prem* FMC, even for virtual platforms.

## Device Platforms

This section lists the devices and management methods supported in Version 7.0.

For details on those management methods, see [Device Management, on page 9](#). For general compatibility information, see the [Cisco Secure Firewall Threat Defense Compatibility Guide](#) or the [Cisco Firepower Classic Device Compatibility Guide](#).

#### FTD Hardware

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

Table 3: 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	YES	YES Requires Version 7.0.3+	YES	YES	Requires FXOS 2.10.1.159 or later build.
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.
ASA 5508-X, 5516-X	YES	YES Requires Version 7.0.3+	YES	YES	Requires the latest ROMMON image. 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	Requires the latest ROMMON image. See the <a href="#">Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide</a> .

### FTDv

Virtual FTD 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 4: Version 7.0 FTDv Public Cloud Platforms

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	CDO + FDM
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+	—	—

Table 5: Version 7.0 FTDv On-Prem/Private Cloud Platforms

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	CDO + FDM
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 6: 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). Requires the latest ROMMON image. 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). Requires the latest ROMMON image. 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.

**Table 7: FMC-Device Compatibility**

<b>FMC Version</b>	<b>Oldest Device Version You Can Manage</b>
Cloud-delivered management center (no version)	7.0.3/7.2
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 Management Center**

The cloud-delivered management center can manage FTD devices running:

- Version 7.0.3 and later maintenance releases
- Version 7.2+

The cloud-delivered 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 the device directly to Version 7.2+.



You can add a cloud-managed device to a Version 7.2+ customer-deployed management center 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.

## Browser Requirements

### Browsers

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

- Google Chrome
- Mozilla Firefox
- Microsoft Edge (Windows only)

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



---

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

---

### Browser Settings and Extensions

Regardless of browser, you must make sure JavaScript, cookies, and TLS v1.2 remain enabled. If you are using Microsoft Edge, do *not* enable IE mode.

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

### Screen Resolution

Interface	Minimum Resolution
FMC	1280 x 720
FDM	1024 x 768
ASDM managing an ASA FirePOWER module	1024 x 768
Firepower Chassis Manager for the Firepower 4100/9300	1024 x 768

### Securing Communications

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

To begin replacing the self-signed certificate:

- FMC: Choose **System > Configuration**, then click **HTTPS Certificates**.
- FDM: Click **Device**, then the **System Settings > Management Access** link, then the **Management Web Server** tab.

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



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

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

### Browsing from a Monitored Network

Many browsers use Transport Layer Security (TLS) v1.3 by default. If you are using an SSL policy to handle encrypted traffic, and people in your monitored network use browsers with TLS v1.3 enabled, websites that support TLS v1.3 may fail to load. For more information, see the software advisory titled: [Failures loading websites using TLS 1.3 with SSL inspection enabled](#).



## CHAPTER 3

# Features and Functionality

---

This document lists the new and deprecated features for Version 7.0, including upgrade impact.

For the cloud-delivered management center, features closely parallel the most recent customer-deployed FMC release. You should also see [What's New for Cisco Defense Orchestrator](#).



---

**Important** New and deprecated features can require pre- or post-upgrade configuration changes, or even prevent upgrade. If your upgrade skips versions, see those release notes for historical feature information and upgrade impact, or see the appropriate [New Features by Release](#) guide.

---

- [New Features, on page 13](#)
- [Deprecated Features, on page 39](#)

## New Features

### New Features in FMC Version 7.0

Although you can manage older devices with a newer customer-deployed FMC, we recommend you always update your entire deployment. You should assume that new traffic-handling features require the latest release on both the FMC *and* device. Features where devices are not obviously involved (cosmetic changes to the

web interface, cloud integrations) may only require the latest version on the FMC, but that is not guaranteed. In the new feature descriptions, we are explicit when version requirements deviate from the standard expectation.

**Table 8: New Features in FMC Version 7.0.5**

Feature	Description
Automatically update CA bundles	<p><b>Upgrade impact.</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><b>Note</b> This feature is not in the base releases for Version 7.0, 7.1, or 7.2, but is (or will be) available in maintenance or patch upgrades to those versions. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco.</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>For more information, see:</p> <ul style="list-style-type: none"> <li>• <a href="#">Firepower Management Center Command Line Reference</a> in the FMC configuration guide</li> <li>• <a href="#">Cisco Secure Firewall Threat Defense Command Reference</a></li> </ul>

Table 9: New Features in FMC Version 7.0.3

Feature	Description
FTD support for cloud-delivered management center.	<p>Version 7.0.3 FTD devices support management by the cloud-delivered management center, which we introduced in spring of 2022. The cloud-delivered 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 management center if:</p> <ul style="list-style-type: none"> <li>• You are currently using a customer-deployed hardware or virtual FMC.</li> <li>• You want to migrate to the cloud-delivered 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 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 customer-deployed 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 management center.               <p>Optionally, leave the devices registered to the customer-deployed 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 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 the device 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 Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator</a>.</p>

Table 10: New Features in FMC Version 7.0.2

Feature	Description
Dynamic object names now support the dash character.	<p>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.</p> <p><b>Note</b> This feature requires Version 7.0.2 on both the FMC and the device.</p>
Improved SecureX integration, SecureX orchestration.	<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><b>Note</b> These changes are temporarily deprecated in Version 7.1, but come back in Version 7.2. Note that if you use the new method to enable SecureX integration, you must disable the feature before you upgrade to Version 7.1. You can re-enable the feature after successful upgrade. Upgrades to Version 7.2+ are not be affected.</p>

Feature	Description
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> <p><b>AMP &gt; AMP Management</b> is now <b>Integration &gt; AMP &gt; AMP Management</b></p> <p><b>AMP &gt; Dynamic Analysis Connections</b> is now <b>Integration &gt; AMP &gt; Dynamic Analysis Connections</b></p> <p><b>Intelligence &gt; Sources</b> is now <b>Integration &gt; Intelligence &gt; Sources</b></p> <p><b>Intelligence &gt; Elements</b> is now <b>Integration &gt; Intelligence &gt; Elements</b></p> <p><b>Intelligence &gt; Settings</b> is now <b>Integration &gt; Intelligence &gt; Settings</b></p> <p><b>Intelligence &gt; Incidents</b> is now <b>Integration &gt; Intelligence &gt; Incidents</b></p> <p><b>System (⚙️) &gt; Integration</b> is now <b>Integration &gt; Other Integrations</b></p> <p><b>System (⚙️) &gt; Logging &gt; Security Analytics &amp; Logging</b> is now <b>Integration &gt; Security Analytics &amp; Logging</b></p> <p><b>System (⚙️) &gt; SecureX</b> is now <b>Integration &gt; SecureX</b></p>

Table 11: New Features in FMC Version 7.0.1

Feature	Description
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><b>Note</b> 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> <p>New/modified pages: Configure the inspector by editing the Snort 3 version of a custom network analysis policy.</p> <p>Supported platforms: FTD</p>


Feature	Description
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> <p>Supported platforms: ISA 3000 with ASA FirePOWER Services</p>

Table 12: New Features in FMC Version 7.0.0

Feature	Description
<b>Platform</b>	
FTDv performance tiered Smart Licensing.	<p><b>Upgrade impact.</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	Description
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>	

Feature	Description
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>
<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>  <b>&gt; Integration &gt; 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 &gt; VPN &gt; 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>

Feature	Description
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 &gt; Object Management &gt; VPN &gt; AnyConnect File</b>). There is a new <b>HostScan Package</b> option in the <b>File Type</b> drop-down list.  This module runs on endpoints and performs a posture assessment that the dynamic access policy will use.</li> <li>2. Create a dynamic access policy (<b>Devices &gt; Dynamic Access Policy</b>).  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.</li> <li>3. Associate the dynamic access policy you created with an RA VPN policy.  In the remote access VPN policy editor, use the new <b>Dynamic Access Policy</b> setting.</li> </ol> <p>Supported platforms: FTD</p>
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>
<b>Access Control</b>	

Feature	Description
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	Description
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>  <b>&gt; Integration &gt; 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>
<b>Event Logging and Analysis</b>	

Feature	Description
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. 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.</li> </ol> <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</b> &gt; <b>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>

Feature	Description
<p>Work with events stored remotely in a Secure Network Analytics on-prem deployment.</p>	<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>
<p>Store all connection events in the Secure Network Analytics cloud.</p>	<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 (⚙️) &gt; 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 &gt; SecureX</b>.</p> <p>Supported platforms: FMC</p>

Feature	Description
Unified event viewer.	<p>The unified event viewer (<b>Analysis &gt; 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>Analysis &gt; SecureX</b>. Note that you must still use <b>System (⚙️) &gt; Integration &gt; 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 (⚙️) &gt; Configuration &gt; 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>
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>	



Feature	Description
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 (⚙️) &gt; 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	Description
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	Description
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	Description
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

Feature	Description
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> <p>Supported platforms: FTD</p>
<p><b>FMC REST API: New Services and Operations</b></p> <p>We added the following FMC REST API services/operations to support new and existing features. For more information, see the <a href="#">Firepower Management Center REST API Quick Start Guide, Version 7.0</a>.</p>	
Device	alerts: GET
Integration	fmchastatuses: GET securexconfigs: GET and PUT

Feature	Description
Object	anyconnectcustomattributes, anyconnectpackages, anyconnectprofiles: GET anyconnectcustomattributes/overrides: GET applicationfilters: PUT, POST, and DELETE certificatemaps: GET dnsservergroups: GET dnsservergroups/overrides: GET dynamicobjectmappings: POST dynamicobjects: GET, PUT, POST, and DELETE dynamicobjects/mappings: GET and PUT geolocations: PUT, POST, and DELETE grouppolicies: GET hostscanpackages: GET intrusionrules, intrusionrulegroups: GET, PUT, POST, and DELETE intrusionrulesupload: POST ipv4addresspools, ipv6addresspools: GET ipv4addresspools/overrides, ipv6addresspools/overrides: GET localrealmusers: GET, PUT, POST, DELETE radiusservergroups: GET realms: PUT, POST, and DELETE sidnsfeeds, sidnslists, sinetworkfeeds, sinetworklists: GET sinkholes: GET ssoservers: GET ssoservers/overrides: GET usage: GET

Feature	Description
Policy	<p>accesspolicies/securityintelligencepolicies: GET</p> <p>dnspolicies: GET</p> <p>dnspolicies/allowdnrules, dnspolicies/blockdnrules: GET</p> <p>dynamicaccesspolicies: GET, PUT, POST, and DELETE</p> <p>identitypolicies: GET</p> <p>intrusionpolicies: PUT, POST, and DELETE</p> <p>intrusionpolicies/intrusionrulegroups, intrusionpolicies/intrusionrules: GET and PUT</p> <p>networkanalysispolicies: GET, PUT, POST, and DELETE</p> <p>networkanalysispolicies/inspectorconfigs: GET</p> <p>networkanalysispolicies/inspectoroverrideconfigs: GET and PUT</p> <p>ravpns: GET</p> <p>ravpns/addressassignmentsettings, ravpns/certificatemapsettings, ravpns/connectionprofiles: GET</p>
Search	globalsearch: GET

## New Features in FDM Version 7.0

*Table 13: New Features in FDM Version 7.0.0*

Feature	Description
<b>Platform Features</b>	
Virtual router support for the ISA 3000.	You can configure up to 10 virtual routers on an ISA 3000 device.
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.
<b>Firewall and IPS Features</b>	
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.

Feature	Description
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>
<b>VPN Features</b>	
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 FTD 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.



Feature	Description
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>	
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 FTD device on any interface within the zone. This capability allows Equal-Cost Multi-Path (ECMP) routing on the FTD device as well as external load balancing of traffic to the FTD 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 FTD 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.
<b>Administrative and Troubleshooting Features</b>	

Feature	Description
DHCP relay configuration using the FTD API.	<p>You can use the FTD 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 FTD API: dhcprelayservices</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 FTD Software 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>

Feature	Description
Automatically update CA bundles	<p>Requires version 7.0.5.</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><b>Note</b> This feature is not in the base releases for Version 7.0, 7.1, or 7.2, but is (or will be) available in maintenance or patch upgrades to those versions. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco.</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>For more information, see the <a href="#">Cisco Secure Firewall Threat Defense Command Reference</a>.</p>
FTD REST API version 6.1 (v6).	<p>The FTD 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>

## New Hardware and Virtual Platforms in Version 7.0

*Table 14: New Hardware and Virtual Platforms in Version 7.0.5*

Feature	Description
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><b>Note</b> Version 7.1 temporarily deprecates support for this feature. Support will return in a later release.</p>

Table 15: New Hardware and Virtual Platforms in Version 7.0.2

Feature	Description
ISA 3000 support for shutting down.	You can now shut down the ISA 3000; previously, you could only reboot the device.  <b>Note</b> Version 7.1 temporarily deprecates support for this feature. Support returns in Version 7.2.

Table 16: New Hardware and Virtual Platforms in Version 7.0.0

Feature	Description
VMware vSphere/VMware ESXi 7.0 support.	You can now deploy FMCv, FTDv, and NGIPSv virtual appliances on VMware vSphere/VMware ESXi 7.0.  Note that Version 7.0 also discontinues support for VMware 6.0. Upgrade the hosting environment to a supported version before you upgrade the Firepower software.
New virtual environments.	We introduced FMCv and FTDv for: <ul style="list-style-type: none"> <li>• Cisco HyperFlex</li> <li>• Nutanix Enterprise Cloud</li> <li>• OpenStack (no support for FDM management)</li> </ul>

## New Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

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

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

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

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

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

# Deprecated Features

## Deprecated Features in FMC Version 7.0

Table 17: Deprecated Features in FMC Version 7.0.2

Feature	Upgrade Impact	Description
Configure SecureX integration in the REST API.	None.	As part of the improved SecureX integration (see <a href="#">New Features in FMC Version 7.0, on page 13</a> ), you can no longer use the REST API to configure SecureX integration. You must use the FMC web interface.

Table 18: Deprecated Features in FMC Version 7.0.0

Feature	Upgrade Impact	Description
RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm.	Prevents post-upgrade VPN connections through FTD devices.	Version 7.0 removes support for RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm.  Before you upgrade, use the object manager to update your PKI certificate enrollments with stronger options: <b>Objects &gt; PKI &gt; Cert Enrollment</b> . Otherwise, although the upgrade preserves your current settings, VPN connections through the device will fail.  To continue managing older FTD devices only (Version 6.4–6.7.x) with these weaker options, select the new <b>Enable Weak-Crypto</b> option for each device on the <b>Devices &gt; Certificates</b> page.
MD5 authentication algorithm and DES encryption for SNMPv3 users (removed).	Prevents post-upgrade deploy.	Version 7.0 removes support for the MD5 authentication algorithm and DES encryption for SNMPv3 users on FTD devices.  Upgrading FTD to Version 7.0 deletes these users from the device, regardless of the configurations on the FMC. If you are still using these options in your platform settings policy, change and verify your configurations before you upgrade FTD.  These options are in the <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> .
Port 32137 comms with AMP clouds.	Prevents FMC upgrade.	Version 7.0 deprecates the FMC option to use port 32137 to obtain file disposition data from public and private AMP clouds. Unless you configure a proxy, the FMC now uses port 443/HTTPS.  Before you upgrade, disable the <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.

Feature	Upgrade Impact	Description
HA Status health module.	None.	Version 7.0 renames the HA Status health module. It is now the <i>FMC</i> HA Status health module. This is to distinguish it from the new FTD HA Status module.
Legacy API Explorer.	None.	Version 7.0 removes support for the FMC REST API legacy API Explorer.
Geolocation details.	None, this is a date-based deprecation.	<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 reimagine the FMC to Version 7.2+ and update the GeoDB.</p>
Web interface changes.	None.	<p>Version 7.0 changes the following:</p> <ul style="list-style-type: none"> <li>• In the access control rule editor, the <b>Dynamic Attributes</b> tab replaces the narrower-focus <b>SGT/ISE Attributes</b> tab. Continue to configure rules with SGT attributes here.</li> <li>• <b>System &gt; SecureX</b> now configures SecureX integration. Previously, these configurations were on <b>System &gt; Integration &gt; Cloud Services</b>.</li> <li>• <b>Help &gt; How-Tos</b> now invokes walkthroughs. Previously, you clicked <b>How-Tos</b> at the bottom of the browser window.</li> </ul>

## Deprecated Features in FDM Version 7.0

Table 19: Deprecated Features in FDM Version 7.0.0

Feature	Upgrade Impact	Description
DHCP relay with FlexConfig.	Prevents post-upgrade deploy.  You should redo your configurations after upgrade.	Version 7.0 deprecates the following FlexConfig CLI commands for FTD with FDM: <ul style="list-style-type: none"> <li>• <b>dhcrelay</b>: You can now use the FTD API to configure DHCP relay. Using DHCP relay on an interface, you can direct DHCP requests to a DHCP server running on a different interface on the device, or to a DHCP server that is accessible through the other interface. You can configure DHCP relay on physical interfaces, subinterfaces, EtherChannels, and VLAN interfaces.</li> </ul> You cannot deploy post-upgrade until you remove any associated FlexConfig objects.

## Deprecated Hardware and Virtual Platforms in Version 7.0

Table 20: Deprecated Hardware and Virtual Platforms in Version 7.0.0

Feature	Description
VMware vSphere/VMware ESXi 6.0 support.	Version 7.0 discontinues 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 FlexConfig Commands

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



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

### About FlexConfig

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

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

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





## CHAPTER 4

# Upgrade Guidelines

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

- [Planning Your Upgrade](#), on page 43
- [Minimum Version to Upgrade](#), on page 44
- [Upgrade Guidelines for Version 7.0](#), on page 45
- [Upgrade Guidelines for FXOS](#), on page 55
- [Unresponsive Upgrades](#), on page 55
- [Traffic Flow and Inspection](#), on page 56
- [Time and Disk Space Tests](#), on page 60

## 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 21: 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 the software. Back up FXOS on the Firepower 4100/9300. Back up ASA for ASA FirePOWER.
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.

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

## Minimum Version to Upgrade

### Minimum Version to Upgrade

You can upgrade directly to Version 7.0 as follows.

**Table 22: 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 6</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 Version 7.0 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 23: Upgrade Guidelines for FTD with FMC Version 7.0**

✓	Guideline	Platforms	Upgrading From	Directly To
	<a href="#">Cisco Secure Firewall Management Center 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="#">Open and Resolved Bugs</a> , on page 81, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	<a href="#">Minimum Version to Upgrade</a> , on page 44	Any	Any	Any
	<a href="#">Patches That Support Uninstall</a> , on page 73	Any	Any	Any
	<a href="#">Upgrade Guidelines for FXOS</a> , on page 55	Firepower 4100/9300	Any	Any
	<a href="#">Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0</a> , on page 46	Any	7.0.4+	7.1.0 only
	<a href="#">Reconnect with Cisco Threat Grid for High Availability FMCs</a> , on page 47	FMC	6.4.0 through 6.7.x	7.0+
	<a href="#">Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs</a> , on page 47	Firepower 1010	6.4.0 through 6.6.x	6.7+
	<a href="#">FMCv Requires 28 GB RAM for Upgrade</a> , on page 47	FMCv	6.2.3 through 6.5.0.x	6.6+
	<a href="#">Firepower 1000 Series Devices Require Post-Upgrade Power Cycle</a> , on page 48	Firepower 1000 series	6.4.0.x	6.5+

✓	Guideline	Platforms	Upgrading From	Directly To
	<a href="#">New URL Categories and Reputations, on page 49</a>	Any	6.2.3 through 6.4.0.x	6.5+

Table 24: Upgrade Guidelines for FTD with FDM Version 7.0

✓	Guideline	Platforms	Upgrading From	Directly To
	<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="#">Open and Resolved Bugs, on page 81</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="#">Minimum Version to Upgrade, on page 44</a>	Any	Any	Any
	<a href="#">Upgrade Guidelines for FXOS, on page 55</a>	Firepower 4100/9300	Any	Any
	<a href="#">Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0, on page 46</a>	Any	7.0.4+	7.1.0 only
	<a href="#">Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 47</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 48</a>	Firepower 1000 series	6.4.0.x	6.5+
	<a href="#">Historical Data Removed During FTD Upgrade with FDM, on page 48</a>	Any	6.2.3 through 6.4.0.x	6.5+
	<a href="#">New URL Categories and Reputations, on page 49</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 25: 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 26: 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>


Change	Details
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 27: 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 28: 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 52</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 29: 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 30: 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 FXOS

For the Firepower 4100/9300, major FTD upgrades also require an FXOS upgrade. Major FTD versions have a specially qualified and recommended companion FXOS version. Use these combinations whenever possible because we perform enhanced testing for them. Maintenance release and patches rarely require FXOS upgrades, but you may still want to upgrade to the latest FXOS build to take advantage of resolved issues.

For critical and release-specific upgrade guidelines, new and deprecated features, and open and resolved bugs, see the [Cisco Firepower 4100/9300 FXOS Release Notes](#).

## Minimum FXOS Version to Upgrade FTD

The minimum FXOS version to run Version 7.0 is FXOS 2.10.1.159.

## Minimum FXOS Version to Upgrade FXOS

You can upgrade to any later FXOS version from as far back as FXOS 2.2.2.

## Time to Upgrade FXOS

An FXOS upgrade can take up to 45 minutes and can affect traffic flow and inspection. For more information, see [Traffic Flow and Inspection for FXOS Upgrades, on page 56](#).

# 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.

## Traffic Flow and Inspection

Device upgrades affect traffic flow and inspection. Schedule maintenance windows when this will have the least impact.

### Traffic Flow and Inspection for FXOS Upgrades

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

**Table 31: Traffic Flow and Inspection: FXOS Upgrades**

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 32: 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 33: 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 34: 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 35: 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 36: 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 Tests

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

### Time Tests

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



**Caution** Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot 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, see [Unresponsive Upgrades, on page 55](#).

Table 37: Time Test Conditions for Software Upgrades

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

### Disk Space Tests

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

We also report the space needed on the FMC (in either /Volume or /var) for the device upgrade package. If you have an internal server for FTD upgrade packages, or if you are using FDM, ignore those values.

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

Without enough free disk space, the upgrade fails.

Table 38: Checking Disk Space

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

## Time and Disk Space for Version 7.0.5

Table 39: Time and Disk Space for Version 7.0.5

Platform		Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC		20.6 GB in /var	20 MB in /	—	57 min	7 min
FMCv: VMware		22.98 GB in /var	29 MB in /	—	41 min	6 min
Firepower 1000 series		—	6.4 GB in /ngfw	860 MB	16 min	17 min
Firepower 2100 series		—	6.2 GB in /ngfw	920 MB	12 min	16 min
Firepower 4100 series		—	6.5 GB in /ngfw	810 MB	12 min	10 min
Firepower 4100 series container instance		—	7.8 GB in /ngfw	810 MB	13 min	7 min
Firepower 9300		—	6.4 GB in /ngfw	810 MB	16 min	11 min
ASA 5500-X series with FTD	from Version 6.4–6.6	4.9 GB in /home	944 KB in /ngfw	1.0 GB	19 min	19 min
	from Version 6.7	4.9 GB in /ngfw/Volume	208 KB in /ngfw			
	from Version 7.0	5.0 GB in /ngfw/var	290 MB in /ngfw/bin			
FTDv: VMware	from Version 6.4–6.6	4.5 GB in /home	936 KB in /ngfw	1.0 GB	9 min	9 min
	from Version 6.7	4.8 GB in /ngfw/Volume	200 KB in /ngfw			
	from Version 7.0	4.4 GB in /ngfw/var	180 MB in /ngfw/bin			
ASA FirePOWER		8.6 GB in /var	26 MB in /	1.2 GB	74 min	9 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
NGIPSv	5.5 GB in /var	21 MB in /	730 MB	10 min	7 min

## Time and Disk Space for Version 7.0.4

Table 40: Time and Disk Space for Version 7.0.4

Platform		Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC		18 GB in /var	20 MB in /	—	59 min	7 min
FMCv: VMware		23 GB in /var	29 MB in /	—	40 min	6 min
Firepower 1000 series		—	6.4 GB in /ngfw	860 MB	16 min	17 min
Firepower 2100 series		—	6.1 GB in /ngfw	910 MB	14 min	16 min
Firepower 4100 series		—	6.6 GB in /ngfw	810 MB	11 min	11 min
Firepower 4100 series container instance		—	7.7 GB in /ngfw	810 MB	13 min	7 min
Firepower 9300		—	6.4 GB in /ngfw	810 MB	12 min	11 min
ASA 5500-X series with FTD	from Version 6.4–6.6	5.1 GB in /home	944 KB in /ngfw	1.0 GB	18 min	19 min
	from Version 6.7	5.2 GB in /ngfw/Volume	180 KB in /ngfw			
	from Version 7.0	5.0 GB in /ngfw/var	340 MB in /ngfw/bin			
FTDv: VMware	from Version 6.4–6.6	5.7 GB in /home	936 KB in /ngfw	1.0 GB	12 min	18 min
	from Version 6.7	5.2 GB in /ngfw/Volume	180 KB in /ngfw			
	from Version 7.0	4.8 GB in /ngfw/var	180 MB in /ngfw/bin			
ASA FirePOWER		8.5 GB in /var	26 MB in /	1.2 GB	38 min	5 min
NGIPSv		5.8 GB in /var	21 MB in /	730 MB	10 min	8 min

## Time and Disk Space for Version 7.0.3

Table 41: Time and Disk Space for Version 7.0.3

Platform		Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC		15.1 GB in /var	20 MB in /	—	52 min	7 min
FMCv: VMware		20.1 GB in /var	29 MB in /	—	40 min	5 min
Firepower 1000 series		—	6.7 GB in /ngfw	860 MB	16 min	16 min
Firepower 2100 series		—	6.7 GB in /ngfw	910 MB	11 min	16 min
Firepower 4100 series		—	6.9 GB in /ngfw	810 MB	12 min	10 min
Firepower 4100 series container instance		—	8.9 GB in /ngfw	810 MB	12 min	8 min
Firepower 9300		—	7.0 GB in /ngfw	810 MB	15 min	11 min
ASA 5500-X series with FTD	from Version 6.4–6.6	5.3 GB in /home	944 KB in /ngfw	1.0 GB	20 min	19 min
	from Version 6.7	5.3 GB in /ngfw/Volume	200 KB in /ngfw			
	from Version 7.0	5.3 GB in /ngfw/var	300 MB in /ngfw/bin			
FTDv: VMware	from Version 6.4–6.6	5.3 GB in /home	936 KB in /ngfw	1.0 GB	12 min	9 min
	from Version 6.7	5.6 GB in /ngfw/Volume	200 KB in /ngfw			
	from Version 7.0	5.7 GB in /ngfw/var	180 MB in /ngfw/bin			
ASA FirePOWER		8.6 GB in /var	26 MB in /	1.2 GB	58 min	7 min
NGIPSv		5.7 GB in /var	21 MB in /	730 MB	10 min	7 min

## Time and Disk Space for Version 7.0.2.1

Table 42: Time and Disk Space for Version 7.0.2.1

Platform		Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC		2 GB in /var	19 MB in /	—	30 min	4 min
FMCv: VMware		1.9 GB in /var	13 MB in /	—	26 min	3 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
Firepower 1000 series	—	1.4 GB in /ngfw	180 MB	7 min	9 min
Firepower 2100 series	—	1.3 GB in /ngfw	180 MB	6 min	10 min
Firepower 4100 series	—	1.4 GB in /ngfw	180 MB	5 min	7 min
Firepower 9300	—	1.3 GB in /ngfw	180 MB	4 min	8 min
ASA 5500-X series with FTD	900 MB in /ngfw/var	190 MB in /ngfw/bin	190 MB	7 min	12 min
FTDv: VMware	900 MB in /ngfw/var	190 MB in /ngfw/bin	190 MB	4 min	5 min
ASA FirePOWER	950 MB in /var	13 MB in /	55 MB	57 min	6 min
NGIPSv	42 MB in /var	13 MB in /	9 MB	5 min	3 min

## Time and Disk Space for Version 7.0.2

Table 43: Time and Disk Space for Version 7.0.2

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time	
FMC	17.2 GB in /var	20 MB in /	—	53 min	7 min	
FMCv: VMware	17.2 GB in /var	29 MB in /	—	40 min	5 min	
Firepower 1000 series	—	7.0 GB in /ngfw	560 MB	16 min	17 min	
Firepower 2100 series	—	6.7 GB in /ngfw	910 MB	11 min	16 min	
Firepower 4100 series	—	6.9 GB in /ngfw	810 MB	13 min	10 min	
Firepower 4100 series container instance	—	8.2 GB in /ngfw	810 MB	12 min	6 min	
Firepower 9300	—	6.9 GB in /ngfw	810 MB	12 min	11 min	
ASA 5500-X series with FTD	from Version 6.4–6.6	5.7 GB in /home	944 KB in /ngfw	1.0 GB	18 min	19 min
	from Version 6.7	5.5 GB in /ngfw/Volume	300 KB in /ngfw			
	from Version 7.0	5.3 GB in /ngfw/var	3.4 GB in /ngfw/bin			

Platform		Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FTDv: VMware	from Version 6.4–6.6	5.3 GB in /home	936 KB in /ngfw	1.0 GB	10 min	8 min
	from Version 6.7	5.5 GB in /ngfw/Volume	200 KB in /ngfw			
	from Version 7.0	5.5 GB in /ngfw/var	180 MB in /ngfw/bin			
ASA FirePOWER		8.0 GB in /var	26 MB in /	1.2 GB	70 min	14 min
NGIPSv		5.8 GB in /var	21 MB in /	730 MB	12 min	7 min

## Time and Disk Space for Version 7.0.1.1

Table 44: Time and Disk Space for Version 7.0.1.1

Platform		Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC		650 MB in /var	29 MB in /	—	9 min	2 min
FMCv: VMware		770 MB in /var	13 MB in /	—	9 min	2 min
Firepower 1000 series		—	2.1 GB in /ngfw	300 MB	8 min	14 min
Firepower 2100 series		—	2.1 GB in /ngfw	300 MB	7 min	not available
Firepower 4100 series		—	1.4 GB in /ngfw	300 MB	5 min	8 min
Firepower 9300		—	1.7 GB in /ngfw	300 MB	4 min	8 min
ASA 5500-X series with FTD		1.3 GB in /ngfw/var	180 MB in /ngfw/bin	310 MB	7 min	11 min
FTDv: VMware		1.4 GB in /ngfw/var	180 MB in /ngfw/bin	310 MB	4 min	5 min
ASA FirePOWER		760 MB in /var	13 MB in /	250 MB	36 min	1 min
NGIPSv		810 MB in /var	13 MB in /	250 MB	5 min	3 min

## Time and Disk Space for Version 7.0.1

Table 45: Time and Disk Space for Version 7.0.1

Platform		Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC		17 GB in /var	20 MB in /	—	51 min	8 min
FMCv: VMware		19.5 GB in /var	29 MB in /	—	41 min	6 min



Platform		Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
Firepower 1000 series		—	7 GB in /ngfw	850 MB	17 min	25 min
Firepower 2100 series		—	6.6 GB in /ngfw	900 MB	12 min	16 min
Firepower 4100 series		—	6.9 GB in /ngfw	800 MB	12 min	11 min
Firepower 4100 series container instance		—	9.3 GB in /ngfw	800 MB	12 min	9 min
Firepower 9300		—	6.8 GB in /ngfw	800 MB	16 min	10 min
ASA 5500-X series with FTD	from Version 6.4–6.6	6 GB in /home	944 KB in /ngfw	1GB	17 min	18 min
	from Version 6.7	4 GB in /ngfw/Volume	208 KB in /ngfw			
	from Version 7.0	5.4 GB in /ngfw/var	320 MB in /ngfw/bin			
FTDv: VMware	from Version 6.4–6.6	5.3 GB in /home	944 KB in /ngfw	1 GB	18 min	18 min
	from Version 6.7	4.7 GB in /ngfw/Volume	200 KB in /ngfw			
	from Version 7.0	4.2 GB in /ngfw/var	175 MB in /ngfw/bin			
ASA FirePOWER		8.6 GB in /var	26 MB in /	1.1 GB	65 min	7 min
NGIPSv		4.5 GB in /var	21 MB in /	720 MB	10 min	5 min

## Time and Disk Space for Version 7.0.0.1

Table 46: Time and Disk Space for Version 7.0.0.1

Platform		Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC		350 MB in /var	19 MB in /	—	8 min	8 min
FMCv: VMware		66 MB in /var	13 MB in /	—	9 min	2 min
Firepower 1000 series		—	720 MB in /ngfw	47 MB	8 min	9 min
Firepower 2100 series		—	710 MB in /ngfw	42 MB	6 min	10 min
Firepower 4100 series		—	800 MB in /ngfw	47 MB	4 min	6 min
Firepower 9300		—	860 MB in /ngfw	47 MB	4 min	32 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
ASA 5500-X series with FTD	470 MB in /ngfw/var	170 MB in /ngfw/bin	54 MB	6 min	10 min
FTDv: VMware	490 MB in /ngfw/var	160 MB in /ngfw/bin	54 MB	4 min	4 min
ASA FirePOWER	54 MB in /var	13 MB in /	8 MB	39 min	4 min
NGIPSv	66 MB in /var	13 MB in /	8 MB	5 min	3 min

## Time and Disk Space for Version 7.0.0

Table 47: Time and Disk Space for Version 7.0.0

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	14 GB in /var	70 MB in /	—	41 min	7 min
FMCv: VMware	16 GB in /var	72 MB in /	—	28 min	4 min
Firepower 1000 series	420 MB in /ngfw/var	7.6 GB in /ngfw	890 MB	12 min	14 min
Firepower 2100 series	480 MB in /ngfw/var	7.7 GB in /ngfw	950 MB	11 min	13 min
Firepower 4100 series	40 MB in /ngfw/var	8.4 GB in /ngfw	830 MB	8 min	9 min
Firepower 4100 series container instance	36 MB in /ngfw/var	9.7 GB in /ngfw	830 MB	8 min	7 min
Firepower 9300	45 MB in /ngfw/var	11.1 GB in /ngfw	830 MB	11 min	11 min
ASA 5500-X series with FTD	5.3 GB in /ngfw/var	95 KB in /ngfw	1.1 GB	25 min	12 min
FTDv: VMware	6.6 GB in /ngfw/var	23 KB in /ngfw	1.1 GB	11 min	6 min
ASA FirePOWER	9.5 GB in /var	64 MB in /	1.1 GB	69 min	8 min
NGIPSv	5 GB in /var	54 MB in /	720 MB	8 min	4 min



## 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 often 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 69](#)
- [Installation Guides, on page 71](#)

## 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 48: 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 device manager.	Unregister automatically, by removing the device from the FMC.
Switch FTD from device manager to FMC.	Unregister manually.

## Removing Devices from Management

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 49: Scenarios for Removing Devices from Management (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 device manager to FMC.	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 50: 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 51: 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	<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 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

# Revert or Uninstall the Software

---

If an upgrade succeeds but the system does not function to your expectations, you may be able to return to the previous version:

- Revert is for major and maintenance upgrades to FTD with FDM.
- Uninstall is for patches in FMC and ASDM deployments.

If neither of these methods will work for you and you still need to return to an earlier version, you must reimage. Note that neither revert nor uninstall is supported for hotfixes. For failed upgrades, see [Unresponsive Upgrades, on page 55](#).

- [Revert FTD with FDM, on page 73](#)
- [Uninstall a Patch in FMC and ASDM Deployments, on page 73](#)

## Revert FTD with FDM

Reverting a major or maintenance upgrade returns the software to its state just before the upgrade, also called a *snapshot*. Reverting after patching necessarily removes patches as well. To revert a successful FTD upgrade with FDM, see the [System Management](#) chapter in the [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 7.0](#).

## Uninstall a Patch in FMC and ASDM Deployments

Uninstalling a patch returns you to the version you upgraded from, and does not change configurations. Because the FMC must run the same or newer version as its managed devices, uninstall patches from devices first.

## Patches That Support Uninstall

Uninstalling specific patches can cause issues, *even when the uninstall itself succeeds*. These issues include:

- Inability to deploy configuration changes after uninstall.
- Incompatibilities between the operating system and the software.
- FSIC (file system integrity check) failure when the appliance reboots, if you patched with security certifications compliance enabled (CC/UCAPL mode).



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

### Version 7.0 Patches That Support Uninstall

Uninstall is currently supported for all Version 7.0 patches.

## Uninstall Order for High Availability/Scalability

In high availability/scalability deployments, minimize disruption by uninstalling from one appliance at a time. Unlike upgrade, the system does not do this for you. Wait until the patch has fully uninstalled from one unit before you move on to the next.

**Table 52: Uninstall Order for FMC High Availability**

Configuration	Uninstall Order
FMC high availability	<p>With synchronization paused, which is a state called <i>split-brain</i>, uninstall from peers one at a time. Do not make or deploy configuration changes while the pair is split-brain.</p> <ol style="list-style-type: none"> <li>1. Pause synchronization (enter split-brain).</li> <li>2. Uninstall from the standby.</li> <li>3. Uninstall from the active.</li> <li>4. Restart synchronization (exit split-brain).</li> </ol>

**Table 53: Uninstall Order for FTD High Availability and Clusters**

Configuration	Uninstall Order
FTD high availability	<p>You cannot uninstall a patch from devices configured for high availability. You must break high availability first.</p> <ol style="list-style-type: none"> <li>1. Break high availability.</li> <li>2. Uninstall from the former standby.</li> <li>3. Uninstall from the former active.</li> <li>4. Reestablish high availability.</li> </ol>



Configuration	Uninstall Order
FTD cluster	<p>Uninstall from one unit at a time, leaving the control unit for last. Clustered units operate in maintenance mode while the patch uninstalls.</p> <ol style="list-style-type: none"> <li>1. Uninstall from the data modules one at a time.</li> <li>2. Make one of the data modules the new control module.</li> <li>3. Uninstall from the former control.</li> </ol>

*Table 54: 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>

## Uninstall Standalone FMC Patches

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



---

**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 reimaging. If you encounter issues with the uninstall, including a failed uninstall or unresponsive appliance, contact Cisco TAC.

---

### Before you begin

- If uninstalling will put the FMC at a lower patch level than its managed devices, uninstall patches from the devices first.
- Make sure your deployment is healthy and successfully communicating.

---

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

Deploying before you uninstall reduces the chance of failure.

**Step 2** Under Available Updates, click the **Install** icon next to the uninstall package, then choose the FMC.

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

**Step 3** Click **Install**, then confirm that you want to uninstall and reboot.

You can monitor uninstall progress in the Message Center until you are logged out.

**Step 4** Log back in when you can and verify uninstall success.

If the system does not notify you of the uninstall's success when you log in, choose **Help > About** to display current software version information.

**Step 5** Redeploy configurations to all managed devices.

---

## Uninstall High Availability FMC Patches

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

Uninstall from high availability peers one at a time. With synchronization paused, first uninstall from the standby, then the active. When the standby starts the uninstall, its status switches from standby to active, so that both peers are active. This temporary state is called *split-brain* and is *not* supported except during upgrade and uninstall.



---

**Caution** Do not make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you restart synchronization. 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

- If uninstalling will put the FMCs at a lower patch level than their managed devices, uninstall patches from the devices first.
- Make sure your deployment is healthy and successfully communicating.

- 
- Step 1** On the active FMC, deploy to managed devices whose configurations are out of date.  
Deploying before you uninstall reduces the chance of failure.
- Step 2** On the active FMC, pause synchronization.
- a) Choose **System > Integration**.
  - b) On the **High Availability** tab, click **Pause Synchronization**.
- Step 3** Uninstall the patch from peers one at a time — first the standby, then the active.  
Follow the instructions in [Uninstall Standalone FMC Patches](#), on page 76, but omit the initial deploy, stopping after you verify uninstall success on each peer. In summary, for each peer:
- a) On the **System > Updates** page, uninstall the patch.
  - b) Monitor progress until you are logged out, then log back in when you can.
  - c) Verify uninstall success.
- Step 4** On the FMC you want to make the active peer, restart synchronization.
- a) Choose **System > Integration**.
  - b) On the **High Availability** tab, click **Make-Me-Active**.
  - c) Wait until synchronization restarts and the other FMC switches to standby mode.
- Step 5** Redeploy configurations to all managed devices.
- 

## Uninstall Device Patches with FMC

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. You cannot use an FMC user account. If you disabled shell access, contact Cisco TAC to reverse the lockdown.



**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

- Break FTD high availability pairs. In other high availability/scalability deployments, make sure you are uninstalling from the correct device; see [Uninstall Order for High Availability/Scalability, on page 74](#).
- Make sure your deployment is healthy and successfully communicating.

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

Deploying before you uninstall reduces the chance of failure. 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.

**Exception:** Do not deploy to mixed-version clusters or high availability pairs. In a high availability/scalability deployment, deploy before you uninstall from the first unit, but then not again until you have uninstalled the patch from all units.

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

You can either SSH to the device's management interface (hostname or IP address) or use the console. If you use the console, some devices default to the operating system CLI, and require an extra step to access the Firepower CLI.

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

**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:

- FTD: `tail /ngfw/var/log/sf/update.status`
- ASA FirePOWER and NGIPSv: `tail /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 device has the correct software version. On the FMC, choose **Devices > Device Management**.

**Step 8** Redeploy configurations.

**Exception:** Do not deploy to mixed-version clusters or high availability pairs. Deploy only after you repeat this procedure for all units.

---

### What to do next

In high availability/scalability deployments, repeat this procedure for each unit in your planned sequence. Then, make any final adjustments. For example:

- For FTD high availability, reestablish high availability.
- For FTD clusters, if you have preferred roles for specific devices, make those changes now.

## 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.



---

**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; see [Uninstall Order for High Availability/Scalability, on page 74](#).
- 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.



# CHAPTER 7

## Open and Resolved Bugs

For your convenience, this document lists open and resolved bugs for Version 7.0.



**Important** Bug lists are auto-generated once and may not be subsequently updated. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes. We also do not list open bugs for maintenance releases or patches. The last-updated date for a bug list does not indicate that the list was fully accurate on that date—only that we made some change to the list. If you have a support contract, you can obtain up-to-date bug lists with the [Cisco Bug Search Tool](#).

- [Open Bugs in Version 7.0, on page 81](#)
- [Resolved Bugs in Version 7.0, on page 83](#)

## Open Bugs in Version 7.0

### Open Bugs in Version 7.0.0

Table last updated: 2022-11-02

**Table 55: 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
<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

Bug ID	Headline
<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="#">CSCwal6654</a>	Firepower release 7.0.x does not support ssl_state or ssl_version keywords for Snort 3



# Resolved Bugs in Version 7.0

## Resolved Bugs in Version 7.0.5

Table last updated: 2022-11-17

**Table 56: 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 sfipproxy 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
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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.

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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



Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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 &lt;&gt; IPv6 NAT translations

Bug ID	Headline
<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&lt;&gt;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
<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

Bug ID	Headline
<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
<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 57: 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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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)
<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.



Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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."

Bug ID	Headline
<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 58: 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 59: 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 60: 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

Bug ID	Headline
<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
<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 hitent 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)

Bug ID	Headline
<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
<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)

Bug ID	Headline
<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
<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"

Bug ID	Headline
<a href="#">CSCvz34149</a>	Update the new location of /opt/cisco/platfom/logs/var/log/messages
<a href="#">CSCvo77184</a>	VMware ASA v 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
<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

Bug ID	Headline
<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
<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



Bug ID	Headline
<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
<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

Bug ID	Headline
<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.
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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"
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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 ASA v9.12
<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
<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



Bug ID	Headline
<a href="#">CSCvz24238</a>	CiscoÂ 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
<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

Bug ID	Headline
<a href="#">CSCvy99348</a>	Shutdown command reboots instead of shutting the FP1k 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.
<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 61: Resolved Bugs in Version 7.0.1.1*

Bug ID	Headline
<a href="#">CSCwa46963</a>	Security: CVE-2021-44228 -> Log4j 2 Vulnerability

Bug ID	Headline
<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 62: 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
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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"

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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 )

Bug ID	Headline
<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 idhttpd 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
<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



Bug ID	Headline
<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
<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

Bug ID	Headline
<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 63: 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 64: 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
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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

Bug ID	Headline
<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
<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)

