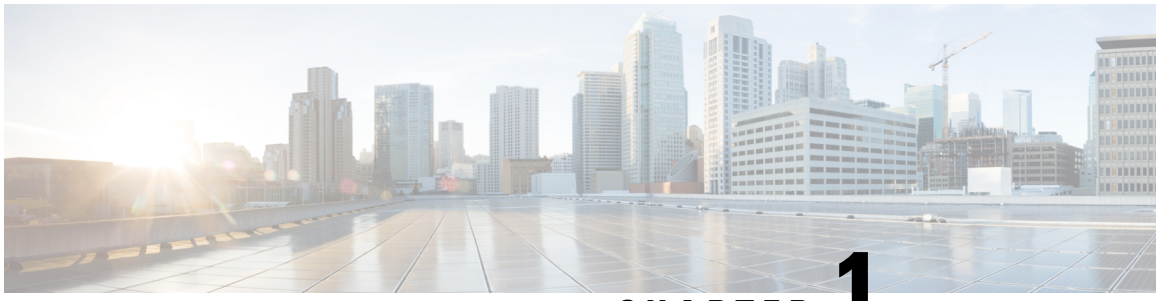
Cisco Firepower Release Notes, Version 7.0

First Published: 2021-05-26

Last Modified: 2022-12-19

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

CONTENTS



CHAPTER 1

Welcome

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

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

Release Highlights

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
7.0.5.1	5	2023-04-26	NGIPSv For devices with security certifications compliance enabled (CC/UCAPL mode). Use with a Version 7.0.5 FMC.
7.0.5	72	2022-11-17	All
7.0.4	55	2022-08-10	All
7.0.3	37	2022-06-30	All
7.0.2.1	10	2022-06-27	All
7.0.2	88	2022-05-05	All

Version	Build	Date	Platforms
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.

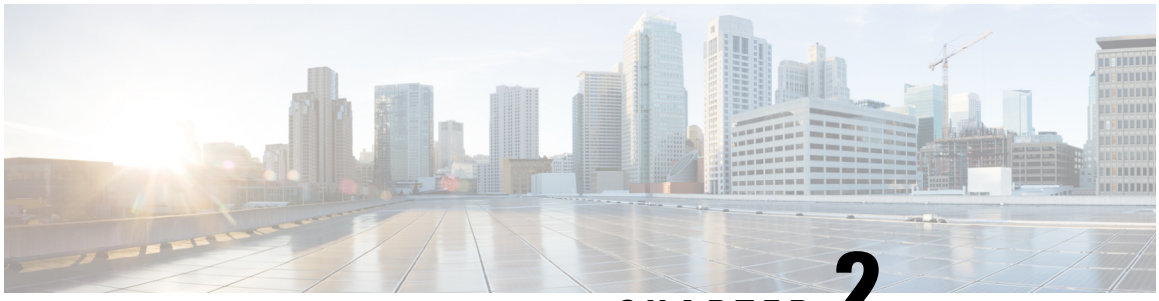
- Documentation: http://www.cisco.com/go/threatdefense-70-docs
- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.cisco.com/cisco/support/notifications.html

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
- 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

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

FMC Hardware

Version 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 some platforms support 300 devices. Also, two-device virtual FMCs do 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	Devices Managed		High Availability
	2, 10, 25	300	
Public Cloud			
Amazon Web Services (AWS)	YES	—	—
Google Cloud Platform (GCP)	YES	—	—
Microsoft Azure	YES	—	—
Oracle Cloud Infrastructure (OCI)	YES	—	—
On-Prem/Private Cloud			
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. The cloud-delivered Firewall Management Center does not have a version, and we take care of feature updates.

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

Device Platforms

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

FTD Hardware

Version 7.0 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 Firepower 9300: SM-24, SM-36, SM-44 modules Firepower 9300: SM-40, SM-48, SM-56 modules	YES	YES Requires Version 7.0.3+	YES	YES	Requires FXOS 2.10.1.159 or later build. We recommend the latest firmware. See the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.
ASA 5508-X, 5516-X	YES	YES Requires Version 7.0.3+	YES	YES	Requires the latest ROMMON image. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
ISA 3000	YES	YES Requires Version 7.0.3+	YES	YES	Requires the latest ROMMON image. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

FTDv

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

Table 4: Version 7.0 FTDv Platforms

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

Firepower Classic: ASA FirePOWER, NGIPSv

Firepower Classic devices run NGIPS software on the following platforms:

- ASA devices can run NGIPS software as a separate application (the *ASA FirePOWER module*). Traffic is sent to the module after ASA firewall policies are applied. Although there is wide compatibility between ASA and ASA FirePOWER versions, upgrading allows you to take advantage of new features and resolved issues.
- NGIPSv runs the software in virtualized environments.

Table 5: 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 Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
ISA 3000	YES	Requires ASDM 7.16(1).	Requires ASA 9.5(2) to 9.16(x). Requires the latest ROMMON image. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
NGIPSv	YES	—	Requires VMware vSphere/VMware ESXi 6.5, 6.7, or 7.0 For supported instances, throughputs, and other hosting requirements, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.

Device Management

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

Customer-Deployed FMC

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

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

Note that in most cases you can upgrade an older device directly to the FMC's major or maintenance version. However, sometimes you can manage an older device that you cannot directly upgrade, even though the target

version is supported on the device. For release-specific requirements, see Minimum Version to Upgrade, on page 42.

Table 6: Customer-Deployed FMC-Device Compatibility

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

Cloud-delivered Firewall Management Center

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

- Version 7.2+
- Version 7.0.3 and later maintenance releases

The cloud-delivered Firewall Management Center cannot manage FTD devices running Version 7.1, or Classic devices running any version. You cannot upgrade a cloud-managed device from Version 7.0.x to Version 7.1

unless you unregister and disable cloud management. We recommend you upgrade 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.

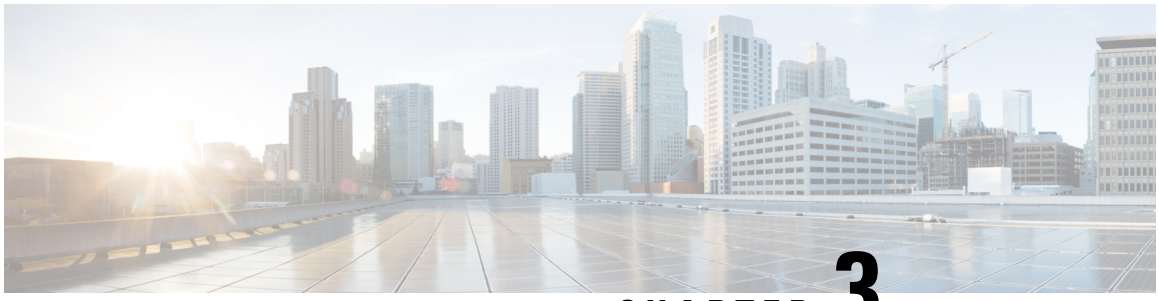
For detailed procedures, see the online help or the configuration guide for your product.

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 describes new and deprecated features for Version 7.0, including upgrade impact. For Cisco Defense Orchestrator (CDO) deployments, 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 in FMC Version 7.0

Although you can manage older devices with a newer FMC, we recommend you always update your entire deployment. New traffic-handling features usually 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 this document, we are explicit when version requirements deviate from the standard expectation.

New Features

Table 7: New Features in FMC Version 7.0.5

New Feature	Description
ISA 3000 System LED support for shutting down.	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. **Note** Version 7.1 temporarily deprecates support for this feature. Support returns in Version 7.3.

New Feature	Description
Automatically update CA bundles.	**Upgrade impact.** 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. **Note** This feature is not supported in Version 7.0.0–7.0.4, 7.1.0–7.1.0.2, or 7.2.0–7.2.3. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco. New/modified CLI commands: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** For more information, see the Firepower Management Center Command Line Reference in the FMC configuration guide, and the Cisco Secure Firewall Threat Defense Command Reference.

Table 8: New Features in FMC Version 7.0.3

New Feature	Description
FTD support for cloud-delivered management center.	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. You should use Version 7.0.3 FTD with the cloud-delivered management center if: • You are currently using a customer-deployed hardware or virtual FMC. • You want to migrate to the cloud-delivered management center right now. • You do not want to upgrade devices to Version 7.2+, which also supports management by the cloud-delivered management center. If this is your situation, you should: **1.** Upgrade the current FMC to Version 7.2+. 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"). **2.** Use the upgraded FMC to upgrade devices to Version 7.0.3. **3.** Enable cloud management on the devices. For Version 7.0.x devices only, you must enable cloud management from the device CLI: **configure manager-cdo enable**. The **show manager-cdo** command displays whether cloud management is enabled. **4.** Use CDO's Migrate FTD to Cloud wizard to migrate the devices to the cloud-delivered management center. 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). The cloud-delivered Firewall Management Center cannot manage FTD devices running Version 7.1, or Classic devices running any version. You cannot upgrade a cloud-managed device from Version 7.0.x to Version 7.1 unless you unregister and disable cloud management. We recommend you upgrade the device directly to Version 7.2+. New/modified CLI commands: **configure manager add**, **configure manager delete**, **configure manager edit**, **show managers** For more information, see Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator.

Table 9: New Features in FMC Version 7.0.2

New Feature	Description
ISA 3000 support for shutting down.	You can now shut down the ISA 3000; previously, you could only reboot the device. **Note** Version 7.1 temporarily deprecates support for this feature. Support returns in Version 7.2.
Dynamic object names now support the dash character.	Dynamic object names now support the dash character. This is especially useful if you are using the ACI endpoint update app (where the dash character is allowed), to create dynamic objects on the FMC that represent tenant endpoint groups. Minimum threat defense: 7.0.2
Improved SecureX integration, SecureX orchestration.	We have streamlined the SecureX integration process. Now, as long as you already have a SecureX account, you just choose your cloud region on the new **Integration > SecureX** page, click **Enable SecureX**, and authenticate to SecureX. The option to send events to the cloud, as well as to enable Cisco Success Network and Cisco Support Diagnostics, are also moved to this new page. When you enable SecureX integration on this new page, licensing and management for the system's cloud connection switches from Cisco Smart Licensing to SecureX. If you already enabled SecureX the "old" way, you must disable and re-enable to get the benefits of this cloud connection management. Note that this page also governs the cloud region for and event types sent to the Secure Network Analytics (Stealthwatch) cloud using Security Analytics and Logging (SaaS), even though the web interface does not indicate this. Previously, these options were on **System** (⚙) **> Integration > Cloud Services**. Enabling SecureX does not affect communications with the Secure Network Analytics cloud; you can send events to both. The 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. As part of this feature, you can no longer use the REST API to configure SecureX integration. You must use the FMC web interface. **Note** This feature is temporarily deprecated in Version 7.1, but returns 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 affected. For more information, see the Cisco Secure Firewall Management Center (7.0.2 and 7.2) and SecureX Integration Guide.

New Feature	Description
Web interface changes: SecureX, threat intelligence, and other integrations.	We changed these FMC menu options. **Note** These changes are temporarily deprecated in Version 7.1, but come back in Version 7.2. **AMP > AMP Management** is now **Integration > AMP > AMP Management** **AMP > Dynamic Analysis Connections** is now **Integration > AMP > Dynamic Analysis Connections** **Intelligence > Sources** is now **Integration > Intelligence > Sources** **Intelligence > Elements** is now **Integration > Intelligence > Elements** **Intelligence > Settings** is now **Integration > Intelligence > Settings** **Intelligence > Incidents** is now **Integration > Intelligence > Incidents** **System (⚙) > Integration** is now **Integration > Other Integrations** **System (⚙) > Logging > Security Analytics & Logging** is now **Integration > Security Analytics & Logging** **System (⚙) > SecureX** is now **Integration > SecureX**

Table 10: New Features in FMC Version 7.0.1

New Feature	Description
Snort 3 rate_filter inspector.	We introduced the Snort 3 rate_filter inspector. This allows you to change the action of an intrusion rule in response to excessive matches on that rule. You can block rate-based attacks for a specific length of time, then return to allowing matching traffic while still generating events. For more information, see the Snort 3 Inspector Reference. **Note** 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 **System (⚙) > Updates > Rule Updates**. New/modified pages: Configure the inspector by editing the Snort 3 version of a custom network analysis policy. Supported platforms: FTD

New Feature	Description
New default password for ISA 3000 with ASA FirePOWER Services	For new devices, the default password for the admin account is now Adm!n123. Previously, the default admin password was Admin123. Upgrading or reimaging to Version 7.0.1+ does not change the password. However, we do recommend that all user accounts—especially those with Admin access—have strong passwords. Supported platforms: ISA 3000 with ASA FirePOWER Services

Table 11: New Features in FMC Version 7.0.0

New Feature	Description
Platform	
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: • Cisco HyperFlex • Nutanix Enterprise Cloud • OpenStack (no support for FDM management)
FTDv performance tiered Smart Licensing.	**Upgrade impact.** FTDv now supports performance-tiered Smart Software Licensing, based on throughput requirements and RA VPN session limits. Options run from FTDv5 (100 Mbps/50 sessions) to FTDv100 (16 Gbps/10,000 sessions). Before you add a new device, make sure your account contains the licenses you need. To purchase additional licenses, contact your Cisco representative or partner contact. Upgrading FTDv to Version 7.0 automatically assigns the device to the FTDv50 tier. To continue using your legacy (non-tiered) license, after upgrade, change the tier to Variable. For more information on supported instances, throughputs, and other hosting requirements, see the appropriate *Getting Started Guide*. New/modified pages: • You can now specify a performance tier when adding or editing an FTDv device on the **Device > Device Management** page. • You can bulk-edit performance tiers on **System** (⚙) > **Licenses** > **Smart Licenses** > page.

New Feature	Description
High Availability/Scalability	
Improved PAT port block allocation for clustering	The improved PAT port block allocation ensures that the control unit keeps ports in reserve for joining nodes, and proactively reclaims unused ports. To best optimize the allocation, you can set the maximum nodes you plan to have in the cluster using the **cluster-member-limit** command using FlexConfig. The control unit can then allocate port blocks to the planned number of nodes, and it will not have to reserve ports for extra nodes you don't plan to use. The default is 16 nodes. You can also monitor syslog 747046 to ensure that there are enough ports available for a new node. New/modified commands: **cluster-member-limit** (FlexConfig), **show nat pool cluster [summary]**, **show nat pool ip detail** Supported platforms: Firepower 4100/9300
FTD CLI **show cluster history** improvements.	New keywords allow you to customize the output of the **show cluster history** command. New/modified commands: **show cluster history** [**brief**] [**latest**] [**reverse**] [**time**] Supported platforms: Firepower 4100/9300
FTD CLI command to permanently leave a cluster.	You can now use the FTD CLI to permanently remove a unit from the cluster, converting its configuration to a standalone device. New/modified commands: **cluster reset-interface-mode** Supported platforms: Firepower 4100/9300
NAT	
Prioritized system-defined NAT rules.	We added a new Section 0 to the NAT rule table. This section is exclusively for the use of the system. Any NAT rules that the system needs for normal functioning are added to this section, and these rules take priority over any rules you create. Previously, system-defined rules were added to Section 1, and user-defined rules could interfere with proper system functioning. You cannot add, edit, or delete Section 0 rules, but you will see them in **show nat detail** command output. Supported platforms: FTD
Virtual Routing	
Virtual router support for the ISA 3000.	You can now configure up to 10 virtual routers on an ISA 3000 device. Supported platforms: ISA 3000
Site to Site VPN	

New Feature	Description
Backup virtual tunnel interfaces (VTI) for route-based site-to-site VPN.	When you configure a site-to-site VPN that uses virtual tunnel interfaces, you can select a backup VTI for the tunnel. Specifying a backup VTI provides resiliency, so that if the primary connection goes down, the backup connection might still be functional. For example, you could point the primary VTI to the endpoint of one service provider, and the backup VTI to the endpoint of a different service provider. New/modified pages: We added the ability to add a backup VTI to the site-to-site VPN wizard when you select Route-Based as the VPN type for a point-to-point connection. Supported platforms: FTD
Remote Access VPN	
Load balancing.	We now support RA VPN load balancing. The system distributes sessions among grouped devices by number of sessions; it does not consider traffic volume or other factors. New/modified screens: We added load balancing options to the Advanced settings in an RA VPN policy. Supported platforms: FTD
Local authentication.	We now support local authentication for RA VPN users. You can use this as the primary or secondary authentication method, or as a fallback in case the configured remote server cannot be reached. **1.** Create a local realm. Local usernames and passwords are stored in local realms. When you create a realm (**System** (⚙) > **Integration** > **Realms**) and select the new **LOCAL** realm type, the system prompts you to add one or more local users. **2.** Configure RA VPN to use local authentication. Create or edit an RA VPN policy (**Devices > VPN > Remote Access**), create a connection profile within that policy, then specify **LOCAL** as the primary, secondary, or fallback authentication server in that connection profile. **3.** Associate the local realm you created with an RA VPN policy. In the RA VPN policy editor, use the new **Local Realm** setting. Every connection profile in the RA VPN policy that uses local authentication will use the local realm you specify here. Supported platforms: FTD

New Feature	Description
Dynamic access policies.	The new dynamic access policy allows you to configure remote access VPN authorization that automatically adapts to a changing environment: **1.** Configure HostScan by uploading the AnyConnect HostScan package as an AnyConnect file (**Objects > Object Management > VPN > AnyConnect File**). There is a new **HostScan Package** option in the **File Type** drop-down list. This module runs on endpoints and performs a posture assessment that the dynamic access policy will use. **2.** Create a dynamic access policy (**Devices > Dynamic Access Policy**). Dynamic access policies specify session attributes (such as group membership and endpoint security) that you want to evaluate each time a user initiates a session. You can then deny or grant access based on that evaluation. **3.** Associate the dynamic access policy you created with an RA VPN policy. In the remote access VPN policy editor, use the new **Dynamic Access Policy** setting. Supported platforms: FTD
Multi-certificate authentication.	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. Supported platforms: FTD
AnyConnect custom attributes.	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. Supported platforms: FTD
Access Control	

New Feature	Description
Snort 3 for FTD.	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. Supported platforms: FTD

New Feature	Description
Dynamic objects.	You can now use *dynamic objects* in access control rules. A dynamic object is just a list of IP addresses/subnets (no ranges, no FQDN). But unlike a network object, changes to dynamic objects take effect immediately, without having to redeploy. This is useful in virtual and cloud environments, where IP addresses often dynamically map to workload resources. To create and manage dynamic objects, we recommend the Cisco Secure Dynamic Attributes Connector. The connector is a separate, lightweight application that quickly and seamlessly updates firewall policies based on workload changes. To do this, it gets workload attributes from tagged resources in your environment, and compiles an IP list based on criteria you specify (a "dynamic attributes filter"). It then creates a dynamic object on the FMC and populates it with the IP list. When your workload changes, the connector updates the dynamic object and the system immediately starts handling traffic based on the new mappings. For more information, see the Cisco Secure Dynamic Attributes Connector Configuration Guide. After you create a dynamic object, you can add it to access control rules on the new **Dynamic Attributes** tab in the access control rule editor. This tab replaces the narrower-focus **SGT/ISE Attributes** tab; continue to configure rules with SGT attributes here. **Note** You can also create a dynamic object on the FMC: **Objects > Object Management > External Attributes > Dynamic Objects**. However, this creates the container only; you must then populate and manage it using the REST API. See the Firepower Management Center REST API Quick Start Guide, Version 7.0. Supported platforms: FMC Supported virtual/cloud workloads for Cisco Secure Dynamic Attributes Connector integration: Microsoft Azure, AWS, VMware
Cross-domain trust for Active Directory domains.	You can now configure user identity rules with users from Microsoft Active Directory forests (groupings of AD domains that trust each other). New/modified pages: • You now configure a realm and directories at the same time. • A new Sync Results page (**System** (⚙) > **Integration** > **Sync Results**) displays any errors related to downloading users and groups in a cross-domain trust relationship. Supported platforms: FMC
DNS filtering.	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. Supported platforms: Any
Event Logging and Analysis	

New Feature	Description
Improved process for storing events in a Secure Network Analytics on-prem deployment.	A new Cisco Security Analytics and Logging (On Premises) app and a new FMC wizard make it easier to configure remote data storage for on-prem Secure Network Analytics solutions: **1.** Deploy hardware or virtual Stealthwatch appliances. You can use a Stealthwatch Management Console alone, or you can configure Stealthwatch Management Console, flow collector, and data store. **2.** Install the new Cisco Security Analytics and Logging (On Premises) app on your Stealthwatch Management Console to configure Stealthwatch as a remote data store. **3.** On the FMC, use one of the new wizards on **System** (⚙) > **Logging** > **Security Analytics & Logging** to connect to your Stealthwatch deployment. Note that the wizards replace the narrower-focus page where you used to configure Stealthwatch contextual cross-launch; that is now a step in the wizard. For upgraded deployments where you were using syslog to send Firepower events to Stealthwatch, disable those configurations before you use the wizard. Otherwise, you will get double events. To remove the syslog connection to Stealthwatch use FTD platform settings (**Devices > Platform Settings**); to disable sending events to syslog, edit your access control rules. For more information, including Stealthwatch hardware and software requirements, see Cisco Security Analytics and Logging (On Premises): Firewall Event Integration Guide. Supported platforms: FMC

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

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

New Feature	Description
Improved FTD upgrade performance and status reporting.	FTD upgrades are now easier faster, more reliable, and take up less disk space. A new **Upgrades** tab in the Message Center provides further enhancements to upgrade status and error reporting. Supported platforms: FTD
Upgrade wizard for FTD.	A new device upgrade page (**Devices > Device Upgrade**) on the FMC provides an easy-to-follow wizard for upgrading Version 6.4+ FTD devices. It walks you through important pre-upgrade stages, including selecting devices to upgrade, copying the upgrade package to the devices, and compatibility and readiness checks. To begin, use the new **Upgrade Firepower Software** action on the Device Management page (**Devices > Device Management > Select Action**). As you proceed, the system displays basic information about your selected devices, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a device does not "pass" a stage in the wizard, it does not appear in the next stage. If you navigate away from wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the wizard. **Note** You must still use **System** (⚙) > **Updates** to upload or specify the location of FTD upgrade packages. You must also use the System Updates page to upgrade the FMC itself, as well as all non-FTD managed devices. **Note** In Version 7.0, the wizard does not correctly display devices in clusters or high availability pairs. Even though you must select and upgrade these devices as a unit, the wizard displays them as standalone devices. Device status and upgrade readiness are evaluated and reported on an individual basis. This means it is possible for one unit to appear to "pass" to the next stage while the other unit or units do not. However, these devices are still grouped. Running a readiness check on one, runs it on all. Starting the upgrade on one, starts it on all. To avoid possible time-consuming upgrade failures, *manually* ensure all group members are ready to move on to the next step of the wizard before you click **Next**. Supported platforms: FTD

New Feature	Description
Upgrade more FTD devices at once.	The FTD upgrade wizard lifts the following restrictions: • Simultaneous device upgrades. The number of devices you can upgrade at once is now limited by your management network bandwidth—not the system's ability to manage simultaneous upgrades. Previously, we recommended against upgrading more than five devices at a time. **Important** Only upgrades to FTD Version 6.7+ 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. • Grouping upgrades by device model. 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. Previously, you would choose an upgrade package, then choose the devices to upgrade using that package. That meant that you could upgrade multiple devices at the same time *only* if they shared an upgrade package. For example, you could upgrade two Firepower 2100 series devices at the same time, but not a Firepower 2100 series and a Firepower 1000 series. Supported platforms: FTD
Administration and Troubleshooting	
Zero-touch restore for the ISA 3000 using the SD card.	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. Supported platforms: ISA 3000
Selectively deploy RA and site-to-site VPN policies.	Selective policy deployment, which was introduced in Version 6.6, now supports remote access and site-to-site VPN policies. New/modified pages: We added VPN policy options on the **Deploy > Deployment** page. Supported platforms: FTD

New Feature	Description
New health modules.	We added the following health modules: • AMP Connection Status • AMP Threat Grid Status • ASP Drop • Advanced Snort Statistics • Chassis Status FTD • Event Stream Status • FMC Access Configuration Changes • FMC HA Status (replaces HA Status) • FTD HA Status • File System Integrity Check • Flow Offload • Hit Count • MySQL Status • NTP Status FTD • Rabbit MQ Status • Routing Statistics • SSE Connection Status • Sybase Status • Unresolved Groups Monitor • VPN Statistics • xTLS Counters Additionally, full support returns for the Configuration Memory Allocation module, which was introduced in Version 6.6.3 as the Appliance Configuration Resource Utilization module, but was not fully supported in Version 6.7. Supported platforms: FMC
Security and Hardening	
New default password for AWS deployments.	The default password for the admin account is now the AWS Instance ID, unless you define a default password with user data (**Advanced Details > User Data**) during the initial deployment. Previously, the default admin password was Admin123. Supported platforms: FMCv for AWS, FTDv for AWS

New 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 **Objects > PKI > Cert Enrollment > CA Information** 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 **Objects > PKI > Cert Enrollment > Key** 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: **System** (⚙) > **Configuration** > **Time Synchronization**. 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: **Devices > Platform Settings > SNMP > Users > Auth Algorithm Type** Supported platforms: FTD
Usability and Performance	
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 **Search** icon and field on the FMC menu bar, to the left of the **Deploy** menu. Supported platforms: FMC
Hardware crypto acceleration on FTDv using Intel QuickAssist Technology (QAT).	We now support hardware crypto acceleration (CBC cipher only) on FTDv for VMware and FTDv for KVM. This feature requires a Intel QAT 8970 PCI adapter/Version 1.7+ driver on the hosting platform. After you reboot, hardware crypto acceleration is automatically enabled. Supported platforms: FTDv for VMware, FTDv for KVM
Improved CPU usage and performance for many-to-one and one-to-many connections.	The system no longer creates local host objects and locks them when creating connections, except for connections that involve dynamic NAT/PAT and scanning threat detection and host statistics. This improves performance and CPU usage in situations where many connections are going to the same server (such as a load balancer or web server), or one endpoint is making connections to many remote hosts. We changed the following commands: **clear local-host** (deprecated), **show local-host** Supported platforms: FTD

New Feature	Description
How-to location has changed.	**Help** > **How-Tos** now invokes walkthroughs. Previously, you clicked **How-Tos** at the bottom of the browser window.
FMC REST API We added the following FMC REST API services/operations to support new and existing features. For more information, see the Firepower Management Center REST API Quick Start Guide, Version 7.0.	
Device	alerts: GET
Integration	fmchastatuses: GET securexconfigs: GET and PUT
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

New Feature	Description
Policy	accesspolicies/securityintelligencepolicies: GET dnspolicies: GET dnspolicies/allowdnsrules, dnspolicies/blockdnsrules: GET dynamicaccesspolicies: GET, PUT, POST, and DELETE identitypolicies: GET intrusionpolicies: PUT, POST, and DELETE intrusionpolicies/intrusionrulegroups, intrusionpolicies/intrusionrules: GET and PUT networkanalysispolicies: GET, PUT, POST, and DELETE networkanalysispolicies/inspectorconfigs: GET networkanalysispolicies/inspectoroverrideconfigs: GET and PUT ravpns: GET ravpns/addressassignmentsettings, ravpns/certificatemapsettings, ravpns/connectionprofiles: GET
Search	globalsearch: GET

Deprecated Features

Table 12: Deprecated Features in FMC Version 7.0.0

Deprecated Feature	Description
End of support: VMware vSphere/VMware ESXi 6.0.	We discontinued support for virtual deployments on VMware vSphere/VMware ESXi 6.0. Upgrade the hosting environment to a supported version before you upgrade the Firepower software.
Deprecated: RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm.	**Prevents post-upgrade VPN connections through FTD devices.** We removed support for RSA certificates with keys smaller than 2048 bits, or that use SHA-1 in their signature algorithm. Before you upgrade, use the object manager to update your PKI certificate enrollments with stronger options: **Objects > PKI > Cert Enrollment**. Otherwise, although the upgrade preserves your current settings, VPN connections through the device will fail. To continue managing older FTD devices only (Version 6.4–6.7.x) with these weaker options, select the new **Enable Weak-Crypto** option for each device on the **Devices > Certificates** page.

Deprecated Feature	Description
Deprecated: MD5 authentication algorithm and DES encryption for SNMPv3 users.	**Deletes Users. Prevents post-upgrade deploy.** We removed support for the MD5 authentication algorithm and DES encryption for SNMPv3 users on FTD devices. Upgrading FTD to Version 7.0+ deletes these users from the device, regardless of the configurations on the FMC. If you are still using these options in your platform settings policy, change and verify your configurations before you upgrade FTD. These options are in the **Auth Algorithm Type** and **Encryption Type** drop-downs when creating or editing an SNMPv3 user in a Threat Defense platform settings policy: **Devices > Platform Settings**.
Deprecated: Port 32137 comms with AMP clouds.	**Prevents FMC upgrade.** We deprecated the FMC option to use port 32137 to obtain file disposition data from public and private AMP clouds. Unless you configure a proxy, the FMC now uses port 443/HTTPS. Before you upgrade, disable the **Use Legacy Port 32137 for AMP for Networks** option on the **System > Integration > Cloud Services** page. Do not proceed with upgrade until your AMP for Networks deployment is working as expected.
Deprecated: HA Status health module.	We renamed the HA Status health module to the *FMC* HA Status health module. This is to distinguish it from the new FTD HA Status module.
Deprecated: Legacy API Explorer.	We removed support for the FMC REST API legacy API Explorer.
Deprecated: Geolocation details.	In May 2022 we split the GeoDB into two packages: a country code package that maps IP addresses to countries/continents, and an IP package that contains additional contextual data associated with routable IP addresses. The contextual data in the IP package can include additional location details, as well as connection information such as ISP, connection type, proxy type, domain name, and so on. The new country code package has the same file name as the old all-in-one package: Cisco_GEODB_Update-*date-build*. This allows deployments running Version 7.1 and earlier to continue to obtain GeoDB updates. If you manually download GeoDB updates—for example, in an air-gapped deployment—make sure you get the country code package and not the IP package. **Important** This split does not affect geolocation rules or traffic handling in any way—those rules rely only on the data in the country code package. However, because the country code package essentially replaces the all-in-one package, the contextual data is no longer updated and will grow stale. To obtain fresh data, upgrade or reimage the FMC to Version 7.2+ and update the GeoDB.

New Features in FDM Version 7.0

Table 13: New and Deprecated Features in FDM Version 7.0

Feature	Description
Platform Features	
FTDv for HyperFlex and Nutanix.	We introduced FTDv for Cisco HyperFlex and Nutanix Enterprise Cloud.
FTDv for VMware vSphere/VMware ESXi 7.0.	You can now deploy FTDv on VMware vSphere/VMware ESXi 7.0. Note that Version 7.0 also discontinues support for VMware 6.0. Upgrade the hosting environment to a supported version before you upgrade the FTD.
New default password for the 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 (**Advanced Details** > **User Data**) during the initial deployment.
ISA 3000 support for shutting down.	In Version 7.0.2+, you can shut down the ISA 3000; previously, you could only reboot the device. In Version 7.0.5+, when you shut down the ISA 3000, the System LED turns off. Wait at least 10 seconds after that before you remove power from the device. **Note** Version 7.1 temporarily deprecates support for this feature. Support returns in Version 7.2.
Firewall and IPS Features	
New Section 0 for system-defined NAT rules.	A new Section 0 has been added to the NAT rule table. This section is exclusively for the use of the system. Any NAT rules that the system needs for normal functioning are added to this section, and these rules take priority over any rules you create. Previously, system-defined rules were added to Section 1, and user-defined rules could interfere with proper system functioning. You cannot add, edit, or delete Section 0 rules, but you will see them in **show nat detail** command output.
Custom intrusion rules for Snort 3.	You can use offline tools to create custom intrusion rules for use with Snort 3, and upload them into an intrusion policy. You can organize custom rules in your own custom rule groups, to make it easy to update them as needed. You can also create the rules directly in 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. We added support for custom groups and rules to the **Policies** > **Intrusion** page, when you edit an intrusion policy.

Feature	Description
Snort 3 new features for FDM-managed systems.	You can now configure the following additional features when using Snort 3 as the inspection engine on an FDM-managed system: • Time-based access control rules. (FTD API only.) • Multiple virtual routers. • The decryption of TLS 1.1 or lower connections using the SSL Decryption policy. • The decryption of the following protocols using the SSL Decryption policy: FTPS, SMTPS, IMAPS, POP3S.
DNS request filtering based on URL category and reputation.	You can apply your URL filtering category and reputation rules to DNS lookup requests. If the fully-qualified domain name (FQDN) in the lookup request has a category and reputation that you are blocking, the system blocks the DNS reply. Because the user does not receive a DNS resolution, the user cannot complete the connection. Use this option to apply URL category and reputation filtering to non-web traffic. You must have the URL filtering license to use this feature. We added the **Reputation Enforcement on DNS Traffic** option to the access control policy settings.
VPN Features	
FDM SSL cipher settings for remote access VPN.	You can define the TLS versions and encryption ciphers to use for remote access VPN connections in FDM. Previously, you needed to use the Firepower Threat Defense API to configure SSL settings. We added the following pages: **Objects** > **SSL Ciphers**; **Device** > **System Settings** > **SSL Settings**.
Support for Diffie-Hellman group 31.	You can now use Diffie-Hellman (DH) group 31 in IKEv2 proposals and policies.
The maximum number of Virtual Tunnel Interfaces on the device is 1024.	The maximum number of Virtual Tunnel Interfaces (VTI) that you can create is 1024. In previous versions, the maximum was 100 per source interface.
IPsec lifetime settings for site-to-site VPN security associations.	You can change the default settings for how long a security association is maintained before it must be re-negotiated. We added the **Lifetime Duration** and **Lifetime Size** options to the site-to-site VPN wizard.
Routing Features	
Virtual router support for the ISA 3000.	You can configure up to 10 virtual routers on an ISA 3000 device.

Feature	Description
Equal-Cost Multi-Path (ECMP) routing.	You can configure ECMP traffic zones to contain multiple interfaces, which lets traffic from an existing connection exit or enter the Firepower Threat Defense device on any interface within the zone. This capability allows Equal-Cost Multi-Path (ECMP) routing on the Firepower Threat Defense device as well as external load balancing of traffic to the Firepower Threat Defense device across multiple interfaces. ECMP traffic zones are used for routing only. They are not the same as security zones. We added the **ECMP Traffic Zones** tab to the Routing pages. In the Firepower Threat Defense API, we added the ECMPZones resources.
Interface Features	
New default inside IP address.	The default IP address for the inside interface is being changed to **192.168.95.1** from 192.168.1.1 to avoid an IP address conflict when an address on 192.168.1.0/24 is assigned to the outside interface using DHCP.
Default outside IP address now has IPv6 autoconfiguration enabled; new default IPv6 DNS server for Management.	The default configuration on the outside interface now includes IPv6 autoconfiguration, in addition to the IPv4 DHCP client. The default Management DNS servers now also include an IPv6 server: 2620:119:35::35.
EtherChannel support for the ISA 3000.	You can now use FDM to configure EtherChannels on the ISA 3000. New/Modified screens: **Devices** > **Interfaces** > **EtherChannels**
Licensing Features	
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.
Administrative and Troubleshooting Features	

Feature	Description
DHCP relay configuration using the Firepower Threat Defense API.	**Upgrade impact. Can prevent post-upgrade deploy.** You can use the Firepower Threat Defense API to configure DHCP relay. Using DHCP relay on an interface, you can direct DHCP requests to a DHCP server that is accessible through the other interface. You can configure DHCP relay on physical interfaces, subinterfaces, EtherChannels, and VLAN interfaces. You cannot configure DHCP relay if you configure a DHCP server on any interface. Note that if you used FlexConfig in prior releases to configure DHCP relay (the **dhcprelay** command), you must re-do the configuration using the API, and delete the FlexConfig object, after you upgrade. We added the following model to the Firepower Threat Defense API: dhcprelayservices
Faster bootstrap processing and early login to FDM.	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.
Improved CPU usage and performance for many-to-one and one-to-many connections.	The system no longer creates local host objects and locks them when creating connections, except for connections that involve dynamic NAT/PAT and scanning threat detection and host statistics. This improves performance and CPU usage in situations where many connections are going to the same server (such as a load balancer or web server), or one endpoint is making connections to many remote hosts. We changed the following commands: **clear local-host** (deprecated), **show local-host**
Upgrade readiness check for FDM-managed devices.	You can run an upgrade readiness check on an uploaded Firepower Threat Defense upgrade package before attempting to install it. The readiness check verifies that the upgrade is valid for the system, and that the system meets other requirements needed to install the package. Running an upgrade readiness check helps you avoid failed installations. A link to run the upgrade readiness check was added to the **System Upgrade** section of the **Device** > **Updates** page.

Feature	Description
Automatically update CA bundles.	**Upgrade impact.** The 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. **Note** This feature is not supported in Version 7.0.0–7.0.4, 7.1.0–7.1.0.2, or 7.2.0–7.2.3. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco. New/modified CLI commands: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** For more information, see the Cisco Secure Firewall Threat Defense Command Reference. Minimum FTD: 7.0.5.
FTD REST API version 6.1 (v6).	The Firepower Threat Defense REST API for software version 7.0 is version 6.1 You can use v6 in the API URLs, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. Note that the URL version path element for 6.1 is the same as 6.0: v6. Please re-evaluate all existing calls, as changes might have been mode to the resource models you are using. To open the API Explorer, where you can view the resources, log into FDM, then click the more options button ( ) and choose **API Explorer**.

Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

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

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

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

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

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

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.

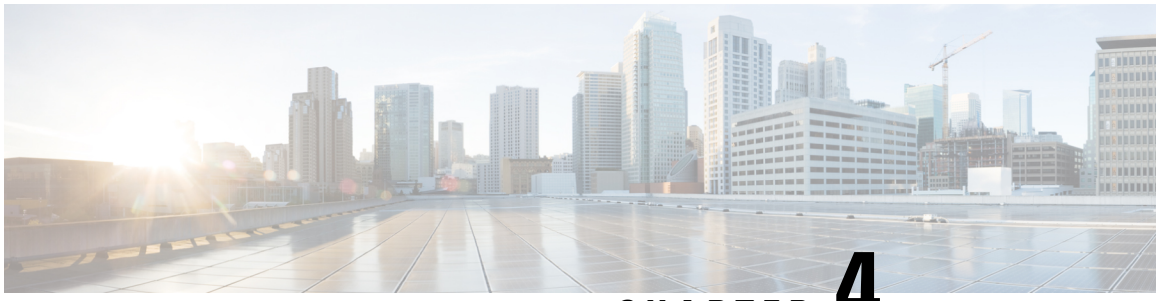
Caution In most cases, your existing FlexConfig configurations continue to work post-upgrade and you can still deploy. However, in some cases, using deprecated commands can cause deployment issues.

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

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 14: Upgrade Planning Phases

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

Planning Phase	Includes
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.
Associated Upgrades	Upgrade virtual hosting in virtual deployments. Upgrade firmware on the Firepower 4100/9300. Upgrade FXOS on the Firepower 4100/9300. Upgrade ASA for ASA FirePOWER.
Final Checks	Check configurations. Check NTP synchronization. Deploy configurations. Run readiness checks. Check disk space. Check running tasks. Check deployment health and communications.

Minimum Version to Upgrade

Minimum Version to Upgrade

You can upgrade directly to Version 7.0, including maintenance releases, as follows.

Table 15: 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 Cisco Firepower 4100/9300 FXOS Release Notes, 2.10(1).
ASA with FirePOWER Services	6.4 See Device Platforms, on page 6 for ASA requirements for your model. Although there is wide compatibility between ASA and ASA FirePOWER versions, upgrading allows you to take advantage of new features and resolved issues. To help you decide, see the Cisco Secure Firewall ASA Release Notes.
NGIPSv	6.4

Minimum Version to Patch

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

Guidelines for Cloud-delivered Firewall Management Center

You do not upgrade the cloud-delivered Firewall Management Center. It does not have a version and we take care of feature updates.

Upgrading FTD with Cloud-delivered Firewall Management Center

To upgrade FTD with the cloud-delivered Firewall Management Center, use the *latest released version* of the Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center.

Note The cloud-delivered Firewall Management Center cannot manage FTD Version 7.1. You cannot upgrade a cloud-managed device from Version 7.0 to Version 7.1 unless you unregister and disable cloud management. We recommend you upgrade the device directly to Version 7.2+.

Upgrading Co-Managed Devices

Customer-deployed FMCs running Version 7.2+ can co-manage cloud-managed FTD devices, but for event logging and analytics purposes only. You must use the cloud-delivered Firewall Management Center to manage and configure all other aspects of FTD, including upgrade.

Remember, a customer-deployed FMC must run the *same or newer* version as its managed devices—and this includes devices co-managed by the cloud-delivered Firewall Management Center. That is, you cannot use the cloud-delivered Firewall Management Center to upgrade a co-managed device past its customer-deployed FMC.

For example, consider a threat defense device with two managers:

- Device, running Version A.
- Customer-deployed FMC, running Version B.
- Cloud-delivered Firewall Management Center, no version.

In this scenario, you can use the cloud-delivered Firewall Management Center to upgrade the device to Version B (the same version as the co-manager), but not to Version C (past the co-manager).

Upgrade Guidelines for Version 7.0

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

Table 16: Upgrade Guidelines for FTD with FMC Version 7.0

✓	Guideline	Platforms	Upgrading From	Directly To
	Cisco Secure Firewall Management Center New Features by Release, for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	Open and Resolved Bugs, on page 75, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	Minimum Version to Upgrade, on page 42	Any	Any	Any
	Upgrade Guidelines for FXOS, on page 54	Firepower 4100/9300	Any	Any
	Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0, on page 45	Any	7.0.4+	7.1.0 only
	Reconnect with Cisco Threat Grid for High Availability FMCs, on page 46	FMC	6.4.0 through 6.7.x	7.0+
	Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 46	Firepower 1010	6.4.0 through 6.6.x	6.7+
	FMCv Requires 28 GB RAM for Upgrade, on page 46	FMCv	6.2.3 through 6.5.0.x	6.6+
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 47	Firepower 1000 series	6.4.0.x	6.5+

✓	Guideline	Platforms	Upgrading From	Directly To
	New URL Categories and Reputations, on page 48	Any	6.2.3 through 6.4.0.x	6.5+

Table 17: Upgrade Guidelines for FTD with FDM Version 7.0

✓	Guideline	Platforms	Upgrading From	Directly To
	Cisco Secure Firewall Device Manager New Features by Release, for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	Open and Resolved Bugs, on page 75, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	Minimum Version to Upgrade, on page 42	Any	Any	Any
	Upgrade Guidelines for FXOS, on page 54	Firepower 4100/9300	Any	Any
	Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0, on page 45	Any	7.0.4+	7.1.0 only
	Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 46	Firepower 1010	6.4.0 through 6.6.x	6.7+
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 47	Firepower 1000 series	6.4.0.x	6.5+
	Historical Data Removed During FTD Upgrade with FDM, on page 47	Any	6.2.3 through 6.4.0.x	6.5+
	New URL Categories and Reputations, on page 48	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 18: 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: • **From** c3.xlarge **to** c3.4xlarge. • **From** c3.2.xlarge **to** c3.4xlarge. • **From** c4.xlarge **to** c4.4xlarge. • **From** c4.2xlarge **to** c4.4xlarge. We also offer a c5.4xlarge instance for new deployments.	Stop the instance before you resize. Note that when you do this, data on the instance store volume is lost, so migrate your instance store-backed instance first. Additionally, if your management interface does not have an Elastic IP address, its public IP address is released. For instructions, see the documentation on changing your instance type in the AWS user guide for Linux instances.
Azure	Resize instances: • **From** Standard_D3_v2 **to** Standard_D4_v2.	Use the Azure portal or PowerShell. You do not need to stop the instance before you resize, but stopping may reveal additional sizes. Resizing restarts a running virtual machine. For instructions, see the Azure documentation on resizing a Windows VM.

Firepower 1000 Series Devices Require Post-Upgrade Power Cycle

Deployments: Firepower 1000 series

Upgrading from: Version 6.4.0.x

Directly to: Version 6.5.0+

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

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

Historical Data Removed During 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 19: Deployment Changes on Upgrade

Change	Details
Modifies URL rule categories.	The upgrade modifies URL rules to use the nearest equivalents in the new category set, in the following policies: • Access control • SSL • QoS (FMC only) • Correlation (FMC only) These changes may create redundant or preempted rules, which can slow performance. If your configuration includes merged categories, you may experience minor changes to the URLs that are allowed or blocked.

Change	Details
Renames URL rule reputations.	The upgrade modifies URL rules to use the new reputation names: **1.** Untrusted (was *High Risk*) **2.** Questionable (was *Suspicious sites*) **3.** Neutral (was *Benign sites with security risks*) **4.** Favorable (was *Benign sites*) **5.** Trusted (was *Well Known*)
Clears the URL cache.	The upgrade clears the URL cache, which contains results that the system previously looked up in the cloud. Your users may temporarily experience slightly longer access times for URLs that are not in the local data set.
Labels 'legacy' events.	For already-logged events, the upgrade labels any associated URL category and reputation information as `Legacy`. These legacy events will age out of the database over time.

Pre-Upgrade Actions for URL Categories and Reputations

Before upgrade, take the following actions.

Table 20: Pre-Upgrade Actions

Action	Details
Make sure your appliances can reach Talos resources.	The system must be able to communicate with the following Cisco resources after the upgrade: • https://regsvc.sco.cisco.com/ — Registration • https://est.sco.cisco.com/ — Obtain certificates for secure communications • https://updates-talos.sco.cisco.com/ — Obtain client/server manifests • http://updates.ironport.com/ — Download database (note: uses port 80) • https://v3.sds.cisco.com/ — Cloud queries The cloud query service also uses the following IP address blocks: • IPv4 cloud queries: • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 • IPv6 cloud queries: • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
Identify potential rule issues.	Understand the upcoming changes. Examine your current URL filtering configuration and determine what post-upgrade actions you will need to take (see the next section). **Note** You may want to modify URL rules that use deprecated categories now. Otherwise, rules that use them will prevent deploy after the upgrade. In FMC deployments, we recommend you generate an *access control policy report*, which provides details on the policy's current saved configuration, including access control rules and rules in subordinate policies (such as SSL). For each URL rule, you can see the current categories, reputations, and associated rule actions. On the FMC, choose **Policies** > **Access Control**, then click the report icon () next to the appropriate policy.

Post-Upgrade Actions for URL Categories and Reputations

After upgrade, you should reexamine your URL filtering configuration and take the following actions as soon as possible. Depending on deployment type and the changes made by the upgrade, some — but not all —

issues may be marked in the GUI. For example, in access control policies on FMC/FDM, you can click **Show Warnings** (FMC) or **Show Problem Rules** (FDM).

Table 21: Post-Upgrade Actions

Action	Details
Remove **deprecated categories** from rules. Required.	The upgrade does not modify URL rules that use deprecated categories. Rules that use them will prevent deploy. On the FMC, these rules are marked.
Create or modify rules to include the **new categories**.	Most of the new categories identify threats. We strongly recommend you use them. On the FMC, these new categories are not marked after *this* upgrade, but Talos may add additional categories in the future. When that happens, new categories are marked.
Evaluate rules changed as a result of **merged categories**.	Each rule that included any of the affected categories now include all of the affected categories. If the original categories were associated with different reputations, the new rule is associated with the broader, more inclusive reputation. To filter URLs as before, you may have to modify or delete some configurations; see Guidelines for Rules with Merged URL Categories, on page 51. Depending on what changed and how your platform handles rule warnings, changes may be marked. For example, the FMC marks wholly redundant and wholly preempted rules, but not rules that have partial overlap.
Evaluate rules changed as a result of **split categories**.	The upgrade replaces each old, single category in URL rules with *all* the new categories that map to the old one. This will not change the way you filter URLs, but you can modify affected rules to take advantage of the new granularity. These changes are not marked.
Understand which categories were **renamed** or are **unchanged**.	Although no action is required, you should be aware of these changes. These changes are not marked.
Evaluate how you handle **uncategorized** and **reputationless** URLs.	Even though it is now possible to have uncategorized and reputationless URLs, you cannot still cannot filter uncategorized URLs by reputation, nor can you filter reputationless URLs. Make sure that rules that filter by the **Uncategorized** category, or by **Any** reputation, will behave as you expect.

Guidelines for Rules with Merged URL Categories

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

Table 22: Guidelines for Rules with Merged URL Categories

Guideline	Details
Rule Order Determines Which Rule Matches Traffic	When considering rules that include the same category, remember that traffic matches the first rule in the list that includes the condition.
Categories in the Same Rule vs Categories in Different Rules	Merging categories in a single rule will merge into a single category in the rule. For example, if Category A and Category B are merging to become Category AB, and you have a rule with both Category A and Category B, then after merge the rule will have a single Category AB. Merging categories in different rules will result in separate rules with the same category in each rule after the merge. For example, if Category A and Category B are merging to become Category AB, and you have Rule 1 with Category A and Rule 2 with Category B, then after merge Rule 1 and Rule 2 will each include Category AB. How you choose to resolve this situation depends on the rule order, on the actions and reputation levels associated with the rules, on the other URL categories included in the rule, and on the non-URL conditions that are included in the rule.
Associated Action	If merged categories in different rules were associated with different actions, then after merge you may have two or more rules with different actions for the same category.
Associated Reputation Level	If a single rule includes categories that were associated with different reputation levels before merging, the merged category will be associated with the more inclusive reputation level. For example, if Category A was associated in a particular rule with **Any reputation** and Category B was associated in the same rule with reputation level **3 - Benign sites with security risks**, then after merge Category AB in that rule will be associated with **Any reputation**.
Duplicate and Redundant Categories and Rules	After merge, different rules may have the same category associated with different actions and reputation levels. Redundant rules may not be exact duplicates, but they may no longer match traffic if another rule earlier in the rule order matches instead. For example, if you have pre-merge Rule 1 with Category A that applies to Any Reputation, and Rule 2 with Category B that applies only to Reputation 1-3, then after merge, both Rule 1 and Rule 2 will have Category AB, but Rule 2 will never match if Rule 1 is higher in the rule order. On the FMC, rules with an identical category and reputation will show a warning. However, these warnings will not indicate rules that include the same category but a different reputation. Caution: Consider all conditions in the rule when determining how to resolve duplicate or redundant categories.
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 23: 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.

We also recommend the latest firmware; see the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.

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 57.

Unresponsive Upgrades

Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down during upgrade. You could place the system in an unusable state and require a reimage.

Unresponsive FMC or Classic Device Upgrade

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

Unresponsive FTD Upgrade

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

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

You can also use the FTD CLI.

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

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

Revert or Uninstall the Upgrade

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

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

  See System Management in the FDM configuration guide.

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

  See Uninstall a Patch in the FMC upgrade guide, or Uninstall ASA FirePOWER Patches with ASDM, on page 55 in these release notes.

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

Uninstall ASA FirePOWER Patches with ASDM

Use the Linux shell (*expert mode*) to uninstall device patches. You must have access to the device shell as the `admin` user for the device, or as another local user with CLI configuration access. If you disabled shell access, contact Cisco TAC to reverse the lockdown.

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

Table 24: Uninstall Order for ASA with FirePOWER Services in ASA Failover Pairs/Clusters

Configuration	Uninstall Order
ASA active/standby failover pair, with ASA FirePOWER	Always uninstall from the standby. **1.** Uninstall from the ASA FirePOWER module on the standby ASA device. **2.** Fail over. **3.** Uninstall from the ASA FirePOWER module on the new standby ASA device.

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

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

Before you begin

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

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

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

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

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

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

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

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

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

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

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

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

Step 6 Monitor the uninstall until you are logged out.

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

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

Otherwise, monitor progress in the console or terminal.

Step 7 Verify uninstall success.

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

Step 8 Redeploy configurations.

What to do next

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

Traffic Flow and Inspection

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

Traffic Flow and Inspection for 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 25: Traffic Flow and Inspection: FXOS Upgrades

FTD Deployment	Traffic Behavior	Method
Standalone	Dropped.	—

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

Traffic Flow and Inspection for FTD Upgrades with FMC

Software Upgrades for Standalone Devices

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

Table 26: 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.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force**	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby**	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: **Bypass: Disabled**	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability/Scalability

You should not experience interruptions in traffic flow or inspection while upgrading high availability or clustered devices. For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.

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

Software Uninstall (Patches)

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

Deploying Configuration Changes

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

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

Table 27: Traffic Flow and Inspection: Deploying Configuration Changes

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

Traffic Flow and Inspection for FTD Upgrades with FDM

Software Upgrades

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

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

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 28: Traffic Flow and Inspection: ASA FirePOWER Upgrades

Traffic Redirection Policy	Traffic Behavior
Fail open (**sfr fail-open**)	Passed without inspection
Fail closed (**sfr fail-close**)	Dropped
Monitor only (**sfr {fail-close}|{fail-open} monitor-only**)	Egress packet immediately, copy not inspected

Software Uninstall (Patches)

Interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In ASA failover/cluster deployments, you must explicitly plan an uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.

Deploying Configuration Changes

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

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

Traffic Flow and Inspection for NGIPSv Upgrades with FMC

Software Upgrades

Interface configurations determine how NGIPSv handles traffic during the upgrade.

Table 29: 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 30: Traffic Flow and Inspection: Deploying Configuration Changes

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

Time and Disk Space Tests

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

Time Tests

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

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot 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 54.

Table 31: 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.

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

Disk Space Tests

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

We also report the space needed on the FMC (in either /Volume or /var) for the device upgrade package. If you 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 32: Checking Disk Space

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

Time and Disk Space for Version 7.0.5.1

Time and disk space test reports are not available for this limited release.

Time and Disk Space for Version 7.0.5

Table 33: 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 MBin /	—	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
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 34: 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 35: 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

Platform		Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
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 36: 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
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

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
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 37: 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			
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 38: 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 39: 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
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

Platform		Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
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

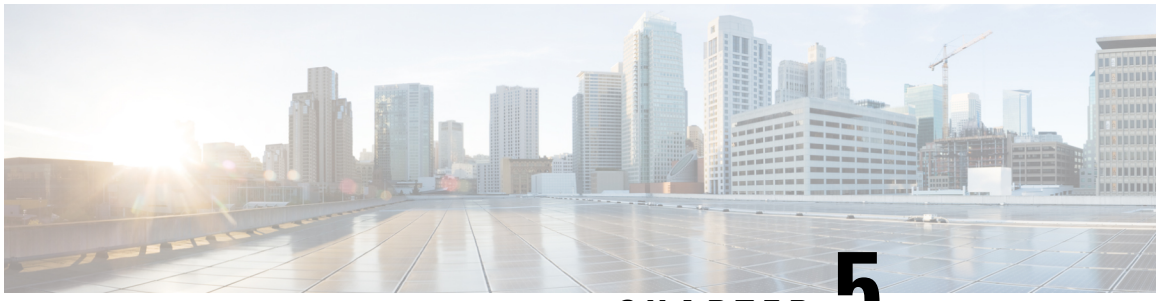
Table 40: Time and Disk Space for Version 7.0.0.1

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

Installation Guidelines

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 able to access the FMC's management interface without traversing the device.

Unregistering from Smart Software Manager

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

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

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

Table 42: Scenarios for Unregistering from CSSM (Not Restoring from Backup)

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

Removing Devices from the FMC

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

Table 43: Scenarios for Removing Devices from the FMC (Not Restoring from Backup)

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

Fully Reimaging FTD Hardware to Downgrade FXOS

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

Table 44: Scenarios for Full Reimages

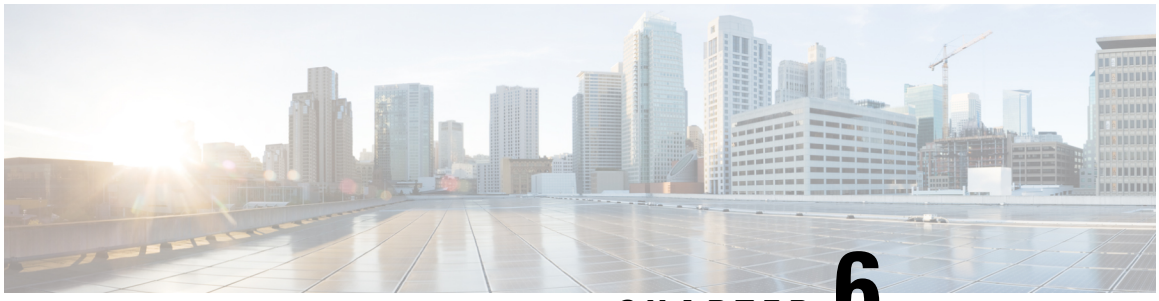
Model	Details
Firepower 1000 series Firepower 2100 series	If you use the **erase configuration** method to reimage, FXOS may not downgrade along with the software. This can cause failures, especially in high availability deployments. We recommend that you perform full reimages of these devices.
Firepower 4100/9300	Reverting 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 45: Installation Guides

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

Platform	Guide
ISA 3000	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide
FTDv	Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
ASA FirePOWER/NGIPSv	
ASA FirePOWER	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware



CHAPTER 6

Open and Resolved Bugs

This document lists open and resolved bugs for Version 7.0 devices and customer-deployed management centers.

For cloud-delivered Firewall Management Center bugs, see the Cisco Cloud-Delivered Firewall Management Center Release Notes.

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

Open Bugs

Open Bugs in Version 7.0.0

Table last updated: 2022-11-02

Table 46: Open Bugs in Version 7.0.0

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

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

Resolved Bugs

Resolved Bugs in Version 7.0.5.1

Table last updated: 2022-04-26

Table 47: Resolved Bugs in Version 7.0.5.1

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

Resolved Bugs in Version 7.0.5

Table last updated: 2022-11-17

Table 48: Resolved Bugs in Version 7.0.5

Bug ID	Headline
CSCvo17612	Return error messages when failing to retrieve objects from database
CSCvq70838	Traceback in the output of tail-logs command
CSCvr06065	Snort core due to DAQ IOQ Corruption
CSCvw82067	ASA/FTD 9344 blocks depleted due to high volume of fragmented traffic
CSCvw90399	FMC HA issues with too many open file descriptors for sfipproxy UDP conn
CSCvx24207	FQDN Object Containing IPv4 and IPv6 Addresses Only Install IPv6 Entries
CSCvx68586	Not able to login to UI/SSH on FMC, console login doesn't prompt for password
CSCvx75743	Inconsistent FMC audit log severity
CSCvx86569	Access Control Rule - Comment disappears if clicked to another tab before saving the comment.
CSCvy24180	Default variable set missing on FMC
CSCvy38070	File/Malware Event Report fails when date is x-axis and count y-axis for table chart
CSCvy38650	Unable to download captured file from FMC Captured files UI
CSCvy45048	Subsystem query parameter not filtering records for "auditrecords" restapi
CSCvy47927	Unable to select multiple policies for scheduled firepower recommended rules
CSCvy50598	BGP table not removing connected route when interface goes down

Bug ID	Headline
CSCvy63463	Error deleting users due to special characters
CSCvy65178	Need dedicated Rx rings for to the box BGP traffic on Firepower platform
CSCvy67765	FTD VTI reports TUNNEL_SRC_IS_UP false despite source interface is up/up and working
CSCvy68974	ActionQueue process is killed by OOM killer due to process utilizing more than 3 GB limit for memory
CSCvy73130	FP4100 platform: Active-Standby changed to dual Active after running "show conn" command
CSCvy75131	Occasionally deleted sensor/interfaces are not removed from security zones
CSCvy93607	Health monitor alert indicates QP HA in split brain when one device reboots and re-joins
CSCvy95520	Cisco Firepower Management Center and Firepower Threat Defense Software SSH DoS Vulnerability
CSCvy95809	Crashinfo script is invoked on SFR running snort2 and device fails to upgrade to 7.0
CSCvz07004	SNORT2: FTD is performing Full proxy even when SSL rule has DND action.
CSCvz09106	Cisco ASA and FTD Software SSL VPN Denial of Service Vulnerability
CSCvz13564	Firepower 2100 FTD: ssh-access-list configuration are lost after upgrading
CSCvz19364	FXOS does not send any syslog messages when the duplex changes to "Half Duplex"
CSCvz31184	Validation of unsupported flow-offload using pre-filter in passive/inline interfaces in FPR4100/9300
CSCvz32593	FPR4110 and FPR4115 in disabled state CD App Sync error is Rsync is not enabled on active device
CSCvz35669	KP-2110 Standby disabled upgrade 6.6.4-64 to 7.0.1-30 "CD App Sync error is App Config Apply Failed"
CSCvz36903	ASA traceback and reload while allocating a new block for cluster keepalive packet
CSCvz40542	FMC : Remote Storage Device's SMB share password does not make it when upgrading from 6.6 to 7
CSCvz40765	FMC CPU graph displays the wrong number of Snort and System cores
CSCvz42823	Bulk Operation of AC Policy REST API taking time
CSCvz43325	Active FMC not deregistering sensors after breaking HA
CSCvz49163	Observed some time drift in seconds in the output when we execute show rule hits multiple times

Bug ID	Headline
CSCvz52785	Management interface flaps every 13mins post upgrade from 9.12 to 9.14.2.15
CSCvz57917	High unmanaged disk usage on /ngfw filled with module-xxxx-x86_64.tgz files in packages folder
CSCvz60142	ASA/FTD stops serving SSL connections
CSCvz61456	Software upgrade on ASA application may failure without obvious reasons
CSCvz61463	FP9k SM-44 High CPU on radware vdp Cores after upgrade
CSCvz62517	SRU install should validate files upon completion
CSCvz68713	PLR license reservation for ASAv5 is requesting ASAv10
CSCvz69729	Unstable client processes may cause LINA zmqio traceback on FTD
CSCvz71596	"Number of interfaces on Active and Standby are not consistent" should trigger warning syslog
CSCvz77050	Occasionally policy deployment failure are reported as successful
CSCvz78331	SNMP polling fails after a re-image
CSCvz84733	LACP packets through inline-set are silently dropped
CSCvz85234	Facilities ALERT, AUDIT, CLOCK and KERN do not work in sending Audit Log to syslog from FMC.
CSCvz94841	Grammatical errors in failover operating mode mismatch error message
CSCwa03341	Standby's sub interface mac doesn't revert to old mac with no mac-address command
CSCwa06608	WM 1010 HA Failover is not successful when we give failover active in secondary.
CSCwa07390	Config only FMC: SI feed downloaded file does not match expected checksum
CSCwa15093	Access Policy Control Clear Hit Count throwing Error 403: Forbidden
CSCwa16626	Syslog over TLS accepting wildcard in middle of FQDN
CSCwa33248	Auto LSP update not getting triggered, missing Talos registration (beakerd)
CSCwa36535	Standby unit failed to join failover due to large config size.
CSCwa38996	Big number of repetitive messages in snmpd.log leading to huge log size
CSCwa41936	Cisco FTD Bleichenbacher Attack Vulnerability
CSCwa42596	ASA with SNMPv3 configuration observes unexpected reloads with snmpd cores
CSCwa43311	Snort blocking and dropping packet, with bigger size(1G) file download
CSCwa47737	ASA/FTD may hit a watchdog traceback related to snmp config writing

Bug ID	Headline
CSCwa49480	SNMP OID , stop working after around one hour and a half - FTD
CSCwa55142	SNORT3 / SSL / Definitive DND verdict when there's an extra DND bottom rule, instead of regular DND
CSCwa59907	LINA observed traceback on thread name "snmp_client_callback_thread"
CSCwa61361	ASAv traceback when SD_WAN ACL enabled, then disabled (or vice-versa) in PBR
CSCwa62025	IPv6: Some of egress interfaces of global and user vrf routes are missing in asp table
CSCwa64739	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwa68552	All type-8 passwords are lost upon upgrade from ASA 9.12-9.15 to 9.16, failover gets disabled
CSCwa72528	username form cert feature does not work with SER option
CSCwa72530	FTD: Time gap/mismatch seen when new node joins a Cluster Control node under history
CSCwa72641	URL incorrectly extracted for TLS v1.2 self signed URLs when "Early application detection" enabled
CSCwa72929	SNMPv3 polling may fail using privacy algorithms AES192/AES256
CSCwa73172	ASA reload and traceback in Thread Name: PIX Garbage Collector
CSCwa75966	ASA: Reload and Traceback in Thread Name: Unicorn Proxy Thread with Page fault: Address not mapped
CSCwa77083	Host information is missing when Security Zones are configured in Network Discovery rules
CSCwa78082	FMC intrusion event search produces inconsistent results
CSCwa80040	FMC NFS configuration failling after upgrade from 6.4.0.4 to 7.0.1
CSCwa81143	Unable to save the application policy filter. Save tab is stuck and its continuously loading.
CSCwa85492	URL lookup responding with two categories
CSCwa85709	Cisco Firepower Management Center Information Disclosure Vulnerability
CSCwa87298	ASA conn data-rate: incorrect "current rate" and "data-rate-filter" doesn't work properly
CSCwa89347	Cannot add object to network group on FMC
CSCwa90735	FTD/FXOS - ASAconsole.log files fail to rotate causing excessive disk space used in /ngfw
CSCwa91070	Cgroup triggering oom-k for backup process

Bug ID	Headline
CSCwa92596	Access Control File policy rule message is misleading and unnecessary
CSCwa92822	TLS client in the sftunnel TLS tunnel offers curves in CC mode that are not allowed by CC
CSCwa92883	Deployment Failed at phase-2 with domain snapshot error
CSCwa93499	Cisco Firepower Management Center Stored Cross-Site Scripting Vulnerability
CSCwa95079	ASA/FTD Traceback and reload due to NAT configuration
CSCwa97541	Cisco ASA FirePOWER Module, FMC and NGIPS SNMP Default Credential Vulnerability
CSCwa97917	ISA3000 in boot loop after powercycle
CSCwa98853	Error F0854 FDM Keyring's RSA modulus is invalid
CSCwa98983	Upgrade failed on FPR2100-HA at 800_post/901_reapply_sensor_policy.pl
CSCwa99171	Chassis and application sets the time to Jan 1, 2010 after reboot
CSCwa99931	ASA/FTD: Tuning of update_mem_reference process
CSCwa99932	ASA/FTD stuck after crash and reboot
CSCwb00749	FMC upgrade failure: 114_DB_table_data_integrity_check.pl failed
CSCwb01983	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb01990	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb01995	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb02006	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb02018	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb02026	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb02060	snmp-group host with Invalid host range and subnet causing traceback and reload
CSCwb03704	ASA/FTD datapath threads may run into deadlock and generate traceback
CSCwb04000	ASA/FTD: DF bit is being set on packets routed into VTI
CSCwb05148	Cisco ASA Software and FTD Software SNMP Denial of Service Vulnerability
CSCwb05291	Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability
CSCwb05920	Crash in KP at webVpn free, HTTPCleanUp and mem_mh_free from Scaled AC-IK/IPSec TVM test.
CSCwb06273	Continuous memory leak in the process hmlsd (SF::Messaging::smartSend)

Bug ID	Headline
CSCwb06847	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-9-11543'
CSCwb07908	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
CSCwb07981	Traceback: Standby FTD reboots and generates crashinfo and lina core on thread name cli_xml_server
CSCwb08644	ASA/FTD traceback and reload at IKEv2 from Scaled S2S+AC-DTLS+SNMP long duration test
CSCwb08773	FPR2130 LED is off when power supply module 1 is back
CSCwb08828	FP1010 Switchport access vlan interface in up/up status but not passing traffic
CSCwb12730	Policy deployment failed in FMC however FTD deployment status shows "INPROGRESS"
CSCwb16037	Unable to replace the anyconnect image when maximum memory used for anyconnect images.
CSCwb16663	Unable to configure NAP under Advanced Tab in AC policy
CSCwb16920	CPU profile cannot be reactivated even if previously active memory tracking is disabled
CSCwb17187	SNMP cores are generated every minute while running snmpwalk on HA
CSCwb17963	Unable to identify dynamic rate liming mechanism & not following msg limit per/sec at syslog server.
CSCwb19648	SNMP queries for crasLocalAddress are not returning the assigned IPs for SSL/DTLS tunnels.
CSCwb22592	SSH Functionalty stopped working after running long duration tests of SCP + Scaled TVM VPN Profiles
CSCwb23029	Cisco Firepower Management Center Software Command Injection Vulnerability
CSCwb23048	Cisco Firepower Management Center Software Command Injection Vulnerability
CSCwb24039	ASA traceback and reload on routing
CSCwb25809	Single Pass - Traceback due to stale ifc
CSCwb28123	FTD HA deployment fails with error "Deployment failed due to major version change on device"
CSCwb29126	Cannot use underscore (_) in FMC's realm AD Primary Domain configuration
CSCwb31551	When inbound packet contains SGT header, FPR2100 cannot distribute properly per 5 tuple
CSCwb31699	Primary takes active role after reload

Bug ID	Headline
CSCwb32267	Crash on KP Active node while clearing vpnsessiondb with AnyConnect-SSL TVM Profile running
CSCwb32418	Cisco FirePOWER Software for ASA FirePOWER Module Command Injection Vulnerability
CSCwb32841	NAT (any,any) statements in-states the failover interface and resulting on Split Brain events
CSCwb33184	Memory leak in MessageService causes UI slowness
CSCwb35675	Snort3 is partially in sync with Snort 2 warning alert
CSCwb37077	“show access-control-config” for DNS Reputation Enforcement does not work.
CSCwb37999	Customized Variables name cause Snort3 validation failure
CSCwb38406	GeoDB updates on multi-domain environment requires a manual policy deployment
CSCwb39431	FTD unified logs do not print the log as per rfc5424 standard
CSCwb40001	Long delays when executing SNMP commands
CSCwb41739	debug crypto conditional need to be made multi-ctx aware
CSCwb41854	Cisco FTD Software and Cisco FXOS Software Command Injection Vulnerability
CSCwb42978	ASA accepting invalid netmask in SSH/TELNET/HTTP/TFTP config
CSCwb43018	Implement SNP API to check ifc and ip belongs to HA LU or CMD interface
CSCwb43433	Jumbo frame performance has degraded up to -45% on Firepower 2100 series
CSCwb50405	ASA/FTD Traceback in crypto hash function
CSCwb51707	ASA Traceback and reload in process name: lina
CSCwb52401	Cisco Firepower Threat Defense Software Privilege Escalation Vulnerability
CSCwb53172	FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated
CSCwb53191	Certificate validation fails post upgrade to 9.17.1
CSCwb53328	ASA/FTD Traceback and reload caused by Smart Call Home process sch_dispatch_to_url
CSCwb53694	Cisco Firepower Management Center Software XML External Entity Injection Vulnerability
CSCwb54791	ASA DHCP server fails to bind reserved address to Linux devices
CSCwb56718	Policy deployment fails with error- Rule update is running but there are no updates in progress.

Bug ID	Headline
CSCwb56905	ASA blocking 0.0.0.0 IP and netmask combination in SSH/TELNET/HTTP config
CSCwb57524	FTD upgrade fails - not enough disk space from old FXOS bundles in distributables partition
CSCwb57615	Configuring pbr access-list with line number failed.
CSCwb59465	ASA/FTD may traceback (watchdog) and reload when generating a syslog from the VPN Failover subsystem
CSCwb59488	ASA/FTD Traceback in memory allocation failed
CSCwb59619	PM needs to restart the Disk Manager after creating ramdisk to make DM aware of the ramdisk
CSCwb60993	FDM Need to block the deployment when a Security zone object is not associated with an interface
CSCwb61901	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb61908	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb62059	Unable to login to FTD using external authentication after upgrade
CSCwb64620	CC mode is not properly enabled on NGIPSv impacting syslog over TLS and SSH
CSCwb65447	FTD: AAB cores are not complete and not decoding
CSCwb65718	FMC is stuck on loading SI objects page
CSCwb66761	Cisco Firepower Threat Defense Software Generic Routing Encapsulation DoS Vulnerability
CSCwb67040	FP4112|4115 Traceback & reload on Thread Name: netfs_thread_init
CSCwb68642	ASA traceback in Thread Name: SXP CORE
CSCwb68993	FTD/FDM: SSL connections to sites using RSA certs with 3072 bit keys may fail
CSCwb69503	ASA unable to configure aes128-gcm@openssh.com when FIPS enabled
CSCwb71460	ASA traceback in Thread Name: fover_parse and triggered by snmp related functions
CSCwb73248	FW traceback in timer infra / netflow timer
CSCwb74571	PBR not working on ASA routed mode with zone-members
CSCwb76129	Some SSL patterns not detected after VDB 356 or higher is installed
CSCwb76423	ASA crashes on fp2100 when checking CRL
CSCwb79812	RIP is advertising all connected Anyconnect users and not matching route-map for redistribution

Bug ID	Headline
CSCwb80108	FP2100/FP1000: Built-in RJ45 ports randomly not coming up after portmanager restart events
CSCwb80559	FTD offloads SGT tagged packets although it should not
CSCwb80862	ASA/FTD proxy arps any traffic when using the built-in 'any' object in translated destination
CSCwb82796	ASA/FTD firewall may traceback and reload when tearing down IKE tunnels
CSCwb83388	ASA HA Active/standby tracebacks seen approximately every two months.
CSCwb83691	ASA/FTD traceback and reload due to the initiated capture from FMC
CSCwb84901	CIAM: heimdal 1.0.1
CSCwb85633	Snmpwalk output of memory does not match show memory/show memory detail
CSCwb85822	Deployment failing when collecting policies.
CSCwb86118	TPK ASA: Device might get stuck on ftp copy to disk
CSCwb86565	FMC upgrade fails due Mismatch in number of entries between /etc/passwd and /etc/shadow
CSCwb87498	Lina traceback and reload during EIGRP route update processing.
CSCwb87950	Cisco ASA Software and FTD Software Web Services Interface Denial of Service Vulnerability
CSCwb88587	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb88651	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwb89187	Flex Config allow - "timeout icmp-error hh:mm:ss"
CSCwb90074	ASA: Multiple Context Mixed Mode SFR Redirection Validation
CSCwb90532	ASA/FTD traceback and reload on NAT related function nat_policy_find_location
CSCwb91101	SNMP interface threshold doesn't trigger properly when traffic sent to interface ~4gbps
CSCwb92376	FMC syslog-ng daemon fails to start if log facility is set to ALERT
CSCwb92709	We can't monitor the interface via "snmpwalk" once interface is removed from context.
CSCwb92937	Error 403: Forbidden when expanding in view group objects
CSCwb93932	ASA/FTD traceback and reload with timer services assertion
CSCwb94170	merovingian.log file extremly big size can fill the disk
CSCwb94190	ASA graceful shut down when applying ACL's with forward reference feature and FIPS enabled.

Bug ID	Headline
CSCwb94312	Unable to apply SSH settings to ASA version 9.16 or later
CSCwb95112	Intrusion Policy shows last modified by admin even though changes are made by a different user
CSCwb95787	FPR1010 - No ARP on switchport VLAN interface after portmanager DIED event
CSCwb97251	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCwc02488	ASA/FTD may traceback and reload in Thread Name 'None'
CSCwc02700	Fragmented packets are dropped when unit leaves cluster
CSCwc03069	Interface internal data0/0 is up/up from cli but up/down from SNMP polling
CSCwc03393	Lina traceback and core file size is beyond 40G and compression fails on FTD
CSCwc04959	Disk usage is 100% on secondary FMC .dmp files created utilized all the disk space
CSCwc05132	Unable to disable "Retrieve to Management Center
CSCwc06833	Deployment failure with ERROR Process Manager failed to verify LSP ICDB
CSCwc07262	Standby ASA goes to booting loop during configuration replication after upgrade to 9.16(3).
CSCwc08374	Azure ASA NIC MAC address for Gigeth 0/1 and 0/2 become out of order when adding interfaces
CSCwc09414	ASA/FTD may traceback and reload in Thread Name 'ci/console'
CSCwc10037	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwc10483	ASA/FTD - Traceback in Thread Name: appAgent_subscribe_nd_thread
CSCwc10792	ASA/FTD IPSEC debugs missing reason for change of peer address and timer delete
CSCwc11511	FTD: SNMP failures after upgrade to 7.0.2
CSCwc11597	ASA tracebacks after SFR was upgraded to 6.7.0.3
CSCwc11663	ASA traceback and reload when modifying DNS inspection policy via CSM or CLI
CSCwc13017	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
CSCwc13994	ASA - Restore not remove the new configuration for an interface setup after backup
CSCwc15530	Syslog facility "ALERT" should be changed on FDM since is not supported anymore by syslog-ng
CSCwc18285	Conn data-rate command can be enabled or disabled in unprivileged user EXEC mode
CSCwc18312	"show nat pool cluster" commands run within EEM scripts lead to traceback and reload

Bug ID	Headline
CSCwc18524	ASA/FTD Voltage information is missing in the command "show environment"
CSCwc23075	Upgrade to MariaDB 10.5.16 to get security vulnerability fixes
CSCwc23356	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-20-7695'
CSCwc23695	ASA/FTD can not parse UPN from SAN field of user's certificate
CSCwc24582	Update diskmanager to monitor deploy directories in /ngfw/var/cisco/deploy/db
CSCwc24906	ASA/FTD traceback and reload on Thread id: 1637
CSCwc25207	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 33)
CSCwc26406	FMC: Slowness in Device management page
CSCwc27236	FMC Health Monitoring JSON error
CSCwc27797	ASA mgmt ip cannot be released
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwc28532	9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwc28660	Snort3: NFSv3 mount may fail for traffic through FTD
CSCwc28806	ASA Traceback and Reload on process name Lina
CSCwc28854	Incorrect IF-MIB response when failover is configured on multiple contexts
CSCwc28928	ASA: SLA debugs not showing up on VTY sessions
CSCwc29591	Retrospective file disposition updates fail due to incorrect eventsecond values in fileevent tables
CSCwc30487	High unmanaged disk usage on Firepower 2110 device
CSCwc31163	FPR1010 upgrade failed - Error running script 200_pre/100_get_snort_from_dc.pl
CSCwc32246	NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used
CSCwc33036	Observed Logs at syslog server side as more than configured message limit per/sec.
CSCwc33076	JOBS_TABLE not getting purged due to foreign Key constraint violation in policy_diff_main
CSCwc33323	FMC 7.0 - Receiving alert "health monitor process: no events received yet" for multiple devices
CSCwc34818	The device is unregistered when Rest API calls script.

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

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

Bug ID	Headline
CSCwd09341	Multiple log files have zero bytes on the FMC
CSCwd24072	rsc_5_min.log store location should move to a different partition

Resolved Bugs in Version 7.0.4

Table last updated: 2022-08-10

Table 49: Resolved Bugs in Version 7.0.4

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

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

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

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

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

Bug ID	Headline
CSCwc23695	ASA/FTD can not parse UPN from SAN field of user's certificate
CSCwc24906	ASA/FTD traceback and reload on Thread id: 1637
CSCwc27797	ASA mgmt ip cannot be released
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwc28532	9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwc32246	NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used
CSCwc41590	Upgrade fail & App Instance fail to start with err "CSP_OP_ERROR. CSP signature verification error."
CSCwc53680	MonetDB crashing due to file size error (7.2.0-7.4.0)

Resolved Bugs in Version 7.0.3

Table last updated: 2022-06-30

Table 50: Resolved Bugs in Version 7.0.3

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

Resolved Bugs in Version 7.0.2.1

Table last updated: 2022-06-27

Table 51: Resolved Bugs in Version 7.0.2.1

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

Resolved Bugs in Version 7.0.2

Table last updated: 2022-05-05

Table 52: Resolved Bugs in Version 7.0.2

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Bug ID	Headline
CSCwa85138	Multiple issues with transactional commit diagnostics
CSCwa51241	Switch detected unknown MAC address from FPR1140 Management Interface
CSCwa03275	BGP routes shows unresolved and dropping packet with asp-drop reason "No route to host"
CSCvz73709	ASA/FTD Standby unit fails to join HA
CSCvz21886	Twice nat's un-nat not happening if nat matches a pbr acl that matches a port number instead of IP
CSCvy63464	FTD 1100/ 2100 series reboots with clock set to 2033
CSCvz19634	FTD software upgrade may fail at 200_pre/505_revert_prep.sh
CSCwa94894	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-4-9608'
CSCvx89451	ISA3000 shutdown command reboots system and does not shut system down.
CSCwa61218	Polling OID "1.3.6.1.4.1.9.9.171.1.3.2.1.2" gives negative index value of the associated tunnel
CSCvy02247	Cisco Firepower System Software Rule Editor Non-impactful Buffer Overflow Vulnerability
CSCvy99348	Shutdown command reboots instead of shutting the FP1k device down.
CSCvz71825	MAC algorithms on Firepower 2K devices are not correct for CC and UCAPL mode
CSCwa18858	ASA drops non DNS traffic with reason "label length 164 bytes exceeds protocol limit of 63 bytes"
CSCvz54471	ASA:Failed ASA in HA pair not recovering by itself, after an "HA state progression failed"
CSCvs27336	Traceback on ASA by Smart Call Home process
CSCwa67209	FMC may disable autonegotiation for port-channels with 1Gbps SFP fiber members after FTD upgrade
CSCwb33334	ASA: crash after sending some traffic over RAVPN tunnel
CSCwa75077	Time-range objects incorrectly populated in prefilter rules
CSCwa40237	Cisco Firepower Management Center File Upload Security Bypass Vulnerability
CSCvz94153	NTP sync on IPV6 will fail if the IPV4 address is not configured
CSCwa55562	Different CG-NAT port-block allocated for same source IP causing per-host PAT port block exhaustion
CSCvz31880	ASA Crashing with 'Unicorn Proxy Thread cpu: 9 watchdog_cycles' after stopping scaled stress test.

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

Resolved Bugs in Version 7.0.1.1

Table last updated: 2022-02-17

Table 53: Resolved Bugs in Version 7.0.1.1

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

Resolved Bugs in Version 7.0.1

Table last updated: 2021-10-07

Table 54: Resolved Bugs in Version 7.0.1

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

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

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

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

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

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

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

Bug ID	Headline
CSCvz25434	ASA/FTD blackholes traffic due to 1550 block depletion when BVI is configured as DHCP client
CSCvz25663	FTD/FDM upgrade error due to snmp-server host community string validation failure
CSCvz26950	[DOC] The Appliance Information Widget missing High Availability information in FMC Documentation
CSCvz29233	ASA: ARP entries from custom context not removed when an interface flap occurs on system context
CSCvz30333	FTD/Lina may traceback when "show capture" command is executed
CSCvz30933	ASA tracebacks and reload when clear configure snmp-server command is issued
CSCvz32386	FTD Deployment error when FMC pushes PFS21 and IKEv1 settings on same crypto map entry
CSCvz34831	If ASA fails to download DACL it will never stop trying
CSCvz35201	Upgrade failure / Stuck on 999_finish/989_update_ngfw_conf_aquila_ssp.sh
CSCvz38361	BGP packets dropped for non directly connected neighbors
CSCvz38811	Deleted files holding disk space under Java process
CSCvz46333	FTD policy deployment failure due to internal socket connection loss
CSCvz66506	Continuous ADI crash is seen on FPR2100 after upgrade to 7.0 registered to FMC HA

Resolved Bugs in Version 7.0.0.1

Table last updated: 2021-07-15

Table 55: Resolved Bugs in Version 7.0.0.1

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

Resolved Bugs in Version 7.0.0

Table last updated: 2021-05-25

Table 56: Resolved Bugs in Version 7.0.0

Bug ID	Headline
CSCvi96835	No validation err when changing host thats part of a group object used in a routing policy, to Range

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

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

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

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

Bug ID	Headline
CSCvw13395	FMC 6.6.0 "Reset Connection Upon Timeout" Checkbox missing in Light Theme of UI
CSCvw16565	Policy Deployment fails after enabling "SMB Auto-Detect Ports" in DCE/RPC Configuration.
CSCvw21145	Duplicate NAT rule error when saving the policy (caused by duplicate Auto NAT rules)
CSCvw21161	Duplicate NAT rule error when saving the policy (different rules are detected as duplicates)
CSCvw21628	Upgrade from pre-6.6.x to 6.6.x and above breaks Intrusion Event Packet-Drill down
CSCvw27966	Policy deployment fails with object names starts with 'any'
CSCvw28894	SFDataCorrelator slow startup and vuln remap due to duplicate entries in vuln tables
CSCvw28946	When deploying VxLan config the command mtu is sent out of order causing deployment failures
CSCvw29561	FMC SLR license 'shows continuous Smart agent communication with Smart Licensing Cloud' alert
CSCvw29563	repair_users.pl script no longer works
CSCvw29581	VDB upgrade doesn't work when mysql user table is damaged.
CSCvw30252	ASA/FTD may traceback and reload due to memory corruption in SNMP
CSCvw33939	FMC Deployment failure due to VPN split-tunnel standard ACL with Network Group containing IPv6object
CSCvw34692	Not possible to change after the first time the TTL Hops for BGP neighbor
CSCvw38708	AC policy save, validateActivity not using cache for building blocks
CSCvw38870	FMC upgrade failure to 6.6.0, 6.6.1, 6.6.3, or 6.7.0 at 800_post/1027_ldap_external_auth_fix.pl
CSCvw41901	Deleting System Defined objects via FMC's REST API returns HTTP 500 error code.
CSCvw42497	Error during policy validation while navigating through AC policy
CSCvw45125	Block deployment while secondary nodes are in config or bulk sync
CSCvw47943	Optimization of the query for scan results in Firepower Recommendations
CSCvw51307	ASA/FTD traceback and reload in process name "Lina"
CSCvw60177	Standby/Secondary cluster unit might crash in Thread Name: fover_parse and "cluster config sync"
CSCvw79294	sftunnel logging huge number of logs to messages file

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