



Cisco Firepower Release Notes, Version 7.1

First Published: 2021-12-15

Last Modified: 2023-03-15

Americas Headquarters

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



CONTENTS

CHAPTER 1	Welcome	1
	Release Highlights	1
	Release Dates	1
	Suggested Release	2
	Sharing Data with Cisco	2
	For Assistance	3

CHAPTER 2	System Requirements	5
	FMC Platforms	5
	FTD Platforms	6
	Threat Defense Management	8
	Browser Requirements	10

CHAPTER 3	Features and Functionality	13
	New Features in FMC Version 7.1	13
	New Features in FDM Version 7.1	31
	Intrusion Rules and Keywords	37
	Deprecated FlexConfig Commands	38

CHAPTER 4	Upgrade Guidelines	39
	Planning Your Upgrade	39
	Minimum Version to Upgrade	40
	Guidelines for Cloud-delivered Firewall Management Center	41
	Upgrade Guidelines for Version 7.1	42
	Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0	43
	Reconnect with Cisco Secure Malware Analytics for High Availability FMCs	43

- Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs 44
- FMCv Requires 28 GB RAM for Upgrade 44
- Upgrade Guidelines for FXOS 45
- Unresponsive Upgrades 46
- Revert or Uninstall the Upgrade 46
- Traffic Flow and Inspection 47
 - Traffic Flow and Inspection for FXOS Upgrades 47
 - Traffic Flow and Inspection for FTD Upgrades with FMC 47
 - Traffic Flow and Inspection for FTD Upgrades with FDM 49
- Time and Disk Space Tests 50
 - Time and Disk Space for Version 7.1.0.3 52
 - Time and Disk Space for Version 7.1.0.2 52
 - Time and Disk Space for Version 7.1.0.1 52
 - Time and Disk Space for Version 7.1.0 53

CHAPTER 5

Install the Software 55

- Installation Guidelines 55
- Installation Guides 57

CHAPTER 6

Open and Resolved Bugs 59

- Open Bugs 59
 - Open Bugs in Version 7.1.0 59
- Resolved Bugs 60
 - Resolved Bugs in Version 7.1.0.3 60
 - Resolved Bugs in Version 7.1.0.2 72
 - Resolved Bugs in Version 7.1.0.1 72
 - Resolved Bugs in Version 7.1.0 73



CHAPTER 1

Welcome

This document contains release information for Version 7.1 of Cisco Firepower Threat Defense, Firepower Management Center, and Firepower Device Manager.

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

- [Release Highlights, on page 1](#)
- [Release Dates, on page 1](#)
- [Suggested Release, on page 2](#)
- [Sharing Data with Cisco, on page 2](#)
- [For Assistance, on page 3](#)

Release Highlights

All-FTD Release

Version 7.1 is supported on the FMC and on FTD devices only. It is not supported on ASA FirePOWER or NGIPSv devices.

You can still use a Version 7.1 FMC to manage older devices — FTD as well as ASA FirePOWER and NGIPSv — that are running Version 6.5 through 7.0.

Release Dates

Table 1: Version 7.1 Dates

Version	Build	Date	Platforms
7.1.0.3	108	2022-03-15	All
7.1.0.2	28	2022-08-03	FMC/FMCv Secure Firewall 3100 series

Version	Build	Date	Platforms
7.1.0.1	28	2022-02-24	FMC/FMCv All devices except Secure Firewall 3100 series
7.1.0	90	2021-12-01	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-71-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 7.1.

- [FMC Platforms, on page 5](#)
- [FTD Platforms, on page 6](#)
- [Threat Defense Management, on page 8](#)
- [Browser Requirements, on page 10](#)

FMC Platforms

The FMC provides a centralized firewall management console. For device compatibility with the FMC, see [Threat Defense Management, on page 8](#). For general compatibility information, see the [Cisco Secure Firewall Management Center Compatibility Guide](#).

FMC Hardware

Version 7.1 supports the following FMC hardware:

- FMC 1600
- FMC 2600
- FMC 4600

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 7.1 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 7.1 FMCv Platforms

Platform	Devices Managed		High Availability
	2, 10, 25	300	
Public Cloud			
Amazon Web Services (AWS)	YES	YES	YES
Google Cloud Platform (GCP)	YES	—	—
Microsoft Azure	YES	—	—
Oracle Cloud Infrastructure (OCI)	YES	YES	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.



Note The cloud-delivered management center cannot manage Version 7.1 devices.

FTD 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 [Threat Defense Management, on page 8](#). For general compatibility information, see the [Cisco Secure Firewall Threat Defense Compatibility Guide](#).

FTD Hardware

Version 7.1 FTD hardware comes in a range of throughputs, scalability capabilities, and form factors.

Table 3: Version 7.1 FTD Hardware

Platform	FMC Compatibility		FDM Compatibility		Notes
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO	
Firepower 1010, 1120, 1140, 1150	YES	—	YES	YES	—
Firepower 2110, 2120, 2130, 2140	YES	—	YES	YES	—
Secure Firewall 3110, 3120, 3130, 3140	YES	—	YES	YES	The Version 7.1.0 release does not include online help for these devices. For the FMC, new online help is included in Version 7.1.0.2. For FDM, see the documentation posted on Cisco.com.
Firepower 4110, 4120, 4140, 4150 Firepower 4112, 4115, 4125, 4145	YES	—	YES	YES	Requires FXOS 2.11.1.154 or later build. We recommend the latest firmware. See the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide .
Firepower 9300: SM-24, SM-36, SM-44 modules Firepower 9300: SM-40, SM-48, SM-56 modules	YES	—	YES	YES	Requires FXOS 2.11.1.154 or later build. We recommend the latest firmware. See the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide .
ISA 3000	YES	—	YES	YES	Requires the latest ROMMON image. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide .

FTDv

Version 7.1 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 7.1 FTDv Platforms

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

Threat Defense Management

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

Customer-Deployed FMC

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

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

Table 5: 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.

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
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 7.1, 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 7.1, on page 13](#)
- [New Features in FDM Version 7.1, on page 31](#)
- [Intrusion Rules and Keywords, on page 37](#)
- [Deprecated FlexConfig Commands, on page 38](#)

New Features in FMC Version 7.1

Although you can manage older devices with a newer customer-deployed FMC, we recommend you always update your entire deployment. You should assume that new traffic-handling features require the latest release on both the FMC *and* device. Features where devices are not obviously involved (cosmetic changes to the web interface, cloud integrations) may only require the latest version on the FMC, but that is not guaranteed. In the new feature descriptions, we are explicit when version requirements deviate from the standard expectation.

New Features

Table 6: New Features in FMC Version 7.1 Patches

New Feature	Description
<p>Version 7.1.0.3</p> <p>Automatically update CA bundles</p>	<p>Upgrade impact.</p> <p>The local CA bundle contains certificates to access several Cisco services. The system now automatically queries Cisco for new CA certificates at a daily system-defined time. Previously, you had to upgrade the software to update CA certificates. You can use the CLI to disable this feature.</p> <p>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.</p> <p>New/modified CLI commands: configure cert-update auto-update, configure cert-update run-now, configure cert-update test, show cert-update</p> <p>For more information, see the Firepower Management Center Command Line Reference in the management center administration guide, and the Cisco Secure Firewall Threat Defense Command Reference.</p>

Table 7: New Features in FMC Version 7.1.0

New Feature	Description
<p>Platform</p>	

New Feature	Description
Secure Firewall 3100	<p>We introduced the Secure Firewall 3110, 3120, 3130, and 3140.</p> <p>You can hot swap a network module of the same type while the firewall is powered up without having to reboot; making other module changes requires a reboot. Secure Firewall 3100 25 Gbps interfaces support Forward Error Correction as well as speed detection based on the SFP installed. The SSDs are self-encrypting drives (SEDs), and if you have 2 SSDs, they form a software RAID. These devices support up to 8 units for Spanned EtherChannel clustering.</p> <p>Note that the Version 7.1.0 release does not include online help for these devices; new online help is included in Version 7.1.0.2.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Devices > Device Management > Add Cluster • Devices > Device Management > More • Devices > Device Management > Cluster • Devices > Device Management > Chassis Operations • Devices > Device Management > Interfaces > edit physical interface > Hardware Configuration • Devices > Device Management <p>New/modified FTD CLI commands: configure network speed, configure raid, show raid, show ssd</p>
FMCv300 for AWS FMCv300 for OCI	<p>We introduced the FMCv300 for both AWS and OCI. The FMCv300 can manage up to 300 devices.</p>

New Feature	Description
FTDv for AWS instances.	FTDv for AWS adds support for these instances: <ul style="list-style-type: none"> • c5a.xlarge, c5a.2xlarge, c5a.4xlarge • c5ad.xlarge, c5ad.2xlarge, c5ad.4xlarge • c5d.xlarge, c5d.2xlarge, c5d.4xlarge • c5n.xlarge, c5n.2xlarge, c5n.4xlarge • i3en.xlarge, i3en.2xlarge, i3en.3xlarge • inf1.xlarge, inf1.2xlarge • m5.xlarge, m5.2xlarge, m5.4xlarge • m5a.xlarge, m5a.2xlarge, m5a.4xlarge • m5ad.xlarge, m5ad.2xlarge, m5ad.4xlarge • m5d.xlarge, m5d.2xlarge, m5d.4xlarge • m5dn.xlarge, m5dn.2xlarge, m5dn.4xlarge • m5n.xlarge, m5n.2xlarge, m5n.4xlarge • m5zn.xlarge, m5zn.2xlarge, m5zn.3xlarge • r5.xlarge, r5.2xlarge, r5.4xlarge • r5a.xlarge, r5a.2xlarge, r5a.4xlarge • r5ad.xlarge, r5ad.2xlarge, r5ad.4xlarge • r5b.xlarge, r5b.2xlarge, r5b.4xlarge • r5d.xlarge, r5d.2xlarge, r5d.4xlarge • r5dn.xlarge, r5dn.2xlarge, r5dn.4xlarge • r5n.xlarge, r5n.2xlarge, r5n.4xlarge • z1d.xlarge, z1d.2xlarge, z1d.3xlarge
FTDv for Azure instances.	FTDv for Azure adds support for these instances: <ul style="list-style-type: none"> • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2

New Feature	Description
Use FDM to configure the FTD for management by the FMC.	<p>When you perform initial setup using FDM, all interface configuration completed in FDM is retained when you switch to FMC for management, in addition to the Management and FMC access settings. Note that other default configuration settings, such as the access control policy or security zones, are not retained. When you use the FTD CLI, only the Management and FMC access settings are retained (for example, the default inside interface configuration is not retained).</p> <p>After you switch to FMC, you can no longer use FDM to manage the FTD.</p> <p>New/modified FDM screens: System Settings > Management Center</p>
Device Upgrade	
Revert a successful device upgrade.	<p>You can now revert major and maintenance upgrades to FTD. Reverting returns the software to its state just before the last upgrade, also called a <i>snapshot</i>. If you revert an upgrade after installing a patch, you revert the patch as well as the major and/or maintenance upgrade.</p> <p>Important If you think you might need to revert, you must use System (⚙️) > Updates to upgrade FTD. The System Updates page is the only place you can enable the Enable revert after successful upgrade option, which configures the system to save a revert snapshot when you initiate the upgrade. This is in contrast to our usual recommendation to use the wizard on the Devices > Device Upgrade page.</p> <p>This feature is not supported for container instances.</p> <p>Minimum FTD: 7.1</p>
Improvements to the upgrade workflow for clustered and high availability devices.	<p>We made the following improvements to the upgrade workflow for clustered and high availability devices:</p> <ul style="list-style-type: none"> • The upgrade wizard now correctly displays clustered and high availability units as groups, rather than as individual devices. The system can identify, report, and preemptively require fixes for group-related issues you might have. For example, you cannot upgrade a cluster on the Firepower 4100/9300 if you have made unsynced changes on Firepower Chassis Manager. • We improved the speed and efficiency of copying upgrade packages to clusters and high availability pairs. Previously, the FMC copied the package to each group member sequentially. Now, group members can get the package from each other as part of their normal sync process. • You can now specify the upgrade order of data units in a cluster. The control unit always upgrades last.

New Feature	Description
Snort 3 backwards compatibility.	<p>For Snort 3, new features and resolved bugs require that you fully upgrade the FMC <i>and</i> its managed devices. Unlike Snort 2, you cannot update the inspection engine on an older device (for example, Version 7.0) by deploying from a newer FMC (for example, Version 7.1).</p> <p>When you deploy to an older device, the system lists any unsupported configurations and warns you that they will be skipped. We recommend you always update your entire deployment.</p>
Device Management	
Geneve interface support for an FTDv on AWS instances.	<p>Geneve encapsulation support was added to support single-arm proxy for the AWS Gateway Load Balancer (GWLB). The AWS GWLB combines a transparent network gateway (with a single entry and exit point for all traffic) and a load balancer that distributes traffic and scales FTDv to match the traffic demand.</p> <p>This support requires FMC with Snort 3 enabled and is available on the following performance tiers:</p> <ul style="list-style-type: none"> • FTDv20 • FTDv30 • FTDv50 • FTDv100
Single Root I/O Virtualization (SR-IOV) support for FTDv on OCI.	<p>You can now implement Single Root Input/Output Virtualization (SR-IOV) for FTDv on OCI. SR-IOV can provide performance improvements for an FTDv. Mellanox 5 as vNICs are not supported in SR-IOV mode.</p>
LLDP support for the Firepower 1100.	<p>You can now enable Link Layer Discovery Protocol (LLDP) for Firepower 1100 interfaces.</p> <p>New/modified screens: Devices > Device Management > Interfaces > Hardware Configuration > LLDP</p> <p>New/modified commands: show lldp status, show lldp neighbors, show lldp statistics</p> <p>Supported platforms: Firepower 1100 (1120, 1140, and 1150)</p>
Interface auto-negotiation is now set independently from speed and duplex, interface sync improved.	<p>Interface auto-negotiation is now set independently from speed and duplex. Also, when you sync the interfaces in FMC, hardware changes are detected more effectively.</p> <p>New/modified screens: Devices > Device Management > Interfaces > Hardware Configuration > Speed</p> <p>Supported platforms: Firepower 1000/2100, Secure Firewall 3100</p>
Support to specify trusted DNS servers.	<p>You can use FTD platform settings to specify trusted DNS servers for DNS snooping. This helps detect applications on the first packet by mapping domains to IP addresses. By default, trusted DNS servers include those in DNS server objects, and those discovered by dhcp-pool, dhcp-relay, and dhcp-client.</p>

New Feature	Description
Import and export device configurations.	<p>You can export the device-specific configuration, and you can then import the saved configuration for the same device in the following use cases:</p> <ul style="list-style-type: none"> • Moving the device to a different FMC. • Restore an old configuration. • Reregistering a device. <p>New/modified screens: Devices > Device Management > Device > General</p>
High Availability/Scalability	
High availability for: <ul style="list-style-type: none"> • FMCv for AWS • FMCv for OCI 	<p>We now support high availability on FMCv for AWS and FMCv for OCI.</p> <p>In an FTD deployment, you need two identically licensed FMCs, as well as one FTD entitlement for each managed device. For example, to manage 10 FTD devices with an FMCv10 high availability pair, you need two FMCv10 entitlements and 10 FTD entitlements. If you are managing Version 6.5.0–7.0.x Classic devices only (NGIPSv or ASA FirePOWER), you do not need FMCv entitlements.</p> <p>Supported platforms: FMCv10, FMCv25, FMCv300 (not supported for FMCv2)</p>
Autoscale on FTDv for OCI.	<p>We now support autoscaling on FTDv for OCI.</p> <p>The serverless infrastructure in cloud-based deployments allow you to automatically adjust the number of FTDv instances in an autoscale group based on capacity needs. This includes automatic registering/unregistering to and from the managing FMC.</p>
Cluster deployment for firewall changes completes faster.	<p>Cluster deployment for firewall changes now completes faster.</p> <p>Supported platforms: Firepower 4100/9300, Secure Firewall 3100</p>
Clearing routes in a high availability group or cluster.	<p>In previous releases, the clear route command cleared the routing table on the unit only. Now, when operating in a high availability group or cluster, the command is available on the active or control unit only, and clears the routing table on all units in the group or cluster.</p>
NAT	
Manual NAT support for fully-qualified domain name (FQDN) objects as the translated destination.	<p>You can use an FQDN network object, such as one specifying www.example.com, as the translated destination address in manual NAT rules. The system configures the rule based on the IP address returned from the DNS server.</p>
Routing	

New Feature	Description
BGP configuration to interconnect virtual routers.	<p>You can configure BGP settings to dynamically leak routes among user-defined virtual routers, and between global virtual router and user-defined virtual routers. The import and export routes feature was introduced to exchange routes among the virtual routers by tagging them with route targets and optionally, filtering the matched routes with route maps. This BGP feature is accessible only when you select a user-defined virtual router.</p> <p>New/modified screens: For a selected user-defined virtual router, Devices > Device Management > Routing > BGPv4/v6 > Route Import/Export</p>
BGPv6 support for user-defined virtual routers.	<p>FTD now supports configuring BGPv6 on user-defined virtual routers.</p> <p>New/modified screens: For a selected user-defined virtual router, Devices > Device Management > Routing > BGPv6</p>
Equal-Cost-Multi-Path (ECMP) zone support.	<p>You can now group interfaces in traffic zones and configure Equal-Cost-Multi-Path (ECMP) routing in FMC.</p> <p>ECMP routing was previously supported through FlexConfig policies.</p> <p>New/modified screens: Devices > Device Management > Routing > ECMP</p>
Direct Internet Access/Policy Based Routing	
Direct internet access with policy based routing.	<p>You can now configure policy based routing through the FMC to classify network traffic based on applications and to implement Direct Internet Access (DIA) to send traffic to the internet from a branch deployment. You can define a PBR policy and configure it on ingress interfaces, specifying match criteria and egress interfaces. Network traffic that matches the access control policy is forwarded through the egress interface based on priority or the order as configured in the policy.</p> <p>New/modified screens: New policy page for configuring the policy based routing policy: Devices > Device Management > Routing > Policy Based Routing</p> <p>Supported platforms: FTD</p>
FMC REST API enhancements for direct internet access and policy based routing.	<p>You can use the FMC REST API to configure Direct Internet Access through Policy Based Routing. The following enhancements have been made to the FMC REST API to support this:</p> <ul style="list-style-type: none"> • New APIs were added to enable you to create, view, edit, and delete your Policy Based Routing configuration • New parameters added to existing APIs for Extended Access Control Lists to define applications • New parameters added to existing APIs for device interfaces to define interface priority
Remote Access VPN	
Copy RA VPN policies.	<p>You can now create a new RA VPN policy by copying an existing policy. We added a copy button next to each policy on Devices > VPN > Remote Access.</p>

New Feature	Description
AnyConnect VPN SAML external browser.	<p>You can now configure AnyConnect VPN SAML External Browser to enable additional authentication choices, such as passwordless authentication, WebAuthN, FIDO, SSO, U2F, and an improved SAML experience due to the persistence of cookies. When you use SAML as the primary authentication method for a remote access VPN connection profile, you can elect to have the AnyConnect client use the client's local browser instead of the AnyConnect embedded browser to perform the web authentication. This option enables single sign-on (SSO) between your VPN authentication and other corporate logins. Also choose this option if you want to support web authentication methods, such as biometric authentication and Yubikeys, that cannot be performed in the embedded browser.</p> <p>We updated the remote access VPN connection profile wizard to allow you to configure the SAML Login Experience.</p>
Multiple trustpoints for SAML identity providers on Microsoft Azure.	<p>You can now add multiple RA VPN trustpoints for SAML identity providers, as required by Microsoft Azure.</p> <p>In a Microsoft Azure network, Azure can support multiple applications for the same Entity ID. Each application (typically mapped to a different tunnel group) requires a unique certificate. This feature enables you to add multiple trustpoints for RA VPN in FTDv for Microsoft Azure.</p>
Site to Site VPN	
VPN filters.	<p>You can now configure site to site VPN filters with rules that determine whether to allow or reject tunneled data packets based on criteria such as source address, destination address, and protocol.</p> <p>The VPN filter is applied to post-decrypted traffic after it exits a tunnel and to pre-encrypted traffic before it enters a tunnel.</p>
Unique local tunnel ID for IKEv2.	<p>You can now configure a Local Tunnel ID per IKEv2 tunnel for both policy-based and route-based Site to Site VPNs. You can configure the local tunnel ID with the FMC web interface or from the REST API.</p> <p>This local tunnel ID configuration enables Umbrella SIG integration with FTD.</p>
Multiple IKE policies.	<p>You can now configure multiple IKE policies for both policy-based and route-based Site to Site VPNs.</p> <p>Multiple IKE policies can be configured through the FMC GUI and the REST API.</p>

New Feature	Description
VPN monitoring dashboard.	<p>Beta.</p> <p>The Site to Site VPN Monitoring Dashboard provides:</p> <ul style="list-style-type: none"> • Visualization of tunnel status distribution across all devices • Visualization of network topology consisting of VPN tunnels • Ability to visually isolate and examine tunnels based on criteria like Topology, Device and Status <p>Note The Site to Site Monitoring Dashboard is a Beta feature and may not work as expected. Do not use it in production environments.</p>
Security Intelligence	
Snort 3 support for Security Intelligence on proxied traffic.	With Snort 3, you can now apply Security Intelligence to HTTP proxy traffic where the IP address is embedded into the HTTP request. For example, when a user uploads a Block list or an Allow list containing IP addresses or networks, the system matches on the destination server IP instead of proxy IP. As a result, traffic to the destination server can be blocked, monitored, or allowed (according to your Security Intelligence configuration).
Intrusion Detection and Prevention	
Snort 3 support for drop, reject, rewrite, and pass rule actions.	<p>Version 7.1 FMCs now support the following intrusion rule actions for FTD devices with Snort 3, including Version 7.0 devices:</p> <ul style="list-style-type: none"> • Drop: Drops the matching packet, but does not block further traffic in this connection. Generates an intrusion event. • Reject: Drops the matching packet and blocks further traffic in this connection. For TCP traffic, sends a TCP reset. For UDP traffic, sends ICMP port unreachable to the source and destination hosts. Generates an intrusion event. • Rewrite: Overwrites the matching packet based on the replace option in the rule. Generates an intrusion event. • Pass: Allows matching packet to pass without further evaluation by any other intrusion rules. Does not generate an intrusion event. <p>To configure these new rule actions, edit the Snort 3 version of an intrusion policy and use the Rule Action drop-down for each rule.</p>
Snort 3 support for TLS-based intrusion rules.	You can now create TLS-based intrusion rules to inspect decrypted TLS traffic with Snort 3. This feature allows Snort 3 intrusion rules to use TLS information.

New Feature	Description
Snort 3 support for inspection of DCE/RPC over SMB2.	<p>Upgrade impact.</p> <p>Version 7.1 with Snort 3 supports DCE/RPC inspection over SMB2.</p> <p>After the first post-upgrade deploy to Snort 3 devices, existing DCE/RPC rules begin inspecting DCE/RPC over SMB2; previously these rules only inspected DCE/RPC over SMB1.</p>
Snort 3 support for intrusion rule recommendations.	<p>Version 7.1 FMCs now support intrusion rule recommendations for FTD devices with Snort 3, including Version 7.0 devices.</p> <p>To configure this feature, edit the Snort 3 version of an intrusion policy and click the Recommendations button (in the left pane, next to All Rules).</p>
Snort 3 support for ssl_version and ssl_state keywords.	<p>Upgrade impact.</p> <p>Version 7.1 with Snort 3 supports the ssl_version and ssl_state intrusion rule keywords.</p> <p>Cisco-provided intrusion policies include active rules using those keywords. You can also create, upload, and deploy custom/third party rules using them. In Version 7.0.x, we supported those keywords with Snort 2 only. With Snort 3, rules with those keywords did not match traffic, and thus could not generate alerts or affect traffic. There was no indication that the rules were not working as expected. After the first post-upgrade deploy to Version 7.1+ Snort 3 devices, existing rules with those keywords can match traffic.</p>
Identity Services and User Control	
Snort 3 captive portal support for interception of HTTP/2 traffic.	<p>You can now intercept and redirect HTTP/2 traffic for user authentication with captive portal.</p> <p>When a redirect is received by the browser, the browser follows the redirect and authenticates with idhttpsd (Apache web server) using the same process as the HTTP/1 captive portal. After authentication, idhttpsd redirects the user back to the original URL.</p>
Snort 3 captive portal support for hostname-based redirect.	<p>You can configure active authentication for identity policy rules to redirect the user's authentication to a fully-qualified domain name (FQDN) rather than the IP address of the interface through which the user's connection enters the device.</p> <p>The FQDN must resolve to the IP address of one of the interfaces on the device. By using an FQDN, you can assign a certificate for active authentication that the client will recognize, thus avoiding the untrusted certificate warning users get when being redirected to an IP address. The certificate can specify the FQDN, a wildcard FQDN, or multiple FQDNs in the Subject Alternate Names (SAN) in the certificate.</p> <p>New/modified screens: We added the Redirect to Host Name option in the identity policy settings.</p>
Encrypted Traffic Handling (TLS/SSL)	

New Feature	Description
Advanced TLS/SSL policy options.	<p>You can now configure the following advanced TLS/SSL policy options in the Advanced Settings tab on the SSL Policy page:</p> <ul style="list-style-type: none"> • Block flows requesting ESNI (Encrypted Server Name Identification) • Disable HTTP/3 advertisement • Propagate untrusted server certificates to clients
Encrypted Visibility Engine for visibility into encrypted sessions.	<p>Beta.</p> <p>You can enable the Encrypted Visibility Engine to gain visibility into an encrypted session without needing to decrypt it. The engine fingerprints and analyzes encrypted traffic. In FMC 7.1, the Encrypted Visibility Engine provides more visibility into encrypted traffic, including protocols such as TLS and QUIC. It does not enforce any actions on that traffic.</p> <p>The Encrypted Visibility Engine is disabled by default. You can enable it on the Advanced tab of an access control policy in the Experimental Features section.</p> <p>New/modified screens: Policies > Access Control > Access Control Policy name > Advanced</p> <p>Note The Encrypted Visibility Engine is an experimental Beta feature provided for visibility. It may cause false positives.</p>
Service Policy	
Configure the maximum segment size (MSS) for embryonic connections.	<p>You can configure a service policy to set the server maximum segment size (MSS) for SYN-cookie generation for embryonic connections upon reaching the embryonic connections limit. This is meaningful for service policies where you are also setting embryonic connection maximums.</p> <p>New/modified screens: Connection Settings in the Add/Edit Service Policy wizard.</p>
Network Discovery	

New Feature	Description
Improved Snort 3 support for network discovery (remote network access support).	<p>With improvements to network discovery and remote network access support, Snort 3 is now at parity with Snort 2 for those features. The improvements include:</p> <ul style="list-style-type: none"> • Discovery of hosts and applications for SMB traffic: For SMB traffic on your network, the host is discovered in the network map, and the SMB application protocol and associated operating system information are discovered. • Discovery of NetBIOS traffic: For NetBIOS traffic, the NetBIOS name is discovered as well as associated information related to applications, such as the client application and operating system. • Discovery of applications only for hosts/networks monitored by the network discovery policy: This enhancement to the filtering logic enables you to discover applications for networks that are being monitored based on a network discovery rule. <p>In Snort 3, application detection is always enabled for all networks by default.</p>
Event Logging and Analysis	
Snort 3 support for elephant flow identification and monitoring.	<p>With FTD running Snort 3, you can now identify <i>elephant flows</i>—single-session network connections that are large enough to affect overall system performance. By default, elephant flow detection is automatically enabled, and tracks and logs connections larger than 1GB/10 seconds.</p> <p>A new predefined search for connection events (Reason = Elephant Flow) allows you to quickly identify elephant flows. You can also use the health monitor to view active elephant flows on your devices, and to create a custom health dashboard to correlate elephant flow incidence with other device metrics such as CPU usage.</p> <p>To disable this feature or to configure the size and time thresholds, use the FTD CLI.</p> <p>New/modified FTD CLI commands:</p> <ul style="list-style-type: none"> • show elephant-flow status • show elephant-flow detection-config • system support elephant-flow-detection enable • system support elephant-flow-detection disable • system support elephant-flow-detection bytes-threshold <i>bytes-in-MB</i> • system support elephant-flow-detection time-threshold <i>time-in-seconds</i>

New Feature	Description
Send intrusion events and retrospective malware events to the Secure Network Analytics cloud from the FMC.	<p>Upgrade impact.</p> <p>When you configure the system to send security events to the Stealthwatch cloud using Cisco Security Analytics and Logging (SaaS), the FMC now sends:</p> <ul style="list-style-type: none"> • Intrusion events. This allows remotely stored intrusion events to include impact flag data. Previously, these events were sent to the cloud by FTD and did not include the impact flag. • Retrospective malware events. These supplement the "original disposition" file and malware events that are still sent to the cloud by devices. <p>If you already enabled this feature, the FMC starts sending this information after a successful upgrade.</p>
New datastore for intrusion events improves performance.	<p>To improve performance, Version 7.1 uses a new datastore for intrusion events. After the upgrade finishes and the FMC reboots, historical events are migrated in the background, newest events first.</p> <p>As part of this migration, we deprecated intrusion incidents, the intrusion event clipboard, and custom tables for intrusion events. We also introduced two new fields in the intrusion event table: Source Host Criticality and Destination Host Criticality.</p>
NAT IP address and port information in connection and Security Intelligence events.	<p>For additional visibility into NAT translations, we added the following fields to connection and Security Intelligence events:</p> <ul style="list-style-type: none"> • NAT Source IP • NAT Destination IP • NAT Source Port • NAT Destination Port <p>In the table view of events, these fields are hidden by default. To change the fields that appear, click the x in any column name to display a field chooser.</p>

New Feature	Description
Packet tracer enhancements.	<p>Version 7.1 updates the packet tracer interface for better usability. In addition, you can now:</p> <ul style="list-style-type: none"> • Access the packet tracer directly from the main menu: Devices > Troubleshoot > Packet Tracer. • Save packet traces. • Run parallel packet traces across multiple devices. • Replay PCAPs through a device. • For Snort 3 devices, view enhanced output that provides new details on the phases of traffic evaluation from L2 to L7 (application identification, file/malware detection, intrusion detection, Security Intelligence, and so on), as well as how long each phase takes. <p>New/modified FTD CLI commands:</p> <ul style="list-style-type: none"> • packet-tracer input<i>source_interface</i>pcap<i>cap_filename</i>
Object Management	
Network object support for HTTP, ICMP, and SSH platform settings.	You can now use network object groups that contain network objects for hosts or networks when configuring the IP addresses in the Threat Defense Platform Settings policy.
Snort 3 support for network wildcard mask objects.	You can now create and manage network wildcard mask objects on the Object Management page. You can use network wildcard mask objects in access control, prefilter, and NAT policies.
Deployment preview enhancements for objects.	<p>You can now preview deployment changes to Geolocation, File List, and Security Intelligence objects.</p> <p>Updated screen: Deploy > Deployment. In the Preview column, click the Preview icon for a device to see the changes to the file list objects.</p>
Integrations	
Support for Cisco ACI Endpoint Update App, Version 2.0 and remediation module.	<p>Version 2.0 of the Cisco ACI Endpoint Update App has the following improvements over previous versions:</p> <ul style="list-style-type: none"> • The minimum update interval (how often the app updates the FMC) is now 10 seconds. Previously, it was 30 seconds. • The site prefix (a string that creates a network group object on the FMC associated with each APIC tenant) is now limited to 10 characters. Previously, it was 5 characters. <p>A new Cisco ACI Endpoint remediation module is also available with this update.</p>
Usability, Performance, and Troubleshooting	

New Feature	Description
Health monitoring enhancements.	<p>We updated the health monitor as follows:</p> <ul style="list-style-type: none"> • The health policy editor now groups similar health modules. You can enable and disable entire module groups. • The health policy exclusion editor is updated for better usability. Also, when you exclude a device or health module from alerting, you can now specify a time period for the exclusion, from 15 minutes to permanently. • The health monitor alert editor is updated for better usability. • The health policy deployment interface is updated for better usability. <p>Note To use the updated health monitor, you must enable REST API access on System (⚙️) > Configuration > REST API Preferences.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • System (⚙️) > Health > Policy > Edit Policy • System (⚙️) > Health > Exclude • System (⚙️) > Health > Monitor Alerts • System (⚙️) > Health > Policy > Deploy Policy
Deployment history enhancements.	<p>You can now bookmark a deployment job, edit the deployment notes for a job, and generate a report.</p>
Global search enhancements.	<p>Global search now has the following capabilities:</p> <ul style="list-style-type: none"> • You can search the full text of FMC walkthroughs (<i>how-tos</i>). • You can search extended community list names or configured values. • You can restrict searches by domain.
New walkthroughs.	<p>We added the following walkthroughs:</p> <ul style="list-style-type: none"> • Create a Snort 3 intrusion policy. • Enable or disable Snort 3 on an individual device. • Create a Snort 3 network analysis policy. • View the network analysis policy mapping. • Upgrade FTD. • Create and manage a cluster. • Change the FMC access interface from Management to Data. • Change the FMC access interface from Data to Management.

New Feature	Description
<p>Snort memory usage telemetry sent to Cisco Success Network.</p>	<p>For improved serviceability, we now send telemetry on Snort memory and swap usage, including out-of-memory events, to Cisco Success Network.</p> <p>We send this information for both Snort 2 and Snort 3. You can change your Cisco Success Network enrollment at any time.</p>
<p>Snort 3 support for statistics on start-of-flow and end-of-flow events.</p>	<p>For FTD with Snort 3, the output of the show snort statistics command now reports statistics on start-of-flow and end-of-flow events.</p>
<p>Web interface changes: SecureX, threat intelligence, and other integrations.</p>	<p>Version 7.1 changes these FMC menu options if you are upgrading from Version 7.0.2 or any later Version 7.0.x maintenance release.</p> <p>Note These changes will switch back in Version 7.2.</p> <p>Integration > AMP > AMP Management is now AMP > AMP Management</p> <p>Integration > AMP > Dynamic Analysis Connections is now AMP > Dynamic Analysis Connections</p> <p>Integration > Intelligence > Sources is now Intelligence > Sources</p> <p>Integration > Intelligence > Elements is now Intelligence > Elements</p> <p>Integration > Intelligence > Settings is now Intelligence > Settings</p> <p>Integration > Intelligence > Incidents is now Intelligence > Incidents</p> <p>Integration > Other Integrations is now System (⚙️) > Integration</p> <p>Integration > Security Analytics & Logging is now System (⚙️) > Logging > Security Analytics & Logging</p> <p>Integration > SecureX is now System (⚙️) > SecureX</p>
<p>FMC REST API</p>	
<p>FMC REST API services/operations.</p>	<p>For information on changes to the FMC REST API, see What's New in 7.1 in the REST API quick start guide.</p>

Deprecated Features

Table 8: Deprecated Features in FMC Version 7.1.0

Deprecated Feature	Description
End of support: FMC 1000, 2500, 4500	You cannot run Version 7.1+ on the FMC models FMC 1000, 2500, and 4500. You cannot manage Version 7.1+ devices with these FMCs.
End of support: ASA 5508-X and 5516-X	You cannot run Version 7.1+ on the ASA 5508-X or 5516-X.
End of support: NGIPS software (ASA FirePOWER/NGIPSv).	Version 7.1 is supported on the FMC and on FTD devices only. It is not supported on ASA FirePOWER or NGIPSv devices. You can still use a Version 7.1 FMC to manage older devices — FTD as well as ASA FirePOWER and NGIPSv — that are running Version 6.5 through 7.0.
Deprecated: Intrusion incidents and the intrusion event clipboard.	<p>Data and configurations can be deleted.</p> <p>We removed the intrusion incidents feature and the related intrusion event clipboard. The upgrade removes all data related to incidents, and deletes report templates sections that use the clipboard as a data source.</p> <p>Deprecated screens/options:</p> <ul style="list-style-type: none"> • Analysis > Intrusions > Incidents • Analysis > Intrusions > Clipboard • Copy and Copy All on intrusion event workflow pages and packet views • When adding sections to a report template (Overview > Reporting > Report Templates), you can no longer choose the Clipboard table as a data source.
Deprecated: Custom tables for intrusion events.	<p>Custom tables can be deleted.</p> <p>Version 7.1 ends support for custom tables for intrusion events. The upgrade deletes custom tables that contain fields from the intrusion event table.</p> <p>When adding fields to a custom table (Analysis > Advanced > Custom Tables), you can no longer choose the Intrusion Events table as a data source.</p>
Deprecated: ECMP zones with FlexConfig.	<p>FlexConfig settings ignored. Can prevent deploy.</p> <p>You can now group interfaces in traffic zones and configure Equal-Cost-Multi-Path (ECMP) routing in the management center web interface. After upgrade, the system ignores ECMP zones configured with FlexConfig. You cannot deploy with equal-cost static routes exist and must assign their interfaces to an ECMP zone.</p>

Deprecated Feature	Description
Temporarily deprecated: Improved SecureX integration, SecureX orchestration.	<p>Can prevent upgrade.</p> <p>Version 7.1 temporarily deprecates the SecureX integration and orchestration improvements introduced in Version 7.0.2. The improved experience returns in Version 7.2.</p> <p>If you newly enabled SecureX integration in Version 7.0.2 or later maintenance release, you must disable the feature before you upgrade to Version 7.1. You can re-enable the feature after successful upgrade, using the older method. There are no upgrade issues if you enabled SecureX integration in Version 7.0.0 or 7.0.1, or if you upgrade to Version 7.2.</p>
Deprecated: Geolocation details.	<p>In May 2022 we split the GeoDB into two packages: a country code package that maps IP addresses to countries/continents, and an IP package that contains additional contextual data associated with routable IP addresses. The contextual data in the IP package can include additional location details, as well as connection information such as ISP, connection type, proxy type, domain name, and so on.</p> <p>The new country code package has the same file name as the old all-in-one package: <code>Cisco_GEODB_Update-<i>date-build</i></code>. This allows deployments running Version 7.1 and earlier to continue to obtain GeoDB updates. If you manually download GeoDB updates—for example, in an air-gapped deployment—make sure you get the country code package and not the IP package.</p> <p>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 reimagine the FMC to Version 7.2+ and update the GeoDB.</p>

New Features in FDM Version 7.1

Table 9: New and Deprecated Features in FDM Version 7.1

Feature	Description
Platform Features	


Feature	Description
Secure Firewall 3100	<p>We introduced the Secure Firewall 3110, 3120, 3130, and 3140.</p> <p>You can hot swap a network module of the same type while the firewall is powered up without having to reboot; making other module changes requires a reboot. Secure Firewall 3100 25 Gbps interfaces support Forward Error Correction as well as speed detection based on the SFP installed. The SSDs are self-encrypting drives (SEDs), and if you have 2 SSDs, they form a software RAID.</p> <p>Note that the Version 7.1 device manager does not include online help for these devices. See the documentation posted on Cisco.com.</p> <p>New/Modified screens: Device > Interfaces</p> <p>New/Modified Firepower Threat Defense commands: configure network speed, configure raid, show raid, show ssd</p>

Feature	Description
FTDv for AWS instances.	<p>FTDv for AWS adds support for these instances:</p> <ul style="list-style-type: none"> • c5a.xlarge, c5a.2xlarge, c5a.4xlarge • c5ad.xlarge, c5ad.2xlarge, c5ad.4xlarge • c5d.xlarge, c5d.2xlarge, c5d.4xlarge • c5n.xlarge, c5n.2xlarge, c5n.4xlarge • i3en.xlarge, i3en.2xlarge, i3en.3xlarge • inf1.xlarge, inf1.2xlarge • m5.xlarge, m5.2xlarge, m5.4xlarge • m5a.xlarge, m5a.2xlarge, m5a.4xlarge • m5ad.xlarge, m5ad.2xlarge, m5ad.4xlarge • m5d.xlarge, m5d.2xlarge, m5d.4xlarge • m5dn.xlarge, m5dn.2xlarge, m5dn.4xlarge • m5n.xlarge, m5n.2xlarge, m5n.4xlarge • m5zn.xlarge, m5zn.2xlarge, m5zn.3xlarge • r5.xlarge, r5.2xlarge, r5.4xlarge • r5a.xlarge, r5a.2xlarge, r5a.4xlarge • r5ad.xlarge, r5ad.2xlarge, r5ad.4xlarge • r5b.xlarge, r5b.2xlarge, r5b.4xlarge • r5d.xlarge, r5d.2xlarge, r5d.4xlarge • r5dn.xlarge, r5dn.2xlarge, r5dn.4xlarge • r5n.xlarge, r5n.2xlarge, r5n.4xlarge • z1d.xlarge, z1d.2xlarge, z1d.3xlarge
FTDv for Azure instances.	<p>FTDv for Azure adds support for these instances:</p> <ul style="list-style-type: none"> • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2
Support ends for the ASA 5508-X and 5516-X. The last supported release is Firepower Threat Defense 7.0.	<p>You cannot install Firepower Threat Defense 7.1 on an ASA 5508-X or 5516-X. The last supported release for these models is Firepower Threat Defense 7.0.</p>

Feature	Description
Firewall and IPS Features	
Network Analysis Policy (NAP) configuration for Snort 3.	<p>You can use FDM to configure the Network Analysis Policy (NAP) when running Snort 3. Network analysis policies control traffic preprocessing inspection. Inspectors prepare traffic to be further inspected by normalizing traffic and identifying protocol anomalies. You can select which NAP is used for all traffic, and customize the settings to work best with the traffic in your network. You cannot configure the NAP when running Snort 2.</p> <p>We added the Network Analysis Policy to the Policies > Intrusion settings dialog box, with an embedded JSON editor to allow direct changes, and other features to let you upload overrides, or download the ones you create.</p>
Manual NAT support for fully-qualified domain name (FQDN) objects as the translated destination.	<p>You can use an FQDN network object, such as one specifying www.example.com, as the translated destination address in manual NAT rules. The system configures the rule based on the IP address returned from the DNS server.</p>
Improved active authentication for identity rules.	<p>You can configure active authentication for identity policy rules to redirect the user's authentication to a fully-qualified domain name (FQDN) rather than the IP address of the interface through which the user's connection enters the device. The FQDN must resolve to the IP address of one of the interfaces on the device. By using an FQDN, you can assign a certificate for active authentication that the client will recognize, thus avoiding the untrusted certificate warning users get when being redirected to an IP address. The certificate can specify the FQDN, a wildcard FQDN, or multiple FQDNs in the Subject Alternate Names (SAN) in the certificate.</p> <p>We added the Redirect to Host Name option in the identity policy settings.</p>
VPN Features	
Backup remote peers for site-to-site VPN.	<p>You can configure a site-to-site VPN connection to include remote backup peers. If the primary remote peer is unavailable, the system will try to re-establish the VPN connection using one of the backup peers. You can configure separate pre-shared keys or certificates for each backup peer. Backup peers are supported for policy-based connections only, and are not available for route-based (virtual tunnel interface) connections.</p> <p>We updated the site-to-site VPN wizard to include backup peer configuration.</p>

Feature	Description
Password management for remote access VPN (MSCHAPv2).	<p>You can enable password management for remote access VPN. This allows AnyConnect to prompt the user to change an expired password. Without password management, users must change expired passwords directly with the AAA server, and AnyConnect does not prompt the user to change passwords. For LDAP servers, you can also set a warning period to notify users of upcoming password expiration.</p> <p>We added the Enable Password Management option to the authentication settings for remote access VPN connection profiles.</p>
AnyConnect VPN SAML External Browser	<p>When you use SAML as the primary authentication method for a remote access VPN connection profile, you can elect to have the AnyConnect client use the client's local browser instead of the AnyConnect embedded browser to perform the web authentication. This option enables single sign-on (SSO) between your VPN authentication and other corporate logins. Also choose this option if you want to support web authentication methods, such as biometric authentication, that cannot be performed in the embedded browser.</p> <p>We updated the remote access VPN connection profile wizard to allow you to configure the SAML Login Experience.</p>
Administrative and Troubleshooting Features	
Dynamic Domain Name System (DDNS) support for updating fully-qualified domain name (FQDN) to IP address mappings for system interfaces.	<p>You can configure DDNS for the interfaces on the system to send dynamic updates to DNS servers. This helps ensure that FQDNs defined for the interfaces resolve to the correct address, making it easier for users to access the system using a hostname rather than an IP address. This is especially useful for interfaces that get their addresses using DHCP, but it is also useful for statically-addressed interfaces.</p> <p>After upgrade, if you had used FlexConfig to configure DDNS, you must redo your configuration using FDM or the Firepower Threat Defense API, and remove the DDNS FlexConfig object from the FlexConfig policy, before you can deploy changes again.</p> <p>If you configure DDNS using FDM, then switch to FMC management, the DDNS configuration is retained so that FMC can find the system using the DNS name.</p> <p>In FDM, we added the System Settings > DDNS Service page. In the Firepower Threat Defense API, we added the DDNSService and DDNSInterfaceSettings resources.</p>
The dig command replaces the nslookup command in the device CLI.	To look up the IP address of a fully-qualified domain name (FQDN) in the device CLI, use the dig command. The nslookup command has been removed.

Feature	Description
DHCP relay configuration using FDM.	<p>You can use FDM to configure DHCP relay. Using DHCP relay on an interface, you can direct DHCP requests to a DHCP server that is accessible through the other interface. You can configure DHCP relay on physical interfaces, subinterfaces, EtherChannels, and VLAN interfaces. You cannot configure DHCP relay if you configure a DHCP server on any interface.</p> <p>We added the System Settings > DHCP > DHCP Relay page, and moved DHCP Server under the new DHCP heading.</p>
Key type and size for self-signed certificates in FDM.	<p>You can specify the key type and size when generating new self-signed internal and internal CA certificates in FDM. Key types include RSA, ECDSA, and EDDSA. The allowed sizes differ by key type. We now warn you if you upload a certificate whose key size is smaller than the minimum recommended length. There is also a weak key pre-defined search filter to help you find weak certificates, which you should replace if possible.</p>
Usage validation restrictions for trusted CA certificates.	<p>You can specify whether a trusted CA certificate can be used to validate certain types of connections. You can allow, or prevent, validation for SSL server (used by dynamic DNS), SSL client (used by remote access VPN), IPsec client (used by site-to-site VPN), or other features that are not managed by the Snort inspection engine, such as LDAPS. The primary purpose of these options is to let you prevent VPN connections from getting established because they can be validated against a particular certificate.</p> <p>We added Validation Usage as a property for trusted CA certificates.</p>
Generating the admin password in FDM.	<p>During initial system configuration in FDM, or when you change the admin password through FDM, you can now click a button to generate a random 16 character password.</p>
Startup time and tmatch compilation status.	<p>The show version command now includes information on how long it took to start (boot) up the system. Note that the larger the configuration, the longer it takes to boot up the system.</p> <p>The new show asp rule-engine command shows status on tmatch compilation. Tmatch compilation is used for an access list that is used as an access group, the NAT table, and some other items. It is an internal process that can consume CPU resources and impact performance while in progress, if you have very large ACLs and NAT tables. Compilation time depends on the size of the access list, NAT table, and so forth.</p>
Enhancements to show access-list element-count output.	<p>The output of the show access-list element-count command has been enhanced. When used with object-group search enabled, the output includes details about the number of object groups in the element count.</p> <p>In addition, the show tech-support output now includes the output from show access-list element-count and show asp rule-engine.</p>

Feature	Description
Use FDM to configure the Firepower Threat Defense for management by a FMC.	<p>When you perform initial setup using FDM, all interface configuration completed in FDM is retained when you switch to FMC for management, in addition to the Management and FMC access settings. Note that other default configuration settings, such as the access control policy or security zones, are not retained. When you use the Firepower Threat Defense CLI, only the Management and FMC access settings are retained (for example, the default inside interface configuration is not retained).</p> <p>After you switch to FMC, you can no longer use FDM to manage the Firepower Threat Defense.</p> <p>New/Modified screens: System Settings > Management Center</p>
Automatically update CA bundles	<p>The local CA bundle contains certificates to access several Cisco services. The system now automatically queries Cisco for new CA certificates at a daily system-defined time. Previously, you had to upgrade the software to update CA certificates. You can use the CLI to disable this feature.</p> <p>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.</p> <p>New/modified CLI commands: configure cert-update auto-update, configure cert-update run-now, configure cert-update test, show cert-update</p> <p>For more information, see the Cisco Secure Firewall Threat Defense Command Reference.</p>
FTD REST API version 6.2 (v6).	<p>The Firepower Threat Defense REST API for software version 7.1 is version 6.2. 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 6.2 is the same as 6.0/1: v6.</p> <p>Please re-evaluate all existing calls, as changes might have been made to the resource models you are using. To open the API Explorer, where you can view the resources, log into FDM, then click the more options button () and choose API Explorer.</p>

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 7.1.

- [Planning Your Upgrade](#), on page 39
- [Minimum Version to Upgrade](#), on page 40
- [Guidelines for Cloud-delivered Firewall Management Center](#), on page 41
- [Upgrade Guidelines for Version 7.1](#), on page 42
- [Upgrade Guidelines for FXOS](#), on page 45
- [Unresponsive Upgrades](#), on page 46
- [Revert or Uninstall the Upgrade](#), on page 46
- [Traffic Flow and Inspection](#), on page 47
- [Time and Disk Space Tests](#), on page 50

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-71-docs>.

Table 10: Upgrade Planning Phases

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

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.
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 7.1, including maintenance releases, as follows.

Table 11: Minimum Version to Upgrade to Version 7.1

Platform	Minimum Version
FMC	6.5
FTD	6.5 FXOS 2.11.1.154 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, 2.11(1) .

Minimum Version to Patch

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

Guidelines for Cloud-delivered Firewall Management Center

Upgrading 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](#).

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).

Upgrading Version 7.0 Devices

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+.

Upgrade Guidelines for Version 7.1

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

Table 12: Upgrade Guidelines for FTD with FMC Version 7.1

✓	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 59 , 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 40	Any	Any	Any
	Upgrade Guidelines for FXOS, on page 45	Firepower 4100/9300	Any	Any
	Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0, on page 43	Any	7.0.4+	7.1.0 only
	Reconnect with Cisco Secure Malware Analytics for High Availability FMCs, on page 43	FMC	6.4.0 through 6.7.x	7.0+
	Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 44	Firepower 1010	6.4.0 through 6.6.x	6.7+
	FMCv Requires 28 GB RAM for Upgrade, on page 44	FMCv	6.2.3 through 6.5.0.x	6.6+

Table 13: Upgrade Guidelines for FTD with FDM Version 7.1

✓	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

✓	Guideline	Platforms	Upgrading From	Directly To
	Open and Resolved Bugs, on page 59 , 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 40	Any	Any	Any
	Upgrade Guidelines for FXOS, on page 45	Firepower 4100/9300	Any	Any
	Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0, on page 43	Any	7.0.4+	7.1.0 only
	Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 44	Firepower 1010	6.4.0 through 6.6.x	6.7+

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 Secure Malware Analytics 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 Secure Malware Analytics 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 14: 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.

Platform	Pre-Upgrade Action	Details
AWS	Resize instances: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.

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 7.1 is FXOS 2.11.1.154.

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 47.

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 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, regardless of manager.
- Uninstall is supported for patches to FTD with FMC. You can also uninstall FMC patches.

If this will not work for you and you still need to return to an earlier version, you must reimage. For guidelines, limitations, and procedures, see the [upgrade guide](#) for the version of the management center/device manager you are currently running.

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 15: Traffic Flow and Inspection: FXOS Upgrades

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

Traffic Flow and Inspection for FTD Upgrades with FMC

Software Upgrades for Standalone Devices

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

Table 16: Traffic Flow and Inspection: Software Upgrades for Standalone Devices

Interface Configuration	Traffic Behavior	
Firewall interfaces Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped. For bridge group interfaces on the ISA 3000 only, you can use a FlexConfig policy to configure hardware bypass for power failure. This causes traffic to drop during software upgrades but pass without inspection while the device completes its post-upgrade reboot.	
IPS-only interfaces	Inline set, hardware bypass force-enabled: Bypass: Force	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: Bypass: Standby	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: Bypass: Disabled	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability/Scalability

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

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

Software Revert (Major/Maintenance Releases)

You should expect interruptions to traffic flow and inspection during revert, even in a high availability/scalability deployment. This is because revert is more successful when all units are reverted simultaneously. Simultaneous revert means that interruptions to traffic flow and inspection depend on interface configurations only, as if every device were standalone.

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 17: 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.

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 46](#).

Table 18: Time Test Conditions for Software Upgrades

Condition	Details
Deployment	Times for device upgrades are from tests in a FMC deployments. Raw upgrade times for remotely and locally managed devices are similar, given similar conditions.
Versions	For major and maintenance releases, we test upgrades from all eligible previous major versions. For patches, we test upgrades from the base version. Upgrade time usually increases if your upgrade skips versions.
Models	In most cases, we test on the lowest-end models in each series, and sometimes on multiple models in a series.
Virtual appliances	We test with the default settings for memory and resources. However, note that upgrade time in virtual deployments is highly hardware dependent.

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

Disk Space Tests

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

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

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

Without enough free disk space, the upgrade fails.

Table 19: 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 7.1.0.3

Table 20: Time and Disk Space for Version 7.1.0.3

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	2.9 GB in /var	29 MB in /	—	20 min	7 min
FMCv: VMware	4.0 GB in /var	25 MB in /	—	23 min	6 min
Firepower 1000 series	—	3.2 GB in /ngfw	1.0 GB	9 min	13 min
Firepower 2100 series	—	3.2 GB in /ngfw	1.1 GB	7 min	14 min
Secure Firewall 3100 series	—	3.5 GB in /ngfw	1.1 GB	4 min	15 min
Firepower 4100 series	—	2.8 GB in /ngfw	780 MB	5 min	7 min
Firepower 4100 series container instance	—	2.9 GB in /ngfw	780 MB	6 min	5 min
Firepower 9300	—	2.3 GB in /ngfw	780 MB	5 min	10 min
ISA 3000	1.7 GB in /ngfw/var	270 MB in /ngfw/bin	780 MB	11 min	14 min
FTDv: VMware	2.1 GB in /ngfw/var	270 MB in /ngfw/bin	350 MB	5 min	6 min

Time and Disk Space for Version 7.1.0.2

Table 21: Time and Disk Space for Version 7.1.0.2

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	2.0 GB in /var	19 MB in /	—	20 min	4 min
FMCv: VMware	2.5 GB in /var	14 MB in /	—	21 min	1 min
Secure Firewall 3100 series	—	3.2 GB in /ngfw	—	4 min	46 min

Time and Disk Space for Version 7.1.0.1

Table 22: Time and Disk Space for Version 7.1.0.1

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	2.0 GB in /var	19 MB in /	—	18 min	8 min
FMCv: VMware	2.2 GB in /var	14 MB in /	—	21 min	4 min
Firepower 1000 series	—	5.6 GB in /ngfw	430 MB	10 min	11 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
Firepower 2100 series	—	5.6 GB in /ngfw	420 MB	10 min	10 min
Firepower 4100 series	—	5.6 GB in /ngfw	430 MB	7 min	7 min
Firepower 4100 series container instance	—	5.6 GB in /ngfw	430 MB	6 min	4 min
Firepower 9300	—	5.1 GB in /ngfw	430 MB	7 min	8 min
ISA 3000	2.0 GB in /ngfw/var	240 MB in /ngfw/bin	430 MB	4 min	13 min
FTDv: VMware	1.5 GB in /ngfw/var	240 MN in /ngfw/bin	430 MB	4 min	4 min

Time and Disk Space for Version 7.1.0

Table 23: Time and Disk Space for Version 7.1.0

Platform		Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC		16.9 GB in /var	43 MB in /	—	33 min	15 min
FMCv: VMware		17 GB in /var	50 MB in /	—	34 min	5 min
Firepower 1000 series		—	8.2 GB in /ngfw	930 MB	16 min	11 min
Firepower 2100 series		—	8.3 GB in /ngfw	1 GB	13 min	13 min
Firepower 4100 series		—	8.6 GB in /ngfw	870 MB	15 min	9 min
Firepower 4100 series container instance		—	8.6 GB in /ngfw	870 MB	16 min	8 min
Firepower 9300		—	11.2 GB in /ngfw	870 MB	11 min	12 min
ISA 3000	from Version 6.5–6.6	9.3 GB in /home	256 KB in /ngfw	1 GB	21 min	8 min
	from Version 6.7	9.3 GB in /ngfw/Volume	270 KB in /ngfw			
	from Version 7.0	9.2 GB in /ngfw/var	260 KB in /ngfw/bin			
FTDv: VMware	from Version 6.5–6.6	4.6 GB in /home	925 KB in /ngfw	1 GB	11 min	6 min
	from Version 6.7	4.4 GB in /ngfw/Volume	210 KB in /ngfw			
	from Version 7.0	5.3 GB in /ngfw/var	220 KB in /ngfw/bin			



CHAPTER 5

Install the Software

If you cannot or do not want to upgrade to Version 7.1, you can freshly install major and maintenance releases. This is also called *reimaging*. We do not provide installation packages for patches. To run a particular patch, install the appropriate major or maintenance release, then apply the patch.

- [Installation Guidelines, on page 55](#)
- [Installation Guides, on page 57](#)

Installation Guidelines

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

Backups

Before you reimage, we *strongly* recommend you back up to a secure remote location and verify transfer success. Reimaging returns most settings to factory defaults, including the system password. It deletes any backups left on the appliance.



Note If you want to reimage so that you don't have to upgrade, due to version restrictions you cannot use a backup to import your old configurations. You must recreate your configurations manually.

Appliance Access

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

For devices, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also be able to access the FMC's management interface without traversing the device.

Unregistering from Smart Software Manager

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

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

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

Table 24: 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 25: 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 26: Scenarios for Full Reimages

Model	Details
Firepower 1000 series Firepower 2100 series Secure Firewall 3100 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 27: Installation Guides

Platform	Guide
FMC	
FMC 1600, 2600, 4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
FMCv	Cisco Secure Firewall Management Center Virtual Getting Started Guide
FTD	
Firepower 1000/2100 series Secure Firewall 3100 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: <i>Image Management</i> chapters Cisco Firepower 4100 Getting Started Guide Cisco Firepower 9300 Getting Started Guide
ISA 3000	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide
FTDv	Cisco Secure Firewall Threat Defense Virtual Getting Started Guide



CHAPTER 6

Open and Resolved Bugs

This document lists open and resolved bugs for Version 7.1 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, on page 59](#)
- [Resolved Bugs, on page 60](#)

Open Bugs

Open Bugs in Version 7.1.0

Table last updated: 2022-08-01

Table 28: Open Bugs in Version 7.1.0

Bug ID	Headline
CSCvz38976	7.1/Firepower Threat Defense device occasionally unable to pass large packets/Fragmentation failures
CSCvz83796	Multiple Cisco Products affected by SMBv2 Denial of Service Vulnerability in Snort Rules
CSCvz96487	SSL rules with certfeed conditions can cause unexpected handshake failures
CSCwa23353	Rate filter is shown as an unsupported config when deployed to 7.0.1 FTDv managed by 7.1 FMCv

Bug ID	Headline
CSCwa33452	FTD data plane (Lina) cores found on Azure D5 during 7.1.0/7.2.0 regression

Resolved Bugs

Resolved Bugs in Version 7.1.0.3

Table last updated: 2023-03-15

Table 29: Resolved Bugs in Version 7.1.0.3

Bug ID	Headline
CSCvp15884	FMC SI Health Alerts: SI URL List and Feeds - Failure False Positives
CSCvq29993	FPR2100 ONLY - PERMANENT block leak of size 9472 and 1550 memory blocks & blackholes traffic
CSCvw56551	ASA displays cosmetic NAT warning message when making the interface config changes
CSCvw62288	ASA: 256 byte block depletion when syslog rate is high
CSCvx68173	Observed few snort instances stuck at 100%
CSCvx68586	Not able to login to UI/SSH on FMC, console login doesn't prompt for password
CSCvx97053	Unable to configure ipv6 address/prefix to same interface and network in different context
CSCvy04430	Management Sessions fail to connect after several weeks
CSCvy24180	Default variable set missing on FMC
CSCvy38650	Unable to download captured file from FMC Captured files UI
CSCvy40401	L2L VPN session bringup fails when using NULL encryption in ipsec configuration
CSCvy43002	Observed crash while running SNMPWalk + S2S-IKEv2 and AnyConnect TVM Profiles
CSCvy67765	FTD VTI reports TUNNEL_SRC_IS_UP false despite source interface is up/up and working
CSCvy72841	Firepower 1K FTD sends LLDP packets with internal MAC address of eth2 interface
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

Bug ID	Headline
CSCvy99348	Shutdown command reboots instead of shutting the FP1k device down.
CSCvz03524	PKI "OCSP revocation check" failing due to sha256 request instead of sha1
CSCvz05541	ASA55XX: Expansion module interfaces not coming up after a software upgrade
CSCvz09106	Cisco ASA and FTD Software SSL VPN Denial of Service Vulnerability
CSCvz13143	FMC GUI is not accessible. MariaDB getting restarted since configured memory threshold is exceeded
CSCvz40765	FMC CPU graph displays the wrong number of Snort and System cores
CSCvz44645	FTD may traceback and reload in Thread Name 'lina'
CSCvz60142	ASA/FTD stops serving SSL connections
CSCvz60578	Cluster unit in MASTER_POST_CONFIG state does not notify cluster if moved to DISABLED
CSCvz61463	FP9k SM-44 High CPU on radware vdp Cores after upgrade
CSCvz61689	Port-channel member interfaces are lost and status is down after software upgrade
CSCvz68336	SSL decryption not working due to single connection on multiple in-line pairs
CSCvz69699	FMC UI may become inaccessible due to connection leaks in internal database
CSCvz70958	High Control Plane CPU due to dhcp_add_ip_l_stby
CSCvz72771	ASA/FTD may traceback and reload. "c_assert_cond_terminate" in stack trace
CSCvz76746	While implementing management tunnel a user can use open connect to bypass anyconnect.
CSCvz77050	Occasionally policy deployment failure are reported as successful
CSCvz81888	NTP will not change to *(synced) status after upgrade to asa-9.15.1/9.16.1.28 from asa-9.14.3
CSCvz83432	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 121, seq 18)
CSCvz84733	LACP packets through inline-set are silently dropped
CSCvz86256	Primary ASA should send GARP as soon as split-brain is detected and peer becomes cold standby
CSCvz88149	Lina traceback and reload during block free causing FTD boot loop
CSCvz89126	ASDM session/quota count mismatch in ASA when multiple context switchover is done from ASDM
CSCvz89327	OSPFv2 flow missing cluster centralized "c" flag

Bug ID	Headline
CSCvz90375	Low available DMA memory on ASA 9.14 at boot reduces AnyConnect sessions supported
CSCvz91218	Statelink hello messages dropped on Standby unit due to interface ring drops on high rate traffic
CSCvz92016	Cisco ASA and FTD Software Web Services Interface Privilege Escalation Vulnerability
CSCvz92932	ASA show tech execution causing spike on CPU and impacting to IKEv2 sessions
CSCvz94153	NTP sync on IPV6 will fail if the IPV4 address is not configured
CSCvz95108	FTD Deployment failure post upgrade due to major version change on device
CSCvz95949	FP1120 9.14.3 : temporary split brain happened after active device reboot
CSCvz98540	Cisco ASA and FTD Software SSL/TLS Client Denial of Service Vulnerability
CSCvz99222	Clear and show conn for inline-set is not working
CSCwa00038	Disk corruption occurs when /mnt/disk0 partition is full and blade is rebooted
CSCwa02929	FTD Blocks Traffic with SSL Flow Error CORRUPT_MESSAGE
CSCwa03732	Deployment gets hung at snapshot generation phase during deploy or causes deploy slowness
CSCwa05385	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 19)
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
CSCwa08262	AnyConnect users with mapped group-policies take attributes from default GP under the tunnel-group
CSCwa11052	SNMP Stopped Responding After Upgrading to Version- 9.14(2)15
CSCwa11079	Pre allocate sub context for DRBG health test
CSCwa13873	ASA Failover Split Brain caused by delay on state transition after "failover active" command run
CSCwa14725	ASA/FTD traceback and reload on IKE Daemon Thread
CSCwa15185	ASA/FTD: remove unwanted process call from LUA
CSCwa18858	ASA drops non DNS traffic with reason "label length 164 bytes exceeds protocol limit of 63 bytes"
CSCwa18889	Clock drift observed between Lina and FXOS on multi-instance
CSCwa19443	Flow Offload - Compare state values remains in error state for longer periods

Bug ID	Headline
CSCwa19713	Traffic dropped by ASA configured with BVI interfaces due to asp drop type "no-adjacency"
CSCwa20758	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 20)
CSCwa21061	FTD upgrade fails on 800_post/100_ftd_onbox_data_import.sh
CSCwa26038	ICMP inspection causes packet drops that are not logged appropriately
CSCwa26310	ASA/FTD may traceback during config read or failover sync due to certain SNMP-Server commands
CSCwa28822	FTD moving UI management from FDM to FMC causes traffic to fail
CSCwa28895	FTD SSL Decryption Traffic Latency SSL Proxy to allow configurable/dynamic maximum TCP window size
CSCwa29956	"Interface configuration has changed on device" message may be shown after FTD upgrade
CSCwa30114	"Error:NAT unable to reserve ports" when using a range of ports in an object service
CSCwa31508	Continuous deployment failure on QW-4145 device
CSCwa32286	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 125, seq 21)
CSCwa32367	Creation of dedicated CRITICAL cgroup for tackling MIO HeartBeat failure issue
CSCwa32527	7.1 to 7.2 upgrade crash if SNMP configured on ngfw-management interface
CSCwa32628	SFDataCorrelator crash at AddFileToPendingHash() due to race condition
CSCwa33248	Auto LSP update not getting triggered, missing Talos registration (beakerd)
CSCwa34287	ASA: Loss of NTP sync following a reload after upgrade
CSCwa35200	Some syslogs for AnyConnect SSL are generated in admin context instead of user context
CSCwa36661	Traffic is not hitting on some egress interfaces of user vrf due to routes missing in asp table
CSCwa36672	ASA on FPR4100 traceback and reload when running captures using ASDM
CSCwa36678	Random FTD reloads with the traceback during deployment from FMC
CSCwa38277	ASA NAT66 with big range as a pool don't works with IPv6
CSCwa38996	Big number of repetitive messages in snmpd.log leading to huge log size
CSCwa39680	Snort stops processing packets when SSL decryption debug enabled - Snort2
CSCwa40719	Traceback: Secondary firewall reloading in Threadname: fover_parse

Bug ID	Headline
CSCwa41834	ASA/FTD traceback and reload due to pix_startup_thread
CSCwa41918	ssl inspection may have unexpected behavior when evicting certificates
CSCwa41936	Cisco FTD Bleichenbacher Attack Vulnerability
CSCwa42350	ASA installation/upgrade fails due to internal error "Available resources not updated by module"
CSCwa42594	ASA: IP Header check validation failure when GTP Header have SEQ and EXT field
CSCwa42596	ASA with SNMPv3 configuration observes unexpected reloads with snmpd cores
CSCwa43311	Snort blocking and dropping packet, with bigger size(1G) file download
CSCwa43497	Datapath deadlocks seen on when sending ICMP PMTU for AnyConnect-SSL
CSCwa45656	SLR license application fails on managed devices
CSCwa46905	WM 1010 speed/duplex setting is not getting effect and causes unstable interface
CSCwa47041	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DAP DoS
CSCwa48849	ssl unexpected behavior with resumed sessions
CSCwa53489	Lina Traceback and Reload Due to invalid memory access while accessing Hash Table
CSCwa54045	Memory leaks in SAML native browser processing
CSCwa55404	Multiple Cisco Products Snort SMB2 Detection Engine Policy Bypass and DoS Vulnerability
CSCwa55562	Different CG-NAT port-block allocated for same source IP causing per-host PAT port block exhaustion
CSCwa55868	QP vFTD Policy Deployment with snort2 Failed with Undefined package variable
CSCwa55878	FTD Service Module Failure: False alarm of "ND may have gone down"
CSCwa56449	ASA traceback in HTTP cli EXEC code
CSCwa56975	DHCP Offer not seen on control plane
CSCwa57115	New access-list are not taking effect after removing non-existence ACL with objects.
CSCwa58686	ASA/FTD Change in OGS compilation behavior causing boot loop
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

Bug ID	Headline
CSCwa65389	ASA traceback and reload in Unicorn Admin Handler when change interface configuration via ASDM
CSCwa65681	TPK/KP/WM-RM: Assign FXOS interface MAC address to LLDP linux interfaces
CSCwa67209	FMC may disable autonegotiation for port-channels with 1Gbps SFP fiber members after FTD upgrade
CSCwa68552	All type-8 passwords are lost upon upgrade from ASA 9.12-9.15 to 9.16, failover gets disabled
CSCwa68660	FTP inspection stops working properly after upgrading the ASA to 9.12.4.x
CSCwa68805	FTD Traceback & reload during HA creation
CSCwa69303	ASA running on SSP platform generate critical error "[FSM:FAILED]: sam:dme:MgmtIfSwMgmtOobIfConfig"
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
CSCwa74900	Traceback and reload after enabling debug webvpn cifs 255
CSCwa75204	SNORT3 Certsize 16k traffic failing on 2100 with all SSL rules
CSCwa76564	ASDM session/quota count mismatch in ASA when multiple context switch before and after failover
CSCwa76822	Tune throttling flow control on syslog-ng destinations
CSCwa77073	SNMP is responding to snmpgetbulk with unexpected order of results
CSCwa77777	Adding more logs to watchdog infra
CSCwa79494	Traffic keep failing on Hub when IPSec tunnel from Spoke flaps
CSCwa79676	FPR1010 in HA Printing Broadcast Storm Alerts for Multiple Interfaces
CSCwa79980	SNMP get command in FPR does not show interface index.
CSCwa80040	FMC NFS configuration failling after upgrade from 6.4.0.4 to 7.0.1
CSCwa81795	Cisco ASA and FTD Software VPN Authorization Bypass Vulnerability
CSCwa83078	snort3 - resumed sessions not being decrypted can fail
CSCwa85043	Traceback: ASA/FTD may traceback and reload in Thread Name 'Logger'
CSCwa85138	Multiple issues with transactional commit diagnostics
CSCwa85492	URL lookup responding with two categories

Bug ID	Headline
CSCwa85709	Cisco Firepower Management Center Information Disclosure Vulnerability
CSCwa87315	ASA/FTD may traceback and reload in Thread Name 'IP Address Assign'
CSCwa87597	ASA/FTD Failover: Joining Standby reboots when receiving configuration replication from Active mate
CSCwa88571	Unable to register FMC with the Smart Portal
CSCwa89243	SNMP no longer responds to polls after upgrade to 9.15.1.17
CSCwa89689	Server hello done on TLS stripped by FTD after enabling 'early application detection' with snort3
CSCwa90615	WR8 and LTS18 commit id update in CCM layer (seq 24)
CSCwa90735	FTD/FXOS - ASAconsole.log files fail to rotate causing excessive disk space used in /ngfw
CSCwa91070	Cgroup triggering oom-k for backup process
CSCwa91090	SSL handshake logging showing unknown session during AnyConnect TLSv1.2 Session establishment
CSCwa93499	Cisco Firepower Management Center Stored Cross-Site Scripting Vulnerability
CSCwa94894	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-4-9608'
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
CSCwa96759	Lina may traceback and reload on tcpmod_proxy_handle_mixed_mode
CSCwa97784	ASA: Jumbo sized packets are not fragmented over the L2TP tunnel
CSCwa98684	Console has an excessive rate of warnings during policy deployment
CSCwa98853	Error F0854 FDM Keyring's RSA modulus is invalid
CSCwa99171	Chassis and application sets the time to Jan 1, 2010 after reboot
CSCwa99931	ASA/FTD: Tuning of update_mem_reference process
CSCwb00595	Mempool_DMA allocation issue / memory leakage
CSCwb01126	DNS server configuration is lost if configuring through RA VPN page on FDM 7.1.0
CSCwb01633	FXOS misses logs to diagnose root cause of module show-tech file generation failure
CSCwb01700	ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA

Bug ID	Headline
CSCwb01919	FP2140 ASA 9.16.2 HA units traceback and reload at lua_getinfo (getfuncname)
CSCwb01976	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
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
CSCwb02020	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
CSCwb02316	"Non stop forwarding not supported on '1'" error while configuring MAC address
CSCwb04975	FTD Snort3 traceback in daq-pdts while handling FQDN based traffic
CSCwb05148	Cisco ASA Software and FTD Software SNMP Denial of Service Vulnerability
CSCwb05291	Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability
CSCwb06273	Continuous memory leak in the process hmlsd (SF::Messaging::smartSend)
CSCwb06543	Increase logging level to diagnose LACP process unexpected restart events
CSCwb06847	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-9-11543'
CSCwb07319	Entitlement tags contain invalid character.
CSCwb07908	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
CSCwb07981	Traceback: Standby FTD reboots and generates crashinfo and lina core on thread name cli_xml_server
CSCwb08393	SSL policy deploy failing when using special characters on SSL rule names
CSCwb08773	FPR2130 LED is off when power supply module 1 is back
CSCwb11939	ASA/FTD MAC modification is seen in handling fragmented packets with INSPECT on
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)
CSCwb15170	RM 1120 Port state going down, speed is 100/10 and duplex full/Half, speed and duplexmismatchpresent

Bug ID	Headline
CSCwb16561	FMC GUI does not load Intrusion Policies
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
CSCwb18252	FTD/ASA: Traceback on BFD function causing unexpected reboot
CSCwb19387	ASA SNMP Poll is failing & show display "Unable to honour this request now.Please try again later."
CSCwb19648	SNMP queries for crasLocalAddress are not returning the assigned IPs for SSL/DTLS tunnels.
CSCwb20940	FMC: Add validation checks for the combination of SSL/Snort3/NAP in Detection mode
CSCwb21704	FDM: Add validation checks for the combination of SSL/Snort3/NAP in Detection mode
CSCwb22359	Portmanager/LACP improvement to avoid false restarts and increase of logging events
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
CSCwb31699	Primary takes active role after reload
CSCwb32841	NAT (any,any) statements in-states the failover interface and resulting on Split Brain events
CSCwb33184	Memory leak in MessageService causes UI slowness
CSCwb33334	ASA: crash after sending some traffic over RAVPN tunnel
CSCwb34035	ASA CLI gets hung randomly while configuring SNMP
CSCwb35675	Snort3 is partially in sync with Snort 2 warning alert
CSCwb36256	Increase size of System cgroup so that more of available memory will be used
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
CSCwb40001	Long delays when executing SNMP commands
CSCwb41361	WR8, LTS18 and LTS21 commit id update in CCM layer (seq 26)

Bug ID	Headline
CSCwb41854	Cisco FTD Software and Cisco FXOS Software Command Injection Vulnerability
CSCwb42846	Snort instance CPU stuck at 100%
CSCwb43018	Implement SNP API to check ifc and ip belongs to HA LU or CMD interface
CSCwb43629	License and rule counts telemetry data incorrectly generated for HA managed devices
CSCwb46949	LTS18 commit id update in CCM layer (seq 27)
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
CSCwb57615	Configuring pbr access-list with line number failed.
CSCwb58007	CVE-2022-28199: Evaluation for FTDv and ASA v
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
CSCwb61901	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb61908	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb61919	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb65718	FMC is stuck on loading SI objects page
CSCwb66736	Multiple Cisco Products Snort SMB2 Detection Engine Policy Bypass and DoS Vulnerability
CSCwb66761	Cisco Firepower Threat Defense Software Generic Routing Encapsulation DoS Vulnerability
CSCwb67040	FP4112 4115 Traceback & reload on Thread Name: netfs_thread_init

Bug ID	Headline
CSCwb68642	ASA traceback in Thread Name: SXP CORE
CSCwb71460	ASA traceback in Thread Name: fover_parse and triggered by snmp related functions
CSCwb74357	FXOS is not rotating log files for partition opt_cisco_platform_logs
CSCwb74571	PBR not working on ASA routed mode with zone-members
CSCwb76129	Some SSL patterns not detected after VDB 356 or higher is installed
CSCwb80108	FP2100/FP1000: Built-in RJ45 ports randomly not coming up after portmanager restart events
CSCwb80192	WR6, WR8 commit id update in CCM layer(Seq 30)
CSCwb82796	ASA/FTD firewall may traceback and reload when tearing down IKE tunnels
CSCwb84638	Portmanager/LACP improvement to capture logging events on external event restarts
CSCwb85822	Deployment failing when collecting policies.
CSCwb86118	TPK ASA: Device might get stuck on ftp copy to disk
CSCwb87762	Multiple Cisco Products Snort SMB2 Detection Engine Policy Bypass and DoS Vulnerability
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
CSCwb89004	FMC DBcheck.pl hungs at "Checking mysql.rna_flow_stats_template against the current schema"
CSCwb89187	Flex Config allow - "timeout icmp-error hh:mm:ss"
CSCwb89963	ASA Traceback & reload in thread name: Datapath
CSCwb94170	merovingian.log file extremely big size can fill the disk
CSCwb95787	FPR1010 - No ARP on switchport VLAN interface after portmanager DIED event
CSCwc02133	Cisco FTD Software and Cisco FXOS Software Command Injection Vulnerability
CSCwc03507	No-buffer drops on Internal Data interfaces despite little evidence of CPU hog
CSCwc06833	Deployment failure with ERROR Process Manager failed to verify LSP ICDB
CSCwc08676	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 32)
CSCwc08683	The interface's LED remains green blinking when the optical fiber is unplugged on FPR1150

Bug ID	Headline
CSCwc10037	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwc12322	Digitally signed ASDM image verification error on FPR3100 platforms
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
CSCwc18218	Database files on disk grow larger than expected for some frequently updated tables
CSCwc25207	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 33)
CSCwc28334	Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
CSCwc28660	Snort3: NFSv3 mount may fail for traffic through FTD
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
CSCwc34818	The device is unregistered when Rest API calls script.
CSCwc35969	cannot add IP from event to global lists (block or do-not-block) if similar IP is already on list
CSCwc37061	SNMP: FMC doesn't reply to OID 1.3.6.1.2.1.25.3.3.1.2
CSCwc41590	Upgrade fail & App Instance fail to start with err "CSP_OP_ERROR. CSP signature verification error."
CSCwc41661	High disk usage due to process_stdout.log and process_stderr.log logrotate failure (deleted files)
CSCwc44289	FTD - Traceback and reload when performing IPv4 & IPv6 NAT translations
CSCwc44608	Selective deployment of IPS may cause outage due to incorrectly written FTD configuration files
CSCwc46569	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 34)
CSCwc50519	Excessive logging from hm_du.pm may lead to syslog-ng process restarts
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
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

Bug ID	Headline
CSCwc82188	FTD Traceback and reload when applying long capture commands from FMC UI
CSCwc83886	To get pre-committed tests passed for https://sp4-fp-swarm.cisco.com/reviews/3058043
CSCwd05814	PDTS write from Daq can fail when PDTS buffer is full eventually leads to block depletion
CSCwd24639	Functional: FMCv patch upgrade is fails
CSCwd49758	Pre-deployment failure seen in FMC due to huge number policies
CSCwd52995	FMC not opening deployment preview window
CSCwd53340	FTD PDTS LINA RX queue can become stuck when snort send messages with 4085-4096 bytes size
CSCwd66815	Lina changes to support - Snort3 traceback in daq-pdts while handling FQDN based traffic
CSCwd74116	S2S Tunnels do not come up due to DH computation failure caused by DSID Leak
CSCwd78123	ASA/FTD traceback and reload when IPSec/Ikev2 vpn session bringup with dh group 31 in fips mode

Resolved Bugs in Version 7.1.0.2

Version 7.1.0.2 is a limited release for the Secure Firewall 3100 and for the FMC. All bugs fixed in Version 7.1.0.1 (which was not available for the Secure Firewall 3100) are also fixed in Version 7.1.0.2. For the FMC, new online help is included in Version 7.1.0.2.

Resolved Bugs in Version 7.1.0.1

Table last updated: 2022-02-23

Table 30: Resolved Bugs in Version 7.1.0.1

Bug ID	Headline
CSCvz77254	Hotfix patch upgrade doesn't clean old snort3 binaries
CSCwa51862	LSP downloads fail when using proxy
CSCwa58060	LSP download fails if no ICMP reply is received from updates-talos.sco.cisco.com
CSCwa70008	Expired certs cause Security Intelligence updates to fail

Resolved Bugs in Version 7.1.0

Table last updated: 2022-08-01

Table 31: Resolved Bugs in Version 7.1.0

Bug ID	Headline
CSCvq26114	Cron jobs (Scheduled tasks) stop working if FMC is under constant ssh login attempt (DOS)
CSCvr11958	AWS FTD: Deployment failure with ERROR: failed to set interface to promiscuous mode
CSCvs37955	Confusing message about 'without removing the physical hardware' during Acknowledge Security Module
CSCvs44109	FMC: PPPoE password restrictions are too strict; should match the underlying code
CSCvs50538	Firewall engine should fall back on info from SSL handshake if SSL engine does not return a verdict
CSCvs73924	Chassis Mgr should say you cannot change AAA server when same protocol is configured for Auth
CSCvu12734	Watchdog traceback on both FTD and ASA devices at boot time
CSCvu23149	Backup generation in FMC fails due to corrupt SID_GID_ORD index in database table rule_opts
CSCvu97242	FTD 2100: Corefile and crashinfo might both be truncated and incomplete in the event of a crash
CSCvu98260	Stale route present on DRP database when HA is nsf enabled in specific scenario.
CSCvv24647	FTD 2100 - SNMP: incorrect values returned for Ethernet statistics polling
CSCvv40916	3 min delay caused by AbstractBaseDeploymentValidationHandler.validatePreApply during deploy.
CSCvv59676	Snort2: Implement aggressive pruning for certificate cache for TLS to free up memory
CSCvv87594	FXOS - jQuery vulnerabilities
CSCvv89715	Fastpath rules for Firepower 8000 series stack disappear randomly from the FMC
CSCvw22435	Error "No such file or directory" happened when using "copy ftp: workspace:" in FXOS 2.8.1
CSCvw30887	FXOS crashed due to HA policy of Reset with Service: bcm_usd hap reset
CSCvw62255	"Link not connected" error when using WSP-Q40GLR4L transceiver and Arista switch with Firepower 4100

Bug ID	Headline
CSCvw62435	AnyConnect Cannot Coexist in an Interface where Security Zone/Interface Group is Used by a VTI
CSCvw63283	The link in Cloud Services redirects user to NAM CTR portal even FTD is registered to EU or APJC
CSCvw67974	SSH access with public key authentication fails after FXOS upgrade
CSCvw77924	Radius Key with the ASCII character " configured on FXOS does not work after chassis reload.
CSCvw79465	FXOS upgrade does not do proper compatibility check for FTD image
CSCvw90634	FP2100 ASA - 1 Gbps SFP in network module down/down after upgrade to 9.15.1.1
CSCvw93159	Firepower 2100: ASA/FTD generates message "Local disk 2 missing on server 1/1"
CSCvw95181	FXOS upgrade fails with error "does not support application instances of deployment type container"
CSCvx04436	Forbidden to run multiple SFDaCo processes, but pidfile not successful at blocking second instance
CSCvx16317	Failure accessing FXOS with connect fxos admin from Multi-Context ASA if admin context is changed
CSCvx24555	Identity Policy rule validation may impact FMC performance
CSCvx26927	TLS site not loading when it has segmented and retransmitted CH
CSCvx27744	Policy deployment may fail on FTD after 6.6.1 due to failure to get version upgrade information
CSCvx32017	Smart License shows "Out of Compliance" but doesn't point which License Type
CSCvx33904	Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privilege escalation
CSCvx43150	On the FMC, process of registration of member device post RMA is not successful
CSCvx44283	Static route checking is too restrictive on FDM UI
CSCvx48862	Unable to save new cluster node configs on FCM due to java error
CSCvx54562	High System Overhead memory on FTD
CSCvx57417	Smart Tunnel Code signing certificate renewal
CSCvx62422	License page stuck for the devices in clustered_device table
CSCvx64683	White space characters in NAP portscan ignore_scanners field can cause FATAL snort crashes
CSCvx67856	FTD7.0: Prometheus process doesnt come up when system ungracefully rebooted

Bug ID	Headline
CSCvx68803	FMC (API) replies a 500 HTTP code instead of 400 due to a bad request
CSCvx70480	403 error when accessing Policies & Access Control after exporting User Role from FMC(4600) to FMCv
CSCvx75445	No option to create inline set with bypass standby on Firepower 2130
CSCvx75743	Inconsistent FMC audit log severity
CSCvx76665	Error messages "Updating Interface Status failed" seen on 2100 and 1010
CSCvx78238	multi context Firepower services on ASA traffic goes to incorrect interfaces
CSCvx80830	VPN conn fails from same user if Radius server sends a dACL and vpn-simultaneous-logins is set to 1
CSCvx82705	Evaluation of ssp for OpenSSL March 2021 vulnerabilities
CSCvx82957	Smart CLI taking much time to load.
CSCvx86177	inet6_ntoa and unix_timestamp Functions used to externally poll FMC database return errors
CSCvx89113	Object group with mix of IPv4/6 addresses not searchable while creating new object group
CSCvx89827	Not able to set Bangkok time zone in FPR 2110
CSCvx92932	Missing events on FMC due to SFDataCorrelator process exiting
CSCvx94732	Firepower Threat Defense (FTD) Health Monitor Alert - High unmanaged disk usage on /ngfw
CSCvx95652	ASAv Azure: Some or all interfaces might stop passing traffic after a certain period of run time
CSCvy01482	Realm Sync Results Page Hangs After Upgrade
CSCvy02240	Cisco Firepower Threat Defense Ethernet Industrial Protocol Policy Bypass Vulnerabilities
CSCvy02950	Need Stack and Cluster EO's history in TS
CSCvy03115	FDM UI crashed when we try to download deployable configuration
CSCvy03907	Creation/Edit of Access Control Policy fails with error 'Rule Name Already Exists'
CSCvy06393	UI failure when adding source feed
CSCvy07957	FMC - 'Open in context explorer' redirection/option cannot fetch data
CSCvy08351	Intrusion and Correlation Email Alerts stop being sent to mail server
CSCvy08908	Port-forwarding application blocked by Java

Bug ID	Headline
CSCvy10789	FTD 2110 ascii characters are disallowed in LDAP password
CSCvy13229	FDM - GUI Inaccessible - tomcat is opening too many file descriptors
CSCvy13543	Cisco Firepower Threat Defense Software SSH Connections Denial of Service Vulnerability
CSCvy14721	ssl traffic dropped by FTD while CH packet has a destination port no greater than source port
CSCvy15396	ClamAV downloads failing on the standby FMC produce overwhelming amount of logs in /var directory
CSCvy16004	Delay in DIFF calculations can cause deployment issues and HA App sync timeout in FTDs
CSCvy16559	Cisco Firepower Threat Defense Software Command Injection Vulnerabilities
CSCvy16573	Cisco Firepower Threat Defense Command Injection Vulnerability
CSCvy17030	FMC Connection Events page "Error: Unable to process this query. Please contact support."
CSCvy17365	REST API Login Page Issue
CSCvy19136	Web portal persistent redirects when certificate authentication is used.
CSCvy19453	SFDataCorrelator performance problems involving redundant new host events with only MAC addresses
CSCvy20605	Warning health alert should not be triggered while refreshing the diskmanager process
CSCvy21334	Active tries to send CoA update to Standby in case of "No Switchover"
CSCvy22765	Synchronization daemon exited. Syncd crashing. var/sf/tds/cloud-events.json is empty.
CSCvy23126	FMC upgrade to 6.6.1 failing on 800_post/097_upgrade_ssl_inspection.pl.log
CSCvy24435	FMC GUI can be accessed by an expired password when using .cgi with https://FMCIP/login.cgi
CSCvy24921	SNMPv3 - SNMP EngineID changes after every configuration change
CSCvy26511	Tune unmanaged disk alert thresholds for low end platforms
CSCvy30016	SSL decryption policy may cause performance degradation in Snort
CSCvy30101	snort2 memory usage can grow beyond expected limits when using ssl decryption
CSCvy30392	Backup generation on FMC fails due to corrupt int_id index in table ids_event_msg_map
CSCvy31400	FMC may disable autonegotiation for physical interfaces with 1Gbps SFP after FTD upgrade

Bug ID	Headline
CSCvy31424	QP FTD application fails to start due to outdated affinity.conf following FXOS/FTD upgrade
CSCvy31521	Add syslog-ng monitor to the FMC and NGIPS
CSCvy31793	ibdatafix.sh does not fail in unattended mode on backup if the backup runs out of disk space
CSCvy33044	Bad user session processing rate when floating at device user accounts limit
CSCvy33879	FTD: repair_users.pl creates rogue .firstboot file that causes FTD reboot failure
CSCvy34333	When ASA upgrade fails, version status is desynched between platform and application
CSCvy34941	false alarm 'Health monitoring severely behind schedule'
CSCvy35416	Deploy failure from global domain when parallel deploy triggered to different child domains
CSCvy36694	FTDv 6.7 on Azure is unable to set 1000 speed on GigabitEthernet interfaces
CSCvy37484	Entries in device_policy_ref is huge causing slow performance when opening DeviceManagement page
CSCvy38558	After upgrade to 6.6.1, Edit/Save in the BGP config throws Invalid scan time error
CSCvy39191	An internal server error 500 in T-ufin when doing API calls to the FMC
CSCvy39791	Lina traceback and core file size is beyond 40G and compression fails.
CSCvy41157	HA formation failing after restore
CSCvy41757	Cisco Firepower Threat Defense Software CLI Arbitrary File Write Vulnerability
CSCvy43349	Internal error thrown while adding an ACP as base for another ACP
CSCvy43447	FTD traceback and reload on Lic TMR Thread on Multi Instance FTD
CSCvy43911	FDM: OSPF Interface SmartCLI fails to save update and shows new fields on edit
CSCvy44566	FTD deployment failure during App config validation due to AQ memory consumption
CSCvy44752	Interface creation failed
CSCvy47786	Deployment preview will show unchanged/unadded comments to ACP rules
CSCvy47927	Unable to select multiple policies for scheduled firepower recommended rules
CSCvy48730	ASA/FTD may traceback and reload in Thread Name 'Unicorn Proxy Thread'
CSCvy48764	SSH access with public key authentication requires user password
CSCvy50009	Incorrect error reported when running installation readiness check

Bug ID	Headline
CSCvy52617	FMC6.7 changes IPSec Profiles on VTI with each deployment resulting in tunnel flap
CSCvy53301	HA Configuration fails on FDM with 'Internal error during deployment'
CSCvy55054	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS
CSCvy55676	FMC Deployment failed due to internal errors
CSCvy57905	VTI tunnel interface stays down post reload on KP/WM platform in HA
CSCvy59958	Continuous memory leak in the process hmlsd (SF::Messaging::smartSend)
CSCvy63463	Error deleting users due to special characters
CSCvy63464	FTD 1100/ 2100 series reboots with clock set to 2033
CSCvy65248	FTDv in Azure D5_v2 instance - Interface drops before CPU maxed out
CSCvy66065	Multiple Cisco Products Snort Rule Denial of Service Vulnerability
CSCvy66849	The device is unregistered when Rest API calls script run every 5 min
CSCvy66942	FPR4100/9300 IPv6 config cannot be applied using Rest API LTP on 9300/4100 Supervisor
CSCvy68166	Realm page is not loading after upgrade to 7.0
CSCvy68859	DB Conn not released with LSP and category filter in Intrusion rules
CSCvy68974	ActionQueue process is killed by OOM killer due to process utilizing more than 3 GB limit for memory
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
CSCvy71478	Delay in the response received for the request made to LINA using ASALinaCliUtilShow
CSCvy72118	High snort cpu usage while copying navl attribute - (Fragmented metadata)
CSCvy72185	FXOS Apache HTTP Server Multiple Vulnerabilities (CVE-2020-11993) and (CVE-2020-9490)
CSCvy73930	EventHandler deployment error due to syntax error due to special characters in AC rule name
CSCvy74984	ASAv on Azure loses connectivity to Metadata server once default outside route is used
CSCvy78573	cloudagent should not send zero-length urls to beaker for lookup
CSCvy79015	FMC 6.7 > 7.0 Upgrade failure on 800_post/800_manager_install_lsp.pl

Bug ID	Headline
CSCvy79186	Pull_Upgrade job stuck and blocking device upgrade
CSCvy82655	REST API - Bulk AC rules creation fails with 422 Unprocessable Entity
CSCvy83116	FTD 1000 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
CSCvy86780	Error Could not complete LSP installation. Please try again.
CSCvy86817	Cruz ASIC CLU filter has the incorrect src/dst IP subnet when a custom CCL IP subnet is set
CSCvy88381	INET6_NTOA(location_ip) fails when externally polling FMC Database
CSCvy89440	s2sCryptoMap Configuration Loss
CSCvy93480	Cisco ASA and FTD Software IKEv2 Site-to-Site VPN Denial of Service Vulnerability
CSCvy95329	Incorrect Access rule matching because of ac rule entry missing
CSCvy95554	Unable to download LDAP due to database MERGE failure on group_fsp_reference table
CSCvy96325	FTD/ASA: Adding new ACE entries to ACP causes removal and re-add of ACE elements in LINA
CSCvy96698	Resolve spurious status actions checking speed values twice in FXOS portmgr
CSCvy98027	Application interface down whereas physical interface Up on FXOS
CSCvy98458	FP21xx -traceback "Panic:DATAPATH-10-xxxx -remove_mem_from_head: Error - found a bad header"
CSCvy99373	ADI Session Processing Delays when resolving adSamAccountName with AD
CSCvz00254	FDM 6.7.0 to 7.0.0 Upgrade Failed due to invalid state for site to site VPN during upgrade import
CSCvz00934	Not able to configure VTI with tunnel source as (FMC Access) data-interface
CSCvz01766	Standby FDM's GUI is blank
CSCvz05468	Multiple SSH host entries in platform settings as first feature enable/deploy will break SSH on LINA
CSCvz05687	Fragmented Certificate request failed for DND flow
CSCvz05767	FP-1010 HA link goes down or New hosts unable to connect to the device
CSCvz05921	Auto-negotiation configuration checkbox option for 2100 SFP interfaces not available

Bug ID	Headline
CSCvz06848	Software upgrade on FDM-managed FTD fails due to snmp-server community validation failure
CSCvz12770	Policy Deployment failure at 0% due to clock-reset issues
CSCvz14616	No connection events due to SFDataCor process stuck
CSCvz14628	FMC 2500 upgraded to 6.6.5-78: in purging events database 'eventdb' down, manual intervention needed
CSCvz15676	In Firepower 1010 device, after upgrading ASA app, device going for fail safe mode
CSCvz15755	FTD - Port-channel not coming up after upgrade and may generate core file
CSCvz17046	ASAv crashed when tried to upgrade or reload the 16 node cluster setup
CSCvz17534	FTD Restore Backup CLI does not restore the VPN configuration
CSCvz18341	FMC: Peer/Device UUID in EM_peers table should be removed/cleaned upon executing remove_peers
CSCvz19634	FTD software upgrade may fail at 200_pre/505_revert_prep.sh
CSCvz20544	ASA/FTD may traceback and reload in loop processing Anyconnect profile
CSCvz20679	FTDv - Lina Traceback and reload
CSCvz26998	FMC REST API calls return http error code 500 when processes use same credentials
CSCvz28103	FDM: Saving DHCP relay config throws flex-config/smart CLI error
CSCvz28145	Error "Another operation by another user prevented this operation. Please retry after sometime."
CSCvz31184	Validation of unsupported flow-offload using pre-filter in passive/inline interfaces in FPR4100/9300
CSCvz32386	FTD Deployment error when FMC pushes PFS21 and IKEv1 settings on same crypto map entry
CSCvz33190	SecurityIntelligence URL feed - Failed to download SSL peer certificate or SSH remote key was not OK
CSCvz33468	ASA/FTD - NAT stops translating source addresses after changes to object-groups in manual NAT Rule
CSCvz34831	If ASA fails to download DACL it will never stop trying
CSCvz36862	FMC policy deployment takes more than 15 min on phase 3
CSCvz36933	Sensor SNMP process may restart when policy deploy
CSCvz38361	BGP packets dropped for non directly connected neighbors

Bug ID	Headline
CSCvz40098	FTD HA: Health Monitor page shows "Error in fetching device details Error: validation failed"
CSCvz46333	FTD policy deployment failure due to internal socket connection loss
CSCvz46680	FMC shows empty managed device inventory details and applied policy
CSCvz49289	FMC 6.6 connection events excluding port excludes protocol as well
CSCvz50270	Add a validation check on FMC GUI to validate the dynamic PAT rule modifications
CSCvz50712	TLS server discovery uses incorrect source IP address for probes in AnyConnect deployment
CSCvz51175	FTD HA not forming when SNMP adminState is disabled
CSCvz53372	Snort goes into D state after executing "config log-events-to-ramdisk disable"
CSCvz53606	Specify what changes to Security Zone objects are changing Security Zone UUID
CSCvz53993	Random packet block by Snort in SSL flow
CSCvz55302	FTD/ASA Traceback and reload due to SSL null checks under low memory conditions
CSCvz57917	High unmanaged disk usage on /ngfw filled with module-xxxx-x86_64.tgz files in packages folder
CSCvz59464	IPReputation Feed Error Message-Method Not Allowed
CSCvz61477	RAVPN Authorization fails if same RADIUS server is used as authentication and authorization server
CSCvz61767	Policy deployment with SNMPv2 or SNMPv1 configuration fails
CSCvz63444	FMC custom widgets keep polling and do not return any data
CSCvz64548	SFTunnel on device not processing event messages
CSCvz65181	Cisco Firepower Threat Defense Software Security Intelligence DNS Feed Bypass Vulnerabilit
CSCvz66506	Continuous ADI traceback and reload on FPR2100 registered to FMC HA
CSCvz71569	FTD Traceback & reload due to process ZeroMQ out of memory condition
CSCvz76745	SFDataCorrelator memory growth with cloud-based malware events
CSCvz77037	FMC user interface access may fail with SSL errors in mojo-server
CSCvz80981	SNMPv3 doesn't work for SFR modules running version 7.0
CSCvz81342	Diskmanager not pruning AMP File Capture files
CSCvz81934	Revert 'fix' introduced by CSCvx95884

Bug ID	Headline
CSCvz82433	Trying to query the FMC database via external DB access for intrusion events interface value missing
CSCvz85493	FTD backup.log increased size out of control to 50GB or more causing /ngfw to 100% full
CSCvz89545	SSL VPN performance degraded and significant stability issues after upgrade
CSCvz90654	FTD Failover unit does not join HA due to "HA state progression failed due to APP SYNC timeout"
CSCvz96462	IP Address 'in use' though no VPN sessions
CSCvz97196	Can't create Flexconfig Object with ldap-naming-attribute pager cause pager is block.
CSCwa20516	FMC policy deployment takes more than 14 min
CSCze92695	LDAP user password stored in the clear in /etc/sf/authconfig*.con...