Cisco Firepower Release Notes, Version 6.5.0

First Published: 2019-09-26

Last Modified: 2022-03-02

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 1

Welcome

This document contains critical and release-specific information.

Release Dates

Sometimes Cisco releases updated builds. In most cases, only the latest build for each platform is available on the Cisco Support & Download site. We *strongly* recommend you use the latest build. If you downloaded an earlier build, do not use it. For more information, see Resolved Issues in New Builds, on page 77.

Table 1: Version 6.5.0 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.5.0	123	2020-02-03	FMC/FMCv	FMC/FMCv
6.5.0	120	2019-10-08	—	—
6.5.0	115	2019-09-26	All devices	All devices

Table 2: Version 6.5.0 Patch Dates

Version	Build	Date	Platforms
6.5.0.5	95	2021-02-09	All
6.5.0.4	57	2020-03-02	All
6.5.0.3	30	2020-02-03	No longer available.
6.5.0.2	57	2019-12-19	All
6.5.0.1	35	2019-11-20	No longer available.

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 Firepower Management Center New Features by Release
- Cisco Firepower 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.

CHAPTER 2

Compatibility

For general compatibility information see:

- Cisco Firepower Compatibility Guide: Detailed compatibility information for all supported versions, including versions and builds of bundled operating systems and other components, as well as links to end-of-sale and end-of-life announcements for deprecated platforms.
- Cisco NGFW Product Line Software Release and Sustaining Bulletin: Support timelines for the Cisco Next Generation Firewall product line, including management platforms and operating systems.

For compatibility information for this version, see:

Firepower Management Center

The Firepower Management Center is a fault-tolerant, purpose-built network appliance that provides a centralized firewall management console. Firepower Management Center Virtual brings full firewall management functionality to virtualized environments.

Firepower Management Center

This release supports the following hardware FMC platforms:

- FMC 1600, 2600, 4600
- FMC 1000, 2500, 4500
- FMC 2000, 4000

We recommend you keep the BIOS and RAID controller firmware up to date. For more information, see the Cisco Firepower Compatibility Guide.

Firepower Management Center Virtual

This release supports the following FMCv public cloud implementations:

- Firepower Management Center Virtual for Amazon Web Services (AWS)
- Firepower Management Center Virtual for Microsoft Azure

This release supports the following FMCv on-prem/private cloud implementations:

- Firepower Management Center Virtual for Kernel-based virtual machine (KVM)
- Firepower Management Center Virtual for VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7

For supported instances, see the Cisco Firepower Management Center Virtual Getting Started Guide.

Firepower Devices

Cisco Firepower devices monitor network traffic and decide whether to allow or block specific traffic based on a defined set of security rules. Some Firepower devices run Firepower Threat Defense (FTD) software; some run NGIPS/ASA FirePOWER software. Some can run either—but not both at the same time.

Note These release notes list the supported devices for *this* release. Even if an older device has reached EOL and you can no longer upgrade, you can still manage that device with a newer FMC, up to a few versions ahead. Similarly, newer versions of ASDM can manage older ASA FirePOWER modules. For supported management methods, including backwards compatibility, see Manager-Device Compatibility, on page 5.

Table 3: Firepower Threat Defense in Version 6.5.0

FTD Platform	OS/Hypervisor	Additional Details
Firepower 1010, 1120, 1140, 1150 Firepower 2110, 2120, 2130, 2140	—	—
Firepower 4110, 4120, 4140, 4150 Firepower 4115, 4125, 4145 Firepower 9300 with SM-24, SM-36, SM-44 modules Firepower 9300 with SM-40, SM-48, SM-56 modules	FXOS 2.7.1.92 or later build	Upgrade FXOS first. To resolve issues, you may need to upgrade FXOS to the latest build. To help you decide, see the Cisco FXOS Release Notes, 2.7(1).
ASA 5508-X, 5516-X ASA 5525-X, 5545-X, 5555-X ISA 3000	—	Although you do not separately upgrade the operating system on these devices in FTD deployments, you should make sure you have the latest ROMMON image on the ISA 3000, ASA 5508-X and 5516-X. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.

FTD Platform	OS/Hypervisor	Additional Details
FTDv	Any of: • AWS: Amazon Web Services • Azure: Microsoft Azure • KVM: Kernel-based Virtual Machine • VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7	For supported instances, see the appropriate FTDv Getting Started guide.

Table 4: NGIPS/ASA FirePOWER in Version 6.5.0

NGIPS/ASA FirePOWER Platform	OS/Hypervisor	Additional Details
ASA 5508-X, 5516-X ISA 3000	ASA 9.5(2) to 9.16(x)	There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues. See the Cisco ASA Upgrade Guide for order of operations. You should also make sure you have the latest ROMMON image on the ISA 3000, ASA 5508-X and 5516-X. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.
ASA 5525-X, 5545-X, 5555-X	ASA 9.5(2) to 9.14(x)	
NGIPSv	VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7	For supported instances, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.

Manager-Device Compatibility

Firepower Management Center

All devices support remote management with the Firepower Management Center, which can manage multiple devices. The FMC must run the *same or newer* version as its managed devices. You *cannot* upgrade a device past the FMC. Even for maintenance (third-digit) releases, you must upgrade the FMC first.

A newer FMC can manage older devices up to a few major versions back, as listed in the following table. 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.

Table 5: FMC-Device Compatibility

FMC Version	Oldest Device Version You Can Manage
6.7.x	6.3.0
6.6.x	6.2.3
6.5.0	6.2.3
6.4.0	6.1.0
6.3.0	6.1.0
6.2.3	6.1.0

Firepower Device Manager and Cisco Defense Orchestrator

As an alternative to the FMC, many FTD devices support Firepower Device Manager and Cisco Defense Orchestrator management:

- Firepower Device Manager is built into FTD and can manage a single device.

  This lets you configure the basic features of the software that are most commonly used for small or mid-size networks.

- Cisco Defense Orchestrator (CDO) is cloud-based and can manage multiple FTD devices.

  This allows you to establish and maintain consistent security policies across your deployment without using the FMC. Although some configurations still require FDM, CDO allows you to establish and maintain consistent security policies across multiple FTD devices.

All FTD devices that support local management with the FDM also support CDO concurrently.

Table 6: FDM/CDO Compatibility with FTD

FTD Platform	FDM Compatibility	CDO Compatibility
Firepower 1000 series	6.4.0+	6.4.0+
Firepower 2100 series	6.2.1+	6.4.0+
Firepower 4100/9300	6.5.0+	6.5.0+
ASA 5500-X series	6.1.0 to 7.0.x	6.4.0 to 7.0.x
ISA 3000	6.2.3+	6.4.0+
FTDv for AWS	6.6.0+	6.6.0+
FTDv for Azure	6.5.0+	6.5.0+
FTDv for KVM	6.2.3+	6.4.0+
FTDv for VMware	6.2.2+	6.4.0+

Adaptive Security Device Manager

ASA with FirePOWER Services is an ASA firewall that runs Firepower NGIPS software as a separate application, also called the ASA FirePOWER module. You can use Cisco Adaptive Security Device Manager (ASDM) to manage both applications.

In most cases, newer ASDM versions are backwards compatible with all previous ASA versions. However, there are some exceptions. For example, ASDM 7.13(1) can manage an ASA 5516-X on ASA 9.10(1). ASDM 7.13(1) and ASDM 7.14(1) did not support ASA 5512-X, 5515-X, 5585-X, and ASASM; you must upgrade to ASDM 7.13(1.101) or 7.14(1.48) to restore ASDM support. For details, see Cisco ASA Compatibility.

A newer ASA FirePOWER module requires a newer version of ASDM, as listed in the following table.

Table 7: ASDM-ASA FirePOWER Compatibility

ASA FirePOWER Version	Minimum ASDM Version
6.7.x	7.15.1
6.6.x	7.14.1
6.5.0	7.13.1
6.4.0	7.12.1
6.3.0	7.10.1
6.2.3	7.9.2

Web Browser Compatibility

Browsers

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

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer 11 (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 or Microsoft Edge, nor do we test Microsoft Internet Explorer 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 Internet Explorer 11:

- For the **Check for newer versions of stored pages** browsing history option, choose **Automatically**.
- Disable the **Include local directory path when uploading files to server** custom security setting.
- Enable **Compatibility View** for the appliance IP address/URL.

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.

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:

- Firepower Management Center: Select **System** > **Configuration**, then click **HTTPS Certificates**.
- Firepower Device Manager: 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*.

Screen Resolution Requirements

Table 8: Screen Resolution Requirements

Interface	Resolution
Firepower Management Center	1280 x 720
Firepower Device Manager	1024 x 768
ASDM managing an ASA FirePOWER module	1024 x 768
Firepower Chassis Manager for the Firepower 4100/9300	1024 x 768

CHAPTER 3

Features and Functionality

Major releases contain new features, functionality, and enhancements. Major releases can also include deprecated features and platforms, menu and terminology changes, changed behavior, and so on.

Note These release notes list the new and deprecated features in *this* version, including any upgrade impact. If your upgrade skips versions, see Cisco Firepower Management Center New Features by Release and Cisco Firepower Device Manager New Features by Release for historical feature information and upgrade impact.

Features for Firepower Management Center Deployments

Note Version 6.6.0/6.6.x is the last release to support the Cisco Firepower User Agent software as an identity source. You cannot upgrade a Firepower Management Center with user agent configurations to Version 6.7.0+. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC). This will also allow you to take advantage of features that are not available with the user agent. To convert your license, contact your Cisco representative or partner contact.

For more information, see the End-of-Life and End-of-Support for the Cisco Firepower User Agent announcement and the Firepower User Identity: Migrating from User Agent to Identity Services Engine TechNote.

New Features in FMC Version 6.5.0

Table 9:

Feature	Description
Hardware and Virtual Appliances	
FTD on the Firepower 1150	We introduced the Firepower 1150.
Larger instances for FTDv for Azure	Firepower Threat Defense Virtual on Microsoft Azure now supports larger instances: D4_v2 and D5_v2.
FMCv 300 for VMware	We introduced the FMCv 300, a larger Firepower Management Center Virtual for VMware. It can manage up to 300 devices, compared to 25 devices for other FMCv instances. You can use the FMC model migration feature to switch to the FMCv 300 from a less powerful platform.
VMware vSphere/VMware ESXi 6.7 support	You can now deploy FMCv, FTDv, and NGIPSv virtual appliances on VMware vSphere/VMware ESXi 6.7.
Firepower Threat Defense	
Firepower 1010 hardware switch support	The Firepower 1010 now supports setting each Ethernet interface to be a switch port or a firewall interface. New/modified pages: • **Devices** > **Device Management** > **Interfaces** • **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** • **Devices** > **Device Management** > **Interfaces** > **Add VLAN Interface** Supported platforms: Firepower 1010
Firepower 1010 PoE+ support on Ethernet 1/7 and Ethernet 1/8	The Firepower 1010 now supports Power over Ethernet+ (PoE+) on Ethernet 1/7 and Ethernet 1/8. New/modified pages: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** > **PoE** Supported platforms: Firepower 1010
Carrier-grade NAT enhancements	For carrier-grade or large-scale PAT, you can allocate a block of ports for each host, rather than have NAT allocate one port translation at a time (see RFC 6888). New/modified pages: **Devices** > **NAT** > add/edit FTD NAT policy > add/edit NAT rule **>** **PAT Pool** tab **>** **Block Allocation** option Supported platforms: FTD

Feature	Description
TLS crypto acceleration for multiple container instances on Firepower 4100/9300	TLS crypto acceleration is now supported on multiple container instances (up to 16) on a Firepower 4100/9300 chassis. Previously, you could enable TLS crypto acceleration for only *one* container instance per module/security engine. New instances have this feature enabled by default. However, the upgrade does *not* enable acceleration on existing instances. Instead, use the **create hw-crypto** and **scope hw-crypto** CLI commands. For more information, see the Cisco Firepower 4100/9300 FXOS Command Reference. New FXOS CLI commands: • **create hw-crypto** • **delete hw-crypto** • **scope hw-crypto** • **show hw-crypto** Removed FXOS CLI commands: • **show hwCrypto** (replaced by **show hw-crypto**) • **config hwCrypto** Removed FTD CLI commands: • **show crypto accelerator status** Supported platforms: Firepower 4100/9300
Security Policies	
Access control rule filtering	You can now filter access control rules based on search criteria. New/modified pages: **Policies** > **Access Control** > **Access Control** > add/edit policy > filter button ('show only rules matching filter criteria') Supported platforms: FMC
Dispute URL category or reputation	You can now dispute the category or reputation of a URL. New/modified pages: • **Analysis** > **Connection Events** > right-click a category or reputation > **Dispute**. • **Analysis** > **Advanced** > **URL** > search for URL > **Dispute** button • **System** > **Integration** > **Cloud Services** > **Dispute** link Supported platforms: FMC

Feature	Description
User control with destination-based Security Group Tags (SGT)	You can now use ISE SGT tags for both source and destination matching criteria in access control rules. SGT tags are tag-to-host/network mappings obtained by ISE. New connection event fields: • Destination SGT (syslog: DestinationSecurityGroupTag): SGT attribute for the connection responder. Renamed connection event fields: • Source SGT (syslog: SourceSecurityGroupTag): SGT attribute for the connection initiator. Replaces Security Group Tag (syslog: SecurityGroup). New/modified pages: **System** > **Integration** > **Identity Sources** > **Identity Services Engine** > Subscribe to **Session Directory Topic** and **SXP Topic** options Supported platforms: Any
Cisco Firepower User Agent Version 2.5 integration	We released Version 2.5 of the Cisco Firepower User Agent, which you can integrate with Firepower Versions 6.4.0 through 6.6.x. **Note** Version 6.6.0/6.6.x is the last release to support the Cisco Firepower User Agent software as an identity source. You cannot upgrade a Firepower Management Center with user agent configurations to Version 6.7.0+. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC). This will also allow you to take advantage of features that are not available with the user agent. To convert your license, contact your Cisco representative or partner contact. For more information, see the End-of-Life and End-of-Support for the Cisco Firepower User Agent announcement and the Firepower User Identity: Migrating from User Agent to Identity Services Engine TechNote. New/modified FMC CLI commands: **configure user-agent** Supported platforms: FMC
Event Logging and Analysis	

Feature	Description
Threat Intelligence Director priorities.	TID blocking/monitoring observable actions now have priority over blocking/monitoring with Security Intelligence Block lists. If you configure the **Block** TID observable action, even if the traffic also matches a Security Intelligence Block list set to **Block**: • The Security Intelligence category in the connection event is a variant of `TID Block`. • The system generates a TID incident with an action taken of `Blocked`. If you configure the **Monitor** TID observable action, even if the traffic also matches a Security Intelligence Block list set to **Monitor**: • The Security Intelligence category in the connection event is a variant of `TID Monitor` • The system generates a TID incident with an action taken of `Monitored`. Previously, in each of these cases, the system reported the category by analysis and did not generate a TID incident. **Note** The system still effectively handles traffic as before. Traffic that was blocked before is still blocked, and monitored traffic is still monitored. This simply changes which component gets the 'credit.' You may also see more TID incidents generated. For complete information on system behavior when you enable both Security Intelligence and TID, see the *TID-Firepower Management Center Action Prioritization* information in the Firepower Management Center Configuration Guide. Supported platforms: FMC
'Packet profile' CLI commands	You can now use the FTD CLI to obtain statistics on how the device handled network traffic. That is, how many packets were fastpathed by a prefilter policy, offloaded as a large flow, fully evaluated by access control (Snort), and so on. New FTD CLI commands: • **asp packet-profile** • **no asp packet-profile** • **show asp packet-profile** • **clear asp packet-profile** Supported platforms: FTD

Feature	Description
Additional event types for Cisco SecureX threat response	Firepower can now send file and malware events to Cisco SecureX threat response, as well as high priority connection events — those related to intrusion, file, malware, and Security Intelligence events. Note that the FMC web interface refers to this offering as *Cisco Threat Response (CTR)*. New/modified pages: **System > Integration > Cloud Services**. Supported platforms: FTD (via syslog or direct integration) and Classic (via syslog) devices
Administration and Troubleshooting	
Precision Time Protocol (PTP) configuration for ISA 3000 devices.	You can use FlexConfig to configure the Precision Time Protocol (PTP) on ISA 3000 devices. PTP is a time-synchronization protocol developed to synchronize the clocks of various devices in a packet-based network. The protocol is designed specifically for industrial, networked measurement and control systems. We now allow you to include the **ptp** (interface mode) command, and the global commands **ptp mode e2etransparent** and **ptp domain**, in FlexConfig objects. New/modified commands: **show ptp** Supported platforms: ISA 3000 with FTD
Configure more domains (multitenancy)	When implementing multitenancy (segment user access to managed devices, configurations, and events), you can create up to 100 subdomains under a top-level Global domain, in two or three levels. The previous maximum was 50 domains. Supported platforms: FMC
ISE Connection Status Monitor enhancements	The ISE Connection Status Monitor health module now alerts you to issues with TrustSec SXP (SGT Exchange Protocol) subscription status. Supported platforms: FMC
Regional clouds	**Upgrade impact.** If you use the Cisco Threat Response integration, Cisco Support Diagnostics, or Cisco Success Network features, you can now select a regional cloud. By default, the upgrade assigns you to the US (North America) region. New/modified pages: **System** > **Integration** > **Cloud Services** Supported platforms: FMC, FTD

Feature	Description
Cisco Support Diagnostics	**Upgrade impact.** *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. For more information, see Sharing Data with Cisco, on page 32. In Version 6.5.0, Cisco Support Diagnostics support is limited to select platforms. New/modified pages: • **System > Smart Licenses** • **System > Smart Licenses > Register** Supported platforms: FMC, Firepower 4100/9300, FTDv for Azure
FMC model migration	You can now use the backup and restore feature to migrate configurations and events between FMCs, even if they are not the same model. This makes it easier to replace FMCs due to technical or business reasons such as a growing organization, migration from a physical to a virtual implementation, hardware refresh, and so on. In general, you can migrate from a lower-end to a higher-end FMC, but not the reverse. Migration from KVM and Microsoft Azure is not supported. You must also unregister and reregister with Cisco Smart Software Manager (CSSM). For details, including supported target and destination models, see the Firepower Management Center Model Migration Guide. Supported platforms: FMC
Security and Hardening	
Secure erase for appliance components on FXOS-based FTD devices	You can now use the FXOS CLI to securely erase a specified appliance component. New FXOS CLI commands: **erase secure** Supported platforms: Firepower 1000/2000 and Firepower 4100/9300

Feature	Description
Stricter password requirements for FMC `admin` accounts during initial setup	FMC initial setup now requires that you choose a 'strong' password for `admin` accounts. The setup process applies this strong password to both the FMC web interface and CLI `admin` accounts. **Note** Upgrading to Version 6.5.0+ does not force you to change weak passwords to strong passwords. With the exception of LOM users on physical FMCs (and this does include the `admin` user), you are not prohibited from choosing a new weak password. However, we do recommend that all Firepower user accounts — especially those with Admin access — have strong passwords. Supported platforms: FMC
Concurrent user session limits	You can now limit the number of users that can be logged into the FMC at the same time. You can limit concurrent sessions for users with read only roles, read/write roles, or both. Note that CLI users are limited by the read/write setting. New/modified pages: **System > Configuration > User Configuration > Max Concurrent Sessions Allowed** options Supported platforms: FMC
Authenticated NTP servers	You can now configure secure communications between the FMC and NTP servers using SHA1 or MD5 symmetric key authentication. For system security, we recommend using this feature. New/modified pages: **System > Configuration > Time Synchronization** Supported platforms: FMC
Usability and Performance	

Feature	Description
Improved initial configuration experience	On new and reimaged FMCs, a wizard replaces the previous initial setup process. If you use the GUI wizard, when initial setup completes, the FMC displays the device management page so that you can immediately begin licensing and setting up your deployment. The setup process also automatically schedules the following: • Software downloads. The system creates a weekly scheduled task to download (but not install) software patches and publicly available hotfixes that apply to your deployment. • FMC configuration-only backups. The system creates a weekly scheduled task to back up FMC configurations and store them locally. • GeoDB updates. The system enables weekly geolocation database updates. These tasks are scheduled in UTC, which means that when they occur *locally* depends on the date and your specific location. Also, because tasks are scheduled in UTC, they do not adjust for Daylight Saving Time, summer time, or any such seasonal adjustments that you may observe in your location. If you are affected, scheduled tasks occur one hour "later" in the summer than in the winter, according to local time. **Note** We *strongly* recommend you review the auto-scheduled tasks/GeoDB updates and adjust them if necessary. Upgraded FMCs are not affected. For details on the initial configuration wizard, see the *Getting Started Guide* for your FMC model; for details on scheduled tasks, see the Firepower Management Center Configuration Guide. Supported platforms: FMC
Light theme	**Beta.** The FMC web interface defaults to the Classic theme, but you can also choose a new Light theme. **Note** The Light theme is a Beta feature. You may see misaligned text or other UI elements. In some cases, you may also experience slower-than-normal response times. If you encounter issues that prevent you from using a page or feature, switch back to the Classic theme. Although we cannot respond to everybody, we also welcome feedback — please use the feedback link on the User Preferences page or contact us at fmc-light-theme-feedback@cisco.com">. New/modified pages: **User Preferences**, from the drop-down list under your username Supported platforms: FMC

Feature	Description
Usability enhancements for viewing objects	We have enhanced 'view object' capabilities for network, port, VLAN, and URL objects, as follows: • In the access control policy and while configuring FTD routing, you can right-click an object and choose **View Objects** to display details about that object. • When you are viewing details about an object, or when you are browsing objects in the object manager, clicking **Find Usage** (🔍) now allows you to drill down into object groups and nested objects. New/modified pages: • **Objects** > **Object Management** > choose a supported object type > **Find Usage** (🔍) • **Policies** > **Access Control** > **Access Control** > create or edit policy > create or edit rule > choose a supported condition type > right-click an object > **View Objects** • **Devices** > **Device Management** > edit FTD device > **Routing** > right-click a supported object > **View Objects** Supported platforms: FMC
Usability enhancements for deploying configuration changes	We streamlined the display of errors and warnings related to deploying configuration changes. Instead of an immediate verbose view, you can now **Click to view all details** to see more information about a particular error or warning. New/modified pages: **Errors and Warnings for Requested Deployment** dialog box Supported platforms: FMC
Usability enhancements to FTD NAT policy management	When configuring FTD NAT, you can now: • View warnings and errors in your NAT policy, by device. Warnings and errors mark configurations that could adversely affect traffic flow or prevent the policy from deploying. • Display up to 1000 NAT rules per page. The default is 100. New/modified pages: **Devices** > **NAT** > create or edit FTD NAT policy > **Show Warnings** and **Rules Per Page** options Supported platforms: FTD
Firepower Management Center REST API	

Feature	Description
New REST API capabilities	Added the following REST API objects to support Version 6.5.0 features: • cloudregions: Regional clouds Added the following REST API objects to support older features: • categories: Categories for access control rules • domain, inheritancesettings: Domains and policy inheritance • prefilterpolicies, prefilterrules, tunneltags: Prefilter policies • vlaninterfaces: VLAN interfaces Supported platforms: FMC

Deprecated Features in FMC Version 6.5.0

Table 10:

Feature	Upgrade Impact	Description
Ability to disable the Firepower Management Center CLI	None.	Version 6.3.0 introduced the Firepower Management Center CLI, which you had to explicitly enable. In Version 6.5.0, the CLI is automatically enabled, for both new and upgraded deployments. If you want to access the Linux shell (also called *expert mode*), you must log in to the CLI and then use the **expert** command. **Caution** We recommend you do not access Firepower appliances using the shell, unless directed by Cisco TAC. Deprecated options: **System** > **Configuration** > **Console Configuration** > **Enable CLI access** check box
MD5 authentication algorithm and DES encryption for SNMPv3 users (deprecated)	None, but you should switch now.	Version 6.5.0 deprecates the MD5 authentication algorithm and DES encryption for SNMPv3 users on Firepower Threat Defense. Although these configurations continue to work post-upgrade, the system displays a warning when you deploy. And, you cannot create new users or edit existing users with these options. Support will be removed in a future release. If you are still using these options in your platform settings policy, we recommend you switch to stronger options now. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Users**

Feature	Upgrade Impact	Description
TLS 1.0 & 1.1	Client may fail to connect with an upgraded appliance.	To enhance security: • Captive portal (active authentication) has removed support for TLS 1.0. • Host input has removed support for TLS 1.0 and TLS 1.1. If your client fails to connect with a Firepower appliance, we recommend you upgrade your client to support TLS 1.2.
TLS crypto acceleration FXOS CLI commands for Firepower 4100/9300	None.	As part of allowing TLS crypto acceleration for multiple container instances on Firepower 4100/9300, we removed the following FXOS CLI commands: • **show hwCrypto** • **config hwCrypto** And this FTD CLI command: • **show crypto accelerator status** For information on their replacements, see the new feature documentation.
Cisco Security Packet Analyzer integration	None, but integration is no longer supported.	Version 6.5.0 ends support for Firepower Management Center integration with Cisco Security Packet Analyzer. Deprecated screens/options: • **System** > **Integration** > **Packet Analyzer** • **Analysis** > **Advanced** > **Packet Analyzer Queries** • **Query Packet Analyzer** when right-clicking on an event in the dashboard or event viewer
Default HTTPS server certificates	None.	If you are upgrading from Version 6.4.0.9+, the *default* HTTPS server certificate's lifespan-on-renew returns to 3 years, but this is again updated to 800 days in Version 6.6.0+. Your current default HTTPS server certificate is set to expire depending on when it was generated, as follows: • 6.4.0.9 and later patches: 800 days • 6.4.0 to 6.4.0.8: 3 years • 6.3.0 and all patches: 3 years • 6.2.3: 20 years

Feature	Upgrade Impact	Description
Firepower Management Center models FMC 750, 1500, 3500	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower Management Center software on the FMC 750, FMC 1500, and FMC 3500. You cannot manage Version 6.5.0+ devices with these Firepower Management Centers.
ASA 5515-X and ASA 5585-X series devices with Firepower software	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower software (both Firepower Threat Defense and ASA FirePOWER) on ASA 5515-X and ASA 5585-X series devices (SSP-10, -20, -40, and -60).
Firepower 7000/8000 series devices	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower software on Firepower 7000/8000 series devices, including AMP models.

Features for Firepower Device Manager Deployments

New Features in FDM Version 6.5.0

Feature	Description
FDM support for the Firepower 4100/9300.	You can now use FDM to configure FTD on the Firepower 4100/9300. Only native instances are supported; container instances are not supported.
FDM support for FTDv for the Microsoft Azure Cloud.	You can configure on FTDv for the Microsoft Azure Cloud using FDM.
Support for the Firepower 1150.	We introduced the FTD for the Firepower 1150.
Firepower 1010 hardware switch support, PoE+ support.	The Firepower 1010 supports setting each Ethernet interface to be a switch port or a regular firewall interface. Assign each switch port to a VLAN interface. The Firepower 1010 also supports Power over Ethernet+ (PoE+) on Ethernet1/7 and Ethernet 1/8. The default configuration now sets Ethernet1/1 as outside, and Ethernet1/2 through 1/8 as switch ports on the inside VLAN1 interface. Upgrading to version 6.5 retains the existing interface configuration.
Interface scan and replace.	An interface scan detects any added, removed, or restored interfaces on the chassis. You can also replace an old interface with a new interface in the configuration, making interface changes seamless.
Improved interfaces display.	The **Device** > **Interfaces** page has been reorganized. There are now separate tabs for physical interfaces, bridge groups, EtherChannels, and VLANs. For any given device model, only those tabs relevant for the model are shown. For example, the VLANs tab is available on the Firepower 1010 model only. In addition, the lists provide more detailed information about the configuration and usage of each interface.

Feature	Description
ISA 3000 new default configuration.	The ISA 3000 default configuration has changed so that: • All interfaces are bridge group members in BVI1, which is unnamed so it does not participate in routing • GigabitEthernet1/1 and 1/3 are outside interfaces, and GigabitEthernet1/2 and 1/4 are inside interfaces • Hardware bypass is enabled for each inside/outside pair, when available • All traffic is allowed from inside to outside, and outside to inside Upgrading to version 6.5 retains the existing interface configuration.
Support ends for the ASA 5515-X. The last supported release is FTD 6.4.	You cannot install FTD 6.5 on an ASA 5515-X. The last supported release for the ASA 5515-X is FTD 6.4.
Support for Common Industrial Protocol (CIP) and Modbus application filtering in access control rules on Cisco ISA 3000 devices.	You can enable the Common Industrial Protocol (CIP) and Modbus preprocessors on Cisco ISA 3000 devices, and filter on CIP and Modbus applications in access control rules. All CIP application names start with “CIP,” such as CIP Write. There is only one application for Modbus. To enable the preprocessors, you must go into expert mode in a CLI session (SSH or Console) and issue the **sudo /usr/local/sf/bin/enable_scada.sh {cip | modbus | both}** command. You must issue this command after every deployment, as deployment turns off the preprocessors.
Precision Time Protocol (PTP) configuration for ISA 3000 devices.	You can use FlexConfig to configure the Precision Time Protocol (PTP) on ISA 3000 devices. PTP is a time-synchronization protocol developed to synchronize the clocks of various devices in a packet-based network. The protocol is designed specifically for industrial, networked measurement and control systems. We now allow you to include the **ptp** and **igmp** (interface mode) commands, and the global commands **ptp mode e2etransparent** and **ptp domain**, in FlexConfig objects. We also added the **show ptp** command to the FTD CLI.
EtherChannel (port channel) interfaces.	You can configure EtherChannel interfaces, which are also known as port channels. **Note** You can only add EtherChannels in FDM to the Firepower 1000 and 2100 series. The Firepower 4100/9300 supports EtherChannels, but you must perform all hardware configuration of EtherChannels in FXOS on the chassis. Firepower 4100/9300 EtherChannels appear in the FDM **Interfaces** page alongside single physical interfaces. We updated the **Device** > **Interfaces** page to allow the creation of EtherChannels.

Feature	Description
Ability to reboot and shut down the system from FDM.	You can now reboot or shut down the system from the new **Reboot/Shutdown** system settings page. Previously, you needed to issue the **reboot** and **shutdown** commands through the CLI Console in FDM or from an SSH or console session. You must have Administrator privileges to use these commands.
Support for the **failover** command in the FDM CLI Console.	You can now issue the **failover** command in the FDM CLI Console.
Service Level Agreement (SLA) Monitor for static routes.	Configure Service Level Agreement (SLA) Monitor objects for use with static routes. By using an SLA monitor, you can track the health of a static route and automatically replace a failed route with a new one. We added **SLA Monitors** to the **Objects** page, and updated static routes so you can select the SLA Monitor object.
Routing changes in Smart CLI and the FTD API.	This release includes some changes to routing configuration in Smart CLI and the FTD API. In previous releases, there was a single Smart CLI template for BGP. Now, there are separate templates for BGP (the routing process configuration) and BGP General Settings (global settings). In the FTD API, the paths for all methods have changed, with "/virtualrouters" inserted in the paths, with the exception of the new BGP general settings methods. • The path for static route methods was /devices/default/routing/{parentId}/staticrouteentries, and it is now /devices/default/routing/virtualrouters/default/staticrouteentries. • BGP methods were split into two new paths: /devices/default/routing/bgpgeneralsettings and /devices/default/routing/virtualrouters/default/bgp. • OSPF paths are now /devices/default/routing/virtualrouters/default/ospf and /devices/default/routing/virtualrouters/default/ospfinterfacesettings. If you are using the FTD API to configure any routing process, please examine your calls and correct as necessary.

Feature	Description
New URL category and reputation database.	The system uses a different URL database, from Cisco Talos. The new database has some differences in URL categories. Upon upgrade, if any access control or SSL decryption rules use categories that no longer exist, the system will replace the category with an appropriate new category. To make the change effective, deploy the configuration after upgrade. The pending changes dialog will show details about the category changes. You might want to examine your URL filtering policies to verify that they continue to provide the desired results. We also added a URL lookup feature to the URL tabs in the access control and SSL decryption policies, and on the **Device** > **System Settings** > **URL Filtering Preferences** page. You can use this feature to check which category a particular URL is assigned to. If you disagree, there is also a link to submit a category dispute. Both of these features take you to an external web site, which will provide detailed information about the URL.
Security Intelligence uses the IP address reputation for URL requests that use IP addresses instead of hostnames.	If an HTTP/HTTPS request is to a URL that uses an IP address instead of a hostname, the system looks up the IP address reputation in the network address lists. You do not need to duplicate IP addresses in the network and URL lists. This makes it harder for end users to use proxies to avoid Security Intelligence reputation blocking.
Support for sending connection and high-priority intrusion, file, and malware events to the Cisco Cloud.	You can send events to the Cisco cloud server. From there, various Cisco cloud services can access the events. You can then use these cloud applications, such as Cisco Threat Response, to analyze the events and to evaluate threats that the device might have encountered. When you enable this service, the device will send connection and high-priority intrusion, file, and malware events to the Cisco cloud. We renamed the Cisco Threat Response item on **Device** > **System Settings** > **Cloud Services** to “Send Events to the Cisco Cloud.”
Cisco Cloud Services region support.	You are now asked to select the Cisco Cloud Services region when you register with smart licensing. This region is used for Cisco Defense Orchestrator, Cisco Threat Response, Cisco Success Network, and any cloud feature that goes through the Cisco Cloud. If you upgrade a registered device from a previous release, you are automatically assigned to the US Region; you must unregister from Smart Licensing, then reregister and select a new region, if you need to change regions. We added a step to the license registration process on the Smart License page and in the initial device setup wizard. You can also see the region on the **Device** > **System Settings** > **Cloud Services** page.

Feature	Description
FTD REST API version 4 (v4).	The FTD REST API for software version 6.5 has been incremented to version 4. You must replace v1/v2/v3 in the API URLs with v4. The v4 API includes many new resources that cover all features added in software version 6.5. Please re-evaluate all existing calls, as changes might have been mode to the resource models you are using. To open the API Explorer, where you can view the resources, log into FDM, then click the more options button (⋮) and choose **API Explorer**.
FTD API support for TrustSec security groups as matching criteria for source and destination in access control rules.	You can use the FTD API to configure access control policy rules that use TrustSec security groups for source or destination traffic matching criteria. The system downloads the list of security group tags (SGTs) from ISE. You can configure the system to listen for SXP updates to obtain static SGT-to-IP address mappings. You can view the list of downloaded tags using the GET /object/securitygrouptag method, and create dynamic objects for one or more tags using the SGTDynamicObject resource. It is the dynamic objects that you can use in access control rules to define traffic matching criteria based on source or destination security group. Note that any changes you make to the ISE object or access control rules related to security group are preserved if you edit those objects in FDM. However, you cannot see the security group criteria in an access rule if you edit the rule in FDM. If you configure security-group-based access rules using the API, please be careful when subsequently editing rules in the access control policy using FDM. We added or modified the following FTD API resources: AccessRule (sourceDynamicObjects and destinationDynamicObjects attributes), IdentityServicesEngine (subscribeToSessionDirectoryTopic and subscribeToSxpTopic attributes), SecurityGroupTag, SGTDynamicObject. We added source and destination security group tag and name as columns in Event Viewer.
Configuration import/export using the FTD API.	You can use the FTD API to export the device configuration and to import a configuration file. You can edit the configuration file to change values, such as the IP addresses assigned to interfaces. Thus, you can use import/export to create a template for new devices, so that you can quickly apply a baseline configuration and get new devices online more quickly. You can also use import/export to restore a configuration after you reimage a device. Or you can simply use it to distribute a set of network objects or other items to a group of devices. We added the ConfigurationImportExport resources and methods (/action/configexport, /jobs/configexportstatus, /action/downloadconfigfile, /action/uploadconfigfile, /action/configfiles, /action/configimport, /jobs/configimportstatus).

Feature	Description
Creation and selection of custom file policies.	You can use the FTD API to create custom file policies, and then select these policies on access control rules using FDM. We added the following FTD API FileAndMalwarePolicies resources: filepolicies, filetypes, filetypecategories, ampcloudconfig, ampservers, and ampcloudconnections. We also removed two pre-defined policies, “Block Office Document and PDF Upload, Block Malware Others” and “Block Office Documents Upload, Block Malware Others.” If you are using these policies, during upgrade they are converted to user-defined policies so that you can edit them.
Security Intelligence DNS policy configuration using the FTD API.	You can configure the Security Intelligence DNS policy using the FTD API. This policy does not appear in FDM. We added the following SecurityIntelligence resources: domainnamefeeds, domainnamegroups, domainnamefeedcategories, securityintelligencednspolicies.
Remote access VPN two-factor authentication using Duo LDAP.	You can configure Duo LDAP as the second authentication source for a remote access VPN connection profile to provide two-factor authentication using Duo passcode, push notification, or phone call. Although you must use the FTD API to create the Duo LDAP identity source object, you can use FDM to select that object as the authentication source for the RA VPN connection profile. We added the duoldapidentitysources resource and methods to the FTD API.
FTD API support for LDAP attribute maps used in authorizing remote access VPN connections.	You can augment LDAP authorization for remote access VPN using custom LDAP attribute maps. An LDAP attribute map equates customer-specific LDAP attribute names and values with Cisco attribute names and values. You can use these mappings to assign group policies to users based on LDAP attribute values. You can configure these maps using the FTD API only; you cannot configure them using FDM. However, if you set these options using the API, you can subsequently edit the Active Directory identity source in FDM and your settings are preserved. We added or modified the following FTD API object models: LdapAttributeMap, LdapAttributeMapping, LdapAttributeToGroupPolicyMapping, LDAPRealm, LdapToCiscoValueMapping, LdapToGroupPolicyValueMapping, RadiusIdentitySource.

Feature	Description
FTD API support for site-to-site VPN connection reverse route injection and security association (SA) lifetime.	You can use the FTD API to enable reverse route injection for a site-to-site VPN connection. Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. By default, static RRI, where routes are added when you configure the connection is enabled. Dynamic RRI, where routes are inserted only when the security association (SA) is established, and then are deleted when the SA is torn down, is disabled. Note that dynamic RRI is supported for IKEv2 connections only. You can also set the security association (SA) lifetime (in seconds or in kilobytes transmitted) for the connection. You can also set an unlimited lifetime. The default lifetimes are 28,800 seconds (eight hours) and 4,608,000 kilobytes (10 megabytes per second for one hour). When the lifetime is reached, the endpoints negotiate a new security association and secret key. You cannot configure these features using FDM. However, if you set these options using the API, you can subsequently edit the connection profile in FDM and your settings are preserved. We added the following attributes to the SToSConnectionProfile resource: dynamicRRIEnabled, ipsecLifetimeInSeconds, ipsecLifetimeInKiloBytes, ipsecLifetimeUnlimited, rriEnabled.
Support for Diffie-Hellman groups 14, 15, and 16 in IKE policies.	You can now configure IKEv1 policies to use DH group 14, and IKEv2 policies to use DH groups 14, 15, and 16. If you are using IKEv1, please upgrade all your policies to DH group 14, as groups 2 and 5 will be removed in a future release. In addition, you should avoid using DH group 24 in IKEv2 policies, and MD5 in any IKE version, as these will also be removed in a future release.
Performance improvements when deploying changes.	If you add, edit, or delete access control rules, the system has been enhanced to deploy your changes more quickly than was done in previous releases. For systems configured in a high availability group for failover, the process for synchronizing the deployed changes to the standby device has been improved so that the synchronization completes more quickly.
Improved CPU and memory usage calculations on the System dashboard.	The method for calculating CPU and memory usage has been improved so that the information shown on the System dashboard more accurately reflects the actual state of the device.
When upgrading to FTD 6.5, historical report data is no longer available.	When you upgrade an existing system to FTD 6.5, historical report data will not be available due to a database schema change. Thus, you will not see usage data in the dashboards for times prior to the upgrade.

Deprecated Features in FDM Version 6.5.0

Table 11:

Feature	Upgrade Impact	Description
Default HTTPS server certificates	None.	If you are upgrading from Version 6.4.0.9+, the *default* HTTPS server certificate's lifespan-on-renew returns to 3 years, but this is again updated to 800 days in Version 6.6.0+. Your current default HTTPS server certificate is set to expire depending on when it was generated, as follows: • 6.4.0.9 and later patches: 800 days • 6.4.0 to 6.4.0.8: 3 years • 6.3.0 and all patches: 3 years • 6.2.3: 20 years
Manually uploading VDB, GeoDB, and SRU updates	None, but feature is deprecated until you upgrade to Version 6.6.0+.	Version 6.5.0 does not support manually uploading VDB, GeoDB, and SRU updates to the device. This feature *is* supported in Version 6.4.0.10 and later patches, and in Version 6.6.0+. If you are running Version 6.4.0.10 or later patch, we recommend you upgrade directly to Version 6.6.0+, without using Version 6.5.0 as an intermediate version.
Universal Permanent License Reservation (PLR) mode	None, but feature is deprecated until you upgrade to Version 6.6.0+.	Version 6.5.0 does not support Universal Permanent License Reservation (PLR) mode, where you can apply a license that does not need direct communication with Cisco Smart Software Manager (CSSM). This feature *is* supported in Version 6.4.0.10 and later patches, and in Version 6.6.0+. If you are running Version 6.4.0.10 or later patch, we recommend you upgrade directly to Version 6.6.0+, without using Version 6.5.0 as an intermediate version.
ASA 5515-X with Firepower Threat Defense	Upgrade prohibited.	You cannot upgrade to or freshly install Firepower Threat Defense Version 6.5.0+ on ASA 5515-X devices.

About Deprecated FlexConfig Commands

This document lists any deprecated FlexConfig objects and commands along with the other deprecated features. For a full list of prohibited commands, including those prohibited when FlexConfig was introduced, 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 Firepower Threat Defense features are configured using ASA configuration commands. Beginning with Version 6.2.0 (FMC deployments) or Version 6.2.3 (FDM deployments), you can use Smart CLI or FlexConfig to manually configure various ASA features that are not otherwise supported in the web interface.

Upgrades to FTD 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.

Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

Intrusion rule updates (SRUs) 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.

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.

Supported keywords depend on your Snort version:

- FMC: Choose **Help** > **About**.
- FTD with FDM: Use the **show summary** CLI command.
- ASA FirePOWER with ASDM: Choose **ASA FirePOWER Configuration** > **System Information**.

You can also find your Snort version in the *Bundled Components* section of the Cisco Firepower Compatibility Guide.

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.

How-To Walkthroughs for the FMC

FMC walkthroughs (also called *how-tos*) guide you through a variety of basic tasks such as device setup and policy configuration. Just click **How To** at the bottom of the browser window, choose a walkthrough, and follow the step-by-step instructions.

Note FMC walkthroughs are tested on the Firefox and Chrome browsers. If you encounter issues with a different browser, we ask that you switch to Firefox or Chrome. If you continue to encounter issues, contact Cisco TAC.

The following table lists some common problems and solutions. To end a walkthrough at any time, click the **x** in the upper right corner.

Table 12: Troubleshooting Walkthroughs

Problem	Solution
Cannot find the **How To** link to start walkthroughs.	Make sure walkthroughs are enabled. From the drop-down list under your username, select **User Preferences** then click **How-To Settings**.
Walkthrough appears when you do not expect it.	If a walkthrough appears when you do not expect it, end the walkthrough.
Walkthrough disappears or quits suddenly.	If a walkthrough disappears: • Move your pointer. Sometimes the FMC stops displaying an in-progress walkthrough. For example, pointing to a different top-level menu can make this happen. • Navigate to a different page and try again. If moving your pointer does not work, the walkthrough may have quit.
Walkthrough is out of sync with the FMC: • Starts on the wrong step. • Advances prematurely. • Will not advance.	If a walkthrough is out of sync, you can: • Attempt to continue. For example, if you enter an invalid value in a field and the FMC displays an error, the walkthrough can prematurely move on. You may need to go back and resolve the error to complete the task. • End the walkthrough, navigate to a different page, and try again. Sometimes you cannot continue. For example, if you do not click **Next** after you complete a step, you may need to end the walkthrough.

Sharing Data with Cisco

Web Analytics tracking

In Version 6.2.3+, *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 in web analytics tracking by default (by accepting the Version 6.5.0+ EULA you consent to web analytics tracking), but you can change your enrollment at any time after you complete initial setup.

Note Upgrades to Version 6.2.3 through 6.6.x can enroll you in web analytics tracking. This can occur even if you purposely unenrolled. If you do not want Cisco to collect this data, unenroll after upgrading.

Cisco Success Network

In Version 6.2.3+, *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

In Version 6.5.0+, *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.

Note This feature is supported on Firepower Management Centers and their managed Firepower Threat Defense devices. In Version 6.5.0 only, FTD support is restricted to the Firepower 4100/9300 with FTD and FTDv for Azure. This feature is not supported with Firepower Device Manager.

CHAPTER 4

Upgrade the Software

This chapter provides critical and release-specific information.

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 the appropriate upgrade or configuration guide for full instructions: Upgrade Instructions, on page 65.

Table 13: Upgrade Planning Phases

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

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

Minimum Version to Upgrade

You can upgrade directly to Version 6.5.0 as follows. You do not need to be running any specific patch level.

Table 14: Minimum Version to Upgrade to Version 6.5.0

Platform	Minimum Version
Firepower Management Center	6.2.3
Firepower devices	6.2.3 FXOS 2.7.1.92 or later build required for the Firepower 4100/9300.

New Upgrade Guidelines for Version 6.5.0

This checklist contains upgrade guidelines that are new or specific to Version 6.5.0.

Table 15: Version 6.5.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 37	Firepower 1000 series	6.4.0.x	6.5.0+

✓	Guideline	Platforms	Upgrading From	Directly To
	Disable Egress Optimization for Version 6.5.0, on page 37	FTD	6.2.3 through 6.4.0.x	6.5.0 only
	Historical Data Removed During FTD/FDM Upgrade, on page 38	FTD with FDM	6.2.3 through 6.4.0.x	6.5.0+
	New URL Categories and Reputations, on page 38	Any	6.2.3 through 6.4.0.x	6.5.0+

Firepower 1000 Series Devices Require Post-Upgrade Power Cycle

Deployments: Firepower 1000 series

Upgrading from: Version 6.4.0.x

Directly to: Version 6.5.0+

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

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

Disable Egress Optimization for Version 6.5.0

Deployments: FTD

Upgrading from: Version 6.2.3 through 6.4.0.x

Directly to: Version 6.5.0 only

To mitigate CSCvq34340, patching an FTD device to Version 6.4.0.7+ or Version 6.5.0.2+ turns off egress optimization processing. This happens regardless of whether the egress optimization feature is enabled or disabled.

Upgrading to Version 6.5.0:

- From Version 6.2.3.x: Enables and turns on egress optimization.
- From Version 6.3.0.x: Enables and turns on egress optimization.
- From Version 6.4.0.x: Respects your current settings. However, if the Version 6.4.0.x patch turned off egress optimization but the feature is still enabled, the upgrade to Version 6.5.0 turns it on again.

Note We recommend you patch to Version 6.5.0.2+ or upgrade to Version 6.6.0. If you remain at Version 6.5.0 or 6.5.0.1, you should manually disable egress optimization from the FTD CLI: **no asp inspect-dp egress-optimization**.

This issue is fixed in Version 6.6.0, where egress optimization works as expected. For more information, see the software advisory: FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature.

Historical Data Removed During FTD/FDM Upgrade

Deployments: Firepower Device Manager

Upgrading from: Version 6.2.3 through 6.4.x

Directly to: 6.5.0+

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

New URL Categories and Reputations

Deployments: Any

Upgrading from: Version 6.2.3 through 6.4.0.x

Directly to: Version 6.5.0+

Cisco Talos Intelligence Group (Talos) has introduced new categories and renamed reputations to classify and filter URLs. For descriptions of the new URL categories, see the Talos Intelligence Categories site.

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

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

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

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

- *Reputationless URLs* can belong to any category.

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

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

Table 16: Deployment Changes on Upgrade

Change	Details
Modifies URL rule categories.	The upgrade modifies URL rules to use the nearest equivalents in the new category set, in the following policies: • Access control • SSL • QoS (FMC only) • Correlation (FMC only) These changes may create redundant or preempted rules, which can slow performance. If your configuration includes merged categories, you may experience minor changes to the URLs that are allowed or blocked. For detailed lists of category changes, see URL Category Changes, on page 44.
Renames URL rule reputations.	The upgrade modifies URL rules to use the new reputation names: **1.** Untrusted (was *High Risk*) **2.** Questionable (was *Suspicious sites*) **3.** Neutral (was *Benign sites with security risks*) **4.** Favorable (was *Benign sites*) **5.** Trusted (was *Well Known*)
Clears the URL cache.	The upgrade clears the URL cache, which contains results that the system previously looked up in the cloud. Your users may temporarily experience slightly longer access times for URLs that are not in the local data set.
Labels 'legacy' events.	For already-logged events, the upgrade labels any associated URL category and reputation information as `Legacy`. These legacy events will age out of the database over time.

Pre-Upgrade Actions for URL Categories and Reputations

Before upgrade, take the following actions.

Table 17: Pre-Upgrade Actions

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

Post-Upgrade Actions for URL Categories and Reputations

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

Table 18: Post-Upgrade Actions

Action	Details
Remove **deprecated categories** from rules. Required. List: Deprecated Categories, on page 48.	The upgrade does not modify URL rules that use deprecated categories. Rules that use them will prevent deploy. On the FMC, these rules are marked.
Create or modify rules to include the **new categories**. List: New Categories, on page 47.	Most of the new categories identify threats. We strongly recommend you use them. On the FMC, these new categories are not marked after *this* upgrade, but Talos may add additional categories in the future. When that happens, new categories are marked.
Evaluate rules changed as a result of **merged categories**. List: Merged Categories, on page 48.	Each rule that included any of the affected categories now include all of the affected categories. If the original categories were associated with different reputations, the new rule is associated with the broader, more inclusive reputation. To filter URLs as before, you may have to modify or delete some configurations; see Guidelines for Rules with Merged URL Categories, on page 41. Depending on what changed and how your platform handles rule warnings, changes may be marked. For example, the FMC marks wholly redundant and wholly preempted rules, but not rules that have partial overlap.
Evaluate rules changed as a result of **split categories**. List: Split Categories, on page 49.	The upgrade replaces each old, single category in URL rules with *all* the new categories that map to the old one. This will not change the way you filter URLs, but you can modify affected rules to take advantage of the new granularity. These changes are not marked.
Understand which categories were **renamed** or are **unchanged**. Lists: Renamed Categories, on page 51 and Unchanged Categories, on page 52.	Although no action is required, you should be aware of these changes. These changes are not marked.
Evaluate how you handle **uncategorized** and **reputationless** URLs.	Even though it is now possible to have uncategorized and reputationless URLs, you cannot still cannot filter uncategorized URLs by reputation, nor can you filter reputationless URLs. Make sure that rules that filter by the **Uncategorized** category, or by **Any** reputation, will behave as you expect.

Guidelines for Rules with Merged URL Categories

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

Table 19: Guidelines for Rules with Merged URL Categories

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

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

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

Table 20: Examples of Rules with Merged URL Categories

Scenario	Before Upgrade	After Upgrade
Merged categories in the same rule	Rule 1 has Category A and Category B.	Rule 1 has Category AB.
Merged categories in different rules	Rule 1 has Category A. Rule 2 has Category B.	Rule 1 has Category AB. Rule 2 has Category AB. The specific result varies by the rules' order in the list, reputation levels, and associated actions. You should also consider all other conditions in the rule when determining how to resolve any redundancy.
Merged categories in different rules have different actions (Reputation is the same)	Rule 1 has Category A set to Allow. Rule 2 has Category B set to Block. (Reputation is the same)	Rule 1 has Category AB set to Allow. Rule 2 has Category AB set to Block. Rule 1 will match all traffic for this category. Rule 2 will never match traffic, and will display a warning indicator if you show warnings after merge, because both category and reputation are the same.
Merged categories in the same rule have different reputation levels	Rule 1 includes: Category A with Reputation Any Category B with Reputation 1-3	Rule 1 includes Category AB with Reputation Any.
Merged categories in different rules have different reputation levels	Rule 1 includes Category A with Reputation Any. Rule 2 includes Category B with Reputation 1-3.	Rule 1 includes Category AB with Reputation Any. Rule 2 includes Category AB with Reputation 1-3. Rule 1 will match all traffic for this category. Rule 2 will never match traffic, but you will not see a warning indicator because the reputations are not identical.

URL Category Changes

Use this table to determine how your URL categories changed.

Table 21: Index of Old URL Categories

Old Category	Change		Old Category	Change
Abortion	Merged Categories, on page 48		Military	Unchanged Categories, on page 52
Abused Drugs	Merged Categories, on page 48		Motor Vehicles	Renamed Categories, on page 51
Adult and Pornography	Split Categories, on page 49		Music	Renamed Categories, on page 51
Alcohol and Tobacco	Split Categories, on page 49		News and Media	Renamed Categories, on page 51
Bot Nets	Renamed Categories, on page 51		Nudity	Renamed Categories, on page 51
Business and Economy	Split Categories, on page 49		Online Greeting cards	Renamed Categories, on page 51
Cheating	Renamed Categories, on page 51		Open HTTP Proxies	Renamed Categories, on page 51
Computer and Internet Info	Split Categories, on page 49		Parked Domains	Unchanged Categories, on page 52
Computer and Internet Security	Split Categories, on page 49		Pay to Surf	Merged Categories, on page 48
Confirmed SPAM Sources	Merged Categories, on page 48		Peer to Peer	Renamed Categories, on page 51
Content Delivery Networks	Merged Categories, on page 48		Personal sites and Blogs	Split Categories, on page 49
Cult and Occult	Split Categories, on page 49		Personal Storage	Split Categories, on page 49

Old Category	Change		Old Category	Change
Dating	Unchanged Categories, on page 52		Philosophy and Political Advocacy	Renamed Categories, on page 51
Dead Sites	Renamed Categories, on page 51		Phishing and Other Frauds	Renamed Categories, on page 51
Dynamically Generated Content	Merged Categories, on page 48		Private IP Address	Deprecated Categories, on page 48
Educational Institutions	Merged Categories, on page 48		Proxy Avoidance and Anonymizers	Renamed Categories, on page 51
Entertainment and Arts	Split Categories, on page 49		Questionable	Renamed Categories, on page 51
Fashion and Beauty	Renamed Categories, on page 51		Real Estate	Unchanged Categories, on page 52
Financial Services	Renamed Categories, on page 51		Recreation and Hobbies	Merged Categories, on page 48
Food and Dining	Renamed Categories, on page 51		Reference and Research	Split Categories, on page 49
Gambling	Split Categories, on page 49		Religion	Unchanged Categories, on page 52
Games	Unchanged Categories, on page 52		Search Engines	Merged Categories, on page 48
Government	Merged Categories, on page 48		Sex Education	Merged Categories, on page 48
Gross	Merged Categories, on page 48		Shareware and Freeware	Renamed Categories, on page 51
Hacking	Merged Categories, on page 48		Shopping	Unchanged Categories, on page 52

Old Category	Change		Old Category	Change
Hate and Racism	Renamed Categories, on page 51		Social Network	Split Categories, on page 49
Health and Medicine	Renamed Categories, on page 51		Society	Split Categories, on page 49
Home and Garden	Split Categories, on page 49		SPAM URLs	Merged Categories, on page 48
Hunting and Fishing	Renamed Categories, on page 51		Sports	Merged Categories, on page 48
Illegal	Split Categories, on page 49		Spyware and Adware	Unchanged Categories, on page 52
Image and Video Search	Renamed Categories, on page 51		Streaming Media	Renamed Categories, on page 51
Individual Stock Advice and Tools	Renamed Categories, on page 51		Swimsuits and Intimate Apparel	Renamed Categories, on page 51
Internet Communications	Split Categories, on page 49		Training and Tools	Merged Categories, on page 48
Internet Portals	Merged Categories, on page 48		Travel	Unchanged Categories, on page 52
Job Search	Unchanged Categories, on page 52		Uncategorized	Deprecated Categories, on page 48
Keyloggers and Monitoring	Merged Categories, on page 48		Uncomfirmed SPAM Sources	Merged Categories, on page 48
Kids	Renamed Categories, on page 51		Violence	Merged Categories, on page 48
Legal	Merged Categories, on page 48		Weapons	Unchanged Categories, on page 52
Local Information	Renamed Categories, on page 51		Web Advertisements	Merged Categories, on page 48

Old Category	Change		Old Category	Change
Malware Sites	Unchanged Categories, on page 52		Web based email	Split Categories, on page 49
Marijuana	Merged Categories, on page 48		Web Hosting Sites	Renamed Categories, on page 51

New Categories

These tables list entirely new URL categories, most of which identify threats. We strongly recommend you create or modify URL rules to include the new threat categories. Note that some existing URL categories do identify threats; we recommend you include those also. For a list of threat categories, see the Talos Intellience Categories site.

Table 22: New Categories

New Category
Dynamic and Residential

Table 23: New Threat Categories

New Threat Category
Bogon
Cryptojacking
DNS Tunneling
Domain Generated Algorithm
Dynamic DNS
Ebanking Fraud
Exploits
High Risk Sites and Locations
Indicators of Compromise (IOC)
Linkshare
Malicious Sites
Mobile Threats
Newly Seen Domains
Open Mail Relay

New Threat Category
P2P Malware Node
Potential DNS Rebinding
TOR exit Nodes

Deprecated Categories

The upgrade does not modify URL rules that use deprecated categories. These rules will prevent deploy; you should delete or modify them.

Table 24: Deprecated Categories

Deprecated Category
Uncategorized
Private IP Address

Merged Categories

Each rule that included any of the affected categories now include all of the affected categories. If the original categories were associated with different reputations, the new rule is associated with the broader, more inclusive reputation. To filter URLs as before, you may have to modify or delete some configurations; see Guidelines for Rules with Merged URL Categories, on page 41.

We also strongly recommend you create or modify URL rules to include newly designated threat categories (Spam).

Table 25: Merged Categories

Old Categories	New Merged Category
Web Advertisements	Advertisements
Pay to Surf	
Educational Institutions	Education
Training and Tools	
Violence	Extreme
Gross	
Government	Government and Law
Legal	
Abused Drugs	Illegal Drugs
Marijuana	

Old Categories	New Merged Category
Dynamically Generated Content	Infrastructure
Content Delivery Networks	
Hacking	Hacking
Keyloggers and Monitoring	
Search Engines	Search Engines and Portals
Internet Portals	
Sex Education	Sex Education
Abortion	
Confirmed SPAM Sources	Spam *(threat category)*
SPAM URLs	
Unconfirmed SPAM Sources	
Recreation and Hobbies	Sports and Recreations
Sports	

Split Categories

The upgrade replaces each old, single category in URL rules with *all* the new categories that map to the old one. After upgrade, you can modify affected rules to take advantage of the new granularity.

Table 26: Split Categories

Old Single Category	New Split Categories
Adult and Pornography	Pornography
	Adult
Alcohol and Tobacco	Alcohol
	Tobacco
Business and Economy	Business and Industry
	Mobile Phones
Computer and Internet Info	Software Updates
	Computers and Internet
	SaaS and B2B
	Online Meetings

Old Single Category	New Split Categories
Computer and Internet Security	Computer Security
	Personal VPN
Cult and Occult	Paranormal
	Astrology
Entertainment and Arts	Arts
	Entertainment
Gambling	Gambling
	Lotteries
Home and Garden	Nature
	DIY Projects
Illegal	Illegal Activities
	Child Abuse Content
	Illegal Downloads
Internet Communications	Internet Telephony
	Chat and Instant Messaging
Personal sites and Blogs	Personal Sites
	Online Communities
Personal Storage	Online Storage and Backup
	File Transfer Services
Reference and Research	Science and Technology
	Social Science
Social Network	Social Networking
	Professional Networking
Society	Society and Culture
	Non-governmental Organisation
Web based email	Web-based Email
	Organisation Email

Renamed Categories

Although no action is required, you should be aware of these changes. We do strongly recommend you create or modify URL rules to include the newly designated threat categories (Botnets, Open HTTP Proxy, Phishing).

Table 27: Renamed Categories

Old Category Name	New Category Name
Bot Nets	Botnets *(threat category)*
Cheating	Cheating and Plagiarism
Dead Sites	Not Actionable
Fashion and Beauty	Fashion
Financial Services	Finance
Food and Dining	Dining and Drinking
Hate and Racism	Hate Speech
Health and Medicine	Health and Nutrition
Hunting and Fishing	Hunting
Image and Video Search	Photo Search and Images
Individual Stock Advice and Tools	Online Trading
Kids	Safe for Kids
Local Information	Reference
Motor Vehicles	Transportation
Music	Streaming Audio
News and Media	News
Nudity	Non-sexual Nudity
Online Greeting cards	Digital Postcards
Open HTTP Proxies	Open HTTP Proxy *(threat category)*
Peer to Peer	Peer File Transfer
Philosophy and Political Advocacy	Politics
Phishing and Other Frauds	Phishing *(threat category)*
Proxy Avoidance and Anonymizers	Filter Avoidance
Questionable	Humor

Old Category Name	New Category Name
Shareware and Freeware	Freeware and Shareware
Streaming Media	Streaming Video
Swimsuits and Intimate Apparel	Lingerie and Swimsuits
Web Hosting Sites	Web Hosting

Unchanged Categories

Although no action is required, you should be aware of these changes. We do strongly recommend you create or modify URL rules to include the newly designated threat categories (Malware Sites, Spyware and Adware).

Table 28: Unchanged Categories

Unchanged Category
Dating
Games
Job Search
Military
Parked Domains
Real Estate
Religion
Shopping
Travel
Weapons

Table 29: Unchanged Threat Categories

Unchanged Threat Category
Malware Sites *(threat category)*
Spyware and Adware *(threat category)*

Previously Published Upgrade Guidelines

This checklist contains older upgrade guidelines.

Table 30: Version 6.5.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: Insufficient Disk Space on Container Instances, on page 53	Firepower 4100/9300	6.3.0 through 6.4.0.x	6.3.0.1 through 6.5.0
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 53	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4.0+
	Readiness Check May Fail on FMC, NGIPSv, on page 54	FMC NGIPSv	6.1.0 through 6.1.0.6 6.2.0 through 6.2.0.6 6.2.1 6.2.2 through 6.2.2.4 6.2.3 through 6.2.3.4	6.3.0+
	RA VPN Default Setting Change Can Block VPN Traffic, on page 54	FTD with FMC	6.2.0 through 6.2.3.x	6.3.0+
	Security Intelligence Enables Application Identification, on page 55	FMC deployments	6.1.0 through 6.2.3.x	6.3.0+
	Update VDB after Upgrade to Enable CIP Detection, on page 55	Any	6.1.0 through 6.2.3.x	6.3.0+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 56	Any	6.1.0 through 6.2.3.x	6.3.0+

Upgrade Failure: Insufficient Disk Space on Container Instances

Deployments: Firepower 4100/9300 with FTD

Upgrading from: Version 6.3.0 through 6.4.0.x

Directly to: Version 6.3.0.1 through Version 6.5.0

Most often during major upgrades — but possible while patching — FTD devices configured with container instances can fail in the precheck stage with an erroneous insufficient-disk-space warning.

If this happens to you, you can try to free up more disk space. If that does not work, contact Cisco TAC.

TLS Crypto Acceleration Enabled/Cannot Disable

Deployments: Firepower 2100 series, Firepower 4100/9300 chassis

Upgrading from: Version 6.1.0 through 6.3.x

Directly to: Version 6.4.0+

SSL hardware acceleration has been renamed *TLS crypto acceleration*.

Depending on the device, TLS crypto acceleration might be performed in software or in hardware. The upgrade automatically enables acceleration on all eligible devices, even if you previously disabled the feature manually. In most cases you cannot configure this feature; it is automatically enabled and you cannot disable it.

Upgrading to Version 6.4.0: If you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can use the FXOS CLI to enable TLS crypto acceleration for *one* container instance per module/security engine. Acceleration is disabled for other container instances, but enabled for native instances.

Upgrading to Version 6.5.0+: If you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can use the FXOS CLI to enable TLS crypto acceleration for multiple container instances (up to 16) on a Firepower 4100/9300 chassis. New instances have this feature enabled by default. However, the upgrade does *not* enable acceleration on existing instances. Instead, use the **config hwCrypto enable** CLI command.

Readiness Check May Fail on FMC, NGIPSv

Deployments: FMC, NGIPSv

Upgrading from: Version 6.1.0 through 6.1.0.6, Version 6.2.0 through 6.2.0.6, Version 6.2.1, Version 6.2.2 through 6.2.2.4, and Version 6.2.3 through 6.2.3.4

Directly to: Version 6.3.0+

You cannot run the readiness check on the listed models when upgrading from one of the listed Firepower versions. This occurs because the readiness check process is incompatible with newer upgrade packages.

Table 31: Patches with Readiness Checks for Version 6.3.0+

Readiness Check Not Supported	First Patch with Fix
6.1.0 through 6.1.0.6	6.1.0.7
6.2.0 through 6.2.0.6	6.2.0.7
6.2.1	None. Upgrade to Version 6.2.3.5+.
6.2.2 through 6.2.2.4	6.2.2.5
6.2.3 through 6.2.3.4	6.2.3.5

RA VPN Default Setting Change Can Block VPN Traffic

Deployments: Firepower Threat Defense configured for remote access VPN

Upgrading from: Version 6.2.x

Directly to: Version 6.3+

Version 6.3 changes the default setting for a hidden option, **sysopt connection permit-vpn**. Upgrading can cause your remote access VPN to stop passing traffic. If this happens, use either of these techniques:

- Create a FlexConfig object that configures the **sysopt connection permit-vpn** command. The new default for this command is **no sysopt connection permit-vpn**.

  This is the more secure method to allow traffic in the VPN, because external users cannot spoof IP addresses in the remote access VPN address pool. The downside is that the VPN traffic will not be inspected, which means that intrusion and file protection, URL filtering, or other advanced features will not be applied to the traffic.

- Create access control rules to allow connections from the remote access VPN address pool.

  This method ensures that VPN traffic is inspected and advanced services can be applied to the connections. The downside is that it opens the possibility for external users to spoof IP addresses and thus gain access to your internal network.

Security Intelligence Enables Application Identification

Deployments: Firepower Management Center

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

In Version 6.3, Security Intelligence configurations enable application detection and identification. If you disabled discovery in your current deployment, the upgrade process may enable it again. Disabling discovery if you don't need it (for example, in an IPS-only deployment) can improve performance.

To disable discovery you must:

- Delete all rules from your network discovery policy.
- Use only simple network-based conditions to perform access control: zone, IP address, VLAN tag, and port. Do not perform any kind of application, user, URL, or geolocation control.
- **(NEW)** Disable network and URL-based Security Intelligence by deleting all whitelists and blacklists from your access control policy's Security Intelligence configuration, including the default Global lists.
- **(NEW)** Disable DNS-based Security Intelligence by deleting or disabling all rules in the associated DNS policy, including the default Global Whitelist for DNS and Global Blacklist for DNS rules.

Update VDB after Upgrade to Enable CIP Detection

Deployments: Any

Upgrading from: Version 6.1.0 through 6.2.3.x, with VDB 299+

Directly to: Version 6.3.0+

If you upgrade while using vulnerability database (VDB) 299 or later, an issue with the upgrade process prevents you from using CIP detection post-upgrade. This includes every VDB released from June 2018 to now, even the latest VDB.

Although we always recommend you update the vulnerability database (VDB) to the latest version after you upgrade, it is especially important in this case.

To check if you are affected by this issue, try to configure an access control rule with a CIP-based application condition. If you cannot find any CIP applications in the rule editor, manually update the VDB.

Invalid Intrusion Variable Sets Can Cause Deploy Failure

Deployments: Any

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3.0+

For network variables in an intrusion variable set, any IP addresses you *exclude* must be a subset of the IP addresses you *include*. This table shows you examples of valid and invalid configurations.

Valid	Invalid
Include: 10.0.0.0/8 Exclude: 10.1.0.0/16	Include: 10.1.0.0/16 Exclude: 172.16.0.0/12 Exclude: 10.0.0.0/8

Before Version 6.3.0, you could successfully save a network variable with this type of invalid configuration. Now, these configurations block deploy with the error: `Variable set has invalid excluded values`.

If this happens, identify and edit the incorrectly configured variable set, then redeploy. Note that you may have to edit network objects and groups referenced by your variable set.

Unresponsive Upgrades

Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot, shut down, or 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, contact Cisco TAC.

Traffic Flow and Inspection

Interruptions in traffic flow and inspection can occur when you:

- Reboot a device.
- Upgrade the device software, operating system, or virtual hosting environment.
- Uninstall the device software.
- Move a device between domains.
- Deploy configuration changes (Snort process restarts).

Device type, high availability/scalibility configurations, and interface configurations determine the nature of the interruptions. We *strongly* recommend performing these tasks in a maintenance window or at a time when any interruption will have the least impact on your deployment.

Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300

FXOS Upgrades

Upgrade FXOS on each chassis independently, even if you have inter-chassis clustering or high availability pairs configured. How you perform the upgrade determines how your devices handle traffic during the FXOS upgrade.

Table 32: Traffic Behavior: FXOS Upgrades

Deployment	Method	Traffic Behavior
Standalone	—	Dropped.
High availability	**Best Practice:** Update FXOS on the standby, switch active peers, upgrade the new standby.	Unaffected.
	Upgrade FXOS on the active peer before the standby is finished upgrading.	Dropped until one peer is online.
Inter-chassis cluster (6.2+)	**Best Practice:** Upgrade one chassis at a time so at least one module is always online.	Unaffected.
	Upgrade chassis at the same time, so all modules are down at some point.	Dropped until at least one module is online.
Intra-chassis cluster (Firepower 9300 only)	Hardware bypass enabled: **Bypass: Standby** or **Bypass-Force**. (6.1+)	Passed without inspection.
	Hardware bypass disabled: **Bypass: Disabled**. (6.1+)	Dropped until at least one module is online.
	No hardware bypass module.	Dropped until at least one module is online.

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 33: Traffic Behavior: 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.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force** (6.1+).	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby** (6.1+).	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** (6.1+).	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.

- FTD with FMC: 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.

- FTD with FDM: For high availability pairs, upgrade the standby, manually switch roles, then upgrade the new standby.

Software Uninstall (Patches)

In Version 6.2.3 and later, uninstalling a patch returns you to the version you upgraded from, and does not change configurations.

- FTD with FMC: 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.
- FTD with FDM: Not supported.

Deploying Configuration Changes

You deploy configurations multiple times during the upgrade process. 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. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

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

Table 34: Traffic Behavior: 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 (6.0.1–6.1).	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 (6.2+).	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled (6.2+).	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Firepower Threat Defense Upgrade Behavior: Other Devices

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 35: Traffic Behavior: 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.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force** (Firepower 2100 series, 6.3+).	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby** (Firepower 2100 series, 6.3+).	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** (Firepower 2100 series, 6.3+).	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 devices.

- Firepower Threat Defense with FMC: For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.
- Firepower Threat Defense with FDM: For high availability pairs, upgrade the standby, manually switch roles, then upgrade the new standby.

Software Uninstall (Patches)

In Version 6.2.3 and later, uninstalling a patch returns you to the version you upgraded from, and does not change configurations.

- FTD with FMC: 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.
- FTD with FDM: Not supported.

Deploying Configuration Changes

You deploy configurations multiple times during the upgrade process. 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. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

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

Table 36: Traffic Behavior: 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 (6.0.1–6.1).	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 (6.2+).	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled (6.2+).	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

ASA FirePOWER Upgrade Behavior

Your ASA service policies for redirecting traffic to the ASA FirePOWER module determine how the module handles traffic during the Firepower software upgrade, including when you deploy certain configurations that restart the Snort process.

Table 37: Traffic Behavior During ASA FirePOWER Upgrade

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

Traffic Behavior During ASA FirePOWER Deployment

Traffic behavior while the Snort process restarts is the same as when you upgrade the ASA FirePOWER module.

You deploy configurations multiple times during the upgrade process. 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. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection. Your service policies determine whether traffic drops or passes without inspection during the interruption.

NGIPSv Upgrade Behavior

This section describes device and traffic behavior when you upgrade NGIPSv.

Firepower Software Upgrade

Interface configurations determine how NGIPSv handles traffic during the upgrade.

Table 38: Traffic Behavior During NGIPSv Upgrade

Interface Configuration	Traffic Behavior
Inline	Dropped
Inline, tap mode	Egress packet immediately, copy not inspected
Passive	Uninterrupted, not inspected

Traffic Behavior During Deployment

You deploy configurations multiple times during the upgrade process. 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. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 39: Traffic Behavior During NGIPSv Deployment

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

Time and Disk Space Tests

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

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 Even if the system appears inactive, do not manually reboot, shut down, or 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, contact Cisco TAC.

Table 40: Time Test Conditions for Software Upgrades

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

Disk Space Tests

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

We also report the space needed on the FMC (in /var) for the device upgrade package. 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.

Table 41: 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.

Version 6.5.0 Time and Disk Space

Table 42: Version 6.5.0 Time and Disk Space

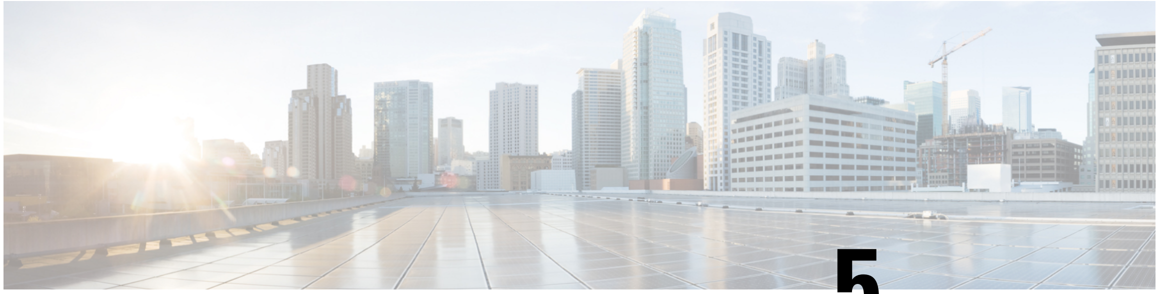
Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	18.6 GB	24 MB	—	47 min
FMCv: VMware	18.7 GB	30 MB	—	35 min
Firepower 1000 series	1.0 GB	11.3 GB	1.1 GB	10 min
Firepower 2100 series	1.1 GB	12.3 GB	1.0 GB	12 min
Firepower 4100 series	20 MB	10.8 GB	990 MB	8 min
Firepower 9300	23 MB	10.9 GB	990 MB	8 min
ASA 5500-X series with FTD	10.4 GB	120 KB	1.1 GB	17 min
FTDv: VMware	10 GB	120 KB	1.1 GB	10 min
ASA FirePOWER	12.2 GB	26 MB	1.3 GB	81 min
NGIPSv	6.6 GB	22 MB	870 MB	

Upgrade Instructions

The release notes do not contain upgrade instructions. After you read the guidelines and warnings in these release notes, see one of the following documents.

Table 43: Firepower Upgrade Instructions

Task	Guide
Upgrade in Firepower Management Center deployments.	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
Upgrade Firepower Threat Defense with Firepower Device Manager.	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager See the *System Management* chapter in the guide for the Firepower Threat Defense version you are currently running—not the version you are upgrading to.
Upgrade FXOS on a Firepower 4100/9300 chassis.	Cisco Firepower 4100/9300 Upgrade Guide, Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1
Upgrade ASA FirePOWER modules with ASDM.	Cisco ASA Upgrade Guide
Upgrade the ROMMON image on the ISA 3000, ASA 5508-X, and ASA 5516-X.	Cisco ASA and Firepower Threat Defense Reimage Guide See the *Upgrade the ROMMON Image* section. You should always make sure you have the latest image.



CHAPTER 5

Install the Software

If you cannot or do not want to upgrade, you can freshly install major and maintenance releases.

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 Checklist and Guidelines, on page 67
- Unregistering Smart Licenses, on page 69
- Installation Instructions, on page 70

Installation Checklist and Guidelines

Reimaging returns most settings to factory defaults, including the system password. This checklist highlights actions that can prevent common reimage issues. However, this checklist is *not* comprehensive. See the appropriate installation guide for full instructions: Installation Instructions, on page 70.

Table 44:

✓	Action/Check
	Check appliance access. If you do not have physical access to an appliance, the reimage process lets you keep management network settings. This allows you to connect to the appliance after you reimage to perform the initial configuration. If you delete network settings, you *must* have physical access to the appliance. You cannot use Lights-Out Management (LOM). **Note** Reimaging to an earlier version automatically deletes network settings. In this rare case, you must have physical access. For devices, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also able to access the FMC management interface without traversing the device.

✓	Action/Check
	Perform backups. Back up before reimaging, when supported. Note that if you are reimaging 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. **Caution** 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. And especially because backup files are unencrypted, do *not* allow unauthorized access. If backup files are modified, the restore process will fail. Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your deployment.
	Determine if you must remove devices from FMC management. If you plan to manually configure the reimaged appliance, remove devices from remote management before you reimage: • If you are reimaging the FMC, remove all its devices from management. • If you are reimaging a single device or switching from remote to local management, remove that one device. If you plan to restore from backup after reimaging, you do not need to remove devices from remote management.
	Address licensing concerns. Before you reimage *any* appliance, address licensing concerns. You may need to unregister from the Cisco Smart Software Manager (CSSM) to avoid accruing orphan entitlements, which can prevent you from reregistering. Or, you may need to contact Sales for new licenses. For more information, see: • The configuration guide for your product. • Unregistering Smart Licenses, on page 69 • Cisco Firepower System Feature Licenses Guide • Frequently Asked Questions (FAQ) about Firepower Licensing

Reimaging Firepower 1000/2100 Series Devices to Earlier Major Versions

We recommend that you perform complete reimages of Firepower 1000/2100 series devices. If you use the erase configuration method, FXOS may not revert along with the Firepower Threat Defense software. This can cause failures, especially in high availability deployments.

For more information, see the reimage procedures in the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 Series Running Firepower Threat Defense.

Reimaging Version 5.x Hardware to Version 6.3.0+

The renamed installation packages in Version 6.3+ cause issues with reimaging older *physical* appliances: FMC 2000 and 4000. If you are currently running Version 5.x and need to freshly install Version 6.5.0, rename the installation package to the "old" name after you download it; see the *Renamed Upgrade and Installation Packages* information in the Cisco Firepower Release Notes, Version 6.3.0.

After you reimage an FMC (Defense Center) from Version 5.x to a more recent version, it cannot manage its older devices. You should also reimage those devices, then re-add them to the FMC. Note that Series 2 devices are EOL and cannot run Firepower software past Version 5.4.0.x. You must replace them.

Unregistering Smart Licenses

Firepower Threat Defense uses Cisco Smart Licensing. To use licensed features, register with Cisco Smart Software Manager (CSSM). If you later decide to reimage or switch management, you must unregister to avoid accruing orphan entitlements. These can prevent you from reregistering.

Note If you need to restore an FMC or FTD device from backup, do *not* unregister before you reimage, and do not remove devices from the FMC. Instead, 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.

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

Manually unregister from CSSM before you:

- Reimage a Firepower Management Center that manages FTD devices.
- Shut down the source Firepower Management Center during model migration.
- Reimage a Firepower Threat Defense device that is locally managed by FDM.
- Switch a Firepower Threat Defense device from FDM to FMC management.

Automatically unregister from CSSM when you remove a device from the FMC so you can:

- Reimage an Firepower Threat Defense device that is managed by an FMC.
- Switch a Firepower Threat Defense device from FMC to FDM management.

Note that in these two cases, removing the device from the FMC is what automatically unregisters the device. You do not have to unregister manually as long as you remove the device from the FMC.

Tip Classic licenses for NGIPS devices are associated with a specific manager (ASDM/FMC), and are not controlled using CSSM. If you are switching management of a Classic device, or if you are migrating from an NGIPS deployment to an FTD deployment, contact Sales.

Installation Instructions

Table 45: Firepower Management Center Installation Instructions

FMC	Guide
FMC 1600, 2600, 4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
FMC 1000, 2500, 4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
FMC 2000, 4000	Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide
FMCv	Cisco Firepower Management Center Virtual Getting Started Guide

Table 46: Firepower Threat Defense Installation Instructions

FTD Platform	Guide
Firepower 1000/2100 series	Cisco ASA and Firepower Threat Defense Reimage Guide Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 Series Running Firepower Threat Defense
Firepower 4100/9300	Cisco Firepower 4100/9300 FXOS Configuration Guides: *Image Management* chapters Cisco Firepower 4100 Getting Started Guide Cisco Firepower 9300 Getting Started Guide
ASA 5500-X series	Cisco ASA and Firepower Threat Defense Reimage Guide
ISA 3000	Cisco ASA and Firepower Threat Defense Reimage Guide
FTDv: AWS	Cisco Firepower Threat Defense Virtual for the AWS Cloud Getting Started Guide
FTDv: Azure	Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide
FTDv: KVM	Cisco Firepower Threat Defense Virtual for KVM Getting Started Guide
FTDv: VMware	Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide

Table 47: NGIPSv and ASA FirePOWER Installation Instructions

NGIPS Platform	Guide
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware

NGIPS Platform	Guide
ASA FirePOWER	Cisco ASA and Firepower Threat Defense Reimage Guide ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide: *Managing the ASA FirePOWER Module*

CHAPTER 6

Documentation

For Firepower documentation, see:

- New and Updated Documentation, on page 73
- Documentation Roadmaps, on page 75

New and Updated Documentation

The following documentation was updated or is newly available for this release. For links to other documentation, see the Documentation Roadmaps, on page 75.

Firepower Configuration Guides and Online Help

- Firepower Management Center Configuration Guide, Version 6.5 and online help
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.5.0 and online help
- Cisco ASA with FirePOWER Services Local Management Configuration Guide, Version 6.5 and online help
- Cisco Firepower Threat Defense Command Reference

FXOS Configuration Guides and Release Notes

- Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide, 2.7(1)
- Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, 2.7(1)
- Cisco Firepower 4100/9300 FXOS Command Reference
- Cisco Firepower 4100/9300 FXOS Release Notes, 2.7(1)

Upgrade Guides

- Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
- Cisco Firepower 4100/9300 Upgrade Guide, Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1

- Cisco ASA Upgrade Guide

Migration Guides

- Firepower Management Center Model Migration Guide ***NEW***

Getting Started Guides

- Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
- Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
- Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide
- Cisco Firepower Management Center Virtual Getting Started Guide
- Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide
- Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide
- Cisco ISA 3000 Getting Started Guide ***NEW***
- Cisco Firepower 1010 Getting Started Guide
- Cisco Firepower 1100 Series Getting Started Guide
- Cisco Firepower 2100 Series Getting Started Guide ***NEW***
- Cisco Firepower 4100 Getting Started Guide
- Cisco Firepower 9300 Getting Started Guide

API and Integration Guides

- Firepower Management Center REST API Quick Start Guide, Version 6.5.0
- Cisco Firepower Threat Defense REST API Guide
- Firepower System Event Streamer Integration Guide, Version 6.5.0
- Firepower System Host Input API Guide v6.5
- Cisco Firepower User Agent Configuration Guide, version 2.5
- Cisco Firepower and SecureX Integration Guide

Compatibility Guides

- Cisco Firepower Compatibility Guide
- Cisco ASA Compatibility
- Cisco Firepower 4100/9300 FXOS Compatibility

Licensing and Open Source

- Cisco Firepower System Feature Licenses

- Frequently Asked Questions (FAQ) about Firepower Licensing

Troubleshooting and Configuration Examples

- Cisco Firepower Threat Defense Syslog Messages
- Using Multi-Instance Capability on the Firepower 4100/9300 ***NEW***
- Deploy a Cluster for Firepower Threat Defense for Scalability and High Availability
- Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 Series Running Firepower Threat Defense

Documentation Roadmaps

Documentation roadmaps provide links to currently available and legacy documentation:

- Navigating the Cisco Firepower Documentation
- Navigating the Cisco ASA Series Documentation
- Navigating the Cisco FXOS Documentation

CHAPTER 7

Resolved Issues

For your convenience, the release notes list the resolved issues for this version.

If you have a support contract, you can use the Cisco Bug Search Tool to obtain up-to-date bug lists. You can constrain searches to bugs affecting specific platforms and versions. You can also search by bug status, bug ID, and for specific keywords.

Important Bug lists are auto-generated *once* and are not subsequently updated. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes. You should regard the Cisco Bug Search Tool as the source of truth.

Resolved Issues in New Builds

Sometimes Cisco releases updated builds. In most cases, only the latest build for each platform is available on the Cisco Support & Download site. We *strongly* recommend you use the latest build. If you downloaded an earlier build, do not use it.

You cannot upgrade from one build to another for the same Firepower version. If a new build would fix your issue, determine if an upgrade or hotfix would work instead. If not, contact Cisco TAC. See the Cisco Firepower Hotfix Release Notes for quicklinks to publicly available Firepower hotfixes.

Use this table to determine if a new build is available for your platform.

Table 48: Version 6.5.0 New Builds

New Build	Released	Packages	Platforms	Resolves
123	2020-02-03	Upgrade Reimage	FMC/FMCv	CSCvr95287: Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability If you are running an earlier build, apply the latest Version 6.5.0.x patch.

New Build	Released	Packages	Platforms	Resolves
120	2019-10-08	—	—	CSCvr47499: Firepower FMC upgrade failure at 800_post/1028_latency_settings_upgrade.pl This build, which is no longer available, was for upgrading FMCs in multidomain deployments.

Version 6.5.0 Resolved Issues

Table 49: Version 6.5.0 Resolved Issues

Bug ID	Headline
CSCvc88690	5.4.x AC Administrator and Root Rules Groups are still 6.x User Role and have full permission
CSCvd80045	Error while switching domains from the Health Policy page
CSCvd87211	ASA traceback when trying to remove configured capture
CSCvh16358	Commands cannot be cancelled on CLI
CSCvh78264	Clamupdates needs working DNS even if FMC has an explicit HTTP proxy configured
CSCvi23774	Firepower Recommendation updates don't consider third party vulnerabilities moved to invalid state
CSCvi93955	Security Header Not Detected - CWE-693: Protection Mechanism Failure
CSCvi95403	Level-5 notification string is missing.
CSCvj53804	SW Upgrade to 6.2.3 failed due to icmp-event domain-id corrupted
CSCvj73432	NTP sends Eth0 ip address out the Eth1 interface
CSCvj74441	SRU installation via CLI on ASDM doesn't update version details in /etc/sf/sru_versions.conf
CSCvk63804	Sensitive Data Detection is enabled when working update Recommended Rules by scheduling
CSCvk66669	FPR2100: Configuring ssl-protocol does not change configuration for FDM GUI certificate
CSCvm31905	OpenSSH Bailout Delaying User Enumeration Vulnerability
CSCvm77115	Lina Traceback due to invalid TSC values
CSCvm80434	Performance degradation on FMC GUI with large number of users
CSCvm84357	File event source and destination is incorrect for active transfer mode

Bug ID	Headline
CSCvm89006	FTD: Syslog for configuration command "configure user add" in the FTD converged_cli
CSCvn27043	Hostscan: LastSuccessfulInstallParams can not be detected by Hostscan
CSCvn31390	Computing Processor PortSmash Side-Channel Information Disclosure Vuln
CSCvn31886	SSL inspection with TLS 1.3 causes do not decrypt traffic to take session not cached action
CSCvn57267	security intelligence contains the duplicate objects
CSCvn73998	OSPFv2 md5 password which contains equal sign, is getting removed during the second deployment.
CSCvn78076	Firepower:Misleading stats w.r.t "Memory Usage" being displayed under System->Monitoring->Statistics
CSCvn80464	Alert configuration does not keep track of in use policies correctly
CSCvo06680	Under the Help Drop-down the Sourcefire support page is still there
CSCvo11077	Cisco ASA Software and FTD Software IKEv1 Denial of Service Vulnerability
CSCvo30347	UI bug - Extended Access List object drag and drop does not work
CSCvo37273	Adding a validation check in FMC UI to validate the object network configured in static route
CSCvo39231	Deploy policy tab failed to populate the device list from FMC due to stale entries on CSM side
CSCvo39356	Traceback at Thread Name: IP Address Assign
CSCvo40478	FMC Dashboard is showing incorrect value as FMC latest product updates
CSCvo43260	Force Deploy should only load current device instead of going over all registered devices
CSCvo43311	Cannot save VPN site to site policy with error "Unknown endpoint present in the topology"
CSCvo48400	Upgrade of FTD says it succeeded, when it didn't.
CSCvo49295	RabbitMQ constantly fails to start with error "case_clause,undefined"
CSCvo57287	FMC: Not able to login to the RESTAPI UI using the apiuser credentials
CSCvo59424	FMC UI does not allow assigning an IP address to a diagnostic interface for an FTD cluster
CSCvo59683	Large number of stale Objects in EOAttributes table results in high CPU/backup failure
CSCvo61418	FMC event restore fails when the event tables are in huge size and number.

Bug ID	Headline
CSCvo66732	Automatic SRU download during patch update might result into update failure
CSCvo70169	[FMC 6.3] Show rule conflicts it's not working
CSCvo74786	Process Manager does not track Mojo process on ungraceful exit
CSCvo74802	Process Manager does not handle unmanaged processes as expected
CSCvo74833	High unmanaged disk space on Firepower devices due to untracked files
CSCvo76866	Traceback on 2100 - watchdog
CSCvo77024	FMC Jquery needs to be upgraded due to https://nvd.nist.gov/vuln/detail/CVE-2015-9251
CSCvo80725	vFTD 6.4 fails to establish OSPF adjacency due to "ERROR: ip_multicast_ctl failed to get channel"
CSCvo92100	FMC allows space in community string for SNMP under Platform Settings
CSCvo92913	Cisco Firepower Management Center RSS Cross-Site Scripting Vulnerabilities
CSCvp01677	Device reboots if you configure a route on management interface for 203.0.113.0/25 network
CSCvp04610	syncd process exits due to invalid GID and database synchronization issue
CSCvp12526	SSL session resumption attempts can fail on a busy device
CSCvp26173	FMC: Disable TLS 1.0 permanently for Host Input Client, TCP 8307 port
CSCvp26548	FDM upgrade fails due to objects validation failure
CSCvp29803	Apache HTTP Server Modules Scripts Arbitrary Code Execution Vulnerab ...
CSCvp31204	snmp community string doesnt accept special characters
CSCvp33439	Deployment failure on FTD after configuring SI DNS policy using REST API
CSCvp39970	/var/opt/CSCOpx/MDC/tomcat/log/stdout.logs writing excessive log messages which may fill the disk
CSCvp43987	Health policy run time interval should be less than health monitor process alarm thresholds
CSCvp50929	FMC shows the wrong license key after the Backup restore
CSCvp58287	FMC GUI BUG in 'Switch Workflow' of connection event
CSCvp66802	QP-HA is failing while upgrading 6.4.0.1-14
CSCvp66941	FMC Login fails if user has existing session, and has password with spaces in it

Bug ID	Headline
CSCvp70833	ASA/FTD: Twice nat Rule with same service displaying error "ERROR: NAT unable to reserve ports"
CSCvp81615	Routing configuration is removed when deleting Domain.
CSCvp82265	incorrect uuidprefix recorded after forming FMC HA causes errors while editing objects
CSCvp87623	Upload an update gives "update request entity too large" error when using CAC(HTTPS Client Certs)
CSCvp90060	RDP Connections failed after newest Firepower SRU update (24.05.2019)
CSCvp99930	deployment failure with sftunnel exception while primary active.
CSCvq05335	FMC stuck on boot process due to NFS remote storage not responding
CSCvq07624	s2s vpn configured in rest API has non matching IDs
CSCvq11637	6.4 FDM device is not sending TCP syslog
CSCvq12173	Rule configured with echo reply ICMP(1):0 as a parameter is not fired
CSCvq14954	Slave unit having mgmt-only can't join to cluster
CSCvq18237	Documentation Bug - FMC HA config guide - Software Requirements incorrect
CSCvq21935	FTD running 6.3.0.3 traceback on DATAPATH
CSCvq25791	Enable Clean List on Advanced settings of File Policy not correctly described.
CSCvq27739	Backup to remote SSH storage fails if the SSH server is configured to save copy of overwritten files
CSCvq30298	deploy.stats file does not rotate, which may cause it to grow very large
CSCvq34160	traceback and reload when establishing ASDM connection to fp1000 series platform
CSCvq36042	lost heartbeat causing reload
CSCvq46443	Cisco Firepower Management Center Stored Cross-Site Scripting Vulnerability
CSCvq55941	Cisco Firepower Management Center Software Stored Cross-Site Scripting Vulnerability
CSCvq59702	Connection events stop coming from device after lost handshake message
CSCvq61601	OpenSSL vulnerability CVE-2019-1559 on FTD
CSCvq71217	High Disk Utilization due to mysql-server.err failing to rotate after CSCvn30118
CSCvq71351	FMC:Page stuck when editing inline sets
CSCvq75634	Management interface configuration leads to immediate traceback and reload
CSCvq76533	F_RNA_EVENT_LIMIT for MC4000 should be 20 million

Bug ID	Headline
CSCvq76785	username and password printed to logs when there is an unhandled error in authentication
CSCvq79042	FQDN ACL entries incomplete due to DNS response from server is large and truncated
CSCvq87068	Deleted URL Objects are not being removed from the ngfw.rules.
CSCvq87585	Clish becomes unresponsive and High CPU cores after running a ping with a repeat of 50000
CSCvq87703	Active device is not reporting correct peer state.
CSCvq88644	Traceback in tcp-proxy
CSCvr07460	ASA traceback and reload related to crypto PKI operation
CSCvr13278	PPPoE session not coming up after reload.
CSCvr19922	Cluster: BGP route may go in out of sync in some scenarios
CSCvr23986	Cisco ASA & FTD devices may reload under conditions of low memory and frequent complete MIB walks
CSCvr35956	Block double-free when combining ServerKeyExchange and ClientKeyExchange fails causes lina traceback
CSCvr36369	CD should consider failure NodeID in file copy response before proceeding with deployment
CSCvr47499	Firepower FMC upgrade failure at 800_post/1028_latency_settings_upgrade.pl
CSCvr89663	Traceback: with thread name: pix_flash_config_thread WM1010 went into reboot loop
CSCvr90965	FTDv Deployment in Azure causes unrecoverable traceback state due to no dns domain-lookup any"
CSCvs07668	FTD traceback and reload on thread DATAPATH-1-15076 when SIP inspection is enabled
CSCvs09533	FP2100 Traceback and reload when processing traffic through more than two inline sets
CSCvs22608	Regarding disabled SID still being detected from Snort Rules Profiling
CSCvs26402	NAT policy configuration range limit to be imposed for non service cmds as well
CSCvs40531	AnyConnect 4.8 is not working on the FPR1000 series
CSCvs78252	ASA/Lina Offloaded TCP flows interrupted if TCP sequence number randomizer is enabled and SACK used
CSCvs80330	running a duplicate adi process can wipe out health status file
CSCvs81504	WR6 and WR8 commit id update in CCM layer(sprint 77)

Bug ID	Headline
CSCvt02409	9.12.2.151 snp_cluster_ingress traceback on FPR9300 3-node cluster nested VLAN traffic
CSCvt27920	Policy deployment failure on FTD.
CSCvt35366	Excessive logging of lua detector invalid LUA (null)
CSCvt45989	ASAv HA Azure: Deployment of ASAv HA Pair on Azure always fail when using existing virtual network
CSCvt48941	FTD Standby unit does not join HA due to "HA state progression failed due to APP SYNC timeout"
CSCvt51987	Traffic outage due to 80 size block exhaustion on the ASA
CSCvt54182	LINA cores are generated when FTD is configured to do SSL decryption.

CHAPTER 8

Known Issues

For your convenience, the release notes list the known issues for major releases. We do not list known issues for maintenance releases or patches.

If you have a support contract, you can use the Cisco Bug Search Tool to obtain up-to-date bug lists. You can constrain searches to bugs affecting specific platforms and versions. You can also search by bug status, bug ID, and for specific keywords.

Important Bug lists are auto-generated *once* and are not subsequently updated. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes. You should regard the Cisco Bug Search Tool as the source of truth.

Version 6.5.0 Known Issues

Table 50: Version 6.5.0 Known Issues

Bug ID	Headline
CSCvq03466	ISA 3000 FTD deployment fails with hardware-bypass activated
CSCvq11310	FTD performance has dropped approximately 5% in 6.5 SRTS runs
CSCvq30293	Bootstrap configuration is not updated after FTD version downgrade
CSCvq47804	FXOS security module will not power up after shutdown from FDM.
CSCvq91091	ASA 55xx series perform slower than expected on 6.5 in 1024B and MaxCPS tests
CSCvr09194	core.run_hm.pl found post FXOS upgrade
CSCvr17786	API GET call for access policy with HitCount "true" and filter "fetchZeroHitCount" returns all rules
CSCvr21119	Power cycling needed on FP1000 units when upgraded from 6.4 to 6.5 for SSD secure erase

Bug ID	Headline
CSCvr22260	Pair of HA FP2100 may exhibit crash in LINA when under load and low on memory
CSCvr23986	Cisco ASA & FTD devices may reload under conditions of low memory and frequent complete MIB walks
CSCvr24059	Source SGT correlation doesn't work for FMC and FTD 6.5
CSCvr28977	FTD: API Automatic Malware updates are downloaded even when its turned off in API
CSCvr34163	VLAN ID should not be seen under intrusion events when FTD is in routed or transparent mode
CSCvr35470	CloudAgent core on FMCv - 6.5.0
CSCvr37728	ADI process can crash and core after reconnecting to ISE in a corner case
CSCvr39516	lina segfault/reload caused by malloc failure in modexp-octeon
CSCvr39818	FTD: Switching interface IP from static to DHCP causes FTD to use different DHCP client-ids
CSCvr46892	Interface remains shutdown after switching between modes
CSCvr47499	Firepower FMC upgrade failure at 800_post/1028_latency_settings_upgrade.pl
CSCvr82603	Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability
CSCvr98881	Traceback: FTD ZeroMQ memory assertion
CSCvs02233	OpenSSH auth-gss2.c Information Disclosure Vulnerability
CSCvs02234	OpenSSH Bailout Delaying User Enumeration Vulnerability
CSCvs07159	Dev-side fix needed for online help: Fix Duplicate Help IDs
CSCvs07425	Max conn test will not reach 60 M conn after clear conns couple times
CSCvs08696	Firepower Chassis Manager Showing Smart Agent Disabled after upgrade to 2.7.1
CSCvs25517	Race condition for FMC API and GUI to fetch ACPs
CSCvs31114	Warning about not supported bypass revocation checking for FTD 6.5 and higher
CSCvs67534	Allowed to download zipped malware for first time
CSCvs79606	"dns server-group DefaultDNS" cli not getting negated
CSCvt22254	Auto Deploy fails after Restore if FDM cannot reach update server
CSCvt35770	Version mismatch errors after upgrade resulting in policy deployment failures
CSCvt43309	URL Filter license prevents policy deployment on all sensors if any one is missing the URL license

Bug ID	Headline
CSCvt45206	Event search may fail when searching events that existed before upgrade
CSCvt48260	Standby ASA Traceback at fover_parse and boot loop when detecting Active unit
CSCvt49308	ASA Traceback in thread name: CERT API memory leak while processing CRLs
CSCvt52604	Interfaces page from Objects section of the FMC does not load (domains page is likely affected also)
CSCvt52782	ASA traceback Thread name - webvpn_task
CSCvt54182	LINA cores are generated when FTD is configured to do SSL decryption.
CSCvt54286	FTD-UI: Self signed Certificate UI has hardcoded life of 5 years
CSCvt54286	FTD-UI: Self signed Certificate UI has hardcoded life of 5 years
CSCvt59253	ASA 9.13.1.7 traceback and reload on process name LINA
CSCvt63484	ASA High CPU with igb_saleen_io_sfp_mod_poll_thre process in 9.13(1)7
CSCvt63501	check heaps process failure seen on WM when uploading a 150Mb+ file
CSCvt63746	FDM /ngfw/var/sf/fwcfg/zones.conf is empty
CSCvt74893	FMCv Ethernet driver indicates vmxnet3 TCP performance compromised
CSCvt77813	High unmanaged disk usage on /ngfw due to cisco_uridb* files
CSCvt79777	duplicate ip addresses in sfipproxy.conf
CSCvt86439	marked version 0.3.6 and earlier is vulnerable to an XSS attack in the
CSCvt86583	marked is an application that is meant to parse and compile markdown.
CSCvt95268	idn in GNU libidn before 1.33 might allow remote attackers to obtain s
CSCvt95284	PCRE 7.8 and 8.32 through 8.37, and PCRE2 10.10 mishandle group empty
CSCvt95288	res_query in libresolv in glibc before 2.25 allows remote attackers to
CSCvt95323	Stack-based buffer overflow in the glob implementation in GNU C Librar
CSCvt95348	The makecontext function in the GNU C Library (aka glibc or libc6) bef
CSCvt95349	idn in libidn before 1.33 might allow remote attackers to obtain sensi
CSCvt95350	The idna_to_ascii_4i function in lib/idna.c in libidn before 1.33 allo
CSCvt95355	Stack-based buffer overflow in the getaddrinfo function in sysdeps/pos
CSCvt95375	The compile_branch function in pcre_compile.c in PCRE 8.x before 8.39
CSCvt95399	Memory leak in the __res_vinit function in the IPv6 name server manage

Bug ID	Headline
CSCvt95451	An SSE2-optimized memmove implementation for i386 in sysdeps/i386/i686
CSCvt95468	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-
CSCvt95469	The glob function in glob.c in the GNU C Library (aka glibc or libc6)
CSCvt95492	In shadow before 4.5, the newusers tool could be made to manipulate in
CSCvt95514	An issue was discovered in ide_dma_cb() in hw/ide/core.
CSCvt95564	In the GNU C Library (aka glibc or libc6) through 2.29,
CSCvt95651	GNU glibc elf/dl-load.c Local Privilege Escalation Vulnerability
CSCvt95675	Glibc in_realpath() Underflow Local Code Execution Vulnerability
CSCvt95719	GNU glibc getnetbyname Function Buffer Overflow Vulnerability
CSCvu05331	Cloud configuration links don't support the new APJ region
CSCvu05418	Import fails with local user password contains consecutive characters message
CSCvu20600	A use-after-free vulnerability introduced in glibc upstream version 2.
CSCvu26476	FTD Cluster unable to rejoin due to "process_create: out of stack memory "
CSCvu38870	The jQuery framework exchanges data using JavaScript Object Notation (
CSCvu43156	Upgrade appears hung on FMC at 11% but shows failed on sensor
CSCvu45952	Stack-based buffer overflow in the clntudp_call function in sunrpc/cln
CSCvu46890	FMCv300 requesting wrong license after migration using sf-migration.pl
CSCvu47941	Unexpected FTD traceback and reboot due to Lina core
CSCvu73496	Internal1/1 data interface goes down without any reason or logs.
CSCvu75855	stunnel process enabled on managed device when it should not be
CSCvu80802	FTD Traceback On Thread Name: CP DP SFR Event Processing
CSCvu82820	Traceback: ASDM Deployment causing ASA to reboot
CSCvu93834	FDM/FTD-API: Password cannot be changed on standby for the admin user
CSCvu94706	FXOS dynamically learning mac-address of external machine causing outage
CSCvu94715	FXOS "clear mac address-table dynamic" only removes entry from front end (not backend)
CSCvu95025	PPPoE fails to establish on ASA and FTD running on FP1010

CHAPTER 9

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-65-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